CASSANDRA

"Common Assessment and Analysis of Risk in Global Supply Chains"

Grant agreement no: 261795

CASSANDRA is part of the European Commission’s Seventh Framework programme for Security

www.cassandra-project.eu

Edited by Dr. Juha Hintsa and Ms. Kaisa Uronen

Cross-border Research Association, Switzerland, 2012

Contact information:

cassandra@isl.org
Executive summary

The main challenges facing international intermodal container logistics include efficiency and security. These seemingly conflicting issues have a common solution: supply chain visibility, where visibility data can be shared between business and government. Technical solutions for supply chain visibility already exist, but the challenge lies in integrating solutions across the supply chain. CASSANDRA is the acronym for the project “Common assessment and analysis of risk in global supply chains” supported by the European Commission under the 7th Framework Programme theme SEC-2010.3.2-1 “Monitoring and tracking of shipping containers”. The CASSANDRA research problem has been formulated as follows: “How to integrate existing commercial supply chain visibility solutions and data capture technologies across supply chains to enhance risk assessment and to enable the adoption of a risk based approach to supply chain management for both private sector companies and government authorities?”

The purpose of this Compendium is to provide a common reference document for CASSANDRA scope, concepts and terminology. It discusses different aspects regarding Supply Chain Visibility, presents the different actors and highlights various problem areas. The Compendium also discusses future trends in the different Supply Chain Visibility-related areas and presents conclusions and implications to the CASSANDRA project. The main outcome of the Compendium is a concrete framework for the CASSANDRA scope, including following four “CASSANDRA tenets”:

- **Innovative system-based and risk-based approach in the whole project** – CASSANDRA project will design, implement and evaluate a set of system-based and risk-based approaches to supply chain management, based on exploitation of information and data existing in the supply chain. Multiple types of risks are included explicitly, based for example on the actor priorities, and (indicator) data availability in the supply chain.

- **Open, inclusive approach in the supply chain** – CASSANDRA is open for the participation of all relevant supply chain actors and public authorities, operating in a variety of supply chain systems, in terms of different supply chain configurations and typologies, and start and end points.

- **Facilitating the implementation of governmental policies and regulations** – CASSANDRA is in line with all relevant existing governmental policies and regulations; while in parallel proposing innovative ways to enhance trust in the supply chain, including through public-private partnership approaches.

- **Avoiding reinventing the wheel** - CASSANDRA exploits existing data elements, standards and technologies in the supply chain to the maximum extent. CASSANDRA also takes lessons learned from previous relevant research projects into consideration.

Ultimately, the objective of CASSANDRA is the development of integral supply chain data that will set a new standard for efficient and secure global door-to-door goods flows to and from Europe – and this Compendium will support achieving this objective.
Compendium authors and reviewers

Ahokas, Juha (CBRA)
Arsenault, Shirley (GS1)
Baptista, João (GMV)
Çagri Gürbüz, Mustafa (ZLC)
Castellvi, Silvia (ATOS)
Cipres, Carolina (ZLC)
Engler, Marcus (ISL)
Heijmann, Frank (DCA)
Hesketh, David (HMRC)
Hintsa, Juha (CBRA)
Hofman, Wout (TNO)
Klievink, Bram (TUD)
Liu, Lingzhe (EUR)
Lucassen, Inge (TNO)
Martin, Jaume (ATOS)
Meyer-Larsen, Nils (ISL)
Monsreal, Mario (ZLC)
Mueller, Rainer (ISL)
Männistö, Toni (CBRA)
van Oosterhout, Marcel (EUR)
Pérez, Pilar (ATOS)
Pourakbar, Morteza (EUR)
Rook, Hans (Portbase)
van Stijn, Eveline (TUD)
Tan, Yao-Hua (TUD)
Thurlow, Sally (HMRC)
Urciuoli, Luca (CBRA)
Uronen, Kaisa (CBRA)
Veenstra, Albert (TNO)
Venancio, Rui (GMV)
Visscher, Wim (DCA)
Zomer, Gerwin (TNO)
Zuidwijk, Rob (EUR)
## Table of Contents

- Executive summary ................................................................................................................ 2
- Compendium authors and reviewers ...................................................................................... 3
- Content .................................................................................................................................. 4
- Table of Figures ..................................................................................................................... 9
- Table of Tables .................................................................................................................... 11
- 1 Introduction ................................................................................................................... 12
  - 1.1 Overview .................................................................................................................. 12
  - 1.2 Document purpose and partners .............................................................................. 12
  - 1.3 CASSANDRA research problem .......................................................................... 13
  - 1.4 Structure of the Compendium ............................................................................. 13
- 2 Supply chain management ............................................................................................ 15
  - 2.1 Introduction .............................................................................................................. 15
    - 2.1.1 Aspects of supply chain management ............................................................... 15
    - 2.1.2 Supply chain management paradigms ............................................................... 16
  - 2.2 Structuring and design of global supply chains ........................................................ 17
    - 2.2.1 Stakeholders in global supply chains ................................................................. 17
    - 2.2.2 Global trade process and management ............................................................. 18
    - 2.2.3 Global Logistics Network Configurations ........................................................... 19
    - 2.2.4 FCL versus LCL Supply Chain configurations ................................................... 20
    - 2.2.5 Oosterhout 3-layer model .................................................................................. 21
  - 2.3 Supply Chain Reference Models .............................................................................. 22
    - 2.3.1 SCOR Model (source: Wikipedia.org) ................................................................ 22
    - 2.3.2 UN/CEFACT buy-ship-pay –model .................................................................... 24
  - 2.4 Management and governance in supply chain management .................................... 25
    - 2.4.1 Management control systems ............................................................................ 25
    - 2.4.2 Governance regimes in global supply chains ..................................................... 27
    - 2.4.3 Supply chain event management (SCEM) .......................................................... 28
  - 2.5 Information management in supply chains ............................................................... 29
    - 2.5.1 Supply Chain Information Management ............................................................. 29
    - 2.5.2 Introduction to Supply Chain Visibility ............................................................... 30
    - 2.5.3 Current visibility and information exchange model .......................................... 31
    - 2.5.4 Visibility based on data pipeline model ............................................................ 34
  - 2.6 Future trends in supply chain management ............................................................. 36
  - 2.7 Conclusions and implications for CASSANDRA ....................................................... 37
6.4 Case study on practical security management in a high risk supply chain .................80
   6.4.1 Threat assessment as a starting point ...............................................................80
   6.4.2 Supply chain stages covered by the study .........................................................81
   6.4.3 Security measures implemented .......................................................................81
   6.4.4 Cost distribution, on a single site level (including transport security equipment) 83
   6.4.5 Benefits from security activities and measures for the case company ...............83
6.5 Security versus quality management ........................................................................84
6.6 Supply chain security regulations and standards .....................................................86
   6.6.1 Introduction .......................................................................................................86
   6.6.2 Mandatory data requirements ............................................................................86
   6.6.3 Company level binding regulations ....................................................................87
   6.6.4 Company level voluntary certifications ...............................................................87
6.7 Future trends in supply chain security management ................................................89
6.8 CASSANDRA implications .......................................................................................90
7 Governmental procedures, compliance and risk management ......................................91
   7.1 Overview ................................................................................................................91
   7.2 Procedures ..............................................................................................................91
   7.3 Compliance management ........................................................................................93
      7.3.1 Social Compliance ..........................................................................................93
      7.3.2 Responsive Regulation ..................................................................................94
      7.3.3 The Facilitation and Compliance Continuum ................................................69
   7.4 Risk management ....................................................................................................97
   7.5 Future trends .........................................................................................................102
      7.5.1 Single Window ................................................................................................102
      7.5.2 Consignment Completion Point .......................................................................105
      7.5.3 Coordinated border management ....................................................................106
      7.5.4 Mutual recognition ........................................................................................106
   7.6 Conclusions and implications for CASSANDRA .....................................................107
      7.6.1 Risk assessment issues ..................................................................................108
      7.6.2 Strategic benefits ..........................................................................................109
8 Technologies for supply chain visibility and security ....................................................110
   8.1 Overview ..............................................................................................................110
       8.1.1 Concerns and obstacles ..............................................................................110
       8.1.2 Security risks in the supply chain .................................................................110
       8.1.3 Practical implications ..................................................................................111
8.2 Supply chain visibility technologies ................................................................. 112
  8.2.1 Introduction to visibility systems ............................................................... 112
8.3 Supply chain security technologies ................................................................. 115
  8.3.1 Introduction ............................................................................................... 115
  8.3.2 Container security technologies ............................................................... 115
  8.3.3 Container seals ......................................................................................... 116
  8.3.4 Security Sensors ....................................................................................... 116
  8.3.5 Wide area communication ........................................................................ 116
  8.3.6 Biometrics devices .................................................................................... 116
8.4 Other relevant supply chain technologies ...................................................... 117
  8.4.1 Data handling and information platforms .................................................. 117
8.5 Future trends in supply chain technologies .................................................... 119
8.6 Conclusions and implications for CASSANDRA .......................................... 120

9 Standards in supply chain management ............................................................ 122
  9.1 Overview ..................................................................................................... 122
    9.1.1 Management standards .......................................................................... 122
    9.1.2 Data standards ....................................................................................... 122
    9.1.3 Other relevant standards ....................................................................... 123
  9.2 Future trends in supply chain standardization .............................................. 123
    9.2.1 Trends in Standards Drafting .................................................................. 123
    9.2.2 Standards Harmonisation Trends ............................................................ 124
    9.2.3 Technology Trends ................................................................................ 125
    9.2.4 National vs. Global Standards .............................................................. 126
  9.3 Conclusions and implications for CASSANDRA .......................................... 126

10 Specific lessons learned from previous related European projects .................. 128
  10.1 Overview .................................................................................................. 128
  10.2 INTEGRITY ............................................................................................... 128
    10.2.1 Role of interoperability ....................................................................... 128
    10.2.2 Lessons on Container Security Devices (CSDs) ................................... 129
    10.2.3 Lessons on exploitation ....................................................................... 129
  10.3 SMART-CM .............................................................................................. 129
    10.3.1 The SMART-CM Platform ................................................................... 130
    10.3.2 Lessons on Container Security Devices (CSDs) ................................... 131
    10.3.3 Lessons on exploitation ....................................................................... 131
  10.4 ITAIDE ..................................................................................................... 131
10.4.1 Piggy-backing and data pull ............................................................... 131
10.4.2 The Living Lab approach ................................................................. 133
10.5 Other past European projects ............................................................... 134
  10.5.1 Promit .................................................................................... 135
  10.5.2 D2D ..................................................................................... 135
  10.5.3 CHINOS .............................................................................. 136
  10.5.4 FREIGHTWISE ................................................................. 136
  10.5.5 MarNIS .............................................................................. 137
  10.5.6 KOMODA ........................................................................... 137
  10.5.7 GLOBE ............................................................................. 138
  10.5.8 M-TRADE ......................................................................... 138
  10.5.9 LOGSEC ............................................................................ 139
10.6 Relevant parallel projects ....................................................................... 139
10.7 Conclusions and implications for CASSANDRA ..................................... 142
11 Proposal for the CASSANDRA scope ..................................................... 147
12 Disclaimer and acknowledgement .......................................................... 149
  12.1 Disclaimer ............................................................................... 149
  12.2 Acknowledgement ..................................................................... 149
13 References ............................................................................................. 150
Table of Figures
Figure 2-1 Global Logistic Network Configurations (adapted from Eazza et al., 2010) ..............20
Figure 2-2 FCL versus LCL supply chain structure (source: RSM) ........................................21
Figure 2-3 Layered model of global supply chains (Oosterhout et al., 2000) ......................22
Figure 2-4 SCOR Framework levels (Source: Wikipedia) .........................................................23
Figure 2-5 UN/CEFACT buy-ship-pay –model ..................................................................24
Figure 2-6 Merchant haulage versus carrier haulage governance (source: RSM) .............28
Figure 2-7 Trigger-generating mechanism (Source: RSM) ...................................................29
Figure 2-8 Example of sequential information exchange (Source: Veenstra et al., 2009) ...34
Figure 2-9 Seamless Integrated Data Pipeline (Hesketh, 2009) ...........................................35
Figure 3-1 Contract types in a transport transaction .............................................................39
Figure 3-2 responsibilities for documents, costs, risks and insurance ...............................42
Figure 3-3 Basic flows for a commercial letter of credit transaction ..................................45
Figure 4-1 Organizational chart of the WTO (Source: http://wto.org/english/thewto_e/whatis_e/tif_e/organigram_e.pdf) .................................................................58
Figure 5-1 Framework for supply chain risk management (source: Waters, 2007) ............60
Figure 5-2 Levels of risk identification ...............................................................................62
Figure 5-3 Company-specific risk map (source: Kajüter, 2003) .........................................63
Figure 5-4 Supply Chain Risk Matrix (source: Kajüter, 2003) ...........................................64
Figure 5-5 Assessing the impact of various mitigation strategies (Chopra and Sodhi, 2004)66
Figure 5-6 Rules of Thumb for Tailored Risk Management (Chopra and Sodhi, 2004)......67
Figure 5-7 Typology of supply chain risks (source: Mentzer, 2001) ....................................69
Figure 6-1 Supply Chain Security Framework (Source: adapted from Juettner et al., 2003).73
Figure 6-2 Relationship between security, risk and compliance management disciplines – layman interpretation .......................................................................................74
Figure 6-3 Supply chain crime classified in three groups: economic, facilitating crime and other types ..................................................................................................................76
Figure 6-4 Supply chain operator ranking of criminal and terrorist threats in the supply chain (Source: FP7-LOGSEC). .......................................................................................77
Figure 6-5 8-layer supply chain security management model (Hintsa J. 2011) .................78
Figure 6-6 Case company supply chain – rectangle indicates the stages covered by the study ..............................................................................................................................81
Figure 6-7 Distribution of security (procurement) budget, example on a single site level ......83
Figure 7-1 Example of regulatory practice with ATO Compliance Model (Braithwaite, 2003)95
Figure 7-2 Visualization of a compliance continuum (Her Majesty's Revenue and Customs)97
Figure 7-3 Security threats in the global supply chain (Oosterhout et al., 2007) ...............98
Table of Figures

Figure 7-4 Risk-based auditing approach in general ............................................................ 99
Figure 7-5 A risk-based auditing approach for regulatory compliance ............................ 101
Figure 7-6 Cloud of many challenges implementing Single Window (Adopted from Van Stijn et al., 2011a, p.291) ........................................................................................................ 104
Figure 9-1 Dagang-Net system in Malaysia ....................................................................... 125
Table of Tables

Table 2-1 Organizations involved in container transport; adopted from (Wagenaar, 1992) ... 17
Table 3-1 Descriptions for Incoterms ................................................................. 41
Table 4-1. Overview of involved Dutch authorities and their roles in cross-border trade (Van Stijn et al., 2011c, p. 74) ....................................................................................................... 52
Table 4-2 Overview of key Directorates General and offices of the EC ......................... 54
Table 5-1 Supply chain risks (adapted from Chopra and Sodhi (2004)) ......................... 67
Table 5-2 Typology of supply chain risks ...................................................................... 69
Table 6-1 Security measures and activities at the case company supply chain ................. 82
1 Introduction

1.1 Overview

The main challenges facing international intermodal container logistics include efficiency and security. These seemingly conflicting issues have a common solution: supply chain visibility, where visibility data can be shared between business and government. Technical solutions for supply chain visibility already exist, but the challenge lies in integrating solutions across the supply chain.

CASSANDRA is the acronym for the project “Common assessment and analysis of risk in global supply chains” supported by the European Commission under the 7th Framework Programme theme SEC-2010.3.2-1 “Monitoring and tracking of shipping containers”. CASSANDRA will:

• Facilitate the adoption of a risk based approach in the supply chain, on the basis of integral monitoring data on cargo flows and container integrity;
• Build interfaces between existing visibility solutions, and visualisation tools, in an open architecture;
• Demonstrate the integration of data and risk assessment in supply chains in three major trading routes to and from Europe;
• Evaluate the quality of the integral data with business and government; and
• Facilitate a dialogue between business and government to reach consensus on the criteria for data sharing between business and government.

The project participants cover relevant stakeholders, including some global players. This expertise will assist in the successful adoption of the CASSANDRA solutions. The value drivers in CASSANDRA will include:

1. Logistics efficiency benefits;
2. Security benefits for business as a result of the risk self-assessment; and
3. Security benefits for government as a result of the high quality and complete data for government risk analysis.

The development of integral supply chain data that is the basis for risk based supply chain management and the input for government supervision tasks, as envisaged in CASSANDRA, will set a new standard for efficient and secure global door-to-door goods flows to and from Europe.

1.2 Document purpose and partners

The purpose of this Compendium is to provide a common reference document for CASSANDRA scope, concepts and terminology. It discusses different aspects regarding Supply Chain Visibility, presents the different actors and highlights various problem areas. The Compendium also discusses future trends in the different Supply Chain Visibility-related areas and presents conclusions and implications for the CASSANDRA project. The outcomes of the Compendium will serve the rest of the CASSANDRA project, helping to set the detailed scope for the project.
The Compendium has been developed as a collaborative process in the CASSANDRA project during the six months from July to November 2011. The following partners have participated in the production of the Compendium:

- Erasmus Universiteit Rotterdam, Netherlands, (EUR),
- GMVIS Skysoft SA, Portugal, (GMV)
- GS1 AISBL, Belgium, (GS1)
- Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek, Netherlands, (TNO)
- Cross-border Research Association, Switzerland (CBRA) (as the main responsible partner for the deliverable),
- Technische Universiteit Delft, Netherlands, (TUD)
- Institut für Seeverkehrswirtschaft und Logistik, Germany, (ISL)
- Fundacion Zaragoza Logistics Center, Spain, (ZLC)
- Atos Origin Sociedad Anonima Espanola, Spain, (ATOS)
- Ministerie van Financien Directoraat Generaal Belastingdienst, Netherlands, (DCA)
- HM Revenue and Customs, United Kingdom, (HMRC) and
- Portbase BV, Netherlands. (Portbase)

1.3 CASSANDRA research problem

The CASSANDRA research problem can be formulated as follows: “How to integrate existing supply chain visibility solutions and data capture technologies across supply chains to enhance risk assessment and to enable the adoption of a risk based approach to supply chain management for businesses in global trade as well as public authorities?”

The project focus is on data availability and data quality as regards risk management purposes.

1.4 Structure of the Compendium

In Chapter 2, we take a general look at Supply Chain Management: strategies, structures, management systems and information management.

Chapter 3 discusses financial and liability aspects in supply chains.

Chapter 4 presents the different national, supranational (EU) and international governmental actors regarding supply chain management. The chapter serves as a background to Chapter 7.

Chapter 5 discusses supply chain risk management from the private sector perspective.

Chapter 6 focuses on crime prevention and security management in supply chains.

In Chapter 7, we look at government procedures, compliance management and risk management, particularly from the Customs point of view.
Chapter 8 presents an overview of existing technologies for supply chain visibility and risk management.

Chapter 9 discusses the different relevant standards in supply chain management.

Chapter 10 presents several previous related European projects and discusses the lessons to be learned in CASSANDRA from them.

Finally, in Chapter 11, we propose a tangible scope for the CASSANDRA project, derived from the previous ten chapters.
2 Supply chain management

2.1 Introduction

Supply chain management (SCM) is defined as the management of a network of interconnected businesses involved in the ultimate provision of product and service packages required by end customers (Harland, 1996). Supply chain management spans all movement and storage of raw materials, work-in-process inventory, and finished goods from point of origin to point of consumption. In the sequel of this chapter we briefly present various aspects and configurations of supply chains. Moreover, the structure of the supply chains is investigated and some common SCM models are briefly discussed. This chapter proceeds with an introduction to information management in supply chains as well as supply chain visibility issues.

2.1.1 Aspects of supply chain management

According to the Council of Supply Chain Management Professionals (CSCMP), a second description of SCM is as follows; supply chain management encompasses the planning and management of all activities involved in sourcing, procurement, conversion, and logistics management. It also includes the crucial components of coordination and collaboration with channel partners, which can be suppliers, intermediaries, third-party service providers, and customers. In essence, supply chain management integrates supply and demand management within and across companies. Some of the problems that supply chain management should address are listed as follows (Mentzer et al., 2007):

- **Network Configuration**: number, location and network missions of suppliers, production facilities, distribution centres, warehouses, cross-docks and customers.

- **Distribution Strategy**: questions of operating control (centralized, decentralized or shared); delivery scheme, e.g., direct shipment, pool point shipping, cross docking, DSD (direct store delivery), closed loop shipping; mode of transportation, e.g., motor carrier, including truckload, LTL, parcel; railroad; intermodal transport, including TOFC (trailer on flatcar) and COFC (container on flatcar); ocean freight; airfreight; replenishment strategy (e.g., pull, push or hybrid); and transportation control (e.g., owner-operated, private carrier, common carrier, contract carrier, or 3PL).

- **Trade-Offs in Logistical Activities**: The above activities must be well coordinated in order to achieve the lowest total logistics cost. Trade-offs may increase the total cost if only one of the activities is optimized. It is therefore imperative to take a systems approach when planning logistical activities. These trade-offs are key to developing the most efficient and effective Logistics and SCM strategy.

- **Information**: Integration of processes through the supply chain to share valuable information, including demand signals, forecasts, inventory, transportation, potential collaboration, etc.

- **Inventory Management**: Quantity and location of inventory, including raw materials, work-in-process (WIP) and finished goods.

- **Cash Flow**: Arranging the payment terms and methodologies for exchanging funds across entities within the supply chain.

- **Demand management**: The proactive management of demand with business constraints (supply).
2.1.2 Supply chain management paradigms

Basically, shippers use one or a combination of the following supply chain paradigms, which affects the design of their supply chain (Lee, 2002; Carvalho and Machado, 2009)

- **Efficient supply chains**: supply chains that utilize strategies aimed at creating the highest cost efficiencies in the supply chain, based on scale economies and optimal capacity utilization.

- **Lean supply chains**: lean supply chain management aims to get close to zero inventories and reduce work-in-process. A lean company means nearly zero inventories.

- **Risk-hedging supply chains**: supply chains that utilize strategies aimed at pooling and sharing resources so that the risks in supply chain disruption can also be shared.

- **Responsive supply chains**: supply chains that utilize strategies aimed at being responsive and flexible to the changing and diverse needs of the customers, based on built-to-order and mass customization processes.

- **Agile supply chains**: agile goes for quick response to customer enquiries and market changes while controlling costs and quality. Agile supply chains utilize strategies aimed at being responsive and flexible to customer needs, while the risks of supply chain shortages or disruptions are hedged by pooling inventory or other capacity resources.

- **Resilient supply chains**: Resilience is about sustaining disturbances that may hit supply chains. A resilient company must have enough inventories to react to the effects of disruptions that may occur in a supply chain.

- **Green supply chains**: Green refers to sustainability in supply chains through low emission to nature and the recycling strategy for products. The issue of empty container handling and closed loop supply chains fall under this paradigm.

- **LARGE Supply Chain Management**: attempts to put together Lean, Agile, Resilient, and Green approaches in Supply Chain Management. Lean and resilient seem to be contradictory. However, it would be ideal to have both systems working together in one company. These facts indicate the need for further research in production and supply chain management; lean and resilient concepts need to be modelled on a compatibility basis. LARGE SCM develops a deep understanding of interrelationships (conflicts and trade-offs) across lean, agile, resilient and green supply chain paradigms. This understanding is believed to be vital to make these concepts really compatible. This achievement will provide an important contribution for a competitive and sustainable environment; its justification will be based on better “lean, agile, resilient and green production systems” at the company level, with implications at the overall supply chain level and its agents. LARGE SCM encompasses a variety of related topics such as methodology, characteristics, organizational systems, performance measurement, human factors, information systems, and management integration models.
2.2 Structuring and design of global supply chains

Arntzen et al. (1995) stress the fact that global supply chains are “a set of facilities, technologies, suppliers, customers, products and methods of distribution”. Global supply chains can be quite complex with multiple tiers, depending on the type of products, the sourcing of components, the number of manufacturing locations, the number of fabrication stages and the (location of) customer market(s). Differences in duties (import tax) can have a large influence on the design of global supply chains (Arntzen et al., 1995). Global firms can opt for duty drawbacks and duty avoidance strategies in the design of their global supply chain, which can lead to complex logistics flows and return flows with some value-added activities in between.

In the rest of this section we provide a brief introduction to the SCM models that may be relevant to the scope of CASSANDRA project.

2.2.1 Stakeholders in global supply chains

Global supply chains are complex networks. Based on their roles and responsibilities in the supply chain, organizations manage their processes and business activities with their own goals and objectives. These organizations can be categorized into five different groups (Wagenaar 1992), listed in Table 2-1.

Table 2-1 Organizations involved in container transport; adopted from (Wagenaar, 1992)

<table>
<thead>
<tr>
<th>Group</th>
<th>Examples of organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Commercial group</td>
<td>Seller/supplier (shipper); Buyer/customer (consignee)</td>
</tr>
<tr>
<td>2. Organizing group</td>
<td>Forwarder (merchant haulage); Shipping line agent (carrier haulage); Logistics service provider (4PL)</td>
</tr>
<tr>
<td>3. Physical group</td>
<td>Sea terminal operator; Shipping line/sea carrier; Pre- or On-carrier: carrier inland transport, i.e., barge operator, rail operator, road carrier; Inland terminal operator; Logistics service provider (3PL); Empty container depot operator</td>
</tr>
<tr>
<td>4. Authorizing group</td>
<td>Customs; Port authorities; Seaport police; River police; Inspection authorities</td>
</tr>
<tr>
<td>5. Financial group</td>
<td>Bank; Insurance company</td>
</tr>
</tbody>
</table>

Firms in the commercial group (1.) are concerned with the production and distribution of products, and constitute trade lanes in which commercial transactions (buying/selling) take place. These firms have competencies and direct interests in providing products to end-customers, and are responsible for the quantity and quality of the product. For transporting the products, they employ the logistics services provided by the second and third group. The organizing group (2.) mainly consists of brokers and intermediaries who integrate the cargo transportation, whereas the physical group (3.) actually perform the physical movements. These two groups usually have less interest in the product (c.q. cargo) but focus on the operational efficiency of the physical flow of cargos. The authorizing group (4.) has the
responsibility for monitoring and inspecting the cargo flow for the purpose of enforcing the security and economic regulations. Lastly, the financial group (5.) supports financial transactions between the organizations in the supply chain and facilitates the monetary flows. These five groups depend on one another to achieve their own goals. Without certain supply chain participants’ input or activity, products cannot be produced or transported and thus customer orders may not be fulfilled. These dependencies are to a large extent what makes supply chains vulnerable.

Configuration of such global logistics networks affects many operational, tactical and strategic level decisions of the SCM. Moreover, the notion of full container versus less-than-full container load plays a prominent role in various SCM decisions. Therefore, we first proceed by exploring these concepts.

It is worth discussing the differences of 3PL and 4PL. A 3PL is a company contracted to provide various services. These services are typically logistical in nature and often include many other value added services; examples are packing, e-commerce support, inventory management and transportation. A 4PL is a consultancy organization that manages one or more companies, for example if a company has a contract with some 3PLs together with transportation companies, they may consider hiring a 4PL to manage all of them together.

2.2.2 Global trade process and management

Effective management of trade processes is critical to the efficiency of a global supply chain. Hausman et al. (2009) developed a framework for Global Trade Management to describe these complex trade processes and make it easier to be understood by general supply chain managers. The process of global trade and information exchange was visualized in process charts in Hausman et al. (2009) and are briefly summarized as follows:

1. **Pre-Export**: when the buyer places an order with the seller, the full description of the goods, unit price, Incoterm, payment details, insurance, dates and logistics are negotiated and an international contract of sale agreed upon.

2. **Production**: the goods are produced.

3. **Transport Arrangement & Export Declaration**: the seller obtains approval from inspection agencies and prepares and transmits export declaration / security filings for export Customs clearance. The seller employs a freight forwarder to manage the export, while the buyer employs a freight forwarder to manage the import. The export freight forwarder identifies the sea carrier, the port of loading and port of discharge and orders a container from the carrier to be sent to the seller/consignor. The transport and logistics plan is communicated to the import freight forwarder.

4. **Transport & Import Declaration**: The container is loaded at the seller’s premises and is ready for consigning into the international trade supply chain (Consignment Completion Point, CCP). International ocean or air transport of the goods is done. The buyer generates and submits import documents for import customs clearance.

5. **Post-Import Customs Clearance & Payment**: the final steps include inland delivery from the border to the importer’s site, receipt of goods, review of landed cost, settling payment with the forwarder, broker and exporter, and filing for foreign exchange verification and tax refund if applicable.
2.2.3 Global Logistics Network Configurations

Global shippers use different logistics network configurations to organize the supply of goods to the markets of destination. In general, three main options can be considered to configure a logistics network: direct shipment, one-echelon network and two-echelon logistics network (Simchi-Levi et al., 2003). In the one echelon network, a consolidation hub can be located close to the suppliers (i.e. upstream of the ocean shipping leg) or close to the market (i.e. downstream of the ocean shipping leg). We consider five generic logistics network configurations.

1. **Configuration 1 – Direct shipment with full container load (FCL):** a single supplier (Si) ships a full container load to a regional warehouse (RW) located in Europe, by means of a first container haulage to a loading port, an ocean shipping leg and a final container haulage from the unloading port to a final destination (RW).

2. **Configuration 2 – Direct shipment with groupage container (less than container load (LCL)):** non-containerized goods are shipped by means of road haulage to a freight forwarder’s facility located near the loading port (PL) for container consolidation; after the ocean shipping leg, the container is deconsolidated at the unloading port (PU) and non-containerized goods are hauled to one or more regional warehouses (RWj).

3. **Configuration 3 – One echelon logistics network with consolidation hub (CH):** non-containerized goods are shipped by means of road haulage to the company’s CH where goods are temporarily stored. After consolidation, containers are shipped by means of FCL from a unique LP to a final destination (RWj).

4. **Configuration 4 – One echelon logistics network with central warehouse (CW):** all the suppliers ship their goods by means of FCL to a unique PU, the closest to the CW. Here shipments are deconsolidated and non-containerized goods are hauled to one or more regional warehouses (RWj).

5. **Configuration 5 – Two echelons logistics network with both CH and CW:** non-containerized goods are shipped by means of road haulage to the company’s CH. After consolidation, containers are shipped from the PL by means of FCL to a unique UP the closest to the CW. Here shipments are deconsolidated and non-containerized goods are hauled to one or more regional warehouses (RWj).
Besides the main configurations described above, there are three alternatives entailing the use of LCL along with one or two echelon logistics network. These configurations are hardly used, since the use of these configurations results in a redundancy of logistics activities and, as a consequence, in inefficiencies in terms of costs and delivery lead times.

The five considered configurations differ one from another in terms of cost structure, supply lead times, risk of delay and operational complexity (i.e. the intensity of the effort necessary for logistics network planning and control) and therefore impact risk assessment and the design of the CASSANDRA data pipeline.

2.2.4 FCL versus LCL Supply Chain configurations

Ocean container shipping can be performed in two different ways (Zeng, 2003; Dallari et al., 2006), namely shipment with full container load (FCL) and shipment with groupage container (less than container load (LCL)). Therefore it is possible to optimize the ocean container shipping through a consolidation hub, i.e. a node of the logistics network where shipments from several suppliers are collected and consolidated – similar to a cross-docking facility – and they are shipped to the final destinations (Cheong et al., 2007).
Problems with lack of visibility in buyer-seller relationship exist especially in the case of LCL containers, where multiple consignments are carried in one container. Customs receives information (manifest) from the carrier. Detailed information about individual consignments is missing and only becomes available when the buyer or their freight forwarder sends the import declaration to Customs once goods have been discharged in the country of destination.

![Diagram showing FCL versus LCL supply chain structure](source: RSM)

### 2.2.5 Oosterhout 3-layer model

Supply chains can be analyzed from the perspective of three different but interrelated layers, i.e., sets of activities (Oosterhout *et al.*, 2000; Willis and Ortiz, 2004), the physical logistics layer, the transaction layer, and the governance layer. The first layer relates to physical activities (such as transport and transhipment), transportation infrastructure (such as warehouses, barges), unit loads (such as containers, trailers) and the cargo (products which are transported) itself. The second layer is a layer of contracting or transaction activities that encompass all commercial and non-commercial relationships between parties in the supply chain. In this layer information is created, stored and transmitted in electronic format or otherwise. Finally, there is the governance layer, in which supply chain decision makers allocate resources, monitor performance and cargo flows and optimize costs and efficiency. This layer also includes all governing bodies with their inspection and verification activities, such as Customs, Police and Port Authorities. The second and third layers consist of information and financial flows.
2.3 Supply Chain Reference Models

2.3.1 SCOR Model (source: Wikipedia.org)

Supply-chain operations reference-model (SCOR), endorsed by the Supply-Chain Council (SCC), is the cross-industry de-facto standard diagnostic tool for supply chain management. SCOR enables users to address, improve, and communicate supply chain management practices within and between all interested parties in the supply chain (extended enterprise). The model has been developed to describe the business activities associated with all phases of satisfying a customer's demand. It is based on three major "pillars": Process modelling, Performance measurements, and Best practices.

The process-modelling pillar provides a common set of definitions, consisting of five distinct management processes:

- **Plan** – Processes that balance aggregate demand and supply to develop a course of action which best meets sourcing, production, and delivery requirements.
- **Source** – Processes that procure goods and services to meet planned or actual demand.
- **Make** – Processes that transform products to a finished state to meet planned or actual demand.

![Layered model of global supply chains (Oosterhout et al., 2000)](image-url)
• **Deliver** – Processes that provide finished goods and services to meet planned or actual demand, typically including order management, transportation management, and distribution management.

• **Return** – Processes associated with returning or receiving returned products for any reason. These processes extend into post-delivery customer support.

The scope of SCOR focuses on the following:

• All customer interactions, from order entry to paid invoice.

• All product (physical material and service) transactions, from your supplier’s supplier to your customer’s customer, including equipment, supplies, spare parts, bulk product, software, etc.

• All market interactions, from the understanding of aggregate demand to the fulfilment of each order.

Some other key assumptions addressed by SCOR include: training, quality, information technology, and administration (not supply chain management). These areas are not explicitly addressed in the model but rather assumed to be a fundamental supporting process throughout the model.

SCOR provides three-levels of process detail. Each level of detail assists a company in defining scope.

• Level 1, configuration or type of supply chain;

• Level 2, process element details, including performance attributes;
• Level 3, process elements decomposition and the implementation of specific supply chain management practices. It is at the third level that companies define practices to achieve a competitive advantage, and adapt to changing business conditions.

SCOR is a process reference model designed for effective communication among supply chain partners. Being an industry standard it also facilitates inter and intra supply chain collaboration, horizontal process integration, by explaining the relationships between processes (i.e., Plan-Source, Plan-Make, etc.). It also can be used as a data input to completing an analysis of configuration alternatives (e.g., Level 2) such as: Make-to-Stock or Make-To-Order. SCOR is used to describe, measure, and evaluate supply chains in support of strategic planning and continuous improvement.

2.3.2 UN/CEFACT buy-ship-pay –model

In order to understand the complexity of international trade, to have a clear model of the key elements of a trade transaction and consequently to properly compile the necessary trade facilitation measures, UN/CEFACT has set out to model the international supply chain, using an internationally accepted modelling technique. The ultimate aim is to provide a reference model, which gives a view of the international supply chain in its entirety. It should also pave the way for the creation of simpler and more certain international supply chains in the future.

This model is based on the assumption that an international trade transaction always includes commercial, shipping and payment processes (BSP):

1. **BUY** - covering all commercial activities related to the ordering of goods;
2. **SHIP** - covering all of the activities involved in the physical transfer of the goods, including official controls;
3. **PAY** - covering all of the activities involved in the payment for the goods

![Figure 2-5 UN/CEFACT buy-ship-pay –model](http://www.unece.org/cefact/recommendations/rec18/Rec18_pub_2002_ecetr271.pdf)

The BSP model can be used as a reference for all parties engaged in the supply chain in order to assist in harmonization of trade processes and data. The general principles in the model make recommendations regarding how to simplify the procedure, data and documentary requirements, and also of encouraging the use of information and communication technology with reference to standardized formats.

Concerning the commercial measures, the predominant aims of this model are the reduction of the number of actors in the chain, reduction of intermediate or buffer stores and lead times by way of automation and the integration of information systems. Recommendations include, inter alia, the alignment of seller’s and buyer’s in-house documents, inclusion of packing and delivery instructions in

---

the purchase order, timely arrival of dispatch and shipping advice (from exporter to importer to enable timely arrangement for clearance and transport), and the use of standard conditions of sale and trade terms (such as INCOTERMS of the ICC).

Concerning the international payment measures, the BSP model aims at reducing the seller’s peril against non-payment, late payment or the supply of products for no profit. The recommendations in the model have a focus on open accounts, reflecting an increasing trend towards the use of this payment method in international trade. The measures are directed separately at traders, international banks, national governments and international organisations in order to facilitate implementation. Especially, recommended measures directed at international traders (mainly for sellers) suggest the monitoring of creditworthiness and payment morality by sharing information with their banks, and the managing of prompt payment following dispatch and delivery of the goods. And for national government, recourse mechanisms for preventing delayed payment are highlighted; e.g. following ISO9004:2000 “Quality management systems - Guidelines for performance improvements”, it should be verified that the payment system is adequate for fulfilling the contractual arrangements.

Concerning the measures related to official controls, the BSP model advocate the necessary balance between private and public interests, which should be built on ongoing cooperation, so that the easy and rapid movement of goods across borders can be well facilitated while national and international public interests can be well protected. The official procedures are recommended to be transparent and predictable, and the rules for inspection, control and testing of goods in international trade should be justified in cost benefit analysis. The model highlights audit-based control, using traders’ commercial accounting systems, and at the same time it serves as a reminder that audit-based controls should not preclude physical examination of the goods (see Revised Kyoto Convention Guidelines, Ch 6, 7.2)².

Concerning the transport-related measures, the key procedures recommended in the model mainly involve “the selection and contracting of transport services, the determination of responsibility for goods under custody and of their corresponding insurance coverage, the recording of the goods carried, advice of the action taken, and claims for payment for services rendered”. In addition to the transport operators and carriers, the key players include freight forwarders, Customs agents (brokers), cargo handling agencies and port, warehouse and terminal operators. Computerised cargo tracking and tracing systems should be introduced to provide clients with advance information on the status of their consignments (such as location, integrity, event history, etc.).

2.4 Management and governance in supply chain management

2.4.1 Management control systems

Management Control System (MCS) is “the formal, information-based routines and procedures managers use to maintain or alter patterns in organizational activities” (Simons, 1995). In the inter-organizational settings such as a supply chain, MCS can be used as a research perspective to analyze the interdependency, outsourcing, trust, interaction and coordination between partner companies (Jeschonowski et al., 2009; Kartseva, 2008).

²See http://www.wcoomd.org/Kyoto_New/Content/body_gach6.html
MCS is traditionally studied under the discipline of accounting systems for organizing management information and assessing accountability of an economic entity. It gathers and uses information to evaluate the performance of different organizational resources like human, physical, financial and also the organization as a whole. It is an instrument for implementing organizational strategies, setting targets, and making sure that the targets are met and that the individual employees or economic entities are behaving as they are supposed to.

The basic concept in MCS regards an organization as the combination of a managing system and a managed system, where the managing system directs the operations in the managed system using a plan–do–check–act (PDCA) control cycle. Otley (1999) provides a MCS framework based on performance management:

- **Objectives**: What are the key objectives that are central to the organization’s overall future success, and how does it go about evaluating its achievement for each of these objectives?
- **Strategies and plans**: What strategies and plans has the organization adopted and what are the processes and activities that it has decided will be required for it to successfully implement these? How does it assess and measure the performance of these activities?
- **Targets**: What level of performance does the organization need to achieve in each of the areas defined in the above two questions, and how does it go about setting appropriate performance targets for them?
- **Rewards**: What benefit can the managed group (economy entities) gain by achieving these performance targets (or, conversely, what penalties will they suffer by failing to achieve them)?
- **Information feedback**: What are the information flows (feedback and feed-forward loops) that are necessary to enable the organization to collect historical data and to adapt its current behaviour in using these data?

With necessary adaptations, the Otley framework can be used in supply chain (inter-organization) management, although it was first designed for intra-organization management. The motivation for implementing MCS in the field of SCM roots from the interdependencies between supply chain partners: the performance of one company is affected by and affects other companies in the same supply chain. Such inter-firm dependency demands proper assessment and management of the accountability of the supply chain partners, in either the phase of forming the supply chain (selecting partners) or maintaining the business relation. Jeschonowski et al. (2009) pointed out that “extraordinary efforts into [inter-organizational] MCS can be translated into obvious competitive advantages and visible success”. Morash (2001) illuminates how an overall business strategy (or “competitive strategy”) and the corresponding specific supply chain strategy may be transformed into defined supply chain capabilities and an increased supply chain performance.

The inter-organization MCS can be seen as an extension of the intra-organization MCS, enlarging the management scope to integrate (vertically) the partners’ resources into the focal company and to develop special supply chain capability (implementing the “functional strategy”). The management control on the supply chain (inter-firm) level is in fact a coordination scheme that includes sharing operations data and coordinating supply chain decisions. Such a scheme must align the interests of different partners, so that all the partners have proper incentives to optimize the overall performance of
the supply chain. In practice, a monitoring mechanism must be in place to prevent opportunistic behaviours (Kartseva, 2008). For controlling performance, not only the performance of a partner organization (the managed system) needs to be managed, but also its managing system’s capability to control its own organization needs to be evaluated. The latter type of controlling may be implemented by introducing external auditors (Bukhsh and Weigand, 2011).

2.4.2 Governance regimes in global supply chains

There are different governance regimes in global supply chains. A distinction can be made between merchant haulage, carrier haulage and terminal haulage.

In case of carrier haulage one of the transport operators (usually the deep sea shipping company) is the contract party for the shipper and responsible for final delivery to the consignee. In carrier haulage the ocean carrier subcontracts the transport for the other legs to other trusted transport operators and as such offers a complete door-to-door service to the shipper.

In case of merchant haulage the consignee or the third party representatives (freight forwarder) is responsible for the delivery and remains in control of the transport solution it wants. Carrier haulage allows shipping lines to have a tight control over boxes moving inland. Under the merchant haulage carriers might loose visibility of the box fleet leading to misallocations of boxes (Theofanis and Boile, 2008). The difference between merchant and carrier haulage is depicted in the following figure. In the case of merchant haulage there are more parties involved in the organization of the transport, which makes the information sharing as part of the CASSANDRA data pipeline more complex.

In Europe, the merchant-haulage has the greatest market share of door-to-door service, while carrier haulage is decreasing. An exception is the United Kingdom where 70% of the market is in carrier-haulage hands. 3PL haulage is a new model, where the 3rd party logistic service provider has control of the hinterland transport on behalf of the shipper or consignee.

A recent new governance model is terminal haulage, where the terminal operator is also responsible for (part of) the in-land transport, for instance to an in-land terminal. Recent initiatives like extended gate in Rotterdam exploit this governance model, where ECT is responsible for storage of containers at the deep-sea terminal, in-land carriage via barge and rail and storage of containers at the in-land terminal.
2.4.3 Supply chain event management (SCEM)

SCEM provides information that supports decision-making in supply chain management. It describes the fundamental business problem of disturbances and deviations caused by the outside factors, and inter-organizational process failures. SCEM attempts to identify, as early as possible, the resulting deviations between the plan and its execution across the multitude of processes and actors in the supply chain to trigger corrective actions according to predefined rules (Otto, 2003). The term SCEM indicates both a management concept and a software solution, which have been proven in the EU projects of INTEGRITY and SMART-CM.

The main purpose of SCEM is managing exceptional events in supply chains. Management by exception is a system of identification and communication that signals the manager when his attention is needed; conversely, it remains silent when his attention is not required (Straube, Vogeler and Bensel, 2007).

The main element in SCEM that helps to keep track of progress of order processing is the “milestone”. For example, the milestone “end of assembly” in the whole process is defined as an event, and delayed assembly is communicated via an event message to the SCEM system. This lateness is a deviation from the plan and will be treated as a problem once it exceeds a predefined threshold. SCEM would then trigger a sequence of actions to solve such problems. It may raise alerts to those concerned with re-planning the milestones for the subsequent operations. It would also contact the carrier for the reasons of the delay, and may send emails to the customer. In a more sophisticated system, SCEM may do further work on calculation and proposing to lower priorities of the assembly centres for further orders and give suggestions to insert time buffers in the order network for future plans related to this assembly centre, and finally give suggestions to insert an extra event to identify deviations earlier.

Figure 2-6 Merchant haulage versus carrier haulage governance (source: RSM)
In the supply chain, visibility is a precondition to adequately manage events. Companies implement SCEM solely for the sake of creating supply chain visibility (Kemmeter and Knickle, 2002). SCEM is also seen as a concept that introduces the need for “real-time information” across the entire supply chain (Stelzner and Conrad, 2003). The interaction of milestones, targets and triggers is illustrated in the below figure.

![Figure 2-7 Trigger-generating mechanism (Source: RSM)](image)

**2.5 Information management in supply chains**

**2.5.1 Supply Chain Information Management**

Numerous information exchanges take place in the supply chain facilitated by containerized transport. To support a fast, reliable, and efficient information exchange, various internal and external information systems are used to support planning, execution, managing and reporting. As SCM is within a networked and collaborative environment, the Inter-Organizational System (IOS) plays a major role (Baalen et al., 2008).

Fundamentally, information management consists of the following activities:

1. Data capturing,
2. Data storage and transfer,
3. Data processing,
4. Business intelligence eliciting, and
5. Information sharing.
The **capture of data** can be done in two ways: The data can be retrieved from other information systems, possibly owned by other organizations, or the data can be captured directly from the supply chain. The latter way provides first-hand data, possibly in a real-time fashion. For example, the logistics tracking of the movable asset provides information on the whereabouts of assets, using automatic identification such as radio frequency technologies (RFID). The use of additional devices such as anti-tampering devices, global positioning devices, sensors that register cargo conditions such as temperature, humidity, and air quality, further enhances the possibility to monitor and control the container and its cargo throughout the supply chain.

**Data storage and transfer** facilitates inter-organizational collaboration by connecting two or more geographically and organizationally disparate applications. While trends indicate a move toward non-brokered information exchange, i.e. the modular distributed plug and play architecture (Web Services), information brokers like port-community systems are expected to play a key role in security related IOS in supply chain management.

**Business intelligence technology** processes the raw data to produce decision-support information, which is fit for use by data consumers. Fitness for use means that the data should be accessible to the user, the user should be able to interpret the data, and the data should be relevant to the user. It should be offered to the decision-maker in a timely fashion. In particular, the quality of intelligence relies heavily on accuracy of the input data: inaccurate data can only produce false intelligence.

Inter-organizational information sharing in supply chains is needed since organizations are unable to generate all of their required resources internally. Besides the various benefits of information sharing acknowledged by academia and managers (Samaddar *et al.*, 2006), major concerns are placed on the risk of misappropriation of the information shared and the opportunities for information leakage.

### 2.5.2 Introduction to Supply Chain Visibility

The objective of information management in supply chains is to increase visibility. Without proper IT solutions, many logistics managers describe their transportation system as a “black hole” – shipments disappear when rendered to the carrier and no information is available to either shipper or consignee until the shipment has been delivered (Sheffi, 2001). And in addition, the transportation or logistics link only connects two nodes in a supply chain. Visibility in the supply chain as a whole should be much broader.

According to Haywood and Peck (2004a, 2004b), currently visibility in the supply chain beyond the first tier supplier and/or customer is “an illusion” and true visibility is difficult to achieve. Consequently the access to accurate information in the upstream and downstream supply chains is ambiguous beyond the 1st tier supplier and 1st tier customers (Svensson, 2004).

Visibility is crucial for increased security in the supply chain. Agility for example cannot be achieved without increased visibility and the same applies to adequate analysis. In order to achieve this, information sharing throughout the supply chain is vital. Chen (2003) describes information sharing in supply chains with independent players as being tricky. He further states that a player with superior information could gain strategic advantage or could reveal it to gain cooperation from others. On the other hand several papers have proven the benefits of information sharing in the supply chain. Lee *et al.*
(1997) mention information sharing as one of the remedies against the bullwhip effect. The bullwhip effect (or whiplash effect) is an observed phenomenon in forecast-driven distribution channels. It refers to a trend of larger and larger swings in inventory in response to changes in demand, as one looks at firms further back in the supply chain for a product.

Chen (2003) himself provides a simple example where only the sharing of lead-time information can result in significant cost savings.

Lee and Whang (2000) distinguish six types of information that are shared in the supply chain: a) inventory, b) sales data, c) order status/tracking, d) sales forecast, e) production/delivery schedule and f) other (performance metrics and capacity). The information necessary for security can be attached to order status/tracking, production/delivery schedule and others. One other type of information that may help visibility is the information on the parties in the chain: who are they, and how are they performing. Furthermore, not only real time visibility is required, but also traceability of past activities, for the purpose of audits, verification of integrity of the chain, and so on.

2.5.3 Current visibility and information exchange model

To describe the (lack of) current visibility, we describe an example case of information exchange that accompanies the international transport of goods. This case involves a European importer, who buys FOB from a Chinese manufacturer. The supply chain includes a freight forwarder at origin and at destination. The freight forwarder assumes the cargo responsibility (which includes booking of pre- or on-carriage), customs broking, and ship booking. The description below is taken from the Integrity project (Veenstra et al., 2009).

The sequence of activities is as follows:

1. Purchase order received – manufacturing or sourcing takes place
2. Order complete for dispatch → shipper’s letter of instruction is sent to forwarder
3. Forwarder initiates ship booking
4. Forwarder initiates transport booking at origin → container pick up, packing list
5. Terminal receives container
6. Origin Customs release
7. Container is loaded
8. Shipping line signs B/L
9. Freight forwarder at origin sends data file containing B/L, invoices and other documents to freight forwarder at destination
10. Several days before ship arrival at destination, shipping line signals ETA
11. Freight forwarder at destination performs document check and initiates on-carriage booking
12. Ship arrival → container unloaded
13. Commercial release/Destination Customs release
14. Container pick up for delivery to warehouse

15. Transport operator or warehouse operator generates proof of delivery.

Some important observations in this process are:

1. There are inherent uncertainties in this process, which lead to invisibilities that are difficult to resolve. For instance, the booking of the truck at origin is placed in such a way that the container will be loaded on the right ship on time. This booking is made against a deadline (the cut-off date and time for the ship), but container pick up and delivery can take place somewhere between several days and five minutes before that deadline. Exact pick up time at the factory is not agreed upon in the truck booking or with the factory, and usually remains unrecorded. The truck booking runs from empty container pick up to container delivery at the terminal, for which often 7-10 days is allowed by the shipping line (for the use of the empty container).

2. The main information transfer from origin to destination takes place somewhere around 10 days after ship departure when the freight forwarder at origin sends a file to the freight forwarder at destination. This file includes house and master B/Ls, commercial invoices, certificates and packing lists. This transfer can be done through system-to-system communication, but this does not seem to be very common. In many cases, it is done by email, fax, and regular mail. Considerable administrative effort is spent on checking the accuracy and completeness of this data file.

3. Much of the administrative burden is in the information gathering on ship arrival. Ship arrival is an important deadline for document preparation (transport booking, arrival notification to final destination, customs declaration), but accurate ship arrival information is notoriously difficult to obtain.

4. The customs declaration process at the destination side contains several steps:
   - Initial declaration on basis of the ship manifest by the shipping line
   - Completion of the declaration for import or transit by the ‘customs broker’ (often the freight forwarder)
   - Final declaration for import at the warehouse location
     The first two steps lead to the customs release at the terminal, either directly, or after an inspection activity, which can be asking additional documentation, x-ray, partial inspection or complete inspection of the container. There are costs involved in the inspection activities, and especially full inspection will result in a time delay of up to two days.

5. There can be a considerable difference between the minimum required time and the actual time spent in the on-carriage part of the chain. In principal, container pick up at the terminal could take place almost immediately after unloading of the container, transportation to an inland location by truck, barge or train will not take more than half a day (note: this would be the case e.g. in the Netherlands), and unloading and loading at an inland terminal may also take part of a day. On average, even in the intermodal case, on carriage could be completed in two days. In practice, this is not often the case. Some of the delay is due to the documentary process (release of the container may be delayed), and the container is often only considered available for pick up upon departure of the ship, instead of immediately after unloading. Furthermore, time in stack at the terminal may be extended for other reasons: lack of warehouse space, cost and commercial considerations. As a
result, estimated lead time for the on-carriage part of the chain can easily be 5 – 10 days. This 
effects demurrage and retention costs.

6. In several cases, de-gassing of the container is required (due to the fact that some products generate 
gas in the closed confines of the container). There is usually no advance information if the container 
needs to be de-gassed, and de-gassing takes time. As a result, the discovery of gas in a container 
causes a major and immediate bottleneck in the logistics chain. Information exchange between 
parties (3PL, ultimate user and terminal) could help to find a good location in the chain to perform 
the gas measurement and possible de-gassing activity.

7. Trade lane partners would like to be notified about the delivery of empty containers in depots. This 
delivery date completes their use period of the container, and is the reference for any demurrage 
calculations. Currently, lack of visibility (on gate out at terminal and gate in at depot) can lead to 
demurrage and retention costs.

Most international trade lanes follow more or less the same pattern as specified above, but there are 
variations as to the role and scope of work of freight forwarders, on both ends of the chain and the use 
of information systems.

For instance, if a company uses a freight forwarder only as a customs broker (even if this is the case in 
Europe), then the information exchange in terms of content will be the same, but the parties that send 
or receive information may differ. In some cases, a shipping line agent may actually act as freight 
forwarder, in the sense that they finish the transit declaration of goods, and book hinterland transport, 
but this agent will not be the initial recipient of the data transfer from the freight forwarder at origin. 
The importing company or buyer will receive this data, and send a copy of it to the shipping agent. This 
is a situation that is actually quite common in Rotterdam (and other European ports), where ship agents 
have been developing their portfolio of services into the realm of classic freight forwarding activities.

Another major difference is the use of integral information systems, such as GT Nexus, or internal 
systems, such as Ocean Logic in DHL. In these systems, in principal, the data transfer takes place 
digitally, which prevents data entry at both the origin and destination. This should prevent a lot of 
errors, additional administrative effort, and correction time. On the other hand, the data in these 
systems has to be completely reliable, and this requires (al lot of) additional time as well. As a result, 
time savings from having an integral visibility system may not be attainable, but there should be less 
errors and missing data.
2.5.4 Visibility based on data pipeline model

The international trade supply chain has grown in complexity to a point where clear visibility is masked from those who need to know what is going on. UK and Dutch Customs have jointly developed, not yet implemented, the concept of a seamless, integrated, web-based data pipeline, designed to capture consignment and people data upstream in the supply chain and as the goods move along it (Hesketh, 2009; 2010).
In the process of global trading (see Section 2.2.2), much of the data used by governments for regulatory monitoring and risk assessment resides in the commercial documents such as contracts of sales, bills of lading, and manifests. Risk assessment is carried out by both public and private sector organisations. They often use the same data and ask similar questions but apply them in different ways, depending on business objectives. If the importer and exporter are carrying out effective risk management using common data as part of the ‘buy, ship, pay’ process then could government agencies rely more on this process instead of duplicating it? In this project, we call this the Piggy-Back principle. Government ‘piggy backs’ on the data available in the supply chain and on supply chain risk assessment of businesses, according to pre-agreed protocols.

The concept of the data pipeline is that most of the data required by Customs will be known by the consignor at the Consignment Completion Point as a result of successful negotiations between buyer and seller of the international contract of sale (Figure 2-9 light blue lines). At that point the consignor/exporter/seller or his freight forwarder can provide the required export and import data needed for risk, compliance and admissibility purposes to the regulators in the country of export and the country of import simultaneously using the pipeline (Figure 2-9 green and red lines). When the final shipping details are known prior to loading the remaining details for pre-arrival, pre-departure (PAPD) can be updated in the pipeline and sent to the transit country and import country regulators (Figure 2-9 grey line) for risk assessment and ‘load’, ‘don’t load’ verification. When the goods arrive in the country of destination the consignee/importer/buyer or his freight forwarder, will confirm with customs that the consignment details have not changed and advise Customs which regime the goods will be entered into (Figure 2-9 red line). Thus, within the pipeline concept the key players will be the buyer and seller (consignee and consignor), the freight forwarders in the countries of export and import, the import and export container terminals and the sea carrier.
2.6 Future trends in supply chain management

Some major trends that might affect CASSANDRA are listed as follows. These trends were identified from the literature review and CASSANDRA brain storming sessions held in the WP100 workshop.

1. **Increasing dynamism of supply chains**: Supply chains increasingly become more dynamic (more and changing partners) due to globalization and trends of outsourcing. Outsourcing allows access to global markets and thus contributes to the globalization of supply chains. In general, the degree of company-internal value-added decreases, as companies transfer processes to other members of the supply chain. This is practiced especially in areas with less competence, which are better handled by other, specialized organizations. Outsourcing generally leads to a fragmentation of the supply chain. Business transactions become more complex and firms might face situations in which they only have insufficient control over key processes. Outsourcing is mainly driven by the quest for lower cost of sourcing, manufacturing, logistics and other operations (See Chapter 5 on supply chain risk management).

2. **Synchromodality**: The concept is synonymous with the creation of an optimum flexible and sustainable transport system in which companies can choose from a range of modalities at any given moment. Companies are thus always assured of optimum transport combinations and can easily switch between modalities if necessary. In addition to giving flexibility to companies in choosing the appropriate mode of transport this concept contributes to CO2 reduction.

3. **Risk awareness**: The impact of devastating incidents has led to a growing interest in the area of supply chain risk and its management, as evidenced in the number of industry surveys, practitioner conferences and consultancy reports devoted to the topic, e.g., McKinsey (2006) (See chapter 5 on Supply chain risk management).

4. **4PL**: It is defined as a supply chain integrator that assembles and manages the resources, capabilities and technology of its own organization, with those of complementary service providers, to deliver a comprehensive supply chain solution. As the 4PL industry is still in its infancy and currently being created throughout the world, its definition and function still lead to a lot of confusion, even for professionals of the transportation and supply chain management industries (See 2.2.1 Stakeholders in Global Supply Chains).

5. **Increasing ship size**: With the ship size reaching 15000TEU and expecting to exceed 18000TEU in the near future, the implications of such massive vessels with a very restricted number of port calls in Asia and elsewhere are that there will be an even greater focus on hub-and-spoke and transshipment of cargoes than we have seen to date.

6. **Consolidation in container shipping lines**: The merger of shipping companies engenders a larger scope to service and affects shipping, terminal and haulage operations. Shipping lines also extend their services (shipping, terminals, haulage).

7. **Haulage pattern**: Recently, there has been a transition in haulage patterns from merchant and carrier haulages towards terminal haulage (See 2.2.1 Stakeholders in Global Supply Chains).

8. **Brand and IPR protection**: With companies being hurt from the increasing IPR (Intellectual Property Rights) infringements they are calling for more transparency to avoid IPR violation and counterfeiting product entering legitimate or illegitimate channels (See Chapter 5 on Supply chain risk management).

9. **Extended Gate concept**: The key to this concept is the possibility to send large volumes of containers from the deep-sea terminal to inland terminals immediately after arrival on the deep-sea ship.
clears up the stack, and allows the terminal operations to work without delay (See 2.4.2 Governance regimes in global supply chains).

10. **Environmental impact and social responsibility**: There has been an increasing awareness on environmental issues. Environmental issues with emission quotas will reshape both how supply chains are structured and how companies will seek energy efficient manufacturing and transportation solutions. Moreover, increasing social responsibility awareness calls for higher levels of security (See 2.1.2 Supply chain management paradigms).

11. **Horizontal collaboration of shippers**: This leads to shippers combining loads, having joint warehouses etc. This requires cross-chain control concepts, where 4PLs are one of the candidates who can provide these kinds of services.

12. **Traceability of cargo and containers**: There has been an increasing need for tracing and tracking of containers both at the terminal and supply chain level in order to identify the chain of custody in case any disorder occurs. Moreover, having a traceable containerized SC leads to a boost in operational performance. Moreover, this has led to the introduction of smart product and containers. These are products or containers equipped with track and trace technologies. Traceability of cargo is increasingly important to guarantee product quality and trace back in case of disruptions (See 2.5.2 Introduction to supply chain visibility).

### 2.7 Conclusions and implications for CASSANDRA

The future trends have a number of important implications for CASSANDRA and the design of the data pipeline for visibility:

1. Oosterhout’s 3-layer model analyzes supply chains from the perspective of three different but interrelated layers, the physical logistics, the transaction and the governance layer. It provides a good understanding of how different agents in various layers of the supply chain communicate with each other and the dependencies among the different layers. Moreover, this model can be used to study how risk management is coordinated among these layers.

2. The CASSANDRA data pipeline concept should be very flexible to support different supply chain governance models, logistic network structures and increased dynamism of the supply chain. The global logistics network configuration section provides a good understanding of how various logistics network are structured, which parties are involved and what the responsibilities of different parties are. This assists us in identifying CASSANDRA’s requirements, risks and complexities associated with data sharing.

3. The ‘Hesketh’ pipeline model is based on the piggy-backing principle and takes advantage of importers’ and exporters’ common data of the ‘buy-ship-pay’ process. Using this model enables the traceability of goods and empowers Customs to implement a more effective risk assessment.

4. An important omission in current visibility is lack of information in the case of LCL shipments. Information from house Bills of Lading is required in the CASSANDRA pipeline for Customs to make better risk assessments.
3 Supply chain finance and liabilities

3.1 Overview

Optimisation of the physical flows in the supply chain has always received much attention by industry and research. With substantial developments in information technology this focus is now shifting towards information exchange and the topics in supply chain planning and control. But the information flows are still mostly linked to the physical process; information about containers, consignments, events that can cause disruptions and delays in the physical movement of goods around the globe. Much less is known about the financial flows that drive and support international supply chains. Historically, management of physical chains is executed with different systems and by entirely different company departments than the management of financial resources and transactions. The physical supply chains are only linked to finance by financial management information such as growth indicators, working capital and costs. Finance is usually a board room issue, whilst supply chain management is dealt with at lower levels in the company. Because the links are not clearly defined and effects of supply chain management on finance are not always traceable, the place where the ownership concerning financial supply chain information and processes resides is often difficult to identify.

Bringing financial flows into the discussions around supply chain optimisation can be considered as a logical next step and can bring supply chain automation and optimisation to a next level. The CASSANDRA pipeline concept fits perfectly with the needs of the supply chain partners and financial service providers (banks, insurance companies, etc) for an interoperable system for secure data sharing and visibility. To give the CASSANDRA compendium an extra dimension and to indicate possible areas of potential benefits outside the initial scope, some more details about financing, liabilities and insurance are covered in the next paragraphs. We will first discuss the international trade and transport laws and liabilities that create the basis for trust between a buyer and a seller and then take a look at different aspects of financing trade transactions, trade insurance and financial transactions in the supply chain.

3.2 (Inter)national trade and transport law & liabilities

In traditional trade transactions, goods and money need to be transferred while buyer and seller might not even know each other. A high level of trust is necessary for the buyer to trust he will receive the goods after making the payment, and for the seller to trust he will receive payment after the goods are shipped, or a safe system should create the right basis for this trust. In fact, this system has already existed for hundreds of years. Nowadays, the solution is provided by a structure of (inter)national laws and conventions, predefined trade terms (Incoterms) and Bills of Lading (B/L).

3.2.1 (Inter)national trade law and conventions for contracts of carriage

In international transactions there is first a contract of sale between buyer and seller. For the transport related with this order a multimodal carrier (or freight forwarder) is contracted. This party can cover the whole chain or part of the chain. A multimodal carrier usually does not perform all transport actions so subcontractors are used for the different transport legs. The multimodal carrier then acts as the consignor in these subcontracts, meaning that the original buyer and seller are no longer involved. So with one contract of sale, there could be even 5 transport contracts involved, divided over at least two
levels of contracts for carriage. The different contracts involved in a transport transaction are visualised in Figure 3-1.

![Figure 3-1 Contract types in a transport transaction](image)

The development of international transport practice has resulted in a large number of national laws and international conventions being applicable to the various stages in the transport chain. There are two types of international conventions applicable to modern supply chains:

1. legal conventions that are only related to transport and help solve liability issues;
2. international conventions that address both transport and trade issues and provide the basis for the Bill of Lading process.

Legal conventions are applicable to more regional transport by road, rail and barge. There are numerous regional versions of the COTIF-CIM (rail), CMNI (barge) and CMR (road) conventions. Because of the large number of regional versions, it can be difficult to determine the applicability of a convention for a certain leg when there are several border-crossings involved in that leg. So next to the number of legs involved in multimodal transport and the earlier defined different levels of contracts, there can be different transport conventions and national laws applicable for each leg. This adds to a complicated web of applicable law and conventions that determine (and restrict) the liability of the transport operator at different stages of contract execution.

International conventions are usually applicable to the main carriage leg of the chain, which is often either air or ocean transport. There is, for example, the Warsaw Convention and Montreal Convention for air carriage, and the Hague rules, Hague-Visby rules and Hamburg rules for sea carriage. The United Nations have accepted the new Rotterdam rules (“Convention of Contracts for the International Carrying of Goods Wholly or Partly by Sea”) in 2008. These rules have been designed to provide a basis for multimodal transport solutions, but they only apply when there is sea carriage involved. It is expected that the Rotterdam rules will create a uniform view on liability and to support the use of electronic documentation in sea transport. The Rotterdam rules will only come into force after ratification in at least 20 UN member states.
National regulations and international conventions are especially important when there is a liability issue. For example, when a container was tampered with on its journey, one of the most crucial aspects is the time and location of tampering. This not only points at the party that was in charge of the container at that time, but also the applicable law in that stage of transport. The network approach/system is used to apply liability rules to different stages of the transport system based on the mode of transport involved. Under this system, a carriage convention applies only to the period of time during which the carrier is deemed to be in charge of the goods in relation to the mode of transport covered by the convention. Because the multimodal carrier acts as the consignor in the subcontracts, applicable regulation in these subcontracts can also differ from the main contract of carriage between multimodal carrier and buyer/seller.

3.2.2 ICC trade terms: Incoterms

Apart from the arrangement of the liability of the transport operators, other issues also have to be settled in international trade. These issues are: when does ownership change hand, who arranges transport, and who is responsible for insurance of the cargo.

To facilitate the determination of trade terms in international trade transactions, in 1936 the industry (International Chamber of Commerce) published a first version of the Incoterms. Incoterms are international rules that are accepted by governments, legal authorities and practitioners worldwide for the interpretation of the most commonly used terms in international trade. Currently there are 11 Incoterms of which four are only applicable to sea and inland waterway transport.

The different Incoterms are coded with 3 letters and each specifies document, costs, risk and insurance responsibility for either buyer or seller for the different stages in the transport chain. Table 3-1 gives a short description of each of the Incoterms.

---

3 'Multimodal transport law', M.A.I.H. Hoeks

4 International Chamber of Commerce, [www.iccwbo.org](http://www.iccwbo.org)
### Table 3-1 Descriptions for Incoterms

<table>
<thead>
<tr>
<th>Code</th>
<th>Full name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXW</td>
<td>Ex works (named place of delivery)</td>
<td>Seller makes goods ready for collection at its premises. Buyer organises, pays and bears all responsibilities for transport. Maximum responsibility with buyer.</td>
</tr>
<tr>
<td>FCA</td>
<td>Free carrier (named place of delivery)</td>
<td>Seller clears goods for export and hands over the goods to the first carrier (named by buyer) at a specified location. Risk passes with hand over of the goods.</td>
</tr>
</tbody>
</table>
| FAS* | Free alongside ship (named port of shipment) | Seller clears goods for export and has all responsibilities until goods are alongside the ship.  
Not suitable for multimodal sea transport in containers (Incoterms 2010, ICC publication 715) |
| FOB* | Free on board (named port of shipment) | Seller clears goods for export and has all responsibilities until goods are loaded on the ship (named by the buyer).  
Not suitable for multimodal sea transport in containers (Incoterms 2010, ICC publication 715) |
| CFR* | Cost and freight (named port of destination) | Seller clears goods for export and arranges and pays for carriage to port of destination. Risk transfers to buyer when goods are loaded to the vessel. |
| CIF* | Cost, insurance and freight (named port of destination) | Exactly the same as CFR with the addition that seller procures and pays for insurance (minimum coverage is required). Risk transfer remains at vessel loading so insurance is for buyer’s risk. |
| CPT  | Carriage paid to (named place of destination) | Seller clears goods for export and arranges and pays for carriage to port of destination. Risk transfers to buyer when goods are handed over to first carrier. |
| CIP  | Carriage and insurance paid (named place of destination) | Exactly the same as CPT with the addition that seller procures and pays for insurance (minimum coverage is required). Risk transfer remains at handover to first carrier so insurance is for buyer’s risk. |
| DAT  | Delivered at terminal (named terminal at port or place of destination) | Seller has all responsibility up to point of vessel arrival at destination port. Risk transfers at point of vessel unloading. Buyer has responsibility for import clearance. |
| DAP  | Delivered at place (named place of destination) | Seller has all responsibility up to point of final delivery, except for costs of import clearance. Risks passes to buyer upon unloading (of the container) by the buyer. |
| DDP  | Delivered duty paid (named place of destination) | Seller has all responsibility up to point of final delivery, including import clearance, duties and taxes. Maximum responsibility with seller. |

* Only applicable for sea and inland waterways transportation
The latest version of the Incoterms came into effect 1\textsuperscript{st} January 2011\textsuperscript{5}. This newest version reduced the total number of Incoterms from 13 to 11. A difference with earlier versions is the combination of older terms DAF, DES, DEC, DDU into the new terms DAT and DAP (described in table 3.1). These new terms can be used irrespective of transport mode and therefore make earlier 4 terms superfluous. In these new terms all references to a ship’s rail are omitted with preference for delivery of the goods when they are on board of the vessel. This more closely reflects modern reality and avoids the unclear situation when the liability swings back and forth across an imaginary line. References to export and import formalities have been mentioned as ‘only where applicable’ reflecting the fact that Incoterms are more and more used in domestic trade (or trade within trade blocks such as the EU). An important change in Incoterms 2010 is that now electronic means of communication have the same effect as paper communication (as long as both parties agree). This facilitates the evolution of electronic procedures and data exchange. Due to growing importance of security measures, the new Incoterms also allocate obligations between buyer and seller to obtain security related clearances and chain-of-custody information. For the security related clearance, this is for example relevant when a seller, within the AEO requirements, needs to prove that the exported goods have reached their destination. A copy of the import document is useful here, and the Incoterms now state that the buyer is obliged to cooperate in providing a copy of this document to the seller.

\textbf{Figure 3-2 responsibilities for documents, costs, risks and insurance}

In Figure 3-2 the responsibilities for documents, costs, risks and insurance for the different Incoterms are mapped on the physical process. The locations where most shifts in responsibilities take place are

\textsuperscript{5} ICC WBO, www.iccwbo.org/Incoterms
the terminals of discharge and destination. Shifts in responsibilities are made either alongside the ship at export terminal, and on the vessel on export or import terminal. The moment of handover of the goods to the first carrier is also important from a risk perspective. This usually takes place at the seller’s premises or the location of consolidation.

### 3.2.3 Bill of Lading

A Bill of Lading (B/L) is a document that describes goods, consignor and consignee and the requirements for delivery. It is a document of title that gives ownership of the goods to the keeper of the document. A B/L is issued by the (ocean) carrier and exchanged with the seller of the goods upon handover of these goods. The document thus confirms that the carrier has received the goods and that delivery to the buyer is arranged for in a contract of carriage. The Bill of Lading is passed on to the seller’s bank and reaches the buyer via the letter of credit process described in more detail in paragraph 3.3.1. With the B/L document, the buyer can then officially claim ownership of the goods at arrival. Different types of Bills of Ladings exist:

1. **Straight B/L**: States that the goods are consigned to a specified entity or person and is not negotiable, it also gives the keeper no title to the goods. Also known as a non-negotiable B/L and not considered safe by the banking sector;

2. **Order B/L**: Express words are used to make the bill negotiable. This means that delivery is to be made to the further order of the consignee;

3. **Bearer B/L**: States that delivery shall be made to the keeper of the document;

4. **Surrender B/L**: Used with import documentary credit. Buyer’s bank will handover the documents and title of the goods to the buyer upon receiving payment from the seller’s bank, but the buyer will pay it’s bank on maturity of the credit term.

The FIATA FBL (FIATA Multimodal Transport Bill of Lading) is a Bill of Lading developed by FIATA (International Federation of Freight Forwarders’ Associations) for the multimodal carriage of goods. This enables having one Bill of Lading for several transport modes that together perform door-to-door service. The FBL is approved by the ICC and can be used in Letter of Credit transactions.

A clean Bill of Lading means that the cargo has been received and loaded on the vessel in apparent good order and condition. The opposite is a soiled Bill of Lading. A sea or air waybill is comparable with a straight Bill of Lading in that it is not a document of title. Waybills are used for consolidated cargo (where for example a containers contains several shipments), for intercompany trade or when the goods are likely to arrive before the formal documentary process is finished.

A Bill of Lading supports trade because the B/L is linked to the goods and changes legal ownership along the transport process when the document is passed on as part of the Letter of Credit process. When using a B/L, transport activities and milestones have an important role as drivers for financial settling and document handover. Information on these milestones and quality of the information contained in the Bill of Lading is crucial to the performance and efficiency of this process. Issues concerned with this process are discussed in the next paragraph.

---

6 D. Coker, “Letters of credit, bills of lading & International trade finance documentation issues important in litigation”, HG.org
3.3 International trade finance

When it comes to financing international trade transactions, banks step in to perform an intermediate role by offering various types of services. These services are in the field of financing and also in credit insurance, (export) factoring, forfeiting and (currency) hedging. All these services might be applicable to the parties involved in an international container supply chain. This paragraph will focus on the different options in financing and related risk assessment; some other services will be reviewed in paragraph 3.5.

3.3.1 Financing international trade transactions

Coker distinguishes four basic methods of (international) trade finance:

- Advance payment (buyer pays up front, so most secure for the seller);
- Direct payment (seller ships the goods and buyer pays directly to the seller, so most secure for buyer);
- Documentary collection (bank in the buyer’s country acts as a fiduciary on behalf of the seller in collecting payment for the goods. Seller sends documents to this bank which offers the documents to the buyer in a “documents against payment” transaction);
- Documentary collection (letter of credit transactions)

In international trade, letter of credit transactions are used in most cases. The basic purpose of a letter of credit is to comfort both the buyer and the seller by replacing buyer’s credit by a financial backing of the issuing bank. With a confirmed letter of credit, the seller is guaranteed to receive payment when the goods are shipped according to contract. Commercial letter of credits and Standby letter of credits are most commonly used. A Standby letter of credit is merely a guarantee to the beneficiary that a future payment will be made. Most important difference with a Commercial letter of credit is that a Standby letter of credit can only be drawn on if the buyer has failed to perform some required action. It is therefore a secondary or back up means of payment, which will not be used, when all runs according to contract.

The International Chamber of Commerce (ICC) has published guidelines for the issuance and use of letters of credit in the Uniform customs and practice for documentary credits (UCP) set of rules. The UCP600 is the current set of rules, formally applicable since 1st July 2007, that are used by banks and commercial parties. On 1st of April 2002 a supplemental eUCP came into force that gives necessary rules for the presentation of electronic documents in letter of credit transactions. The expectations for eUCP were high but the concept hasn’t been used much in practice.

The Commercial letter of credit is most common and in general referred to as the “letter of credit” (L/C). It is important to note that the L/C transaction is entirely separated from the sales contract between buyer and seller. The L/C transaction only deals with documents and not with the involved goods. The risks involved in a L/C transaction are therefore related to the required documents and the quality of their data set. The issuing bank can never be liable for the performance of the sales contract.

---

7 D. Coker, “Letters of credit, bills of lading & International trade finance documentation issues important in litigation”, HG.org
Figure 3-3 Basic flows for a commercial letter of credit transaction

Figure 3-3 shows the basic flows for a commercial letter of credit transaction. The process starts when the seller requests for a L/C for a certain sales contract. The buyer applies for a letter of credit at his own bank (Issuing bank). The letter of credit is sent to the seller’s bank(s) for confirmation and advice to the seller. The seller received the original copy of the L/C and then ships the goods to the buyer. A document set is prepared and once complete send to the advising or confirming bank. This bank checks the documents for compliance to the terms in the L/C transaction. When the document set is approved, payment is made to the seller and the documents are forwarded to the issuing bank. The issuing bank also examines the documents for compliance and when approved debits the buyer’s account and forwards payment to the advising/confirming bank. In the last step, the document set is send to the buyer.

The document set involved in a L/C transaction consist of different types of documents depending on the responsibilities of buyer and seller, and thus on Incoterm. The essential document for receiving payments is the L/C draft, also called a bill of exchange. A draft is a payment order by which the party creating it (the seller) orders another party (issuing bank) to pay money to a third party (the advising/confirming bank). The draft is usually accompanied by at least a commercial invoice, Bill of Lading, warranty of title and an indemnification letter. Other documents that can be added are a packing list, insurance certificate, certificate of origin, (agricultural) certifications, different transport documents such as warehouse receipt, etc.

Providing the right documentation and information in the document set of the L/C transaction causes different types of problems according to Coker⁸. The issues he names explicitly are inaccurate

⁸ D. Coker, “Letters of credit, bills of lading & International trade finance documentation issues important in litigation”, HG.org
description of goods, differences in invoice and draft amount, inconsistencies in insurance
documentation, differences in beneficiary name, port of discharge and destination and actual
destination. The risk for non-compliance of documentation increases with the number of external
documents that need to be delivered by the exporter. An external document is for example a proof of
insurance, which is created by the insurance company. Bergami researched the discrepancy rates in L/C
documents for Australian exporters and found discrepancies of 20% for bill of exchange, commercial
invoice and packing list. These are all documents that are usually produced in-house. Discrepancy rates
for external documents such as transport document, insurance document and certificate of origin are
between 13% and 18%. Bergami also states that according to a UK study, the UK lost 113 million GBP
because of non-compliant documents being presented under Letters of Credit. Bergami concludes that
CIF terms are to be resisted by exporting companies as this term demands the highest level of
documentation and data content, making it more risky for the exporter to comply with the bank’s
requirements, and thus jeopardising payment.

3.3.2 Credit risk assessment for international trade
Financial institutions are interested in risks that can harm their investments and financial position. To
assess risks they continuously monitor developments in financial markets, (international) politics and
operations. For financing of international trade between corporations, financial institutions are mainly
interested in corporate credit risk, which is the risk for payment default (or the borrower not making
payments as promised). This default risk is usually determined by investigating quantitative and
qualitative aspects of these corporations and their operations. This analysis supports classification of
these firms into categories according to their creditworthiness. Two major issues influence the process
of classification. First, there is the large number of factors that need to be examined (such as financial
characteristics, strategic variables, relation with the market, macroeconomic factors etc.) and the
decision on which are the most important factors to focus on. Second, there is the aggregation of these
factors in order to come to a balanced decision.

When banks are assessing credit risk for corporations, they focus on the firm as a whole and the large
set of operations that a firm performs in its market. From this, it could be concluded that banks have
limited interest in supply chain visibility for single transactions but that they might be interested in
aggregated visibility information. Banks might only be interested in a single transaction’s risk when it is a
transaction of exceptional value and/or with long payment terms (where forfeiting might be used).

3.4 Financial transactions in the transport chain
The trigger for a financial transaction in a logistics chain is when a certain operational milestone is
reached and activities contributing to the achievement of this milestone become billable. The classic
example of this is delivery of goods under FOB terms, where ownership changes after loading the cargo

---

Victoria University, Melbourne

on board of the ship. The loading action immediately triggers change of ownership, and therefore payment for the goods.

E-Invoicing means that a digital invoice is created and sent to the receiving party by email, EDI or XML. Sending an invoice by EDI or XML gives further possibilities for automation since the invoice can automatically be processed by the receiving party’s financial system. By removing the different time lags, the cash-to-cash cycle of the company that sends the invoice will be reduced, while also reducing labour costs and errors. These benefits can be further improved by the use of a reverse factoring mechanisms (thus limiting the number of days outstanding).

When invoices are paid directly and/or on time, this can provide benefits for the operational process as well. Some activities in the logistics chain are on hold and release is only possible when a payment is received. Automatic invoice generation and payment and capturing of payment data means that the operational process can restart immediately and without further delay. This can for example be beneficial in the commercial release of containers in port areas since this will speed up the process and reduce container dwell-times. Benefits in the operational process are usually for the customer paying the invoice, since this party requested the logistics service and benefits from shorter lead times.

To automate financial transactions in the logistics chain, it is essential to provide timely and accurate data on the milestones that trigger these processes. Historically, there is a gap between the departments of a company involved in supply chain execution and finance. This gap is also visible in the information technology architecture where separated systems are used for operations and finance. This means that information on milestones and invoices is not flowing freely within companies. Before data sharing between chain partners can lead to benefits in this area, internal data sharing needs to be facilitated as well.

Benefits for the operational process can be significant (because these benefits accrue over the value of the cargo) but not much research has been performed until now. An overview of how financial transactions are linked to the physical process would be a good first step to start estimating benefits from the automation of the physical and financial processes.

3.5 Trade insurance

Insurance is a form of risk management where institutions hedge against an uncertain loss. It is a concept of transferring risks from one party to another without eliminating or reducing the risk. Insurance companies thrive on pooling these risks and sharing costs over different insurance participants. Insurance premiums are determined by estimating the expected value of loss added with operating costs and a profit margin. Insurance services are available for a large number of risks. Some important insurable risks related to international trade are:

- Loss of or damage to goods in transit;
- Non-payment for goods or service;
- Political or economic instability in customer/supplier country;
- Customer creditworthiness;
Supply chain finance and liabilities

- Supplier issues (failure to supply according to contract);
- Currency fluctuations (currency hedging);
- Storage of goods in bonded warehouses; etc.

When drafting and offering insurance products, insurance companies are interested in possible risks and associated losses. This means that they are mainly interested in aggregated data and not in having visibility on individual transactions. However, when there is a claim, the insurance company is interested in the exact circumstances of the loss for this claim. This means that although the insurance company might not be interested in having this information available in real time, they might be interested in improved data quality on logistics chain milestones and events. No research results were found on the exact requirements for risk assessment in the logistics chains by insurance companies.

Complete visibility in the supply chain might however change the insurance product that is currently offered, because it makes it possible to adapt insurance for specific transport legs. Insurance for the leg in China might be substantially different from the insurance for the sea leg but this is only possible when good quality milestones are available in real time. This is however a new vision in insurance that is currently investigated in the Dutch Logistics Innovation contract for Supply Chain Finance between business and government\(^{11}\).

3.6 Future trends in supply chain finance and liabilities

The research topic commonly described as ‘supply chain finance’ is a trend in itself. Some research has been performed to define the area and importance of supply chain finance. Some research has also been done within certain disciplines of trade logistics, such as the research study of Hoeks\(^{12}\) on multimodal transport law. But there still are a lot of opportunities for further research on the supply chain from a multidisciplinary viewpoint.

In the last years there has been a trend in transport regulation that gives more importance to electronic documents. The Rotterdam Rules and newest version of the Incoterm\(s\) are an example of this trend. The growing use of e-invoicing and EDI (or XML) messaging in (international) trade indicates that companies are increasingly used to e-documents and electronic data transfer. Several (European) projects (e.g. e-Freight, Freightwise) have already focused on constructing a paper-free logistics chain by standardising electronic messages.

The use of and requirements for certain documents are related to the use of certain Incoterm\(s\). The number of Incoterm\(s\) has been reduced in the 2010 version, but no significant changes that are related to financial transactions and liabilities were made to the Incoterm\(s\).

The trend of growing intra-company business is affecting international transport and the need for Incoterm\(s\) and Letter of credit transactions. Intra-company business, now about 50% of international trade, means that supply chain transactions are executed between two entities of the same company.

\(^{11}\) http://www.rijksoverheid.nl/onderwerpen/ondernemersklimaat-en-innovatie/investeren-in-topsectoren

\(^{12}\) ‘Multimodal transport law’, M.A.I.H. Hoeks
Incoterms and Letters of Credit will not be necessary and document exchange is restricted to the transport operations.

With the new recognition of the importance of supply chain finance, more research should be undertaken to assess the links between the physical and financial flows in the supply chain, and especially triggers in the one for the progression in the other. It currently seems that this trend will not develop easily by itself.

3.7 Conclusions and implications for CASSANDRA

CASSANDRA addresses visibility needs in international supply chains. Visibility can improve financial transactions and trade logistics as well. This paragraph shortly summarizes the possibilities of a CASSANDRA solution in the areas of finance and liabilities related to the transport chain.

The legal framework for logistics is constructed by a large amount of regional, national and international law and conventions. A combination of regulations, conventions and Incoterms provides the basis to solve liability issues. To solve these issues adequately, information on the exact place and time of tampering is needed. Active tracking of the container can give details on the exact moment of loss, damage or tampering. This will result in better risk assessment and help determine applicable law in case of liability issues, thus reducing legal costs. Having good quality information on the physical and administrative process, and thus better visibility of the chain is in the CASSANDRA scope. The CASSANDRA concept can therefore be beneficial here.

Incoterms also determine document requirements (for exporters) and therefore set requirements for compliance in international financing transactions (with Letters of Credit). A Bill of Lading supports trade because the B/L is linked to the goods and changes legal ownership along the transport process when the document is passed on as part of the Letter of Credit process. When using a B/L and L/C process, transport activities and milestones have an important role as drivers for financial settling and document handover. Some of the documentation and information problems in L/C transactions are similar to operational and customs compliance issues with data quality. Guidelines for electronic document sharing already exist in the Incoterms and might be incorporated in an information pipeline concept. This will likely reduce administrative cost.

CASSANDRA looks at risk assessment by the different logistics partners in the chain and by the customs authority. Other parties in the chain that are equally interested in risks, risk mitigation and evaluation are credit facilitators (banks) and insurance providers. These parties look at the logistics chain from their own perspective and in such are interested in other types of risks and detect different consequences and impact of these risks. When the CASSANDRA concept provides better information on trade transactions and their logistics activities, this will help banks and insurance companies to assess risks and improve their products and processes. This again might have a positive impact on insurance and credit rates.

Improved supply chain visibility and data sharing leads to better information on milestones in the operational department. When companies are able to make this milestone data (automatically)
available to their financial departments, this can reduce cash-to-cash cycles for the invoicing company and improve lead times for the customer company.

CASSANDRA addresses visibility needs in international supply chains. From this chapter it can be concluded that visibility can help improve the processes and transactions in trade finance and solve liability conflicts. However, the different topics addressed in this chapter still need more detailed research before a CASSANDRA-like solution can be developed and implemented. The topic of international trade logistics and finance will therefore not be part of the CASSANDRA scope, however some of the benefits could be taken into account when achieved by the system that is currently in scope.
4 Governmental actors in supply chains

4.1 Overview

International trade takes place in a highly regulated context, where a variety of governmental actors are involved in policy making and implementation, establishing legal frameworks, and day-to-day governance, monitoring and control of international trade. In this chapter, we will introduce the key governmental actors in global supply chains. We will address national governmental actors (section 4.1), governmental actors at the EU level (section 4.2), and the role of international governmental actors, like the United Nations (UN) and World Customs Organization (WCO). This serves as a background to the further discussion of procedures, compliance management, and risk management in Chapter 6 and Chapter 6. Moreover, the UN and WCO are also involved in establishing several standards that will be discussed in Chapter 6.

4.2 National governmental actors

The exact form in which the governmental actors are organized is country-specific. It is important to note that even within the EU, there are as many variations as there are Member States as each of the 28 Member States makes their own decisions in terms of how they are organized. In general, Customs administer and enforce the law, regulations and procedures regarding duties and taxes, the international trade in goods, trade statistics and import and export prohibitions and restrictions. This includes duty relief schemes, excise duty, customs duty, VAT, tariff quotas, Common Agriculture Policy controls, commodity codes, import and export licensing, preferential duty rates, strategic exports, intellectual property rights – and safety and security along the international trade supply chain. In the EU, in accordance with the Modernized Customs Code (MCC), “Customs authorities shall be primarily responsible for the supervision of the Community's international trade, thereby contributing to fair and open trade, to the implementation of the external aspects of the internal market, of the common trade policy and of the other common Community policies having a bearing on trade, and to overall supply chain security. Customs authorities shall put in place measures aimed, in particular, at the following:

- Protecting the financial interests of the Community and its Member States;
- Protecting the Community from unfair and illegal trade while supporting legitimate business activity;
- Ensuring the security and safety of the Community and its residents, and the protection of the environment, where appropriate in close cooperation with other authorities;
- Maintaining a proper balance between customs controls and facilitation of legitimate trade.”

Tax administration can be integrated with Customs (which is the case in e.g. the UK and the Netherlands), but might be a separate entity involved in the fiscal aspects of trade. Typically, Customs cooperates, or acts on behalf, of inspection agencies, that govern for example trade in agricultural products, pharmaceutical drugs, hazardous goods, and so forth. Once the cargo has been cleared, the police take on the role of governing inland transport, and they cooperate closely with Customs and other agencies in case of (suspected) illegal activities, like for example human trafficking, smuggling of

---

illegal drugs, or terrorist activities. The Bureau of Statistics requires data for statistical purposes; such statistics provide input to both private and public decision-makers. Trade statistics, which focus on tracing the value and quantities of goods traded between countries (e.g. within the EU and between the EU and other countries) are an important aspect of statistics and are derived from data from Customs procedures.\textsuperscript{14}

Next to these actors directly involved in the day-to-day trade governance, policy making and implementation will also take place within a variety of ministries. The following table illustrates the governing departments and authorities that play a role in cross-border trade and the establishment of Single Window\textsuperscript{15} in The Netherlands (Van Stijn et al., 2011c).

**Table 4-1. Overview of involved Dutch authorities and their roles in cross-border trade (Van Stijn et al., 2011c, p. 74)**

<table>
<thead>
<tr>
<th>Governing department</th>
<th>Authority</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department of Finance (Financiën)</td>
<td>Tax Department - Dutch Customs</td>
<td>Supervises cross-border goods traffic based on tax regulations and, mainly on behalf of other ministries, based on rules with respect to health, safety, the economy and the environment. <a href="http://www.douane.nl">http://www.douane.nl</a></td>
</tr>
<tr>
<td>Department of Mobility and Transport (V&amp;W)</td>
<td>Directorate-General for Public Works and Water Management (RWS)</td>
<td>Manager of the main waterways in the Netherlands. It monitors compliance with traffic legislation and environmental requirements on these waterways. <a href="http://www.rijkswaterstaat.nl">http://www.rijkswaterstaat.nl</a></td>
</tr>
<tr>
<td></td>
<td>Transport and Water Management Inspection (IVW)</td>
<td>Conducts the safety and environmental supervision of seagoing and inland waterway vessels, crews and carriers, and supervises the transport of dangerous goods. <a href="http://www.ivw.nl">http://www.ivw.nl</a></td>
</tr>
<tr>
<td></td>
<td>Harbour masters</td>
<td>Responsible for the swift, safe, clean and secure handling of shipping. This involves the supervision of operational and environmental issues, high-risk activities and compliance with relevant transport legislation. <a href="http://www.portofamsterdam.nl">http://www.portofamsterdam.nl</a> and <a href="http://www.portofrotterdam.com">http://www.portofrotterdam.com</a></td>
</tr>
<tr>
<td>Department of Housing, Spatial Planning and the Environment (VROM)</td>
<td>Food and Consumer Product Safety Authority (VWA)</td>
<td>Supervises the import of food products, consumer products and animal feed. This authority inspects the kitchen hygiene on passenger ships. <a href="http://www.vwa.nl">http://www.vwa.nl</a></td>
</tr>
<tr>
<td></td>
<td>Inspectorate of VROM (VROM-I)</td>
<td>Monitors the rules with respect to dangerous goods, radioactive substances and waste (including shipping waste). Compliance with the EEC Regulation on the supervision and control of shipments of waste within, into and out of the EU (referred to as ‘EVOA’ in Dutch) is a part of this. <a href="http://www.vrominspectie.nl">http://www.vrominspectie.nl</a></td>
</tr>
<tr>
<td>Department of Agriculture (LNV)</td>
<td>Plant Protection Service (PD)</td>
<td>Supervises the import of plants and products of vegetable origin to prevent plant diseases. <a href="http://www.minh.vlaanderen.be">http://www.minh.vlaanderen.be</a></td>
</tr>
<tr>
<td>Department of Inland Water Police Division of</td>
<td>Responsible for supervision and enforcement on the main transport</td>
<td></td>
</tr>
</tbody>
</table>


\textsuperscript{15} A Single Window is defined as “a facility that allows parties involved in trade and transport to lodge standardized information and documents with a single entry point to fulfil all import, export, and transit-related regulatory requirements” ([http://www.unece.org/cefact/forum_grps/itp/welcome.htm](http://www.unece.org/cefact/forum_grps/itp/welcome.htm)) (see section 7.5.1).
### Governmental actors in supply chains

<table>
<thead>
<tr>
<th>Affairs (BZK)</th>
<th>the National Police Services Agency (KLDP/DWP)</th>
<th>corridors, the main waterways, extended water surfaces, the territorial waters, the Exclusive Economic Zone up to the low waterline and the seaports with the exception of the Rotterdam port area. <a href="http://www.politie.nl/klpd">http://www.politie.nl/klpd</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>National Coordinator for Terrorism (NCTb)</td>
<td>Monitoring security in chains including the individual participants in those chains.</td>
<td></td>
</tr>
<tr>
<td>Department of Legal Affairs (Justitie)</td>
<td>Royal Marechaussee (KMar)</td>
<td>Charged with border control in the ports with the exception of the Rotterdam port area. <a href="http://www.dutch-immigration.nl">http://www.dutch-immigration.nl</a></td>
</tr>
<tr>
<td>Seaport Police</td>
<td>Charged with duties concerning border control, port security and crime, nautical issues, the environment and traffic. Responsible for the Port Expertise Centre (Haven expertisecentrum) for information exchange between services. <a href="http://www.politie-rijnmond.nl">http://www.politie-rijnmond.nl</a> and <a href="http://www.dutch-immigration.nl">http://www.dutch-immigration.nl</a></td>
<td></td>
</tr>
<tr>
<td>Department of Social Affairs (SZW)</td>
<td>Labour inspectorate (AI)</td>
<td>Monitors health and safety at work on the quayside in the port areas and aims to prevent labour market fraud. Inspection of working conditions on seagoing vessels is assigned to the Transport and Water Management Inspectorate (IVW). For inland shipping the Seaport Police (ZHP) and the National Police Services Agency (KLPD) are designated as co-supervisors. <a href="http://www.arbeidsinspectie.nl">http://www.arbeidsinspectie.nl</a></td>
</tr>
<tr>
<td>- (private organization with a formal public role)</td>
<td>Alert Supervision (KRVE)</td>
<td>Safety regulations</td>
</tr>
<tr>
<td>- (private organization with a formal public role)</td>
<td>Schiphol Airport (NV Luchthaven Schiphol)</td>
<td>Responsible for spatial planning, (food and water) safety and security of the airport</td>
</tr>
</tbody>
</table>

As mentioned, other countries will be organized differently than The Netherlands. This also goes for the legislations and procedures: the MCC is the strongest legislation of the EU, but there are variations in how the procedures take place. For other areas, there is even less harmonization of legislations and procedures. There, the EU plays a key role in setting policies and strategies, but there are not always formal mechanisms in place to ensure (harmonized) implementation in all Member States.

### 4.3 Key Directorates General and other governmental actors in the EU

In this section, we take a higher-level look at the EU. Table 4-2 provides an overview of key Directorates General and other offices and how they also relate to the policy areas relevant for trade in international supply chains. These policy areas also involve legislative frameworks and deal with compliance management from a governmental perspective, but also broader, they are related to strategic developments in the EU as well.
Table 4-2 Overview of key Directorates General and offices of the EC

<table>
<thead>
<tr>
<th>Directorate General (DG)/Office</th>
<th>Policy areas</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tax and Customs Union</td>
<td>Tax and customs, Modernized Customs Code, trade facilitation and regulation</td>
<td><a href="http://ec.europa.eu/taxation_customs/index_en.htm">http://ec.europa.eu/taxation_customs/index_en.htm</a></td>
</tr>
<tr>
<td>Maritime Affairs and Fisheries</td>
<td>Fisheries, maritime transport and border control</td>
<td><a href="http://ec.europa.eu/dgs/maritimeaffairs_fisheries/index_en.htm">http://ec.europa.eu/dgs/maritimeaffairs_fisheries/index_en.htm</a></td>
</tr>
<tr>
<td>Mobility and transport</td>
<td>Infrastructure, transport safety, sustainable transport</td>
<td><a href="http://ec.europa.eu/dgs/transport/index_en.htm">http://ec.europa.eu/dgs/transport/index_en.htm</a></td>
</tr>
<tr>
<td>Agriculture and rural development</td>
<td>Single payment scheme, cross-compliance, meat</td>
<td><a href="http://ec.europa.eu/dgs/agriculture/index_en.htm">http://ec.europa.eu/dgs/agriculture/index_en.htm</a></td>
</tr>
<tr>
<td>Health and Consumer Production</td>
<td>Agriculture, fisheries, and food as well as environment, consumers and health</td>
<td><a href="http://ec.europa.eu/dgs/health_consumer/index_en.htm">http://ec.europa.eu/dgs/health_consumer/index_en.htm</a></td>
</tr>
<tr>
<td>Trade</td>
<td>External relations and foreign affairs</td>
<td><a href="http://ec.europa.eu/trade/index_en.htm">http://ec.europa.eu/trade/index_en.htm</a></td>
</tr>
<tr>
<td>Justice</td>
<td>Illegal activities, drug control</td>
<td><a href="http://ec.europa.eu/justice/index_en.htm">http://ec.europa.eu/justice/index_en.htm</a></td>
</tr>
<tr>
<td>Informatics</td>
<td>Interoperability, IT strategy, pan-European solutions</td>
<td><a href="http://ec.europa.eu/dgs/informatics/index_en.htm">http://ec.europa.eu/dgs/informatics/index_en.htm</a></td>
</tr>
</tbody>
</table>

It is important to consider that typically, each of these DGs has national counterparts, i.e. ministries or departments, inspection agencies, police, and so forth, in both the EU Member States and in non-EU Member States, and that the regulations that they refer to may have been adapted to fit the national legal frameworks and jurisprudence.

4.4 Role of international governmental organizations

Public International Law provides an international legal framework that spans different places of business, countries and jurisdictions. International law is not statute law but a series of conventions,

---

16 A complete overview can be found at [http://ec.europa.eu/about/ds_en.htm](http://ec.europa.eu/about/ds_en.htm).
agreements and rules adopted by nations through consensus and overseen by bodies such as the United Nations. International law is supported by a country becoming a signatory to a convention then adopting it through translation into national law. In the main, cargo related jurisprudence and national and international law, such as UN transport conventions, relate to the relationship between the parties in terms of contracts of sale, contracts of carriage and liability in the event of loss or damage. They pay particular attention to how the initial information relating to the goods is captured and how the description of the goods influences liability. This section further elaborates on the work of the United Nations (section 4.4.1), World Trade Organization (section 4.4.2), and World Customs Organization (section 4.4.3).

4.4.1 United Nations

A variety of Councils and Commissions of the United Nations (UN) conduct work in the area of international trade. In this sub-section, we first highlight the work of the United Nations Economic Council for Europe (UNECE), and then we discuss the UN Convention on Contracts for the International Sale of Goods as well as international transport conventions – related to the Bill of Lading and manifest – in more detail. A last UN body that we will briefly mention here is the World Health Organization.

UNECE was set up in 1946 and its major purpose is to promote economic integration in the European region. European countries (EU, non-EU), together with countries from other regions (like north-America and Africa) collaborate on specific sectorial and economic issues. The key Programmes of UNECE are: economic cooperation and integration\(^{17}\), environmental policy\(^{18}\), housing and land management\(^{19}\), statistics\(^{20}\), sustainable energy\(^{21}\), technical cooperation\(^{22}\), forestry and timber\(^{23}\), trade\(^{24}\), and transport\(^{25}\). Commissioned by UNECE, UN/CEFACT – the UN Centre for Trade Facilitation and eBusiness – has conducted substantive work in the areas of guidelines and recommendations as well as standardization\(^{26}\). Their work encompasses the development of UN/EDIFACT (the United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport)\(^{27}\), the Core Component Library (CCL)\(^{28}\), the UN/CEFACT Modelling Methodology (UMM)\(^{29}\) and trade facilitation recommendations\(^{30}\) on for example Single Window (SW) implementation (Recommendation 33)\(^{31}\), data simplification and harmonization for international trade (Recommendation 34)\(^{32}\), and the establishment

---

\(^{17}\) [http://live.unece.org/ceci/Welcome.html](http://live.unece.org/ceci/Welcome.html)


\(^{19}\) [http://live.unece.org/hlm/welcome.html](http://live.unece.org/hlm/welcome.html)

\(^{20}\) [http://live.unece.org/stats/stats_h.html](http://live.unece.org/stats/stats_h.html)

\(^{21}\) [http://live.unece.org/energywelcome/energy-home.html](http://live.unece.org/energywelcome/energy-home.html)

\(^{22}\) [http://live.unece.org/operact/welcome.html](http://live.unece.org/operact/welcome.html)

\(^{23}\) [http://live.unece.org/forests/welcome.html](http://live.unece.org/forests/welcome.html)

\(^{24}\) [http://live.unece.org/trade/welcome.html](http://live.unece.org/trade/welcome.html)


\(^{27}\) [http://www.unece.org/cefact/edifact/welcome.html](http://www.unece.org/cefact/edifact/welcome.html)

\(^{28}\) [http://www.unece.org/cefact/codesfortrade/unccl/ccl_index.html](http://www.unece.org/cefact/codesfortrade/unccl/ccl_index.html)

\(^{29}\) [http://www.unece.org/cefact/umm/umm_index.html](http://www.unece.org/cefact/umm/umm_index.html)

\(^{30}\) See [http://www.unece.org/cefact/recommendations/rec_index.html](http://www.unece.org/cefact/recommendations/rec_index.html) for a full list of trade facilitation recommendations.

\(^{31}\) [http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec33/rec33_trd352e.pdf](http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec33/rec33_trd352e.pdf)

\(^{32}\) [http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec34/ECE_TRADE_400_DataSimplificationand_Rec34E.pdf](http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec34/ECE_TRADE_400_DataSimplificationand_Rec34E.pdf)
of a legal framework enabling SW (Recommendation 35)\(^{33}\). UN/CEFACT has recently undergone a major restructuring and has not made the new organizational structure available on their website yet.

Another area of work of the UN is the **United Nations Convention on Contracts for the International Sale of Goods**\(^{34}\) (CISG), which is a treaty offering a uniform international sales law. From the beginning of a commercial relationship differences such as language and the means of describing the goods can lead to the risk of both parties having a different understanding of what is required, despite both thinking they agree. The contract of sale is the backbone of international trade in all countries, irrespective of their legal tradition or level of economic development. The purpose of the CISG is to provide a modern, uniform and fair regime for contracts for the international sale of goods. The CISG governs contracts between private parties whose places of business are in different Contracting States. It contributes significantly to introducing certainty in commercial exchanges and decreasing transaction costs. The first part of the contract specifies the buyer and seller, a description of the goods including a WCO Harmonized System Code, the contract price, Incoterms 2010, the carrier, time of delivery, payment conditions, documents and licenses required, cancellation dates, liability for delay and limitations of liability, applicable law and resolution of disputes. The second part of the CISG deals with the formation of the contract, which is concluded by the exchange of offer and acceptance and the third part deals with the obligations of the parties to the contract. Obligations of the sellers include delivering goods in conformity with the quantity and quality stipulated in the contract, as well as related documents, and transferring the property in the goods. Obligations of the buyer include payment of the price and taking delivery of the goods. In addition, this part provides common rules regarding remedies for breach of the contract. The aggrieved party may require performance, claim damages or avoid the contract in case of fundamental breach. Additional rules regulate passing of risk, anticipatory breach of contract, damages, and exemption from performance of the contract. Finally, while the CISG allows for freedom of form of the contract including electronically, States may lodge a declaration requiring the written form.

**International transport conventions** such as Warsaw\(^{35}\), the Hague Protocol\(^{36}\), and Montreal\(^{37}\) for air, Hague-Visby\(^{38}\), Hamburg\(^{39}\) and Rotterdam Rules\(^{40}\) for sea, the Carriage of Goods by Road (CMR)\(^{41}\), the Carriage of Goods by Rail (COTIF)\(^{42}\), and on International Multimodal Transport of Goods\(^{43}\), provide further international legal frameworks for the carriage of goods. In essence, the conventions are used to establish 1) liabilities of the carriers and those who hand the goods to the carrier, 2) documentation, 3) type of liabilities, 4) applicable laws and place of arbitrage. The conventions were designed primarily to


provide assurance to the shipper (seller or consignor) that the means of carriage for his goods is safe and that the carrier will hand over the goods to the person nominated by the consignor at the point of destination. In reality the conventions concentrate on who is liable in the event of damage or loss. The concept of a Bill of Lading as a receipt between the shipper (the person sending the goods) and the carrier is over 200 years old. Historically British companies were allowed to ‘craft’ Bills of Lading in order to protect themselves if goods were damaged at sea. That principle of protecting the liability of the carrier has remained to this day through different international conventions relating to Bills of Lading, such as The Hague Rules in 1924, the Hague-Visby Rules of 1963 and 1979 and the Hamburg Rules in 1992. The purpose of a Bill of Lading was that the carrier could see the goods he was being asked to carry and could agree their quantity, condition, marks and numbers with the shipper. Bills of Lading are still put together to form a record of all the goods the ship is carrying – the manifest. The manifest is a list of all the cargo carried on an airplane, vessel, train, or road vehicle and is made up from the Bills of Lading or other bills issued by the carrier to the shipper acknowledging receipt and condition. Manifest level information is currently significant for Customs purposes. Customs use this manifest as notification that goods have arrived in a customs territory prior to the customs declaration being made. This all works when the goods being carried can be seen. But the introduction of the container meant that the carrier was, and still is, unable to confirm the description of the goods. As a result, all the carrier is able to do is to issue a Bill of Lading describing one 20 foot container “said to contain” or packed “to shipper’s load and count”. A further complication is that while containers are an efficient way of moving cargo, not all manufacturers or exporters, or consignors or shippers have enough goods to completely fill a container. In this scenario a lot of different goods from different people come together at a ‘consolidators’ place of loading and are loaded into a container as a mixed or ‘groupage’ load. The contract of carriage is between the ‘manufacturer’ and the ‘consolidator’ or ‘agent’ who takes the groupage container to the port for loading. The Bill of Lading becomes a contract between the carrier and the agent, with title for the goods transferring from the agent in the exporting country to the agent at the port of importation. So not only does the carrier not know what he is carrying, he doesn’t know who owns the goods, who is sending them or who is ultimately buying them. And if he doesn’t know then he can’t tell Customs. In the most recent Rotterdam Rules of 2009, the Bill of Lading is replaced with a ‘transport document’ and/or ‘electronic transport record’ but the concept is still the same. These new rules require the shipper to provide to the carrier information and documents about the goods when the carrier is required to comply with the law or requirements of public authorities (Customs and Border Agencies). However, the carrier cannot assume responsibility for the accuracy of the data furnished by the shipper and the new rules allow the carrier to qualify the electronic documents with ‘apparent order and condition’ instead of ‘said to contain’ when the goods are delivered in a closed container. The consignor is still the only one with ‘actual knowledge of the contents’. We will further discuss this in Chapter 7.

A last authority within the United Nations is the World Health Organization (WHO)\(^44\). They are for example important to consider when considering health risks and issues in the international supply chain and when the supply chain deals with pharmaceutical products.

\(^44\) [http://www.who.int/en/](http://www.who.int/en/)
4.4.2 World Trade Organization

The World Trade Organization (WTO)\(^{45}\) can be viewed in particular as a “negotiation forum”, where governments negotiate the legal contracts for international trade; the WTO also oversees the appropriate implementation and monitors compliance; WTO is involved in dispute settlement; and the final role of the WTO is building trade capacity.\(^{46}\) This started out with the General Agreement on Trade and Tariffs (GATT) negotiations. Figure 4-1 provides the organizational chart of the WTO, which visualizes the policy areas as well.

![Organizational chart of the WTO](http://wto.org/english/thewto_e/whatis_e/tif_e/organigram_e.pdf)

Figure 4-1 Organizational chart of the WTO (Source: [http://wto.org/english/thewto_e/whatis_e/tif_e/organigram_e.pdf](http://wto.org/english/thewto_e/whatis_e/tif_e/organigram_e.pdf))

---


\(^{46}\) [http://www.wto.org/english/thewto_e/whatis_e/what_we_do_e.htm](http://www.wto.org/english/thewto_e/whatis_e/what_we_do_e.htm)
4.4.3 World Customs Organization

A key international player is the World Customs Organization (WCO), an inter-governmental organization that focuses solely on customs matters, with about 175 members. An overview of all conventions and agreements by the WCO can be found at the WCO website\footnote{http://www.wcoomd.org/home_about_us_conventionslist.htm}. As stated on its website, WCO “is particularly noted for its work in areas covering the development of global standards, the simplification and harmonization of Customs procedures, trade supply chain security, the facilitation of international trade\footnote{http://www.wcoomd.org/home_pfoverviewboxes_pfoverview.htm}, the enhancement of Customs enforcement and compliance activities\footnote{http://www.wcoomd.org/home_epoverviewboxes_epoverview.htm}, anti-counterfeiting and piracy initiatives, public-private partnerships, integrity promotion, and sustainable global Customs capacity building programmes\footnote{http://www.wcoomd.org/home_cboverviewboxes_cbstrategy.htm}. The WCO also maintains the international Harmonized System goods nomenclature\footnote{http://www.wcoomd.org/home_hsoverviewboxes_hsharmonizedsystem.htm}, and administers the technical aspects of the WTO Agreements on Customs Valuation and Rules of Origin\footnote{http://www.wcoomd.org/learning_valuelearningoncustomsvaluation_orinonpreferentialoverviewchallenges.htm}.\footnote{http://www.wcoomd.org/home_about_us.htm}

A highly relevant area of work for CASSANDRA is the WCO SAFE Framework of standards, which focuses on Customs’ safety and security issues, and also addresses requirements for the Authorized Economic Operator. A relatively new area of interest at WCO is coordinated border management. These topics will be further discussed in Chapters 6 and 7.

4.5 Future trends

There are a couple of trends that we have identified with respect to governmental actors in the international supply chain. Firstly, there appears to be a trend to reduce the number of inspection agencies\footnote{Keynote speech “An evolutionary perspective on government change in the Netherlands” by Mr. Jaap Uijlenbroek, Director General, Dutch Ministry of Interior and Kingdom Relations, EGOV 2011, Delft.}, and in a broader context, given the current economic crisis, many governments have to cut back on budgets and are undergoing significant reorganizations to become more cost-efficient. A second consideration is the trend towards further harmonization: not only has the issue of the differences between legislative requirements and procedures across national agencies to be addressed, this also scales up to the EU level and even an international, global level. Cooperation and coordination are essential prerequisites in this context. We will return to this topic later.

4.6 Conclusions and implications for CASSANDRA

In this chapter, we have introduced a wide variety of governmental actors that are involved in the international supply chain, not only at the national level but also at the EU and international levels. These are essential stakeholders to be involved in some stage of the development, design and ultimately adoption of the data pipeline and risk-based approach. In addition, we have signalled that even within the EU there can be important differences regarding legislation and the ways in which the trade is governed on a daily basis. This has to be taken into account in particular in the Living Labs.
5 Risk management in supply chains – private sector perspectives

5.1 Overview

Supply Chain Risk Management (SCRM) is a particular area of risk management that aims at mitigating supply chain disruptions associated with different types of risks. Indeed, Supply Chain Risk Management can be defined as “the management of supply chain risk through coordination or collaboration among the supply chain partners so as to ensure profitability and continuity” (Tang, 2006).

The above definition shows the main trait of this discipline, i.e. it is focused on an inter-organizational framework, in contrast to traditional risk management that aims at coping with risks at the company level (Thun and Hoenig, 2011). This inter-organizational perspective is one of the complexities of SCRM, as it raises the issue of how to align incentives of different players in the supply chain. In fact, SCRM faces the challenge of tackling growing global complexity of modern supply chains.

Although awareness has increased within the industry, it is in academia where SCRM research has grown in the last years (Jüttner, 2005). Moreover, a literature review has shown that research in this field is much more qualitative than quantitative.

5.2 Models for risk management

Several qualitative and quantitative supply chain risk management models have been developed in the last decade. For the sake of this analysis we will review qualitative models, albeit recognizing the existence of quantitative SCRM models (e.g. optimization models (Tomlin, 2006), decision support systems, (Kirkwood et al, 2005)). In the rest of this section, we elaborate more on Waters (2007) and Kleindorfer and Saad (2005) frameworks, which are better structured, and more comprehensive.

Illustrated in Figure 5-1, Waters (2007) suggests a structured approach of three steps: (1) identifying risk, (2) analysing risks, and (3) responding to risks. These steps are framed by two core concepts: SCRM prerequisites and monitoring and control.

![Figure 5-1 Framework for supply chain risk management (source: Waters, 2007)](image-url)
• **SCRM Prerequisites**

SCRM prerequisites are factors that enhance the successful implementation of a SCRM philosophy. If these are not present, SCRM is severely hampered (Pfohl et al., 2010). In order to be able to define a supply chain-wide risk strategy, organizations have to achieve cooperation and mutual trust. This requires the sharing of ideas, methods, and information (Pfohl et al., 2010; Waters, 2007; Christopher and Peck, 2004; Lee and Whang, 2005).

• **Identifying Risks**

Risk identification is the first step in SCRM. In order to identify risks the entire supply chain should be mapped such that structural factors are identified and insights on processes, relationships, ownership and responsibilities are gained. Second, risk areas have to be defined in order to identify key risks. This should be done in a top-down and a bottom-up approach respectively (Kajüter, 2003). A complete list of key risks can only be obtained if the organizations consider direct risks to their operations, risks to other entities, and risks caused by the linkage between organizations in the supply chain (Jüttner, 2005). Third and in accordance with one of the prerequisites to SCRM, risks have to be identified by each firm individually and then reported to all members of the supply chain (Kajüter, 2003). At this stage, it is important to take into consideration that risks relevant to an individual-firm basis might not be relevant for the entire chain or vice versa (Kajüter 2003). Finally, Waters (2007) proposes specific tools for the identification of risks. He groups them into three different approaches: analyzing past events, collecting opinions, and analyzing operations. Examples of tools are cause-and effect diagrams, interviews, and process charts, respectively.

The identified risk sources can have an effect on information, financial and material flows of supply chains. Furthermore, the identification of risk sources has to be conducted on an operational, tactical, and strategic level in order to elevate a risk management system from a statutory reporting to a planning function. The discussion of supply chain sources can be summarized in Figure 5-2.
Risk management in supply chains – private sector perspectives

Figure 5-2 Levels of risk identification

A key to identifying this kind of risk is the understanding of the contracted responsibility/liability of an entity as well as the dependencies between entities. The concept of “piggy-backing” in system-based auditing is actually built on the trust and self-monitoring according to the (contract of) responsibilities. The logic behind “piggy-backing” is the following: if an entity uses the same information for identifying and analysing its own risk (i.e. to monitor its ability to achieve the goal in a specific instance of activity), this information is reliable for others to do their risk analysis. To further generalize this idea, if an entity has motivation to provide certain information in order to achieve some goal and to benefit from or to be responsible for the result, then this piece of information is trustworthy and reliable.

• Analysing Risks

Most of the papers covering the issue are conceptual or deal with SCRM as a whole. Tools for the analysis of risks are seldom provided (Sodhi et al., 2011). A risk analysis can follow one of the two approaches, a purely qualitative or a quantitative one (Waters, 2007). The qualitative approach solely focuses on describing the risk and its general features. It lays a good basis for discussion but it is limited, as it does not provide any numerical values. A qualitative risk analysis may raise a general sense of alarm in a single firm or in the entire supply chain, but responses will not necessarily be directed to the most relevant risks (Kleindorfer and Saad, 2005). Under the quantitative approach to risk analysis, in contrast, the relevance of each risk is numerically determined.

The results of the risk analysis from a focal organization’s point of view can be illustrated on a risk map (Figure 5-3), which is also referred to as a vulnerability matrix (Stemmler, 2010; Waters, 2007;
Such a risk map facilitates the classification of risks into groups of priority.

Figure 5-3 Company-specific risk map (source: Kajüter, 2003)

The results of the company-specific analyses are reported to all members of the supply chain. Again, risk consolidation has to be performed since risks reported by different members of the supply chain might be interrelated. The result at this stage of the risk analysis is a matrix (Figure 5-3) in which the risks analysed on a firm-specific level are classified according to their company-specific risk category and their impact on the supply chain (Stemmler, 2010; Kajüter, 2003). The company-specific risk map and the supply chain risk matrix provide the basis for risk controlling, i.e. how to respond to risks (Stemmler, 2010).
Responding to risks

After identifying and analysing risks, decision makers have a prioritized list of risks. At this point, appropriate responses have to be selected and implemented (Mullai, 2009; Waters, 2007). Possible responses are as follows:

Risk avoidance: Risks can be so severe that an organization or supply chain decides not to engage in the particular activities that trigger the risk.

Risk reduction: Risk reduction is a common and preferable response to risks (Stemmler, 2010; Kajüter, 2003). It is achieved either by decreasing the probability of a risk occurring or by reducing or limiting its potential damage. In integrated supply chains, higher degrees of standardization as well as intensified collaboration and information exchange reduce risks. These actions are more effective and usually less expensive than those that could be undertaken on a company-specific level.

Risk transfer: Risk transfer moves some of the risk to an external entity. It is achieved by insurance hedging, or other contractual agreements (Waters, 2007; Kajüter, 2003). Risk transfer is comparatively easy to achieve in ERM, but is a difficult approach in SCRM (Stemmler, 2010). In SCRM, it is essential to transfer risks to entities outside the supply chain in order to reduce the overall risk exposure.

Risk acceptance: If the costs of handling risks exceed their potential damage or if there are no other appropriate responses to risks, companies and supply chains have to accept them.

Monitoring and control

As one of the two core concepts of SCRM, monitoring and control transforms the discussed framework from a one-time procedure into a continuing cycle (Waters, 2007). It is necessary for two reasons. First, the effectiveness of risk responses has to be controlled and if necessary adjusted
(Kajüter, 2003). Second, companies and supply chains operate in a dynamic environment. Circumstances and risk exposure are constantly changing. New risks have to be identified and assessed in order to implement appropriate responses. Alternatively, established risk responses might become redundant as certain risks vanish (Waters, 2007).

Likewise, Kleindorfer and Saad (2005) propose a general framework for risk management, the SAM framework, based on four premises: (1) identifying the nature of risk, (2) assessing risk, (3) adapting approaches to the decision environment, (4) integration with supply chain partners.

These four premises result in three main tasks to be performed in order to deploy the SAM Framework:

- Specifying sources of risk and vulnerabilities

Risks may arise from operational, natural or terror-related sources. Once the potential sources of risk are identified, the question managers should answer is how to avoid or mitigate them.

- Risk Assessment

Risk assessment tools comprise, among others, probabilistic risk assessment using fault and event trees, vulnerability assessment using emerging team based approaches for purposeful agents, decision analysis, worst case scenarios and contingent response scenarios.

- Risk Mitigation

Chopra and Sodhi (2004) propose specific mitigation strategies (Figure 5-5) for coping with supply chain risks such as delays, disruptions, forecasts inaccuracies, procurement failures, inventory problems and capacity issues.
Figure 5-5 Assessing the impact of various mitigation strategies (Chopra and Sodhi, 2004)

Nevertheless, they suggest that these strategies be adapted to the specificities of each supply chain. Indeed, managers should understand and prioritize their supply chain risks prior to selecting a specific tailored mitigation strategy.

“What if” scenarios can be used for stress testing the supply chain, hence better understanding the supply chain risks. Chopra argues that stress testing should not be used to assess the likelihood of the events to happen, but to prepare the supply chain for those events and thus lower risk.

In some cases the likelihood of some events (i.e. large-impact, rare events) may be difficult to assess, as there exists little or no previous data and they may be influenced by human behaviours and not only by nature.

Once the specific risks of a given supply chain are understood, managers can implement the following tailored mitigation strategies:
## Table 5-1 Supply chain risks (adapted from Chopra and Sodhi (2004))

<table>
<thead>
<tr>
<th>Mitigation Approach</th>
<th>Tailored Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase Capacity</td>
<td>Focus on low-cost, decentralized capacity for predictable demand</td>
</tr>
<tr>
<td></td>
<td>Build centralized capacity for unpredictable demand</td>
</tr>
<tr>
<td>Acquire Redundant Suppliers</td>
<td>Favour more redundant supply for high-volume products, less redundancy for low-volume products</td>
</tr>
<tr>
<td></td>
<td>Centralize redundancy for low-volume products in a few flexible suppliers</td>
</tr>
<tr>
<td>Increase Responsiveness</td>
<td>Favour cost over responsiveness for commodity products</td>
</tr>
<tr>
<td></td>
<td>Favour responsiveness over cost for short life-cycle products</td>
</tr>
<tr>
<td>Increase Inventory</td>
<td>Decentralize inventory of predictable, lower-value products</td>
</tr>
<tr>
<td></td>
<td>Centralize inventory of less predictable, higher-value products</td>
</tr>
<tr>
<td>Increase Flexibility</td>
<td>Favour cost over flexibility for predictable, high-volume products</td>
</tr>
<tr>
<td></td>
<td>Favour flexibility for low-volume unpredictable products</td>
</tr>
<tr>
<td></td>
<td>Centralize flexibility in a few locations if it is expensive</td>
</tr>
<tr>
<td>Pool or Aggregate Demand</td>
<td>Increase aggregation as unpredictability grows</td>
</tr>
<tr>
<td>Increase Capability</td>
<td>Prefer capability over cost for high-value, high-risk products</td>
</tr>
<tr>
<td></td>
<td>Favour cost over capability for low-value commodity products</td>
</tr>
<tr>
<td></td>
<td>Centralize high capability in flexible source if possible</td>
</tr>
</tbody>
</table>

The tailored strategies identified above can be summarized in the following rules of thumb:

![Figure 5-6 Rules of Thumb for Tailored Risk Management (Chopra and Sodhi, 2004)](image)
5.3 Typology of risks

Supply chain risks can be classified according to different criteria:

Kleindorfer and Saad (2005) classify them according to the source from which they arise, i.e. operational contingencies, natural hazards, and terrorism and political instability (Kleindorfer and Saad, 2005).

Likewise, Christopher (2005) states that risks may be external to the supply chain (e.g. natural disasters, terrorism), or internal risks that can be influenced by management decisions.

Tang and Musa (2011) propose a classification for supply chain risks according to the supply chain flows that they may jeopardize: material, financial or information flows.

1. Materials can be subject to risks at different stages throughout the supply chain: from upstream activities (sourcing) to downstream (demand). Sourcing risks may be related to single sourcing, sourcing flexibility, monitoring of product quality, supply capacity, supplier selection and outsourcing. Demand risks include demand volatility and seasonality, as well as balancing unmet demand and excess inventory.

2. Financial flow risks are driven by, among others, exchange rates and financial strength of supply chain partners.

3. Finally, information accuracy and information systems disruption can imperil information flows.

Adapting Svensson’s (2000, 2002) conceptualization of disturbances in supply chains, the sources of risk can also be classified as atomistic or holistic. Atomistic sources of risk signify that a selected and limited part of the supply chain is required in order to assess risk. The atomistic approach is suitable for low-value, non-complex, and generally available components and materials. Holistic sources of risk signify that an overall analysis of the supply chain is required in order to assess risk. Similarly, risks in the supply chain can be classified as quantitative or qualitative. Quantitative risks include stock-outs (lost sales), overstocking, obsolescence, customer discounts, and/or inadequate availability of components and materials in the supply chain. Qualitative risks include lack of accuracy, reliability, and precision of the components and materials in the supply chain. Both qualitative and quantitative risks may create the need for atomistic or holistic evaluations of supply chains.

To develop a categorization of risk more relevant to global supply chains, the sources of risk can be divided into supply risks, operations risk, demand risks and security risks. The following table summarizes supply chain risks together with some instances for each category of risk. Moreover, Table 5-2 illustrates the domain that each type of risk affects.
Table 5-2 Typology of supply chain risks

<table>
<thead>
<tr>
<th>Type of risk</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply risks</td>
<td>Disruption of supply, inventory, schedules, and technology access; price escalation; quality issues; technology uncertainty; product complexity; frequency of material design changes</td>
</tr>
<tr>
<td>Operational risks</td>
<td>Breakdown of operations; inadequate manufacturing or processing capability; high levels of process variations; changes in technology; changes in operating exposure</td>
</tr>
<tr>
<td>Demand risks</td>
<td>New product introductions; variations in demand (fads, seasonality, and new product introductions by competitors); chaos in the system (the Bullwhip Effect on demand distortion and amplification)</td>
</tr>
<tr>
<td>Security risks</td>
<td>Information systems security; infrastructure security; freight breaches from terrorism, vandalism, crime, counterfeiting and sabotage</td>
</tr>
</tbody>
</table>

Figure 5-7 Typology of supply chain risks (source: Mentzer, 2001)

Supply risk is the possibility of an event occurrence associated with inbound supply that may cause failures from supplier(s) or the supply market, such that the outcome results in the inability of the focal firm to meet customer demand within anticipated costs, or causes threats to customer life and safety (Zsidisin et al. 2004). Supply risks reside in the course of movement of materials from supplier’s suppliers to the focal firm, and include reliability of suppliers, single versus dual sourcing, make or buy decisions, centralized versus decentralized sourcing, and security issues.

Operations risk is the possibility of an event associated with the focal firm that may affect the firm’s internal ability to produce goods and services, quality and timeliness of production, and/or the profitability of the company. Sources of operational risk reside within the firm and may result from a breakdown in core operations, inadequate manufacturing, or processing capability (Simons 1999), high levels of process variations, changes in technology that may render the current facilities obsolete, and/or changes in operating exposure. An example of change in operating exposure is exchange rates that often affect the operating profits of companies that have no foreign operations or exports but face
important foreign competition in the domestic market. The structure of markets in which the company and its competitors source labour and materials and sell products determines operating exposure. Hence, operating profit may not necessarily be linked to the currency in which prices are quoted and may vary with real exchange rates (Lessard and Lightstone 1986).

**Demand risk** is the possibility of an event associated with outbound flows that may affect the likelihood of customers placing orders with the focal firm, and/or variance in the volume and assortment desired by the customer. Sources of demand risk reside in the movement of goods from the focal firm to the customer’s customers. Sources of demand risk could be delayed/inappropriate new product introductions (leading the firm to either miss market opportunities or inventory write-offs/stock-outs due to inaccurate forecasting), variations in demand (caused by fads, seasonality, and new product introductions by competitors), and chaos in the system (caused by overreactions, unnecessary interventions, and distorted information from the downstream supply chain members) (Johnson 2001; Wilding 1998). Demand risks vary with the nature of the product, with functional products less risky than innovative products (Fisher 1997).

**Information security risk** is a threat from an unknown third party who may or may not be a member of the supply chain and whose motivation is to steal proprietary data or knowledge (i.e., intellectual property) and/or destroy, upset, or disable a firm’s operations. The sources of information security risk include individuals within the firm leaking vital information to competitors, system hackers, and weak security/firewalls of members of the supply chain (Spekman and Davis 2004). Significant elements of infrastructure security risks are public and private utility services, for example, waterways, highways, airports, electricity and communications. Freight breaches – i.e., violation of the integrity of cargoes and products, leading to the loss or adulteration of goods (due either to theft or tampering for criminal purpose, e.g. smuggling weapons inside containers) – are a major security risk for supply chains.

### 5.4 Future trends in supply chain risk management

Literature reviewed so far shows the trends in supply chain risk management research. Nevertheless, there is a gap between these findings and the maturity of SCRM in industry. Until now, firms have managed supply risks at the company level. Future trends for industry should be directed to successfully implementing risk management at the supply chain level, which requires coordination of risk management between the parties.

Apart from the traditional supply chain risks (supply-, operational or demand-risks), in the future, information risks will increase in significance as a threat to the supply chain.

Moreover, the already existing trend of globalization, as well as the implementation of lean practices will make supply chains more vulnerable in the future.

As Kleindorfer and Saad (2005) suggested, SCRM standards could be established to provide an international common framework for risk management. Once this is defined, guidelines capturing best practices could be developed for specific industries.

In order to do so, key public and private stakeholders should be involved in the definition of these standards, hence ensuring their practicable deployment.
Unlike the public security initiatives created in the last years, future initiatives should tend to be global, either by mutual recognition of existing programmes, or through the creation of an international common security programme.

5.5 Conclusions and implications for CASSANDRA

The following factors should be taken into consideration when developing a risk based approach methodology to supply chain management for CASSANDRA:

- The existing methodologies should be tailored for the particular case of CASSANDRA, i.e. the global container supply chain.
- The approach should be performed from a supply chain perspective and not from a company perspective (i.e. focus should be on an inter-organizational framework in contrast to traditional risk management)
- The key players involved in CASSANDRA Consortium and Advisory Board (e.g. port authorities, terminal operators, shippers) should collaborate to design a common risk based approach.
- CASSANDRA should be prepared to respond to information risks that might jeopardize its success
- CASSANDRA should tackle vulnerability in the supply chain by assessing the credibility of people and goods, as well as supply chain integrity.
6 Crime prevention and security management in supply chains – private sector perspectives

6.1 Overview

One definition from the literature for Supply chain security is “the application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism and to prevent the introduction or unauthorized contraband, people or weapons of mass destruction into the supply chain” (Closs and McGarrell, 2004). The field of supply chain security is relatively new in the academic literature. Literature is mainly normative, with little research based on primary data (Williams et al., 2008). In the literature supply chain security often is discussed in a wider context, linking it to other fields of research such as risk management (Jüttner et al, 2003; Mittroff and Alpaslan, 2003; Chopra and Sodhi, 2004), total quality management (Lee and Whang, 2005) and supply chain resilience (Rice and Caniato, 2003; Christopher and Peck, 2004; Sheffi, 2005).

An overall framework for crime prevention and security management in supply chain context – with preventive, detective and corrective measures

By exploiting vulnerabilities in the supply chain system, internal and external threats, by criminal and terrorist actors, can lead to security incidents in the supply chain, causing supply chain disruptions, economic damages to companies and societies, and sometimes health and safety damages to the citizens. Preventive measures mostly focus on taking away vulnerabilities having as consequence a lower probability of the occurrence of security incidents. Detective security measures can monitor for and detect possible incidents. Corrective security measures are required to minimize damage and to recover from it. All risk mitigation measures (preventive, detective and corrective) require and/or produce security information elements. The diagram below presents an overall framework for crime prevention and security management in supply chain context (adapted from Juettner et al. 2003).
Crime prevention and security management relationships with risk management and with compliance management

Sometimes the basic concepts behind crime prevention and security management, risk management, and compliance management are mixed in the context of supply chain management. For the purpose of the CASSANDRA project, and this Compendium in particular, a simplistic illustration (figure below) is used to clarify the differences, as well as to highlight their intersections – all this in a layman style approach.

Figure 6-1 Supply Chain Security Framework (Source: adapted from Juettner et al., 2003)
Crime prevention and security management in supply chains – private sector perspectives

Figure 6-2 Relationship between security, risk and compliance management disciplines – layman interpretation

- **Crime prevention and security management**: include a variety of proactive approaches to enhance prevention, detection and recovery capabilities in relation to illicit acts in the supply chain. These include sourcing and route planning, process control and monitoring, physical security measures, security education and training, business partner management and public-private partnerships against crime and terrorism.

- **Risk management**: Crime and terrorism related risks need to be managed in the supply chain. At the same time there are many other types of risks than man-made, deliberate acts for illicit profit making, achieving of ideological goals and so forth. Obvious examples include natural disasters, power cuts, material shortages, and strikes.

- **Compliance management**: Supply chain operators have to comply with the supply chain security regulations, which apply to their business as mandatory ones (e.g. advance cargo information as required by the law). Companies can also choose to comply with voluntary supply chain security programs (e.g. EU AEO). However, there is a huge number of other regulations and standards which influence supply chain operations and compliance management, including safety, health, and environmental regulations.

Looking at the right section of the diagram above, one can note that these three disciplines do have an overlapping section, which can be described as “the aspects of complying with supply chain security regulations and standards, while mitigating the risk of crime and terrorism in supply chains”. However, this would be too narrow approach, taking into consideration the following:

- In crime prevention and security management one has to do much more than comply with regulations and standards; also several layers in supply chain security management are not linked to risk management as such (of course the security management priorities have to follow from risk management processes).
• In risk management, one has to do much more than just worry about crime and terrorism related risks.

• In compliance management, one has to do much more than just to comply with security regulations and standards.

Therefore, for the purpose of CASSANDRA Compendium, Crime prevention and security management in supply chains is treated as its own management discipline – naturally taking into consideration the important links with supply chain risk management and supply chain compliance management.

The rest of this chapter has the following structure:

• Crime taxonomy in supply chains;
• Security management in supply chains;
• Case study on practical security management;
• Security versus quality management in supply chains;
• Supply chain security regulations and standards;
• Other crime prevention and security management aspects;
• Future trends in crime prevention and security management;
• Implications for CASSANDRA project.

6.2 Crime taxonomy in supply chains

The types of crimes committed by various illicit actors in the supply chain – be it individual criminals, “supply chain insiders”, organized crime, terrorist groups, or any other category of actors, or, their combinations – are manifold. The traditional criminology and crime prevention literature has not recognized supply chains as the “focal point of crime”, thus there is a gap in pre-existing classifications, taxonomies and typologies, when it comes to structuring various crime types, and their interdependencies in the supply chain. According to a recent doctoral thesis (Hintsa J. 2011), as well as FP7-LOGSEC project (Final report 31.3.2011), criminal activities in the supply chain can be considered as falling into one of the following three main groupings\(^5\):

1. **Economic crime**: focuses on illicit revenue creation, illicit cost savings, or both;
2. **Other crime types**: consists of ideological, ad-hoc, revenge, and up- and downstream crime types;
3. **Facilitating crime**: consists of crime types that do not deliver direct benefits to the criminal actors, but help them to commit the “main crimes”, with economic, ideological, and possibly other goals.

The establishment of this classification enables the categorisation of threats in terms of the main motivations driving criminal behaviour as well as their direct or indirect relationship with the physical supply chain. For instance, the economic crime concerns the crimes in which cargo and supply chain

---

stakeholders are directly concerned. The outcome of economic crime brings direct monetary benefits to the criminals. Other crime types are motivated by ideologies or revenge, or have a direct link outside the focal company. The facilitating crime concerns activities that act as an indispensable resource for, and enabler of the economic and ‘other crime types’, including terrorism and sabotage.

<table>
<thead>
<tr>
<th>Economic crime (revenue generating and/or cost saving)</th>
<th>Other crime types: ideological, political, ad-hoc, up/downstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft (including robbery, larceny, hijacking, looting etc.)</td>
<td>Terrorism (attacking supply chain, exploiting supply chain etc.)</td>
</tr>
<tr>
<td>Organized immigration crime (human trafficking, illegal immigration)</td>
<td>Sabotage</td>
</tr>
<tr>
<td>IPR violations and counterfeiting</td>
<td>Vandalism</td>
</tr>
<tr>
<td>Customs law violations (tax fraud, prohibited goods)</td>
<td>Gross negligence (with criminal charges)</td>
</tr>
<tr>
<td>Other tax fraud (including sales tax / VAT)</td>
<td>Supplier crime(s), raw material fraud etc.</td>
</tr>
<tr>
<td>Other fraud (including insurance, commercial contracts etc.)</td>
<td>Sales channel crime(s), violations, fraud etc.</td>
</tr>
<tr>
<td>Other government agency law violations (e.g. phytosanitary)</td>
<td></td>
</tr>
<tr>
<td>Parallel trade</td>
<td></td>
</tr>
<tr>
<td>Environmental crime (pollution, wildlife)</td>
<td></td>
</tr>
<tr>
<td>Sea piracy</td>
<td></td>
</tr>
<tr>
<td>Extortion, blackmailing</td>
<td></td>
</tr>
</tbody>
</table>

3. Facilitating other crime(s) – these support groups 1 and/or 2 above

<table>
<thead>
<tr>
<th>Document forgery</th>
<th>Identity theft</th>
<th>Espionage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bogus companies</td>
<td>Cyber crime</td>
<td>Corruption</td>
</tr>
</tbody>
</table>

Figure 6-3 Supply chain crime classified in three groups: economic, facilitating crime and other types

Illustrative definitions for each crime types have been presented in FP7-LOGSEC Roadmap (pp. 21-24).

When asking about criminal and terrorist threat priorities, as part of the FP7-LOGSEC Roadmap study, supply chain operators came up with cargo theft as the main priority, followed by cybercrime, bogus companies, insider fraud, smuggling and counterfeiting. The threat of terrorism had the 6th priority.

---

56 Focal Company refers to the company which is the object of and/or is attempting to mitigate supply chain crime. In global supply chains, this is commonly the “brand owner”, for whom negative consequences of crime incidents typically expand from purely economic losses to reputational damages etc.

within the study participants. These, and importance of another five crime types are visualized in the diagram below.

![Figure 6-4 Supply chain operator ranking of criminal and terrorist threats in the supply chain (Source: FP7-LOGSEC).]

6.3 Security management in supply chains

Crime prevention and security management literature contains several attempts to categorize and interlink the variety of options – strategies, procedures, tools, technologies, standards and so forth – available for supply chain operators to plan and manage their security activities in an informed, balanced and sustainable manner, focusing in the areas which are most critical for them. For a mobile phone company it could be anti-theft measures, for a pharmaceutical anti-counterfeit measures, for a shipping line narcotics anti-smuggling measures and for an air-carrier anti-explosive measures. Every supply chain has its own characteristics, which need to be taken into consideration when optimizing the use of limited security resources in the supply chain.

At the same time, the 8-layer model for supply chain security management lays out a broad variety of options to enhance security in the supply chain, independent of the supply chain characteristics, typologies, commodities or transport modes in question. Thus it has been chosen for a more detailed presentation in this Compendium.
6.3.1 8-layer security management model

First, a visual overview of the 8-layer supply chain security management model is presented (see Figure below), followed by brief explanations of each of the eight layers.

<table>
<thead>
<tr>
<th>Layer Name</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Risk Management Layer</td>
<td>Threats, Vulnerabilities, Risk likelihoods, Risk consequences</td>
</tr>
<tr>
<td>2. Design and Planning Layer</td>
<td>Supply chain design, Security plan, Disaster recovery plan, Training plan, Audit plan, PPP-plan</td>
</tr>
<tr>
<td>3. Process Control Layer</td>
<td>Sourcing, making, transport, distribution processes, Deviation reporting, Control loops</td>
</tr>
<tr>
<td>4. Supply Chain Assets Layer</td>
<td>Facilities, Vehicles, Shipments, Products, Data systems</td>
</tr>
<tr>
<td>5. Human Resources Management Layer</td>
<td>Hiring, Awareness, Training, Controlling, Protection, Exit processes, Incentives</td>
</tr>
<tr>
<td>6. Business Partner Management Layer</td>
<td>Screening, Certifications, Training, Monitoring, Audits</td>
</tr>
<tr>
<td>7. Aftermath Capabilities Layer</td>
<td>Business continuity, Drills, Investigations, Evidence, Compensations, Court/justice</td>
</tr>
<tr>
<td>8. Disrupting Criminal / Illicit Supply Chains</td>
<td>Disrupt sourcing, making, transport/distribution, Influence governments and consumers</td>
</tr>
</tbody>
</table>

Figure 6-5 8-layer supply chain security management model (Hintsa J. 2011)

Brief explanations of the eight layers are as follows:

- **Risk Management layer**: Assesses the threats and vulnerabilities in the supply chain. Looks at risk likelihoods and consequences. Provides the baseline for actual security investments and interventions in the supply chain.

- **Design and planning layer**: Designs supply chain structures, including points for sourcing, transport routes and warehouse locations, in order to minimize criminal risks. Also security, disaster recovery, security training and security auditing plans are performed in this layer.

- **Process control layer**: Manages and controls key business processes in the supply chain, while establishing visibility into them for continuous monitoring purposes – essentially “security through visibility”. Provides stability in the processes, while minimizing variations in lead-times, quality and other critical performance aspects.
• **Supply chain assets layer**: Deals with many aspects of physical security, while securing facilities, vehicles, shipments, products, data systems, and data itself. Exploits a broad set of security procedures, technologies, and solutions.

• **Human resources layer**: Focuses on the problematic of human resources as a weak link in the supply chain. Carries out background checks, training, and personnel motivation. Protects personnel against blackmailing, violence, kidnapping, etc. Minimizes the risk of insider crime.

• **Business partners layer**: Defines selection process for business partners, and requirements for partner security certifications. Carries out continuous monitoring and audit activities within the business partner network, in particular with suppliers of materials and logistics services.

• **Aftermath capabilities layer**: Ensures post-incident recovery with minimum supply chain disruptions. Develops competences for criminal investigations, evidence collection, and facilitation of liability and criminal court procedures.

• **Disrupting criminal activities layer**: Causes problems in the illicit supply chains, by hammering supply, production, logistics operations, distribution, marketing and sales criminal functions. For example organizing “joint raids” (with local police) at counterfeit manufacturing sites; and putting pressure on Internet auction sites to block sales of stolen goods.

### 6.3.2 Further elaboration on layer-4 of the 8-layer model

As stated above, Layer-4, the Supply chain assets layer, deals with many aspects of physical security, while securing facilities, vehicles, shipments, products, data systems, and data itself. Technologies, if well designed and operated, can assist in crime and terrorism prevention and detection phases, as well as post-incident recovery phase. More specifically, as part of the Layer-4, security technologies can deliver and/or facilitate one or more of the following functionalities:

- **Secure design**, e.g. anti-counterfeit or anti-theft functionalities are embedded into a consumer product already at the product design phase (e.g. tags in clothing for anti-theft detection at retail stage).

- **Entry protection**, e.g. access to facilities, cargo, vehicles and IT-systems is protected with a combination of anti-intrusion solutions, including CCTV- and alarm-systems.

- **Authentication**, e.g. data, document and product originality are guaranteed by various techniques, including codes verifiable against databases; inks, nano-fractals and holograms etc.

- **Auditing**, e.g. facility, vehicle and data system audits are made more efficient and accurate with the help of IT-tools.

- **Monitoring**, e.g. global transportation networks for sea, air and land based cargo are constantly under surveillance, to detect any deviations from the standard procedures, routes and schedules.

---

• **Tracking**, e.g. cargo is tracked throughout the logistics chain as an anti-theft measure (e.g. for consumer electronics); or, products are tracked throughout their life-time as an anti-counterfeit measure (e.g. for pharmaceuticals)

• **Inspection**, e.g. taking and assessing images from cargo-in-transit, including maritime and air containers, with x-ray, gamma-ray and other relevant (non-intrusive, where applicable) inspection technologies.

• **Testing**, e.g. products subject to counterfeit activities or to sabotage and terrorism are tested by applicable physical, chemical and other possible techniques.

• **Crime reward decrease** activities, e.g. a stolen consumer electronics product stops functioning after one hour/day/week, when it is no longer connected to the web-based service (password protected.)

### 6.4 Case study on practical security management in a high risk supply chain

There are major differences between industry sectors (or, product categories), when it comes to security related vulnerabilities, risks and risk mitigation measures in the supply chain. Cigarette supply chains are considered to be of high-risk nature, when it comes to man-made illicit acts, both for economic gain as well as for ideological reasons. This case study is based on two conference papers published by the CBRA team in 2010. 59, 60

#### 6.4.1 Threat assessment as a starting point

CBRA team provided a qualitative threat assessment in the case company supply chain, with following high-level observations and outcomes:

1. **Theft**: cigarettes are a very attractive target for theft, whether in small quantities (e.g. theft of packs or cartons), or in truck loads (e.g. hijacking of full trucks) or even larger amounts (e.g. breakage into warehouses). All these forms exist at the case company.

2. **IPR (Intellectual Property Right) violations/ counterfeit**: global cigarette brand owners often become victims of counterfeit manufacturers, who exploit the well-known packages to sell products often of a lower quality, damaging the IPR owners in multiple ways.

3. **Customs duty and excise fraud**: violations of customs regulations by not declaring imports and/or by selling cigarettes without excise stamps (or selling with counterfeited tax stamps) are a major problem in the cigarette industry.

4. **Sales channel violations**: selling cigarettes in un-authorized locations, e.g. over the Internet, as well as selling cigarettes to minors, is a common problem in the industry (even though normally not the legal responsibility of the manufacturer).

5. **Blackmailing / sabotage**: could be an issue with certain products, or certain geographies; discussed in a general level during the interviews.

---

59 Hintsa J., Hameri A-P., Männistö T., Lazarescu M., Ahokas J., Holmström J. Conceptual model for measuring benefits of security in global supply chains, The 3rd International Conference on Transportation and Logistics (T-LOG), Fukuoka City Japan, 6-8 September 2010

6. **Civil unrest / looting:** during a civil riot in one Asian country in year 2007, the production machinery and computers were looted from one factory, bringing production and shipments from that site to a long halt.

6.4.2 **Supply chain stages covered by the study**

Next, out of the total supply chain, the case study was agreed to cover the following five stages, as indicated with the dashed-line rectangle in Figure below:

- Inland transport, warehouse to the manufacturing site
- Cigarette manufacturing site
- Transport to distribution centre
- Warehousing and commissioning
- Distribution to the first customer

![Case company supply chain diagram](image)

**Figure 6-6 Case company supply chain – rectangle indicates the stages covered by the study**

6.4.3 **Security measures implemented**

As the next step, the existing security measures and activities were mapped, covering the five stages as indicated above. In addition, security activities on regional level and on headquarter level were also taken into account (as stages 6 and 7 in the table below).
Table 6-1 Security measures and activities at the case company supply chain

<table>
<thead>
<tr>
<th>Supply chain stage</th>
<th>Security activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Inland transport, warehouse to the manufacturing site</td>
<td>Install plastic seal on truck</td>
</tr>
<tr>
<td>1.2 Use hard-sided truck for transportation</td>
<td></td>
</tr>
<tr>
<td>1.3 Arrange driver training, security aspects</td>
<td></td>
</tr>
<tr>
<td>2. Cigarette manufacturing site</td>
<td>2.1 Manage overall security at the factory</td>
</tr>
<tr>
<td>2.2 Coordinate guard services, security aspects</td>
<td></td>
</tr>
<tr>
<td>2.3 Manage and monitor CCTV-systems</td>
<td></td>
</tr>
<tr>
<td>2.4 Provide fences, security aspects</td>
<td></td>
</tr>
<tr>
<td>2.5 Light the facility, security aspects</td>
<td></td>
</tr>
<tr>
<td>2.6 Manage locking devices, security aspects</td>
<td></td>
</tr>
<tr>
<td>2.7 Organize parking of vehicles, security aspects</td>
<td></td>
</tr>
<tr>
<td>2.8 Manage alarm systems, security aspects</td>
<td></td>
</tr>
<tr>
<td>2.9 Carry out employee exit random controls</td>
<td></td>
</tr>
<tr>
<td>2.10 Control inbound logistics, security aspects</td>
<td></td>
</tr>
<tr>
<td>2.11 Control outbound logistics, security aspects</td>
<td></td>
</tr>
<tr>
<td>2.12 Carry out letter mail screening</td>
<td></td>
</tr>
<tr>
<td>2.13 Carry out security training for all employees</td>
<td></td>
</tr>
<tr>
<td>2.14 Construct solid anti-intrusion buildings</td>
<td></td>
</tr>
<tr>
<td>2.15 Maintain and execute internal control procedures</td>
<td></td>
</tr>
<tr>
<td>2.16 Manage access control procedures including electronic badges</td>
<td></td>
</tr>
<tr>
<td>2.17 Check personnel background before hiring</td>
<td></td>
</tr>
<tr>
<td>3. Transport to distribution center</td>
<td>3.1 Provide GPS tracking for trucks</td>
</tr>
<tr>
<td>3.2 Provide truck security package</td>
<td></td>
</tr>
<tr>
<td>3.3 Manage driver and truck database</td>
<td></td>
</tr>
<tr>
<td>3.4 Create and update loss prevention manual</td>
<td></td>
</tr>
<tr>
<td>3.5 Arrange police certification for drivers</td>
<td></td>
</tr>
<tr>
<td>3.6 Send advance shipping notice</td>
<td></td>
</tr>
<tr>
<td>3.7 Organize parking of vehicles, security aspects</td>
<td></td>
</tr>
<tr>
<td>3.8 Track cigarettes on pallet and case level</td>
<td></td>
</tr>
<tr>
<td>4. Warehousing and commissioning</td>
<td>4.1 Manage the alarm system</td>
</tr>
<tr>
<td>4.2 Provide facility security package</td>
<td></td>
</tr>
<tr>
<td>4.3 Carry out security controls and audits</td>
<td></td>
</tr>
<tr>
<td>4.4 Create and update loss prevention manual</td>
<td></td>
</tr>
<tr>
<td>4.5 Arrange security training</td>
<td></td>
</tr>
<tr>
<td>4.6 Count whole stock every day</td>
<td></td>
</tr>
<tr>
<td>5. Distribution to the first customer</td>
<td>5.1 Manage sales rep warehouse security</td>
</tr>
<tr>
<td>5.2 Use a security consultant</td>
<td></td>
</tr>
<tr>
<td>5.3 Execute the ‘know your customer’ program</td>
<td></td>
</tr>
<tr>
<td>5.4 Carry out transshipment point audits</td>
<td></td>
</tr>
<tr>
<td>5.5 Provide GPS tracking for trucks</td>
<td></td>
</tr>
<tr>
<td>6. Regional security management</td>
<td>6.1 Manage overall security for regional markets</td>
</tr>
<tr>
<td>6.2 Assess risks for the regional business, security aspects</td>
<td></td>
</tr>
<tr>
<td>7. Headquarters security management</td>
<td>7.1 Manage supply chain security for whole corporate</td>
</tr>
<tr>
<td>7.2 Manage supply chain IT-security for whole corporate</td>
<td></td>
</tr>
<tr>
<td>7.3 Manage supply chain security aspects of customs programs</td>
<td></td>
</tr>
</tbody>
</table>

Detailed analysis of these security activities provides following results:
- Most security activities are labeled as Facility security, followed by Cargo and by Multi-goal activities;
• Regarding the security stage, Detection is most common, followed by Prevention and by Multi-purpose SCS activities (e.g. both prevention and detection);
• External services are linked to about half of the activities;
• Most security activities (and their costs) can be allocated directly to the Products; and
• Slight majority of the security activities make contributions to other areas, including safety and quality.

6.4.4 Cost distribution, on a single site level (including transport security equipment)

Below is a realistic example of a site-level security (purchase) budget of 0.9 million euros, and how that budget is spent between five different types of security products and services.

![Figure 6-7 Distribution of security (procurement) budget, example on a single site level](image)

6.4.5 Benefits from security activities and measures for the case company

This study discovered several tangible benefits linked to the professional security management approach in the case company supply chain. Benefits were identified under three main categories:

1. **Direct security benefits** consist of anti-theft, anti-smuggling, anti-counterfeit, reduction in insurance premiums, reduction in government penalties, and reduction in sales to minors.
2. **Government-related benefits** consist of less customs inspections, and better corporate reputation in front of authorities and general public.
3. **Collateral benefits** become a very broad set of operational, safety, marketing and cross-departmental side benefits.
Benefits in all three categories remain complicated to quantify; also showing exact causalities between security investments and success stories in a challenging task. As the last point, a specific interconnected benefit was discovered during the case interviews: “When consumers smoke counterfeit cigarettes thinking that it is a genuine product, and if the quality is lower (as it usually) is and if the lower quality does not taste good for the consumer, s/he would typically change the brand after three days of counterfeit smoking and never return to our brand”. This anecdote again confirms the importance of target-oriented security management approach in supply chains (example itself being of course very specific for this sector, without generalizability as such).

6.5 Security versus quality management

Since the year 2001, it has been a common argument in academic articles – and time to time in practitioner presentations and papers – that security and quality management have a lot in common when it comes to management philosophies and even practices of global supply chains. Professor Hau Lee of the Stanford University has presented an ‘analogy table’ between the two disciplines (in 2005), arguing for example that source inspection is a preferred approach for both security and quality management, alongside with seven other arguments which highlight similarities between the two functions) Professor Chwen Sheu from the Kansas State University emphasizes the importance of prevention and process control both for security and quality management (2006). A recent feasibility study on European SCS standards (2009) carried out by the Cross-border Research Association (CBRA) illustrates an optimization graph for minimizing prevention plus recovery costs in security and in quality management (this applies also to safety, environmental and health management functions; to most regulatory compliance management functions; and possibly even to corporate social responsibility and ‘business ethics’, at least to some extent).

How and why security and quality related challenges and responses are actually different by nature? Below are seven reasons and justifications61:

- Security problems in supply chains are driven by intentional acts by humans aiming to benefit from the supply chain system, in a variety of (criminal) ways. Quality problems are driven by a variety of issues with human resources, process control, even ‘laws of nature’. The role of humans in causing quality problems is normally of unintentional nature, basic reasoning being that they do not benefit from achieving lower quality production, service levels etc. Of course, some gray areas exist - for example gross-negligence leading to an industrial accident, happening unintentionally without any benefits attached to it, but recorded as a criminal act; or, motivation of revenge leads to intentional damaging of product quality – but in majority of cases the role of humans differs regarding security versus quality.

- The dynamics related to fixing a problem somewhere in the supply chain, and another problem appearing somewhere else in the chain, is different between security and quality. In security, the criminal actors can decide to shift to another point in the chain, after previous targets have been hardened ‘too much’ from their perspective – for example from warehouse theft to roadside hijackings. In quality it is common that new problems appear elsewhere in the chain once the most

visible problem has been fixed. There the explanation behind the ‘problem dynamics’ or ‘problem displacement’ is often straightforward: the second quality problem existed already before, but fixing the ‘bigger problem’ made the second problem visible. Even though in some rare cases improving quality at some point in the chain could actually trigger totally new problems in another spot, the ‘normal dynamics’ is quite different between the two disciplines.

• Next, looking at **reporting and statistics creation** challenges within security and quality, one can instantly note that a big part of security problems, including counterfeit production and sales; customs law violations; and human trafficking cannot have accurate measurement and statistics attached to them – as by definition, these acts go unreported. Of course law enforcement and some other institutes create estimates on the frequency and size of the problems, but they are just educated guesses at the best. Even with cargo theft parts of it do not become properly reported. As the opposite, in quality majority of the problems can be measured and statistics can and should be created.

• A certain **level of secrecy** can be beneficial for SCS regarding intelligence gathering and risk analysis, in order to avoid revealing sources and vulnerabilities; specifications of security devices and other measures, in order not to ease circumvention by criminal actors; and security incidents and failures, in order not to worsen consumer confidence in a specific company or product etc. Quality management, in the controversy, should be open and transparent by nature. Even though hiding quality problems can sometimes take place, ‘secrecy in security’ can be seen as a much more serious management issue than ‘secrecy in quality’.

• ‘**Who guards the guardians**’ is an ancient challenge in security, considered already by the Roman poet Juvenal almost 2000 years ago. It becomes public information every now and then that people working for security companies or for government agencies are either doing their jobs in a low-quality manner, due for example to laziness or “don’t-care” -attitude, or are even participating in criminal activities, either for their direct personal benefit or as part of organized crime. Various forms of corruption are also a big problem in security field. Laziness and “don’t-care” – attitude can certainly happen in the world of quality – but the major challenge of having to guard the guardians does exists only in security context.

• The **worst case scenarios** can be horrifying in both disciplines, security as well as quality: lives of hundreds or even thousands of people can be jeopardized by counterfeit products, e.g. pharmaceuticals or aircraft spare parts, as well as by quality errors for example in car break systems. However, the worst nightmare security breaches can lead to instant death of 100.000’s of people, or even in millions, for example in a case of biological or nuclear mega-incident. Thus, once can state the worst cases with security, at least in terms of potential lives lost, is few orders of magnitude higher than in quality.

• Lastly, quality, due to its long history and publicity, as well as overall positive reputation, is a much more **mature discipline** than security. This implies more stable approaches to solve quality problems and to stabilize processes. Security is still in its infancy, lacking widely accepted and exploited standard approaches, both for practitioners and academics alike.
6.6 Supply chain security regulations and standards

6.6.1 Introduction

Supply chain security regulations and standards are designed to fight against one or more types of terrorist and criminal activities in the supply chain. Security regulations are driven by governmental law making and enforcement systems, while security standards are initiated both by public and by private sector actors.

Due to space limitations, CASSANDRA Compendium covers security initiatives only with direct European relevance. For global overviews, references are made to recent work by the World Customs Organization\(^{62}\) and the World Bank.\(^{63}\) Following seven security initiatives, categorized in three intuitive groups, have been chosen for this sub-chapter:

- **Mandatory data requirements**: ICS/ECS
- **Company level binding regulations**: Maritime security regulations, Aviation security regulations
- **Company level voluntary certification**: EU AEO, Regulated agent / Known consignor / Account consignor, ISO28000, TAPA

6.6.2 Mandatory data requirements

**Import Control System (ICS)** is a systems architecture developed by the Community for the lodging and processing of Entry Summary Declarations, and for the exchange of messages between national customs administrations and between them and economic operators and with the European Commission.\(^{64}\) ICS obliges carriers or their representatives to submit pre-arrival information for all cargo entering EU territory for shipment risk analysis purposes. The advanced information must be provided in the form Entry Summary Declaration (ESD) that includes among other things details about contents of cargo, planned routing and traders involved with the movement of the goods.\(^{65,66}\) **Export Control System (ECS)** introduces EU-procedures to computerize and control indirect exports\(^{67}\) and to implement the EU safety and security regulations.\(^{68}\) Just like with ICS, the responsibility to file the required data within the required time schedule lies with the carrier, or another person with the carrier's knowledge and consent.

---

\(^{62}\) WCO AEO Compendium (2010)

\(^{63}\) World Bank Supply Chain Security Guidebook (2009)

\(^{64}\) http://ec.europa.eu/ecip/help/faq/ens7_en.htm#faqsection

\(^{65}\) FAQ's: Import Control System (ICS) – Information for UK Traders. Available at http://customs.hmrc.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?_nfpb=true&_pageLabel=pagImport_ShowContent&id=HMCE_PROD1_030208&propertyType=document

\(^{66}\) Annex 30A of Commission Regulation 1875/2006 lists required data elements of the ESD

\(^{67}\) Where an export leaves the EU from a Member State (MS) other than the MS of export

6.6.3 Company level binding regulations

**Maritime:** International regulations to ensure the security of maritime transportation are being issued by the International Maritime Organization, IMO, in the *International Ship and Port Facility Security (ISPS) code*[^69]. The code contains minimum security requirements for ships, ports and government agencies and is in force since July 1, 2004. Four main articles in the code highlight how security enhancements may be achieved.[^70] ISPS code, and the EU legislation, is mandatory for shipping lines and port terminal operators, requiring them to invest e.g. in sea-side and land-side traffic management and access control equipment, systems, IT, procedures and security personnel.

**Aviation:** Following the terrorist attacks in the United States on 11 September 2001 when commercial aircraft were used as weapons of mass destruction, the Commission made a legislative proposal to bring aviation security under the EU's regulatory umbrella[^71][^72]. Today, three categories of aviation security legislation exist in the EU[^73]: Framework regulation[^74]; Supplementing regulations[^75]; and Implementing regulations[^76]. Requirements are for example for: Airport security; Protection of aircraft; Cargo and mail; Staff recruitment and training; and Security equipment.

6.6.4 Company level voluntary certifications

The World Customs Organization, WCO[^78], in SAFE Framework of Standards considers Authorized Economic Operator, AEO, to be “a party involved in the international movement of goods in whatever function that has been approved by or on behalf of a national Customs Administration as complying with WCO or equivalent supply chain security standards.

The European Union, **EU AEO certification**[^79] is available in following three versions: Customs Simplifications (AEO-C); Security and Safety (AEO-S); and Customs Simplifications/Security and Safety (AEO-F). EU AEO procedure verifies security practices and measures in following 13 areas: Security (self)assessments; Entry and access to premises; Physical security; Cargo units; Logistical processes; Non-fiscal requirements; Incoming goods; Storage of goods; Production of goods; Loading of goods; Security requirements business partners; Personnel security; and External services.[^80]

[^72]: This initiative led to the adoption of framework Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security and thus provided the basis for allowing harmonisation of aviation security rules across the European Union with binding effect.
[^76]: For example Commission Regulation (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security.
Analogical to the EU AEO, specific “trusted trader” status - regulation-based, voluntary to implement – exist in the European air cargo supply chains, in particular the following three:

- **Regulated agent**: an air carrier, agent, freight forwarder or any other entity who ensures security controls in respect of cargo or mail;
- **Known consignor**: a consignor who originates cargo or mail for its own account and whose procedures meet common security rules and standards sufficient to allow carriage of cargo or mail on any aircraft; and
- **Account consignor**: a consignor who originates cargo or mail for its own account and whose procedures meet common security rules and standards sufficient to allow carriage of that cargo on all-cargo aircraft or mail on all-mail aircraft.

According to the International Standards Organization (ISO) the ISO 28000 series of standards on supply chain security management systems has the aim to reduce risks to people and cargo within the supply chain. Moreover, the standards address potential security issues at all stages of the supply process, thus targeting threats such as terrorism, fraud and piracy.

- **ISO 28000:2007** - Specification for security management systems for the supply chain;
- **ISO 28001:2007** - Security management systems for the supply chain – Best practices for implementing supply chain security – Assessments and plans – Requirements and guidance;
- **ISO 28003:2007** - Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems; and

The Transported Asset Protection Association (TAPA) represents businesses fighting back against cargo crime that want to use real-time intelligence and the latest preventative measures to protect goods in the supply chain. TAPA has introduced the following four sets of security requirements and standards in the supply chain:

- **Freight Security Requirements (FSR)** - Established to ensure the safe and secure in-transit storage and warehousing of any TAPA members’ assets throughout the world;
- **Trucking Security Requirements (TSR)** - Specifies the minimum acceptable security standards for assets traveling throughout the supply chain and the methods to be used in maintaining those standards;

---

78 COMMISSION REGULATION (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security.


80 Slightly modified from: http://www.iso.org/iso/pressrelease.htm?refid=Ref1086

81 http://www.tapaemea.com/download/TAPA_Brochure.pdf?PHPSESSID=7619991b32189f73b8cba51512489c1e

82 http://www.tapaemea.com/download/TAPA_Brochure.pdf?PHPSESSID=7619991b32189f73b8cba51512489c1e
- Parking Security Requirements (PSR); and,
- TAPA Air Cargo Security Standards (TACSS).

6.7 Future trends in supply chain security management

Starting with the threat side of the equation, it is likely that in the future the organized crime will become increasingly active in exploiting the global supply chains for a variety of illicit activities especially to achieve economic objectives through the means of illicit revenue generation (e.g. counterfeit products and blackmailing) as well as illicit cost savings (e.g. customs duty and excise tax evasion). Crime types with high profit margins and with low risks of getting caught (and moderate punishments when caught) will be given more priority. At the same time, illicit trade and transport of narcotics will remain as the leading source of illicit revenues. It is possible that organized crime and terrorist activities merge more in the future, especially when it comes to arranging terrorist financing from other supply chain crime, including cargo theft and people smuggling.

Supply chain operators and cargo owners will be responding to criminal and terrorist threats in their supply chains primarily based on their business requirements and sensitivities. Next to the traditional crime incident cost avoidance approaches, broader issues such as brand protection and (perceived) corporate social responsibility will have more weight in their security decision processes than today. New anti-crime and anti-terrorism services and solutions will be developed, piloted, and adapted into daily use – but no silver bullet solutions are foreseen to tackle multiple aspects in supply chain security, in a trustworthy, sustainable manner. As a management topic, supply chain security management will become more professional, target-oriented discipline in the future, covering robust management approaches for example to cost-benefit analysis and security metrics; as well as crime and security interdependency management.

Governmental policy makers, regulators, inspection agencies and law enforcement agencies are facing many challenges in the detailed implementation of regulations (e.g. advance cargo information rules) and voluntary programs (e.g. EU AEO). The overall security-efficiency and the total cost of these approaches is being frequently questioned by the supply chain operator communities. Requirements for recognitions between the variety of supply chain security programs, e.g. mutual recognitions between different AEO-programs around the world, are becoming stronger. At the same time, independently of the private sector opinions, governmental actors will remain the ultimate responsible for the economic security as well as safety and security of the citizens, when it comes to battling against criminal and terrorist threats in global supply chains.
6.8 CASSANDRA implications

Advances in crime prevention and security management capabilities in supply chains form an important underlying objective for CASSANDRA-project. Being able to exploit information and data from the supply chains to detect deliberate criminal and terrorist threats and regulatory violations in a proactive manner is crucial for the success of the project. Collaborative approach, where CASSANDRA end-user partners including customs, police, cargo owners and logistics companies produce a common set of risk indicators and baseline rules, will be highly beneficial. The priorities between the various crime and terrorist threats vary between these actors; but this should not prevent the quest for the “common set”. Naturally CASSANDRA cannot solve all crime and terrorist problems in one go – therefore prioritization in an early stage in the project is required.
7 Governmental procedures, compliance and risk management

7.1 Overview

The far-reaching globalization and increased international trade of the past decades are two key drivers of economic growth, which governments have set out to promote and facilitate, by reducing administrative burdens and logistic disruptions caused by customs’ physical inspections. At the same time, both globalization and the large scale of international trade add to an unprecedented scale of risks related to security, safety, and fraud. In this chapter, we first describe governmental procedures (Section 7.2), compliance (Section 7.3) and risk management (Section 7.4), in particular from the perspective of Customs. We then discuss future trends in Section 7.5 and end with the conclusions and implications for CASSANDRA (Section 7.6).

7.2 Procedures

This section discusses the topic of customs procedures from the perspective of the European Union.

In Europe, 183 million customs declarations were completed in 2007 – 5.5 every second – and each year, 1,545 million tons of sea cargo and 11.7 tons of air cargo are checked each year. In 2008, the Modernized Customs Code (MCC) was established, which is implemented by the Customs administrations of its 27 Member States. This legal framework is the basis for all Customs affairs, regulating the actions which Customs authorities (should) undertake (see Section 4.2). Generally Customs, at times jointly with other governmental (Border) agencies, are accountable for controlling imports and exports for customs, social, health, safety and security purposes. There are two basic ways in which Customs controls the flow of goods, namely by physical inspections and by analysis of the information that businesses are required to submit. Given the sheer amounts of cargo moving in, out, and through the EU, 100% physical inspections are not feasible. Moreover, that would seriously hamper trade, as the physical inspections take additional time and disrupt the logistic flow of the goods. The containers usually have to be transported to other sites in the ports and have to stay there longer. Sometimes, the shipment might even become worthless, for example if the shipment consists of perishable food products, they might be spoilt before all relevant documents are gathered, the tests and inspections are conducted, and the container is cleared by Customs (and the food inspection agency) (Van Stijn et al., 2011b). Therefore, freight targeting is a key tool in customs control. It allows customs and border agencies to target certain consignments for control effort, whilst facilitating the quick and easy release of low risk consignments. It allows for effective use of limited resource and the discharge of:

- Compliance checks;
- Regulatory controls;
- Anti-smuggling controls; and
- Safety, security and counter terrorism checks.

---

Freight targeting supports border security, supply chain integrity and citizen security and can be spread over a wide range of government and commercial systems. For targeted inspections and other risk management purposes (see Section 7.4), the focus thus lies on information provisioning by businesses. Traditionally, the submission of data involved a lot of paperwork (with a high administrative burden). According to research of the Asia-Pacific Economic Cooperation (APEC) Business Advisory Council (1996), each international trade transaction required an average of 40 documents to meet rules and regulations set for international trade and transport. Typically, these documents have a large overlap regarding the data elements: the same data have to be submitted more than once, to different government agencies, and at different points in the supply chain. Costs may also arise from typing and other errors. If something goes wrong with the data exchange, the goods again may be delayed at the border (Tan et al. 2011).

Within the European Union, Annex 37 to Regulation No 2454/93 describes the data required on the import and export Single Administrative Document (SAD), which is the main data capture mechanism for Customs. The use of Information and Communication Technology (ICT) has become more and more important in this international trade setting. The EU Import Control System (ICS) and the Export Control System (ECS) also require advance safety and security information prior to loading. For deep sea voyages the law requires the carrier to make this declaration 24 hours prior to the goods being loaded in the foreign port of export. The security amendment, Annex 30A to regulation 2454/93, describes the data required under the pre-arrival, pre-departure systems. Modern legislation in the European Community and in key trading partner countries, such as the United States, attempts to capture data about cargo upstream prior to loading for export, but it is restricted in legal jurisdiction; the consignor who holds the critical data is out of the legal reach of the importing authorities. The legal requirement therefore focuses on the bodies that do fall within enforceable jurisdiction, namely, the importer and the carrier. However, the current transport systems are designed to limit carrier liability and do not always service that information requirement. Furthermore, it is essential for Customs to know the accurate details about the container’s content and how the goods and payments flow from actor to actor. Customs have, historically, used logistics data such as way bill or manifest data, for pre-arrival or pre-departure risk assessment instead of drawing on the comprehensive commercial data between buyer and seller, which more accurately describes the goods and the people involved. In everyday practice, despite the legal requirement to provide accurate data about the goods being carried, about 60% of vessel manifest information is described as 'agent to agent' rather than buyer/seller, making the data unfit for regulatory pre-arrival risk assessment purposes. Well-established commercial practices are masking the accuracy of data thereby increasing the risks posed by a lack of visibility. The fundamental questions remain: “Who packed the bag and who knows what is in it?”

Though advances have been made with the introduction of information technology, the current ways of data provisioning do not fully support this yet. Overall, the existing ICT infrastructure in the EU is highly complex and there is no definitive alignment across the EU yet. The different Member States of the EU have traditionally each developed and implemented their own information systems, without overarching coordination at the EU-level (Van Stijn et al., 2011a). In this light, the European Commission
has initiated an extensive eCustoms project, laid down in the Multi-Annual Strategic Plan Rev 9 (MASP)\(^85\) of 2008, which focuses on “aims to replace paper format customs procedures with EU wide electronic ones, thus creating a more efficient and modern customs environment. The project’s dual objective is to enhance security at the EU’s external borders and to facilitate trade. It should therefore benefit both businesses and citizens.”\(^86\) The use of common EU-wide information systems is an important step towards improved data provisioning. It should be noted that there are still several issues. First of all, the silo automation appears to remain as these systems are primarily based on a specific function (export, import, transit, etc.). In addition to the systems foreseen in the MASP, other common EU systems are also introduced, like the VAT Information Exchange System (VIES), but those are not clearly coupled. Secondly, the requirements are set at the EU level, but each country still has some degrees of freedom to further develop each system to fit the national infrastructure and legislation. Thirdly, these systems are very costly to introduce, even though that is made mandatory by the EC. For example, an impact assessment study related to the introduction of only the Export Control System in only one EU Member State (United Kingdom) reveals that the estimated costs for the approximately 83,000 affected businesses are a one-time investment of up to € 7.5 million transition costs, and an additional average annual costs of up to € 1.1 million (HM Revenues and Customs 2009). On top of that, given the national differences that still may exist, companies operating from different EU countries will have to implement different interfaces in each of them (Henningsson and Henriksen, 2011).

### 7.3 Compliance management

In this section, we will further provide a background of compliance management, addressing social compliance, responsive regulation, and the facilitation-compliance continuum.

#### 7.3.1 Social Compliance

Modern compliance with laws and regulations is a social and political matter requiring a balance between state imposition and a personal/social acceptance of responsibility. The less socially responsible society is, the more the state needs to intervene to protect the weak, the vulnerable, the economy and national security. In a dictatorship or a central command economy, however, the level of social responsibility and decision-making is reduced and the rule of law is imposed. Many of the world economies and therefore the regulatory authorities within them such as Customs, tax and the police, have social and political cultures and structures that span these ‘extremes’ so building a ‘one size fits all’ compliance model is neither preferable nor achievable.

Voluntary compliance can be described in a similar way to which Valerie Braithwaite (2007, p. 7) describes responsive regulation in that it “engages taxpayers to think about their obligations and accept responsibility for regulating themselves in a manner that is consistent with the law”. It can, of course, also mean voluntarily compliance but that simplistic definition hides the more fundamental question about why people or businesses abide by the law, such as fear of sanction, power and authority, peer or group pressures, values and norms, social honour or visibility by group members within a group. Social order as a means of describing “normal” ways of behaving and relating has been put forward by Thomas

Hobbes, Karl Marx and others and should form an integral part of our understanding of voluntary compliance and thereby building responsive regulation, efficient administrative systems and a balance between trade facilitation and regulatory control. But social order needs to be considered within the context of national culture, national and social stability and the integrity and trustworthiness of those with power, influence and procedural fairness. Social order is also dynamic and ever changing with generations, migration and environmental and economic developments.

Adam Smith, the 18th Century Scottish moral philosopher, described the criteria for a “good tax” in his canons of taxation. He said tax should be:

- **Equitable** – taxpayers of the same equity should pay the same tax and unequally situated taxpayers should be taxed on their ability to pay
- **Convenient** – tax should be easily assessed, collected and administered
- **Certain** – consistent and stable
- **Economical** – compliance and administration should be minimal in terms of cost.

He also said that a tax should produce the sufficient and desired amount of revenue; it should be used to reallocate resources in order to achieve social and economic objectives and it should be neutral in that it should not negatively influence taxpayers’ economic decisions.

### 7.3.2 Responsive Regulation

These points made by Adam Smith have significant relevance when considering what makes people comply and how this, in turn, informs compliance management in Customs. We know, for example, that commitment to compliance and understanding of each other’s business objectives by both Customs and trader adds economic and resource value by increasing efficiency and reducing assurance intervention. Recognizing the legal, moral and social imperatives of a sound Customs and tax regulatory system, as described by Adam Smith, along with the economic and motivational benefits of a largely compliant trading community leads Customs to strive for a balanced approach to both regulatory control and trade facilitation. Critical to this modern balanced approach is intelligence led, risk based, technology driven, responsive regulation and administration. Responsive regulation entails that the focus lies on voluntary compliance by companies, shifting to more trust-based, horizontal relationships between business and governments. Dutch Customs refers to this as so-called “horizontal supervision”, which is an important pillar of their activities.

Sparrow states that “the tools of voluntary compliance are the newer, more politically fashionable, and less adversarial methods: education, outreach, partnership, consensus and facilitation” (Sparrow, 2000, p. 56). Ian Ayres and John Braithwaite put forward the idea of responsive regulation or more flexible responses by the authorities to the level of compliance, risk or social order demonstrated by a company. This means Customs listening and responding to the needs of business. Tyler (1987) describes the critical importance of being able to express opinions or have a “voice” in (legislative) decision-making and being respected in the process. This endorses Sparrow’s support for outreach, partnership, consensus and

---

88 An Inquiry into the Nature and Causes of the Wealth of Nations first published on March 9, 1776
facilitation as tools of voluntary compliance but they are not new. When Parliament in London imposed a tax on tea “to allow a drawback of the duties of customs on the exportation of tea to any of his Majesty’s colonies or plantations in America” on May 10, 1773\(^89\) without consultation or consensus, the level of compliance decreased rapidly by the Sons of Liberty with the cry of “no taxation without representation”. And the rest, as they say, is history.

The link between the sociological understanding of why people (in business) comply with norms, values and the law and how to build responsive regulation as a consequence has been demonstrated by the Australia Taxation Office through their Compliance Model (Braithwaite, 2003), which is shown in Figure 7-1. This has been recognized by a number of Customs Administrations as an effective strategy to respond to the need to reduce regulatory burdens on business and meet growing commercial and economic demands.

![Figure 7-1 Example of regulatory practice with ATO Compliance Model (Braithwaite, 2003)](image)

### 7.3.3 The Facilitation and Compliance Continuum

Trade Facilitation is simply put the process of using intelligence to identify the compliant and non-compliant and applying the appropriate level of control accordingly. The fully compliant will never avoid a level of control simply because assurance is a proper and responsible tool of public service and commercial management - even if they are an Authorized Economic Operator (see section 7.4). There is no standard definition of Trade Facilitation\(^90\). It is generally a means of reducing barriers to legitimate trade and focusing enforcement related resources on trade that does not comply with the legal requirements. It can be applied to international trade related transport, logistics, policy and regulatory requirements including health, agriculture and Customs and commercial transactions including finance and insurance. In addition, the United Nations describes facilitation as “the simplification,


standardization and harmonization of procedures and associated information flows required to move goods from seller to buyer and to make payment\(^{91}\).

Within European Union Customs legislation the Authorized Economic Operator scheme\(^{92}\) recognizes companies whose supply chain is secure and whose Customs controls and procedures are efficient and compliant. These companies gain quicker access to certain simplified Customs procedures. Customs use this scheme to provide facilitation as an incentive or a tool of voluntary compliance. This example of a compliance continuum, as visualized in Figure 7-2, makes the distinction between the fully compliant trader at one end and deliberate evasion at the other. In between is a sliding scale of subjective, qualitative assessment as to the compliance reasoning of the trader and the pro-active or re-active response by Customs.

---

\(^{91}\) United Nations Centre for Trade Facilitation and Electronic Business, (UN/CEFACT)

Any move by Customs towards a more ‘contemporary’ systems based approach to risk and compliance management requires, under this model, up-front education, advice, marketing, customer contact and analysis of risks and business performance. Each aspect has its own difficulties and requires considerable and sustained investment by Customs.

### 7.4 Risk management

There are many definitions of risk. Definitions of risk need to incorporate the concept of assessing the likelihood of something obstructing the achievement of business objectives or something happening that has an adverse impact. In ‘Managing Risk in the Customs Context’ Professor David Widdowson explains that “the concept of risk refers to the possibility of events and activities occurring that may prevent an organization from achieving its objectives”. Definitions of risk need to incorporate the concept of assessing the likelihood of something obstructing the achievement of business objectives or something happening that has an adverse impact. Risk can be described as “The uncertainty of

---

93 See also e.g. the Risk Management Guide for Tax Administrations:  

94 http://www.risksol.co.uk/resources/definitions.php

95 http://www.adb.org/Projects/TradeFacilitation/Documents/Managing-Risk.pdf
outcome, whether positive opportunity or negative threat, of actions and events. The risk has to be assessed in respect to the combination of the likelihood of something happening, and the impact, which arises if it does actually happen. Risk management includes identifying and assessing risks (the ‘inherent risks’) and then responding to them.

Customs is concerned with all the risks related to the cross-border movement of goods, with the following characteristics: 1) Belong to customs responsibilities (as stated in the customs law); 2) Have negative impacts on citizens and/or nations (security, safety, health, economics etc.); 3) Cause problems in supply chains (costs, liabilities, reputational issues etc.). The scope includes risk related e.g. to: misdeclarations of imported or exported goods; smuggling of prohibited goods; intellectual property violations; and violations of international trade agreements, as these can have negative implications for citizens/nations, supply chains and customs administrations. Based on the flow of containers in the international supply chain (see Figure 7-3), several key issues can be identified, such as the loading of unwanted goods (e.g. unsafe/unhealthy goods, counterfeited, or illegal goods), the theft of containers, or the re-routing for the purpose of smuggling or terrorist attacks (Oosterhout et al., 2007), as visualized in Figure 7-3. In addition, there may also be issues with for example overloading containers (too much weight) or fraudulent activities (regarding e.g. import declarations and settlement of the duty and/or VAT payments). For example, fraud with Value Added Tax (VAT) and excise duties in the European Union is estimated to amount to tens of billions of Euros per year. Especially after the terrorist attacks of 9/11 in 2001, governments have also increased control measures to secure international supply chains. Government actors are seeking further means to facilitate international trade while safeguarding public values (Rukanova et al., 2009; Rukanova et al., 2011a).

![Figure 7-3 Security threats in the global supply chain (Oosterhout et al., 2007)](image)

The operating environment of customs is characterized by a constantly changing risk landscape. Customs antagonists (including smugglers, traffickers, and fraudsters) are dynamic enemies who review and reshape their operations constantly. The illicit operators seek high profits and low-risk “business” opportunities, much as their legal counterparts do, while adopting new ways to conceal contraband, forge trading documents, or solicit customs officers. Security issues have become Customs’ primary...
Governmental procedures, compliance and risk management

cargo processing concern, and multiple programs with heavy industry participation are being developed to respond to the new challenges. At the same time, traditional trade compliance and enforcement is being addressed in the new Focused Assessment Program. Overall, importers and exporters must become even more involved in understanding, monitoring, and controlling their entire logistics chain, or face increased Customs cargo exams, reviews, audits, and delays in clearance of their shipments.

Customs and commercial organizations need to manage their risks. Good risk management allows stakeholders to have increased confidence in corporate governance and an organization’s ability to deliver. Organizations should integrate their risk management strategy into their governance arrangements as a key management process. The European Commission definition of risk management is “A technique for the systematic identification and implementation of all measures necessary to limit the likelihood of risk occurring. International and national strategies can be effectively implemented by collecting data and information, analysing and assessing risk, prescribing action and monitoring outcomes.”

There is not a specific “standard” set for risk management. The way in which European Customs and commercial businesses manage risk is driven by a combination of references to the European Commission explanation of Risk Management for Customs in the European Union and various international risk management standards, such as the “Risk Management Standard” produced by the Association of Insurance Risk Managers, AIRMIC in the UK, or the Australian standard, Committee of Sponsoring Organisations of the Treadway Commission (COSO), or the Canadian Government sector standard. More important than adopting any particular standard is the ability to demonstrate that risk is managed in an organization’s particular circumstances and in a way, which effectively supports the delivery of its objectives. In general, risk-based auditing, which is concerned with identifying, assessing, controlling, and monitoring risks, may be visualized as shown in Figure 7-4, which can be seen to include the following:

![Figure 7-4 Risk-based auditing approach in general](image)

---

96 EU standardised framework for risk management in customs administrations of the EU 2007
- **Framework and Context**
  The establishment of the strategic, organizational and risk management context including an understanding of the environment within which organizations are operating and understanding that internal and external events may positively or negatively impact the organization’s strategic and operational performance and need to be identified as risks and opportunities.

- **Identify**
  Identify the risks drawing on quantitative and qualitative data including experience and intelligence from a number of sources in a comprehensive manner so that areas of risk are not overlooked. Data is collected from the identification of ‘proven risk’ where there is a record of the incident and the facts surrounding the case and ‘potential risks’ where something has not yet been uncovered but is suspected.

- **Assess**
  Make sense of the data, ensure completeness, assess the credibility of the source and the accuracy of the data, consider the probability and impact of the risk materializing and weigh its importance against the level and timing of control. Recycle the proven accuracy and credibility back into the system.

- **Control**
  Decide if, how and when to carry out any control. For the risk associated with imports and exports this can include:
  - For Customs - an unreliable exporter or an unreliable importer, goods mis-described or not as described on the invoice, fiscal risk addressed through a guarantee, licence and other certificates not produced, goods interfered with during transport resulting in ‘rip-on’ or ‘rip-off’. Customs controls can take place at the exporting company’s premises, pre-departure prior to loading, on arrival in the country of import or at the importing trader’s premises;
  - For a commercial company - an unreliable seller or an unreliable buyer, goods mis-described or not as described on the invoice, fiscal risk met through a Letter of Credit, licenses and other certificates not produced, goods interfered with during transport resulting in ‘rip-on’ or ‘rip-off’. Commercial controls can take place at the exporting company’s premises, pre-departure prior to loading, on arrival in the country of import or at the importing trader’s premises.

- **Monitor**
  Continuously manage the situation and monitor both the emergence of the risk and the systems surrounding the management of the risk. Ensure clear and regular communication against the risks identified and assessed to enable management to intervene on a timely basis.

Based on such a general framework, the risk-based auditing approach as visualized in Figure 7-5 can be derived for the context of Customs and other regulatory compliance.
Within the context of risk management and voluntary compliance, it is relevant to consider whether actors are Authorized Economic Operators, or not. The **Authorized Economic Operator** (AEO) is defined by WCO as “a party involved in the international movement of goods in whatever function that has been approved by or on behalf of a national Customs administration as complying with WCO or equivalent supply chain security standards. Authorized Economic Operators include inter alia manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses, distributors” (WCO, 2005, p.36). It is an important pillar of the WCO SAFE framework and also adapted by the EU:

“One of the main elements of the security amendment of the Community Customs Code (Regulation (EC) 648/2005) is the creation of the AEO concept. On the basis of Article 5a of the security amendments, Member States can grant the AEO status to any economic operator meeting the following common criteria: customs compliance, appropriate record-keeping, financial solvency and, where relevant, security and safety standards. The status of Authorized Economic Operator granted by one Member State is recognized by the other Member States. This does not automatically allow them to benefit from simplifications provided for in the customs rules in the other Member States. However, other Member States should grant the use of simplifications to Authorized Economic Operators if they meet specific requirements. Economic operators can apply for an AEO status either to have easier access to customs simplifications or to be in a more favourable position to comply with the new security requirements. Under the security framework, which has been applicable since 1 July 2009, economic operators have to submit pre-arrival and pre-departure information on goods entering or leaving the EU. The security type of AEO certificate and the combined one allow their holders to benefit from facilitations with regard to the new customs controls relating to security.”

---

C-TPAT certification in the US is similar, but focuses on security risks only, whereas AEO in the EU also focuses on fiscal risks (financial aspects). Henningsson et al. (2011b) note that the popularity of the current AEO certification is limited, as it is perceived to bring only limited benefits to traders. Within the ITAIDE context, a modularized and extended AEO concept has been proposed in that light (Henningsson et al., 2011a). In that case, the process to obtain other certificates, for which overlapping information has to be submitted to other governmental agencies, is further streamlined. Depending on the type of goods, specific certificates may be needed for export and import. For example, a dairy company has to obtain and submit a Certificate of Origin and a Health Certificate in addition to regular export and import declarations (Henningsson et al., 2011a). Certificates are also required for pharmaceutical products (drugs/medication), dangerous goods, endangered species, and so forth. This topic will be further discussed in terms of mutual recognition in the next section.

7.5 Future trends

In this section, we address the following trends that are of relevance to the CASSANDRA project, namely Single Window, the Consignment Completion Point, Coordinated Border Management, and mutual recognition.

7.5.1 Single Window

Value for money in electronic messaging

In 2008, the HERMES project commissioned by the UK organization for simplified trade procedures, SITPRO, analyzed the use of paper in the whole international supply chain from suppliers in third countries to UK retailers. The project found that documentary systems cost companies moving perishable goods along the international trade supply chain more than US$1.6 billion annually. By contrast, the project also found that potential savings of over US$1 billion could be made by implementing the transfer of data by electronic message through all the parties in the supply chain, including importers, exporters and authorities. The report went on to describe:

- 150 documents in a typical single complete consignment transaction from grower to retailer (= up to 225 pieces of paper);
- 1 billion pieces of paper generated each year by UK perishable food imports supply chain;
- 30% data entered more than once;
- 189 million duplicate consignment entries;
- 0.5% consignment cost savings from each day saved in supply chain.

The report estimates up to 1.4 million incidents of missing or delayed documents in a single year for perishable foods imports into the UK alone. These result in additional costs from securing replacements or amendments, as well as costs that delays can exact in terms of additional spoiled food. It finds that nearly a third of all trade data is re-keyed, creating inefficiencies and risking discrepancies that could be avoided with paperless trading. It also identifies an environmental cost in the form of destroyed paper documents. One billion pieces of paper are produced each year by this supply chain of which over 90%

are destroyed. A considerable volume of this paper is coated with chemicals to create non-carbon reproducing copies and is non-recyclable.

**Single Window implementation**

The ability to handle data efficiently and swiftly has become a key element in international competitiveness, especially in international trade supply chains. However, much emphasis has been placed in the way regulatory data can be provided to border authorities at the expense of studying the efficiency of the commercial and logistics transactions designed to buy, sell and ship goods around the world. One solution to the complexities of border procedures and the interaction with different authorities has been the ‘Single Window’ for centralized information processing that collects and exchanges regulatory information needed for national import and export between the private sector companies and the participating Government agencies.  

The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) (2005, p. 3) defines Single Window (SW) as “a facility that allows parties involved in the international supply chain to lodge data in a standardized format at a single entry point to fulfil all import, export, and transit-related regulatory requirements. If the data are electronic, they should be submitted only once.” As discussed earlier in this chapter, one of the goals of the EU is to establish such a SW. “The long-term ambition is that an EU Single Window would provide a “one-stop shop” for businesses dealing with authorities in one Member State involved in the movement of goods. The vision is that it does not only mean information sharing between businesses and national authorities of one of the Member States becomes as efficient as possible, but also that information is shared amongst national authorities of different Member States and with relevant EU-level government agencies (such as EUROSTAT for statistics). As such, Single Window is part of the national domain of a country and has an international dimension” (Van Stijn et al., 2011a, p. 286).

The establishment of a SW environment is a complex task. It not only involves all kinds of technological questions regarding data harmonization, standardization, interoperability, and ICT architecture, but also faces organizational, managerial, financial, legal, and political challenges, as visualized in Figure 7-7 (Van Stijn et al., 2011a).

---

99 UNECE Recommendation 34

100 The definition of Single Window has been adapted by the International Trade Procedures Working Group (ITPWG – TBG15) of UN/CEFACT (http://www.unece.org/cefact/forum_grps/tp/welcome.htm), placing greater emphasis on the international trade and transport communities as well as standardized documents by stating that “a Single Window facility, that allows parties involved in trade and transport to lodge standardized information and documents with a single entry point to fulfill all import, export, and transit-related regulatory requirements”.

Governmental procedures, compliance and risk management

Within the context of the ITAIDE project, Single Window has been a recurring research topic. The reader is in particular referred to the book “Accelerating Global Supply Chains with IT-Innovation: ITAIDE Tools and Methods” (Tan et al., 2011). The Living Lab solutions are discussed in relation to Single Window and Chapter 16 is specifically devoted to guidelines for establishing Single Window and other e-Solutions for Trade Facilitation in the EU context (Van Stijn et al., 2011a). For further reading, the ITAIDE Deliverable D5.0.4 “State of Art” presents five case studies of Single Window systems implemented by the public authorities and in particular, the Customs of Australia, Denmark, Hong-Kong, Japan and Singapore. Deliverable D1.2d “Single Window Implementation Framework D5.0.4b” is a follow-up (and the basis of the book chapter), introducing the Single Window Implementation Framework (SWIF), which is also available as (advance) publication by UNECE (Van Stijn et al., 2011b). The SWIF presents a holistic approach to implementation of SW based on the TOGAF Architecture Development Methodology and provides a set of guidelines and techniques related to five essential implementation areas that differ substantially from other information system implementation, stakeholder management and interagency collaboration, business process analysis and simplification, data harmonization, interoperability, and the realization of the legal framework. The SWIF has also been applied as a structure for case comparison, to implementation cases of The Netherlands and Thailand. Cross-case comparisons facilitate to synthesize lessons learned and to adapt these to the contexts of Single Window implementations in specific countries (Van Stijn et al., 2011c).

---

101 [Link to Deliverable D5.0.4 State of Art]

102 [Link to Deliverable D1.2d Single Window Implementation Framework]

103 [Link to SWIF publication by UNECE]

---

Figure 7-6 Cloud of many challenges implementing Single Window (Adopted from Van Stijn et al., 2011a, p.291)
A major problem of Single Window is that it focuses on the border processes, which are only one part of an international supply chain process. In developed economies a regulatory Single Window based on the principle of Business to Government and Government to Government data exchange is unlikely to have a significant impact on the efficiency of national trade. The concept of a centralized Single Window operation is now being questioned. Even where the Single Window has been adapted to the situation of developing countries and emerging economies and has increased efficiency of national cross border trade, difficulties of interoperability with developed economy systems means that a new generation of supply chain data management initiatives are called for. In that light, CASSANDRA’s data pipeline can be seen as an alternative, innovative approach for the next generation Single Window. Regarding the implementation of the data pipeline, it is foreseen that whereas some of the guidelines might become obsolete, many of the lessons, for example regarding building consensus, establishing public-private collaboration and public-private governance models, dealing with the different interests of parties, as well as the potential of the Living Lab approach in these areas, remain valid.

7.5.2 Consignment Completion Point

The relationship between buyer and seller or consignor and consignee and the relationship between them and their logistics service providers who move the goods is crucial. It ensures transparency of costs, procedures and value for money along with visibility of activities in order to forecast, plan and monitor progress of the goods from seller to buyer, while managing the anticipated risks. In relation to the purchase or selection of the goods there are two critical points in the process. The first is the agreement between the buyer and seller as to the accurate description of the goods and terms under which they are to be bought and shipped, captured in the purchase order and contract of sale. The second is the completion of the consignment, in accordance with the order and contract, reflected in the packing list, shipping note or dispatch note and the transport document showing that the goods have started their journey along the supply chain. Visibility of those two crucial points by buyer and seller ensures conformity with both the contract of sale and the regulatory requirements for safety, security, admissibility and compliance (Hesketh, 2010; Overbeek et al., 2011).

The Consignment Completion Point (CCP) is the stage just before the completed consignment at either ‘house’ level (in waybill terms for a small individual consignment) or ‘master’ level (for a single, groupage or consolidated consignment) is dispatched into the international trade supply chain. At this point everything about the goods is known and agreed between the consignor and the consignee and their identity and status is known to each other. At this point the sender or consignor can confirm, electronically, with the buyer or consignee that the true packing list matches the purchase order and the contract of sale, as ordered and agreed, are about to be sent. It is similar to the prompt or dialogue box on a computer screen saying “Are you sure?” At that point the data relating to the goods and the people involved in the commercial transaction can be made available to the regulatory authorities in the country of export, transit and import – at the same time by electronic message (Hesketh, 2010).

Moving data exchange and risk checks further upstream to the CCP (or even further), as well as the chain-of-evidence/chain-of-custody philosophy, entailing that the person who packs the container must sign real-time that (s)he is accountable (and identifiable) are important trends to take into account for the design of the data pipeline. For example, according to UK legislation, large companies liable for tax
and duties already have to assign a “Senior Accounting Officer”, a person that is held responsible for the proper tax arrangements and data provisioning to HRMC. Moreover, to accommodate the CCP, the so-called “known consignor scheme” that is used in air freight may expand into sea freight as well.

7.5.3 Coordinated border management

Over time, trade procedures have become highly complex. For example, the methods of valuation are becoming more complicated (e.g. value of import is only determined after selling, during post clearance, done by integrated tax auditors). Improving coordination of border management is considered an important strategic area. Coordinated Border Management (CBM) can be defined as “a coordinated approach by border control agencies, both domestic and international, in the context of seeking greater efficiencies over managing trade and travel flows, while maintaining a balance with compliance requirements” (Aniszweski, 2009, p. 6). In his concept paper, Mr. Stefan Aniszweski (2009) of the World Customs Organization provides an overview of CBM. Instead of CBM, the term integrated border management is also used, but the World Customs Organization (WCO) aims to stress the coordination by different agencies with regards to their policies, programs, and delivery outcomes, while no single solution is preferred. Coordinated border management service delivery builds upon the two pillars of domestic border management through inter-service collaboration and inter-agency collaboration and international border management through international collaboration. At this international level, there is a trend for developing countries to increase capabilities to piggyback on data and procedures in place in other, developed, countries. To realize CBM, the private sector also needs to be fully involved. Coordinated Border Management also relates to AEOs, in the sense that the requirements for these businesses could be further streamlined through the proposed intra-service, inter-agency, and international collaboration, and it could provide a basis to coordinate the control processes. This would increase the trade facilitation advantages for trusted traders. The foundation of CBM is communication (Aniszweski, 2009). On the one hand, this can be understood as the communication needed to negotiate and establish the collaboration. On the other hand, communication can also be understood in terms of data exchange. A Single Window – or innovative adaptation thereof – could provide such information. Though no single solution for CBM is available or preferred, the following trend may strengthen coordinated border management, namely mutual recognition.

7.5.4 Mutual recognition

“Mutual recognition is a broad concept whereby an action or decision taken or an authorization that has been properly granted by one Customs administration is recognized and accepted by another Customs administration.” (WCO, 2005, p.54). Mutual recognition deals with formally recognizing and accepting procedures, data submissions, certificates, and so on. In the context of trade facilitation in general, and in support of trends like coordinated border management, the trend is towards increased mutual recognition.

One aspect that is a subject of mutual recognition is related to the trusted trader certification programmes, like the Authorized Economic Operator and C-TPAT. While countries (or a supranational body like the EU) may all define their own legal requirements for trusted traders, applying for different

105 http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/research/cbm.pdf
certificates in different countries, with different requirements, adds to the administrative burden. Mutual recognition of certificates entails that the certificates obtained in one country are also recognized in another country and the trade facilitation benefits are obtained based on only one certificate. Mutual recognition can also take the shape of agreements to rely on the control procedures and systems of other countries, so that checks that are done in Country A are not repeated in Country B. Concepts like “Import-is-Export” may be introduced based upon mutual recognition, as this would mean that checks that have taken place in the exporting country are recognized at the country of import/destination. Of course, when for example container tracking and monitoring data gives rise to extra concerns, for example e.g. door openings and re-routing are signalled, Customs at the importing side can still stop the cargo, but in principle, the Import-is-Export concept allows for faster clearance without additional inspections (Tan et al., 2011).

7.6 Conclusions and implications for CASSANDRA

This chapter has provided an overview of governmental procedures, compliance management and risk management, in particular from a Customs perspective. With the increased volumes of trade in global supply chains, there is also an unprecedented scale of (public) risks involved, and the procedures as well as the information systems supporting them, have grown to be highly complicated. The ability to handle data efficiently and swiftly has become a key element in international competitiveness, especially in international supply chains. Traders are faced with a set of duplicative and redundant reporting requirements, forms, systems, data sets, data models, and messages. Governments and trade have had to develop and maintain different systems to meet these redundant and duplicative requirements. This adds enormous costs to all parties, in terms of fiscal resources, timeliness and accuracy of data. Seamless, electronic processes between trade and Government would facilitate the submission of information for various purposes and would ensure harmonization and transparency and the creation of a level commercial playing field with the greatest predictability possible. The goal is the single submission of data and will necessitate a major rationalization of the current approach and requirements.

The concept of an international trade supply chain, web-based, seamless electronic data ‘pipeline’ concentrates on:

- the proper source of the key data required by commerce, logistics and border management agencies;
- the accurate and timely capture of that data before and during the movement of the goods from seller to buyer; and
- the secure communication of that data between selected parties.

The ‘pipeline’ concept builds on the previous ‘single window’ models aimed at regulatory convergence and the simplification and harmonization of procedures, electronic messages and data.

The primary aim is to reduce risks and increase the efficiency and security of international trade using parallel logistics and data ‘pipelines’ that are secure, credible and well managed. The objective is to eliminate redundancies and duplication in the submission of data, provide real-time supply chain visibility and create a simplified process with a standard set of data and messages that traders will use to meet government, financial and commercial requirements.
CASSANDRA will support the development to a paperless environment in trade and Customs by integrating data sources across the supply chain, starting as early as possible in the chain, preferably even before the goods are containerized and loaded on the international transport mode. By collecting more elaborate information, not only on the flow of goods but also on the structure of the chain, CASSANDRA will support and facilitate end-to-end visibility for the buyer and seller and control by Customs through the efficient sharing of information along the chain.

Various estimates suggest that the cost of trade procedures may range from 2% to 15% of the value of traded goods. It is also estimated that 77% of the administrative burden on businesses from international trade related regulation is attributed to Customs. The UK Department of Business Innovation and Skills report estimates that a 1% saving in the cost of goods traded across UK borders would be worth almost £6 billion annually in trade administration burden reduction and a 50% reduction in the administrative burden from HMRC could be worth around £370 million. Data inaccuracy among retailers and their suppliers can cost as much as 1% of total revenue. Cassandra and the pipeline present opportunities to address these issues.

In order to form the seamless, integrated, web-based data pipeline CASSANDRA will work with freight forwarders and service providers to join up a number of existing commercial software solutions already designed to provide more accurate and timely supply chain data. This will draw together more accurate data from a number of existing sources, thereby creating greater visibility and more effective risk management.

7.6.1 Risk assessment issues

Risk assessment issues to be addressed within Cassandra include:

- Can risk profiles of Customs and business be aligned? How reliably can the underlying data be received and used by government agencies and how, if at all, can discrepancies between the two approaches be solved?
- How the risk assessment tools of individual companies can be extended over the complete supply chain. This requires the development of advanced ways of system integration for risk assessment purposes between all businesses in a supply chain;
- How to integrate systems for information sharing between business and Customs and to define the contours of the required data. This requires advanced integration of data resources and information evaluation tools among the supply chain partners and government;
- How to determine reliability and trustworthiness of data, the usefulness of particular risk based approaches and risk assessment tools and the necessary arrangements and consensus between business and government on risk identification, mitigating measures and government intervention;
- Can data about the goods, the people and the logistics/location from visibility solutions be provided to Customs in real-time so they can assess risk for each consignment as the goods enter the supply chain and in transit along it, using state-of-the-art, service oriented architecture based risk engines?
7.6.2 Strategic benefits

CASSANDRA represents a long-term opportunity to potentially integrate existing commercial visibility solutions and data capture technologies thereby enhancing risk assessment and a risk-based approach for both business and government, which will facilitate Customs activities to:

1. Make customs clearance more efficient and reduce business administrative burden – so that effective targeting will allow legitimate trade to pass through unhindered;

2. Combat fraud, organized crime and terrorism and increase the safety of goods and the security of international trade – through automation of risk analysis using a wide range of information sources to identify, prioritize and manage perceived risks. It is expected that the risk and response capabilities will increase the quality and consistency of targeting, whilst meeting the minimum legal requirement of EU legislation set out within the Risk Management Framework Guidelines.

3. Improve Customs operational effectiveness and efficiency – using improved performance and management information to facilitate effective use and deployment of resources.

4. Allow Customs to meet its mandatory EU legal obligations set out within the Risk Management Framework Guidelines.

5. Improve targeting reduces the risk of complaints against business partners activities.

6. Enable a targeting and risk assessment tool that supports any cross government agenda regarding data sharing.

The aim is for a new European approach to secure international trade through voluntarily and economically beneficial contributions and participation by businesses and more timely and accurate data and intelligence provided to government. The goal is a more secure international supply chain with reduced loss and disruption and greater visibility, accountability, compliance and efficiency.
8 Technologies for supply chain visibility and security

8.1 Overview

In this chapter we take a look in supply chain visibility and security technologies and also about the future trends. Whereas the supply chain visibility technologies are the technological solutions that focus on visibility and aim to gather and disseminate the data to all the supply chain’s actors, the supply chain security technologies represents more of a technological infrastructure that must be capable of preventing threats and is therefore used for preventing, detecting and managing illegal activities that may occur.

8.1.1 Concerns and obstacles

One of the supply chain management aspects, which raises a major concern, is visibility. Visibility provides supply chain managers and other stakeholders with part of the information required to assist them in a continuous search for improvement of the supply-chain’s processes. It is argued that supply chains experience blind spots, and companies are looking for solutions that allow them to overcome these limitations. As supply chains are required to become more agile and efficient, stakeholders have to cooperate even more closely and share information. As so, information sharing becomes required across all the supply chain’s stakeholders. Examples of information the sharing of which becomes increasingly necessary are: order status, inventory data, shipment data, sales forecast, production/delivery schedules, performance and capacity metrics, among others. Information sharing is also required to occur in a transparent and agile fashion. Stakeholders require complete and accurate reports to improve their business process and, as a result, their participation in the supply chain’s efficiency improvement. Supply chain managers require event monitoring across the entire supply chain so that risks can be monitored, and events can be identified and dealt with in a timely fashion. Dynamic reconfiguration of a supply chain, as a result of some disturbance, can only occur when the supply chain managers’ have near real-time visibility of the events occurring in the supply chain. For these events to be known, information must flow across the supply chain’s stakeholders so that it can be made available in a timely fashion to the appropriate actors. However, several obstacles oppose this desired and seamless flow of data. As the information flows across different organizations and even across national boundaries, the complexity of the information sharing increases. Organizations in most cases are faced with data duplication and redundancy. The reasons can be due to the country specific regulatory and operational requirements or the interoperability on the data synchronization. Data quality and consequently the accuracy of data is a major concern. Supply chain visibility aims to have the technical and operational processes to avoid redundancies and duplication of data, in order to provide real-time supply chain visibility and have a standard set of data that all the stakeholders can use to meet their business and operational requirements.

8.1.2 Security risks in the supply chain

Supply chains are subject not only to unintended events that may disrupt them, but they are also subject to intentional acts, originated outside or inside the supply chain, aiming to benefit from, or cause, disruptions. Theft, smuggling, intellectual property violations and terrorism are only a few examples of the threats pending over supply chains. Supply chain security involves the measures and resources committed to preventing, detecting and assisting the supply chain to recover from criminal
threats. As so, supply chain security is a hot topic, even more due to recent past terrorism events, raising different concerns among different parties. While governments and customs are concerned with guaranteeing national security and reducing the risk of terrorist attacks, companies are mostly concerned with ensuring the integrity of goods, equipment and personnel. Hence arises one of the most sought-after characteristics of a modern supply chain: resilience. Resilience is a supply chain’s ability to recover from disruptions. Its main goal is to minimize the impact of disruptions so that a supply chain can recover from individual failures without coming to a halt.

Security risks arise in supply chains in three major moments: loading of trucks or other transportation means; transportation, transhipment and warehousing; and, unloading/receiving of shipments and containers. During loading of containers onto transportation means, effective measures must ensure that neither weapons, nor explosives nor other prohibited materials are introduced into containers. During transportation, the major concern is for the cargo not to be tampered with and so, the declared goods remain those, and only those, carried in the shipment. Upon unloading/receiving of a shipment, security measures ensure that no undeclared items are added to a shipment, and also that declared items are not subtracted from the cargo, as well. Security measures must ensure that only authorized personnel performs the intended operations, which guarantee that the declared goods are indeed those carried in a shipment. The evolution of supply chains into increasingly global production and supply networks increasingly expose the supply chain to further risks. The distribution of critical responsibility among carriers, freight forwarders, port authorities, among others, also contributes to increase the supply chain’s exposure to security risks. In other words, the supply chain’s evolution growingly exposes it to security risks. Another two issues that work against security in a supply chain, is not only the supply chain’s complexity, but also its intended performance and productivity. Security measures carry a cost and an overhead in performance over supply chain segments that might, occasionally be surpassed by less reliable but more productive and with higher performance alternative segments.

8.1.3 Practical implications

As the required information becomes available, supply chain managers are starting to choose partners based on reliability, punctuality and costs. Container vessels are becoming bigger, operations at ports are growing in automation (so that the human factor is decreasingly relied upon), automatic guide vehicles and container handling equipment are put into place as logistics companies pursue efficiency increase and cost reduction. Dwell times are decreasing in terminals and increasing in inland terminals and, in line with this tendency, port terminals and inland terminals are increasingly combined in shipping companies’ strategies which incorporate dwell times in their management, thus using dwell times as buffer. Shipping lines are moving towards inland in pursuit of further control over the entire supply chain. On the other hand, GPOs (Global Port Operators) are developing as a solution for big shipping companies, which seek a single focal point that can simplify their port terminal operations. Achieving appropriate visibility in face of all the changes that embody supply chain’s demand-required evolution becomes and even more complex task.

Tracing and tracking are two outcomes of properly implemented visibility. Tracking is the near real-time ability for the status and whereabouts of different items in a shipment to be inquired and known. On the other hand, tracing constitutes the ability for the past statuses and whereabouts of different items in a shipment to be known and hopefully compiled in a report. While tracking is a major tool for
attaining visibility, tracing is a very important tool to assessing and implementing security. Tracking can easily be used as an input for forecasting and dynamic reconfiguration of supply chain’s components. Customs authorities can use tracing information, to assess if a particular shipment has gone through less-secure environments, or locations, where its integrity might have been compromised. Tracing information can, therefore, be used in audits not only to assess a particular shipment’s integrity, but on a larger scale, the security of certain supply chain segments, so that transportation managers can avoid less-secure segments in favour of more reliable ones. For this reason, and due to the supply chain’s involvement of both private and public sector stakeholders, security can only be properly implemented through a collaboration of the two.

The measures employed to improve a supply-chain’s security can have a physical, or local, scale; or, a global and supply-chain wide scale. Whereas the first type of measures focus on specific processes or locations, the second type of measures focuses on interactions between different actors in the supply chain. Measures of local scale seek to restrict access to goods and areas to authorized personnel who are to perform only specific and previously foreseen tasks. Global scale measures apply to the supply-chain as a whole and provide individual actors the means to enrich and complement other actors’ measures, in pursuit of increased and collaboratively attained security.

Security and visibility are mutually entwined aspects of supply chains. Much of the tools and actions that are put in place to improve visibility assist in improving a supply chain’s security, and vice-versa.

### 8.2 Supply chain visibility technologies

Supply chain visibility technologies are the technological solutions that aim to gather and disseminate the data that allows the supply chain’s actors to know, among other information, cargo and items location, and status. These technological solutions thus facilitate communication and information sharing and comprise, and, telecommunication systems.

#### 8.2.1 Introduction to visibility systems

Visibility might be defined as distance at which an object or light can be clearly discerned. This applies to the sight usually captured with an eye or camera. Visibility in this sense can be measured in order to give unambiguous information about one dimension of conditions e.g. to aircraft pilots or truck drivers enabling them to prepare and adjust appropriate tasks.

When talking about a Visibility Platform or Visibility System (VS) the above-mentioned explanation is just partly true. The world we move in changes from being tangible, real and analogue to be intangible, abstract and digitized – the computer world. Visibility in this world might be defined as the availability of data about an activity happening somewhere in the world and data being forwarded, maybe stored in some database and transferred to a media where a human being is able to realize about procedures happened of the entity of interest.

Thus a Visibility System gives a trained employee information about business processes in order to continue processing or delivers information. When applying this system to a worldwide containerized transport system, information about purchase orders, packing lists and other fundamental data should be contained as well as transport data which could record the transfer of liability from one organization
in a supply chain to another or might periodically record the state of a container when applying smart containers.

An experienced employee might read the data and draw conclusions from data in order to start corrective actions if needed or appease customers waiting eagerly for cargo to be delivered to run a business. Hopefully we may have visibility systems that support users with alerts only when real disruptions risks occur.

VSs have a broad range of data offered, extra functionality, users, data in- and output. On top of this different software architectures to fit the needs could be employed, as well as the commercial usage, and models to add value can differ a lot. These issues make that there might be no common understanding about VSs, a common features are is presentation of commercial data (PO, LL and such) and / or transport data.

8.2.1.1 Some examples on visibility systems in use

The VS named ‘Kuehne+Nagel Logistics Information’ (KN Login for short) is owned by Kuehne+Nagel and uses a server located in Hamburg, DE. The system is used by KN employees that work with the system where necessary. Furthermore KN customers’ employees (nominated by the customers’ decision makers) work with the customers’ shipments and / or organise transportation. Every individual access can be restricted down to customers’ requirements. KN Login has an interface with the KN operational systems to transmit data directly, data is not transmitted to other systems. Functions contained are overviews over all shipments on shipment or container level, reporting using a reporting tool, online booking and exception management (deviations from original planned route maps).

Similar to K+N the freight forwarder DHL (‘Deutsche Handels Logistik’) supports an own visibility system for data capturing and information purposes. This system is threefold: a DHL-internal backbone named LOGIS is used to monitor inventory, real-time, anywhere in the world. It contains planned transport data and incoming information e.g. from carriers about transport events occurred, furthermore requirements of US and Canada customs (AMS, ACI) are created and sent to relevant authorities with this system. For eligible and registered customers an access to certain data contents is made available with a system called DHL Interactive, for everybody else involved in a DHL-driven container transport the public Tracking and Tracing enables partners to learn about single transport events.

The ‘Electronic Product Code Information Services’ (EPCIS) is an example for an off-the-shelf product to integrate data within a company or a consortium whereas each member could run an own instance. EPCIS’s can be purchased from companies as IBM and Oracle, and an open source software called Fosstrak does exist. Many of GS1 organizations host EPCIS’s for their member companies. EPCIS is a database of supply chain events. End users can access data for query purposes to retrieve data and / or can then be transmitted to other software application such as WMS. Data can be retrieved and displayed in accessing applications either real time or historical, data can be provided in any manner required by the user depending on the functionality of the accessing application i.e. Web application, email alerts, reports in any format. Data can be fed into the database by capturing application for RFID or BAR code read events, experienced programmers created events from EDI transactions reformatted for input to EPCIS. Transactional data such as BOL, UCR might be captured and linked to the event data.
In order to forward data to any other applicable software application the EPCIS accessing application ezTRACK might be used. For Alerts the accessing application epcTrackAlert™ could be used.

The Logistics Information Management Application (LIMA) is owned by Cargo Services Far East, Hong Kong, CN and Allport Limited, High St Cowley, UK and is used for information of container transports consolidated, organised and/or realised by these companies. Information is provided to customers and other involved parties. The VS exchanges data with ediTrack, a supply chain management software. The capabilities of LIMA are storing data about purchase orders and shipment information which could be broken down to individual consignments and a dashboard giving users a high level overview of current status of all customers current shipments and is accessed via a URL thus running in a browser window on a typical computer.

A VS developed within the EC-FP7-project ‘Smart CM’ is the ‘Smart CM - Neutral Layer’, owned by Descartes, Lier, BE whereas the data server is located in a Data centre in Brussels, BE. This system is used by eligible parties involved in the SmartCM project only, whereas identified owners of data forwarded access to their commercial parties. Customs has been given the right to view all data. Data input is realized from following Container Security devices and solution providers: EDC, SPC Global Track, CIMC and the partner project SICIS (see below). Data output is realized to SICIS and the SmartCM VAS plus eMail to eligible and subscribed actors such as Customs, K+N and DHL. Main functions is reception of container voyage data from CSDs and Mail forwarding of this data to eligible and subscribed individuals, Provision of container security related data via SDMF standard and interactivity with CSD providers to allow for specific procedures such as authorized opening/closing of containers. For Customs the ICS SEAP functionality is provided and a link of MRN (obtained from ENS) with container security status is programmed.

Another VS developed within a EC-FP7-project is ‘SICIS’, the ‘Shared Intermodal Container Information System’, owned by HPH with the Server located in Hong Kong, China. Users of this systems are tradelane owners based in the Netherlands and the UK, which were able to follow container movements. Data could be entered into the system by manual key-in via computer or smart phone, container terminal events are obtained by HDN or DPWorld-Southampton, CSD-data is provided by SAVI-Network, CIMC and LongSun and an interface to obtain AIS-data containing vessel position is created. Furthermore data exchange with Smart CM - Neutral Layer is established. With this data a complete voyage of a container can be visualised and milestones of certain container locations can be created for information purposes and alerts can be set in order to warn the user of the system if something (un)usual happens.

Within the ITAIDE project (‘Information Technology for Adoption and Intelligent Design for e-Government’) a VS was created and applied in different Living-Labs in the project. The single Living-Labs were related to transport of beer, paper, food and drugs and for consultancy, various IT-providers developed the systems. Apart from the consignors (brewery, paper manufacturer, food producer, pharmaceutical company) Customs and other government authorities (e.g. for tax and control reasons) used the systems in order to comply with special regulations according to products handled. Data input was given from ERP systems from consignors and asset tracking devices, data output was delivered to an EPCIS-database, back to ERP-systems, a web-based eCustoms system and a web-based Trade Monitoring System. This enabled users to track and monitor containers and packages in own ERP-systems including raising alerts, communication with customs and VAT authorities, provide an
interoperability tool for IT development and introducing a new role of European eCustoms coordinator using fixed and mobile computing devices.

8.3 Supply chain security technologies

8.3.1 Introduction

Ensuring security in the supply chain is essential for the continuity of economic activities, and therefore for the proper functioning and development of society.

There is currently a limited number of SCS solutions implemented in the different scenarios involved in the SCS. Gradually, however, the development and deployment of different methods is being undertaken. It should also be noted that there are significant differences between some scenarios and others. The knowledge required for a scenario that is part of the supply chain is very different from each other, so the detection and incidence rate may require a totally different action depending on the medium.

The technological infrastructure must be capable of preventing the threats and, if an irregularity is detected, collecting the impact that will affect the supply chain, so the management from a global perspective, for the entire supply chain, is to be able to make decisions to make known to all logistics providers the type of incident, so is possible to act accordingly. Sensor networks, identification technologies, tracking of goods and people, digital security, scanning, security devices, monitoring and surveillance, etc. all of this fields of the technology must be used for preventing, detecting and managing the possible illegal activities that may occur in the supply chain.

There are also other kinds of initiatives as the US regulation C-TPAT (Customs-Trade Partnership Against Terrorism) that builds commercial cooperation relations that enforce and enhance the security in international supply chains. Without the adequate regulations and procedures is not possible to face the challenge of the supply chain security.

We now take a look at some supply chain security technologies.

8.3.2 Container security technologies

Container security technologies are those technologies, which enable:

1. The identification of personnel authorized to load a container;
2. The storage and reporting of container/trailer identification data;
3. The detection of breaches in containers;
4. The real-time reporting of container breaches;
5. Container tracking throughout the supply chain;
6. Identification of personnel authorized to interact with, and inspect, a container; and,
7. Different critical data dissemination criteria.

The most common method for keeping unauthorized personnel from loading, interacting with, or inspecting a container, are electronic or cargo or container seals.
8.3.3 Container seals

Container seals are a means to prevent unauthorized personnel to access the inside of a container. Different solutions provide different levels of security. Indicative seals marked with a unique identifier (usually made of plastic, wire, or both) simply provide an indication if the container’s interior might have been accessed. The indicative seals are easily removed using a common wire cutter. Barrier seals provide a harder to beat means of preventing access to a container’s interior (usually needs bolt cutters or special tools to remove it). Although the most protective barriers are bolt seals with a single-use locking nuts. Neither of these solutions, however, provides any indication on when, where or by whom was the container’s interior accessed. Electronic seals, however, are much more sophisticated and provide much more capabilities. Passive RFID electronic seals simply report if they have been broken, when asked by a reader. They have a low-cost and a short-range operation. Active RFID seals, however, can log the time when they are broken; can emit a “mayday” signal thus triggering some action; and, if connected to a GPS, can also record the location where they were broken. More sophisticated solutions can even use satellite communications to report tampering, or allow container’s interior access only in pre-determined zones (e.g.: ZOCA Container Security Service). If electronic seals are not employed in a layered security infrastructure, then they will add little more value if compared to physical container seals.

8.3.4 Security Sensors

One important limitation of basic seals (either manual, barrier or electronic) is that they only detect container breaches that occur through the container’s doors. More elaborate security sensors can not only monitor the condition of cargo (e.g.: moisture, temperature, among others) but also support safe and efficient operations. Intrusion detection devices can furthermore detect additional container breaches, through mechanical, light-sensitive or infrared motion detectors. This solution is gaining increased interest as it allows for non-intrusive inspections.

8.3.5 Wide area communication

Wide area communication technologies include a series of technologies and devices, which interact only if within the range of cooperating components. Communication between sensors, or identification devices, and control centres are the first example of such technologies. The enabling of access to containers interior is another example of this technology, which is closely linked to geo-fencing. If a container is within a certain perimeter, its interior can be accessed (eventually only by authorized persons) without such access being considered a container breach. Conversely, if the container leaves a certain perimeter, out-of-route notices start to be generated, security locks and cut-off switches might be triggered in an attempt to keep cargo within designated areas.

8.3.6 Biometrics devices

Biometric devices are intended to authenticate personnel, thereby granting them access to certain services, areas, equipment or goods. In particular, they can be used to grant access to a container’s interior, to a shipping company’s staff. Examples of such biometric devices are: fingerprint scanners; hand geometry scanners; facial recognition devices; and, eye recognition devices; among others.
8.4 Other relevant supply chain technologies

Apart from solutions that are essentially focused on visibility or security, the following are solutions that, although not to an exclusive purpose, have contributed to the development of either visibility or security in the supply chain.

8.4.1 Data handling and information platforms

Many companies have been performing considerable investments on data handling platforms. Although these are not necessarily focused on security, they can provide a harness for the collection and processing of security-related data. Some of the investments done by companies reside on ERP (Enterprise Resource Planning); CRM (Customer Relationship Management); TMS (Transportation Management Systems); WMS (Warehouse Management Systems); and, MES (Manufacturing Execution Systems); among others. Equipped with all these data sources, supply chain management grows more elaborate in data analysis and so, managers become more data driven. As different systems (i.e.: data sources) proliferate in a company’s IT portfolio, the need to tap into those different systems, for the acquisition of complementing data regarding a supply chain or a shipment, motivates the creation of single points of access, which aggregate data and present it to users, with a strong focus on the user’s business domain.

8.4.1.1 SOA (Service Oriented Architectures)

A Service Oriented Architecture is a set of methodologies and principles in Software Engineering for design and developing software in form of services that can communicate and work with other systems in an interoperable form. The most fundamental unit of a Service oriented solution logic is as the name implies, the service. The interaction between services are defined by using a description language and each interaction is self-contained and loosely coupled in order to maintain their independence of any other interaction.

Service Oriented Architectures are an example of such kind of implementation that has been emerging in the supply chain management domain. By aggregating the necessary data and providing an interface, which is more adapted to different users’ focus, SOA enable an optimization of alignment between business and IT. They are designed to improve, or facilitate the visibility of data related to various supply chain aspects like: suppliers’ inventory and spare parts; in-transit shipments and returns; warehoused good and distribution centres inventory stock; among others. SOA facilitate the response to business’s need for new applications, while optimizing the effectiveness of existing software applications. This way, not only do SOA reduce application development and maintenance costs, but also they ultimately contribute for the development of business agility. By providing a business-wide-transversal viewpoint, SOA create opportunities for companies to reorganize both their organization and operational environments.

SOA, however, experience a set of rather specific or particularly relevant issues which are mostly related to their integrating and distributed nature. The development of SOA applications that rely on complex services is not easy. Data coherence must be maintained across the entire service (and aggregated systems), data updates on different systems must be properly handled and, as so, transaction management becomes a crucial concern. Testing and debugging such applications is not easy, also, not
only due to their distributed nature, but also due to the fact that production data must be appropriately
imitated as to ensure proper scaled testing of services against aimed for SLAs (Service Level Agreement)
regarding reliability and availability. Poorly controlled test-environments have been known to
contaminate production environments thus causing disturbance in business activities.

8.4.1.2 Web-based applications

E-commerce applications have been experiencing considerable development. Customers seamlessly use
e-commerce applications to purchase goods and services. Especially with goods, and driven by
competition to provide the best experience to their customers, traders feel the need to inquire
suppliers’ databases to inquire inventory and monitor production. They also need to forecast transit
times and to provide customers a mean to continuously keep track of their orders.

In the pursuit of continuous improvement, supply chains are equipped with data collecting and
processing capabilities. As so, virtualization of a whole supply chain becomes possible, and so, study and
exercise of such virtualization can have a direct and swift impact on the real world supply chain. This
gives way to simulation and advanced forecasting. Historical data can be used in simulation scenarios,
which reconfigure supply chains into optimal routes.

Cloud computing is like a virtual computer that resides somewhere in the Internet. Basically, they are
computers existent in data centres of large companies like Amazon or Google. Access to a cloud
computing resources is typically via browser and can be used for remote backup services, video
collaborative services and online software applications. One of the big advantages of the cloud
computing is it cost. Business owners instead of investing in expensive infrastructures are looking to
cloud computing because it is delivered as a service rather than a product. However, sharing highly
sensitive information in a virtual cloud environment is the biggest concerns of business management as
well as the need to have localized hardware.

Several industries are evaluating the potential and trying to capitalize the benefits that it offers.

8.4.1.3 Other applications

Other important product of technologies combination is the deployment of initiatives to pre-screen and
pre-process, or authorize, certain shipping and transportation operators. Initiatives like FAST (Free and
Secure Trade), established for the northern U.S. border with Canada, greatly facilitate international flow
of goods, without compromising the level of security. Truck drivers, are previously evaluated and
cleared. They have their biometric data collected, criminal background checked and they must pass an
interview to be entitled to be covered by the program. As a truck approaches a FAST lane, at a border
crossing, the truck and the driver’s identification is collected by an RFID reader, and as so, carrier and
driver’s data are automatically submitted to Customs authorities. RFID is therefore a vital piece of
technology in this initiative. As supply chains evolve from push to pull logistics systems control, several
similar initiatives (like CSI – Container Security Initiative; or C-TPAT – Customs Trade Partnership Against
Terrorism) are developed and deployed in order to increase the level of security associated with the
supply chain, itself, by employing pre-screened shipping origins whose security has been previously
assessed and certified. This way, a shipment’s security level can even be evaluated before arrival and
based on point-of-origin’s data. This characterizes the “elastic border” that has growingly been put into practice at different ports. The destination port expands its control over to shipment’s port of origin.

8.5 Future trends in supply chain technologies

Major trends in supply chain technologies involve the developments that further alleviate the drawback of communication technologies, develop the strengths and cost-effectiveness of terrestrial communications, and foment a wider-use of open access information sharing systems.

RFID technologies are experiencing intense research. The application of cryptographic primitives is being considered and developed as a means to minimize RFID vulnerabilities regarding security. RFID variations are also looked into as a solution for capability development. Flexible tags and conductive ink would allow for the application of RFID tags to irregular surfaces. Interoperability of active and passive tags, wherein active tags would be applied to containers and passive tags to individual items, would allow a hierarchical composition of both tags thus providing a whole new dimension and data aggregation possibility to the supply chain’s visibility. Micro sensory and chip-less tags are expected to surpass current tag’s capabilities, and “agile” RFID tags would support different protocols, thus further developing interoperability and facilitating wide-adoption without the imposition of a generally agreed upon standard, or consensus.

The combination of technologies is yet another field of study that should, through the combination of complementing capabilities from different technologies, improve overall supply chain security and visibility. If RFID tags, and electronic seals, which have the capability of detecting container breaches are combined with satellite communications devices, real-time container breach detection would be possible, across the whole supply chain. Deviation from authorized routes could be detected and shipment tampering could be deal with in a timely fashion. Different sensors can also be added to such a platform thus leading to the concept of “smart containers” whose location and contents can be monitored and inquired from end-to-end in a supply chain route. Devices and maintenance costs are still considerable and would otherwise have to be lowered which, in turn, could be facilitated by mass production and adoption.

Further development trends also encompass software. These developments are guided by three major intertwined vectors: integration, optimization, and information sharing. Further integration of trading partners of a supply chain would improve control and synchronization across disparate systems, and would also develop services integration and scheduling capabilities. This might require further development of inter-actors communication, which can even be incorporated into SOAs, themselves, in the form of voice communication primitives. Further and wider XML adoption as the de facto standard for information sharing, and its incorporation in SOAs, might completely replace EDI (Electronic Data Interchange) messaging and provide a full status visibility platform based on collected tracking and tracing information. With this, simulation can be facilitated and operator can be studied and selected even before a particular supply chain is put in motion. Simulation can also be used for dynamic reconfiguration of supply chains in search of actions to mitigate disturbances that might occur.

The major issues that difficult SOA dissemination, are not of a technical nature. Instead, they are of an institutional nature. Again, as SOA traverse entire organizations or even different organizations across
supply chains, data sharing and dissemination becomes an issue of a delicate nature. SOA applications must, therefore employ the means to properly implement appropriate confidentiality and data dissemination schemes. Voice communication features can also be added to SOA applications, thus improving actors’ interaction and thus increasing the supply chain’s agility and efficiency.

More insightful visibility of the supply chain, as enabled by SOA applications, requires data collection and processing mechanisms, with an appropriate level of detail and accuracy. Here, the concept of accuracy relates not only to the traditional accuracy that may be inferred for data such as position (where accuracy might be defined in meters, for instance) but also in temporal accuracy (where accurate data is data that is up-to-date and whose status or value does not differ from the described artefact’s current data. Such accuracy requires developments also at the middleware and device-driver levels. In a hierarchical view, these software components correspond to device brokers (which connect devices to applications so that the data from the earlier is captured by the latter); software applications (which manage device connectivity); and, application managers (which manage enterprise-level inter-application connectivity).

A good example of a system that embodies developments on most of the software development trends described above, regarding visibility and security, is the recent Finnish initiative for a national transportation telematics architecture: TelemArk. This architecture focuses mostly on the processes involved in the transportation of goods, as well as the information exchanged between those processes. The viewpoint provided is the freight. TelemArk’s objectives are:

- to provide real-time and controlled collection of data regarding location, composition and condition of items that compose and carry a shipment (e.g.: goods, parcels, transportation vehicles, among others);
- to collect and combine the above information; and,
- to disseminate efficiently, and in a timely fashion, the combined information across the partners.

In order to facilitate interaction and maintain appropriate viewpoints for different actors, TelemArk employs a roles schema, which includes roles for senders, receivers, public administration authorities, and service providers. The information exchanged across the system, comprises mostly management data, tracking data and tracing data, among others. This data relates with the process areas of the freight transportation, namely: planning, control, operations, tracking and tracing.

Another important research and development trend is motivated by security issues, in particular, non-intrusive scanning of containers. Research efforts are looking for methods that can overcome traditional x-ray and gamma-ray scanning techniques limitations. Higher spatial resolution for low attenuation materials is sought-for, and hopefully materials differentiation through elemental composition.

### 8.6 Conclusions and implications for CASSANDRA

Projects like CASSANDRA have outcomes, which might be embodied by a set of artefacts, or results, that can easily be adopted by companies and governments. On the other hand, it can also trigger discussions that might lead to the development of legislation and regulation which, in turn, also generate convergence.
Naturally, data requirements should reflect current technological limitations, but may also accommodate foreseeable near-future technological advances. In this way, any agreement draft whose discussion might be triggered by CASSANDRA’s efforts might still remain valid for the near-future, as technological advances make way for new possibilities.

Given the variety of partners that compose CASSANDRA’s consortium, the opportunity exists for agreed data requirements, formats and dissemination schemas to meet the needs of external actors. Thus, external actors will be lead to adopt an approach, which could go beyond CASSANDRA’s scope and greatly contribute for convergence. It is this convergence that might have a strong impact on advances in lowering costs and improving the capabilities of technological devices and infrastructures.

Varied partners also generate varied requirements (and views) on data dissemination and sharing. These must be clearly stated, so that they can be implemented with current technology and software solutions, or guide the development of such solution in a way that they can meet their requirements.

Currently available technology can, most probably, meet the less demanding requirements from widely adopted practices and legislation regarding visibility and security of supply chains. More stringent requirements (either in devices performance, resolution, accuracy, miniaturization, ruggedizing, among others) are usually impelled by profitability and cost-efficiency concerns. It is wide adoption of certain practices and regulations that will impel the industry to find competitive and cost-efficient solutions to meet the business domains requirements.
Standards in supply chain management

9.1 Overview

In this chapter we take a look at standards in supply chain management and their implications to CASSANDRA.

There are several different types of standards that may be relevant for CASSANDRA:

- Management standards
- Technology standards
- Data standards
- Other standards

In the following paragraphs, we take a look at each of these standard types.

9.1.1 Management standards

The International Trade and Business Process Group (TBG) provides several standards that are relevant to CASSANDRA. The purpose of the TBG is to be responsible for business and governmental business requirements and content. This is achieved by initiating developments in the areas of process analysis, best practices, and international trade procedures.

In addition to TBG, there are also several ISO standards regarding supply chain security, GS1 Global Traceability standard, Returnable Transport Item standard and OASIS. Technology standards

Relevant technology standards include eSeal standards, RFID frequency bands and air interface standards, contactless technologies standards Mifare and NFC, and standards regarding SAW Tags, Barcodes and Infrared systems.

9.1.2 Data standards

Data standardisation is required both at the national and international level. At the national level a common data dictionary is required of the maximum set of data elements required for the exchange of information to control the flow of goods through the entire trade transaction process. This involves capturing, defining, analysing, and reconciling government and commercial information requirements.

At the international level, a similar process is required and agreement must be reached regarding the common data dictionary of the maximum set of data elements required for the exchange of information.

Clearly, both of these processes are entirely inter-related, as most national data needs to be transmitted from a trading partner and/or government in one country to a similar entity in another country. It is essential, therefore, that both the national and international data standardisation processes are based on the same standard international data set.

UN/CEFACT, the World Customs Organisation and other organisations have already done much work over the past 20 years on developing tools, standards and methodologies to undertake this process.
These include the United Nations Trade Data Element Directory (UNTDED – ISO 7372). The UNTDED contains a set of standard data elements intended to facilitate interchange of data in international trade. These standard data elements can be used with any method of data interchange, either paper or electronic. They can be selected for transmission one by one or can be used within a particular system of interchange rules (as listed in the UN Trade Data Interchange Directory), e.g. UN/EDIFACT, XML, etc.

The UNTDED is the primary set of standardised data elements used in international trade. It is used in the development of the WCO Data Model, the UN Layout Key (UNLK) aligned series of trade documents and UNeDocs.

9.1.3 Other relevant standards

Other relevant standards include the World Customs Organisation Framework of Standards to Secure and Facilitate Global Trade “SAFE”, the GS1 Global Visibility Framework and several container standards.

The WCO adopted the “SAFE” in June 2005. It is an international instrument containing 17 standards that promotes security, trade facilitation, anti-corruption, and revenue collection.

The GS1 Global Visibility Framework is an integrated suite of global standards that, when used together, enables the visibility of physical assets (i.e. trade items, reusable assets, fixed assets, and work-in-process) through common ways to uniquely identify, capture and share information relating to their movement or their state.

Finally, ISO provides several standards regarding containers – container equipment data exchange, coding, identification, marking and so on.

9.2 Future trends in supply chain standardization

9.2.1 Trends in Standards Drafting

9.2.1.1 Defining Need for Standards

In order to draft standards that support enhanced supply chain security, it will be important for those executing supply chain processes and operations to be more directly involved in defining the need for standards and developing standards that meet those needs. This will increase the probability that what is developed does meet the real needs.

Global trade associations too should play an increasing role in defining needs by providing expert contribution to ISO and other global standards bodies.

9.2.1.2 Drafting Method

The “integrated approach” to drafting standards can be expected to expand as users of the standards become more involved in defining the need for standards and in their drafting. This approach is broken down into phases:

- Build awareness of the need for a new or revised standard by identifying gaps in current practices, processes and standards
- Define specific objectives in filling the identified gaps
Standards in supply chain management

- Agree on how these objectives should be met in terms of standards to be developed
- Draft the necessary standards

9.2.2 Standards Harmonisation Trends

The Integrity (FP7 Project no. 218588) and SMART-CM (FP7 Project no. 218547) projects identified various standards categories across the supply chain:

- Physical Processes standards
- Digital processes standards
- Communication Standards (software standards, documents, data sharing, e-commerce standards)
- Security standards (physical and virtual)
- Technology standards (hardware)
- Trade standards
- Standards for customs

Global supply chains do not lack standards, but they do lack harmonised standards. Existing standards have for the most part been driven by the need of individual actors such as government trade statistics, customs, government departments (such as health, agriculture, transport, safety etc.), carriers and trade associations.

Pressure to enhance supply chain performance, increase visibility and reliability, reduce costs and simplify processes will all create a collective pressure for standards that are harmonised across wherever the supply chain operates. In today’s global trade environment, supply chains operate globally, so there is demand for global harmonisation of standards. The increasing capability and availability of existing and new technologies can be expected to facilitate such harmonisation of standards.

INTEGRITY and SMART-CM also identified the progress in harmonising standards for the exchange of information between supply chain stakeholders such as shippers, carriers, forwarders, consignees, customs and other regulatory bodies – the Single Window concept.

This “Single Window” concept addresses standards for information exchange requirements, where standard exchanged information and document structures for trading, transport, insurance etc, would be combined for electronic business transactions with governmental entities.

An example of this being implemented in practice is the Dagang-Net system in Malaysia where a single system can connect all of the supply chain stakeholders as shown in Figure 9-1.
Standards in supply chain management

It will also be necessary to integrate these standards with other standards used in industry for trading with their partners. For example, as the UCR (Unique Consignment Reference) is implemented, industry will need to provide an identifier that will meet the needs of the UCR. In 2007 customs authorities in the U.K. and Australia collaborated with GS1 and some of its members to establish if the GS1 SSCC (Serial Shipping Container Code) could be used as the UCR. The outcome of those trials led to GS1 developing two further identifiers (GSIN and GINC) to meet the specific requirements of the UCR.

It is very likely that further such collaborations will occur as the needs of industry and of governments merge, driving further harmonisation.

9.2.3 Technology Trends

9.2.3.1 Technology Compatibility

Technology standards need not only be standard in how they apply technology, but also in how they themselves are applied. RFID is an excellent example of this conundrum. Air Interface Protocol (AIP) standards exist for RFID operating at multiple points in the radio spectrum but they are not interoperable. So until, and unless, agreement is reached globally on which AIP standards will be used for specific purposes such as intermodal container processing in seaport operations, then those ports will be reluctant to invest in the new technology to improve port operations. In many cases, the same applies to the data carried on the RFID device.

In this example the standards exist, but the means to implement them consistently across ports does not. The GRIFS (Global RFID Interoperability Forum for Standards), where GS1, CEN and ETSI
collaborated to identify what RFID standards were available, so provided a valuable source of information. But that alone does not initiate efforts to resolve the problem above.

But as with many other similar situations historically, industry and other supply chain stakeholders will not tolerate this anomaly forever. Eventually, the pressure to improve supply chain performance and reduce costs will force a decision on which RFID infrastructure to use in each situation.

In this example and in many other cases, it is fair to state that a broad range of technology standards are available but what we often lack are application standards through which user communities formalise agreements to minimise the options, leading to cost-effective implementations of the technologies.

9.2.4 National vs. Global Standards

Commercial and government pressures are a factor that would drive the global harmonisation of standards for identification, processes, data exchange etc. The logic behind these pressures applies equally to technology. While supply chain players will always have to comply with local/national standards, international movement of trade will continue to exert this pressure for common standards on key areas of technology that are common across countries:

- Data exchange (EDI, XML)
- Barcode
- Optical Recognition
- Security devices
- Container scanning
- Environment sensors (temperature, humidity, air pressure, accelerometer etc.)
- Network infrastructure (Wi-Fi, LAN)
- RFID Air Interface Protocols (AIP)
- Radio regulations

9.3 Conclusions and implications for CASSANDRA

Standards are the backbone of an efficient supply chain – they will not go away. But at the same time they need to be applied across the whole process. When the whole process was contained within a single country, national standards could be applied with no adverse impact on supply chain performance, security and efficiency. But where the supply chain spans multiple countries and regions, the standards need to do so too or the advantages of having standards will be lost. The use of standards by traders in supply chains cannot be enforced, so each chooses its standards. Due to competition amongst sellers/buyers, these will differ because the sellers/buyers seek for commercial advantage. Logistic service providers are faced with those different standards and adhere to them from a commercial perspective. As trade between companies becomes more and more international or even global, the standards that support such trade will have to follow suit.
Since standards mostly exist ultimately for the benefit of those who will use them, then it is essential that the users have a strong voice in the process at some point between identifying the need for a standard and the completion of its development.

While this scenario is simplistic in its explanation, it is often far from simple in implementation. Standards that affect processes are not always easy to change because the process can’t be halted for a day to implement and making the change across multiple time zones simultaneously may not always be practical. Technology standards must not only be followed, but in doing so they must not unduly impede existing users, so they can be even more difficult and time consuming to change. Therefore harmonisation will be required not only in what is standard but also in how and when the standard is implemented.

There are many standards that apply to the security and visibility in the supply chain. For the reasons outlined above, it is essential that global standards be used in the CASSANDRA project. By using global standards in the Living Labs it will increase the likelihood of the adoption of the model developed in CASSANDRA in the real world.
10 Specific lessons learned from previous related European projects

10.1 Overview

This chapter includes a deep analysis of past and parallel projects which scope in somehow could have a relevance in the development and approach of Cassandra.

First of all three projects are analysed as main influence in the Cassandra concept. They are: Integrity (Global Door-to-door Container Supply Chain Visibility), Smart-CM (Container Chain Management) and Itaide (Information Technology for Adoption and Intelligent Design of Egovernment). The analysis of Integrity project and Smart-CM focus on its approach on interoperability, container security devices and exploitation vision as long as the analysis of Itaide focus on piggy-backing and living labs approach.

This chapter takes into consideration a set of past projects as Promit, D2D, Chinos, FreightWeiser, Marnis, Komoda, Globe, M-Trade and Logsec. Projects that run in parallel with Cassandra will be also a source of knowledge for Cassandra and must be analysed in following sections. Conclusions and implications for Cassandra can be extracted from this analysis and are evaluated in this chapter to be taken into account in future stages of the project.

10.2 INTEGRITY

This is a 3-year research project intending to significantly improve the reliability and predictability of door-to-door container chains. INTEGRITY is funded by the European Commission in the 7th Framework Programme for Research & Development and liaises with several EU Directorates.

Kernel of the project is using a data pipeline and demonstrating data gained from all actors involved in start, duration and end of a container voyage collected in one system enhanced by commercial data helps business, industry and authorities to fulfill their tasks and duties towards global supply chain visibility and security. Additional basic elements are reliability and predictability in door-to-door container transport.

Demonstration is realised by developing and using the so-called Shared Intermodal Container Information System (SICIS) allowing authorised companies and authorities to access planning and status information of selected transports. Proactive planning following the Supply Chain Event Management (SCEM) approach allows to forecast problems well before they might occur. Matching logistics data with security information, e.g. from electronic seals, container security devices, and scanning equipment together with the integration of the AEO (authorised economic operator) approach allow to satisfy both the logistics industry and Customs Authorities fulfilling their duties.

10.2.1 Role of interoperability

The project INTEGRITY brought together many diverse actors from different parts of the world, EU, China and US and needed therefore a common platform where all these actors are able to deliver transport data to, and some to receive data from. Data delivered from Consolidation Centres or manufacturers about the start of a container voyage, data from CSDs from different vendors (US, CN) reporting place and status of a container, terminal events like gate-in and out messages were processed
Specific lessons learned from previous related European projects

as well as vessel data containing position of a vessel where a container observed is loaded onto. Furthermore, a data exchange with the partner project Smart-CM with the platform Neutral Layer was established on top.

Apart from this technical interoperability different companies were forced to work together meaning adoption of processes, using common wording and other aspects. This cooperation needs time until it is fully operable, but is a vital part towards common cooperation and finally success.

10.2.2 Lessons on Container Security Devices (CSDs)

CSDs are a kind of equipment, which makes the transport of a container more visible in general. Apart from the pure device attached to a container some more tasks have to be taken into account.

This on the one hand logistics of the device itself like delivery to the place where it is installed at a container, transport from a place where it is removed from a container to a maintenance site for checking, cleaning and recharging. In addition people at all sites have to be trained.

On the other hand, data gained on the device attached to the container has to be forwarded from this device to the place where data is collected. This data forwarding implies data exchange via RFID at gates installed, via cell-phone posts or in order to avoid terrestrial installations – some sort of satellite communication. Additionally from this kind of medium data must be forwarded to the database in question, in INTEGRITY this server is located in Hong Kong, China.

Taking all these needs against the additional data and visibility into account, a CSD is a valuable device to survey container transports and detect breach or delay in a very early stage of the transport while the container is still on its way. Today most times such a problem is detected when a need for the contents is already there, but due to missing information on date a container arrives or contents are lost – reaction can be taken at arrival, not earlier. This threat might lead to severe financial problems of single companies, which might be less when comparing cost for CSDs.

10.2.3 Lessons on exploitation

In the projects various ideas about how to exploit the solution in whole or partly were researched by looking on different types of business models – data, information, platform and consultancy - and applying the specialities of the project solution and the unique situation of a company running this business to gain information what type of business might be used. The different situation in China and Europe has also been taken into account. The plan says a proof-of-concept should bring more clarity on offering an attractive service, approaching the right customers and creating sufficient value with the advanced cargo data. On the other hand parts of the concept, which do not create value but are vital to run the system, which is wanted by authorities, might be run by authorities.

10.3 SMART-CM

This is a 3-year research project with the aim to

Stimulate interoperable B2B co-operation in door-to-door container transport security.
Specific lessons learned from previous related European projects

- Develop compliant application of B2B and B2A container security data solutions with international Customs operations.
- Develop a neutral approach and service platform for secure and interoperable data communications.
- Define added value services and chain visibility enabling techniques for fulfilling operational requirements of the actors in managing global container chains.
- Develop prototypes of advanced applications in global container management, such dynamic scheduling at the containers, resulting from the research and development activity of the project.
- Assess large applicability of the above-mentioned project solutions by considering costs and benefits from solution implementation in real global container chains operational environment.
- Analyze existing business models in global container chain management and operation and study e-managing business models influencing the exploitation of the project technological outcomes (services of SMART-CM platform).
- Contribute to standards development for advancing of interoperability of technologies currently applied to safe container chain management at global level and for messages exchange and process implementation between customs and actors and among actors of the global container transport industry.

SMART-CM is funded by the European Commission in the 7th Framework Programme for Research & Development and liaises with several EU Directorates.

10.3.1 The SMART-CM Platform

The development, demonstration and the after project robustness and operation of the “SMART-CM platform” is the major technological component of the project balanced concept for achieving efficient & secure door-to-door container chain management in the future.

The SMART-CM three-layer platform includes

- Information gateway: Container status information entry point from a variety of available sources, including container security devices/e-seals, other RFID infrastructure, as well as sources such as Port MIS or fleet management systems.
- Visibility (infrastructure): Utilizing web-based mapping software, it will provide a centralized tool for the visualization of the information of interest to logistics operators.
- Value added services: By exploiting the information provided by the Information Gateway and the Visibility Layer additional functionality of interest to the industrial partners will be provided in this layer.

The SMART-CM platform is split into two vertical conceptual components:

- The Neutral component collects information and generates a single verified and standardized message structure to be provided to the customs with the aim of facilitating STL implementation.
- The Logistics Business component collects information and provides a broader range of available status information potentially suitable for applications that do not share the stringent security requirements of customs operations. It is essentially a GUI to the neutral layer. It involves user
management, delta-based updates, reporting capabilities, workflow support, exception management, etc.

10.3.2 Lessons on Container Security Devices (CSDs)

See also INTEGRITY lessons. In addition, cost benefit analysis in SMART-CM identified that the short-term benefits of CSD’s are rather limited. More long-term benefits can be considerable but require structural adjustments in the logistics chain in order to capture them. The business case is strong in high value container business or specific cargo that requires careful monitoring attention (e.g. perishables, fragile parts). There is also a good potential for time sensitive high value cargo. The issues regarding the facilitation of import and export procedures for CSDs, reverse logistics of CSDs present a challenge for a full-scale implementation. Technical CSD issues such as reliability, false alarms, and satellite communication when not on top of the stack need further attention.

10.3.3 Lessons on exploitation

The governance and business model behind operating the neutral platform (with public benefits for enhanced security levels) and exploiting commercial value added services remains challenging.

10.4 ITAIDE

The EU project ITAIDE (Information Technology for Adoption and Intelligent Design of Egovernment) ran from January 2006 to December 2010. It was funded by the 6th Framework Information Society Technology (IST) Programme. The key topic of the ITAIDE project was the trade facilitation and control dilemma faced by government and how it could be addressed by means of innovative solutions (both IT and redesigned procedures). The project applied a Living Lab approach where different industry partners, operating in different sectors and countries, formed the focal organizations. The ITAIDE project ran the Beer Living Lab, Paper Living Lab, Food Living Lab, and Drug Living Lab, where the key themes in the multi-disciplinary research, next to IT design and development, were standardization (cf. Flügge, 2010; Flügge et al., 2011), interoperability (cf. Ulankiewicz et al., 2011), procedural redesign (control) (cf. Baida et al., 2008; Liu, 2010), value assessment (cf. Raus et al., 2010), and network collaboration and adoption (cf. Rukanova et al., 2007; Rukanova et al., 2009; Van Stijn et al., 2009; Raus, 2010; Van Stijn et al., 2011a). A lot of useful information about the project results can be found on the website www.itaide.org and in the book “Accelerating global supply chains with IT-innovation: ITAIDE tools and methods” (Tan et al., 2011). The key lessons learned regarding piggy backing and data pull as well as living labs - themes that are highly relevant for the CASSANDRA project - are discussed here.

10.4.1 Piggy-backing and data pull

The two key principles underpinning the ITAIDE research have been piggy-backing and data pull, for which the proofs-of-concepts have been demonstrated in the Living Labs. The piggy-backing principle focuses on the re-use of available business data and data flows in the international supply chain for different purposes than they were originally intended. In the ITAIDE project, piggybacking was first and foremost seen from a data perspective: re-using business data for control and (regulatory) compliance purposes (Rukanova et al., 2011a).
Specific lessons learned from previous related European projects

For example it was demonstrated in the Beer Living Lab, how business data from the enterprise system of Heineken could be reused for Value Added Tax, excise, and statistical purposes (Rukanova et al., 2011b). In addition, the piggy-backing principle also can be seen to include the re-use of existing control and compliance mechanisms, both as implemented in the business information systems themselves, and in a broader sense, the control mechanisms that companies already apply for their own risk management and compliance purposes (refs).

Based on the piggy-backing principle, the second principle refers to the change in information sharing from “data push” to “data pull”. Following the current legal requirements, the data are “pushed” from business to a variety of government agencies (like Customs, statistics, veterinary), through the obligatory documents and submitting data to the government information systems like the Export Control System (ECS), Import Control System, Excise Movement and Control System (EMCS), VAT Information Exchange System (VIES), etc. (Rukanova et al., 2011). Instead of this data push model, the radical transformation proposed in the ITAIDE project is the shift towards “data pull”, where the governmental agencies requiring information “pull” these from the existing enterprise systems of companies when needed. The key advantage for business is that they would not have to invest in the separate interfaces for submitting the data to the various government agencies. The key advantage for government would be that they can obtain the required data at the source – where all the data that is needed for control purposes is already available. These are the “original” data, that are not processed or aggregated to fit the form, and as such the quality of the data would be better and can be used to improve the compliance management and risk-based auditing of Customs. Data pull also enables real-time data exchange, where the data are not only available at the moment of border crossing, but at any time.

To apply the piggy-backing and data pull principles, there are many aspects to be taken into account. In comparison to the Multi-Annual Strategic Plan (MAST), which the introduction of eCustoms and Single Window for the EU (see Chapter 7), the MAST looks mostly into setting up a new information infrastructure for B2G and G2G collaboration. With the application of piggybacking and data pull, the G2G collaboration does not become less important, on the contrary when considering for example the changes in procedures and likely also in legal environments nationally as well as at the EU level (Rukanova et al., 2009; Van Stijn et al., 2009), but the focus simultaneously becomes much more on the B2B information infrastructure of the supply chain and the enterprise systems and inter-organizational supply chain systems as well as the control mechanisms already in-use (Rukanova et al., 2011). This also means a major shift towards an increased collaboration between government and business to successfully negotiate the conditions of the piggy-backing, like under which the data are shared, how the reliability of the data is guaranteed, who is responsible for which data, who owns it, who can view it, data security, and so forth. Furthermore, data standardization and interoperability are necessary conditions for the successful application of both principles and government collaboration is also seen to intensify in this area. There is no single prevailing standard at the moment, but there are trends regarding for example the convergence of the UN/CEFACT standards and the WCO standards, which are important to take into account. The following activities for successfully deployed standards have been identified in the ITAIDE research (Flügge et al., 2011, p. 198):

• “Find consensus upon global standards usage such as UN/CEFACT;
Specific lessons learned from previous related European projects

• Resolve overlying vertical standards;
• Resolve cost implications in standard deployment;
• Automate [standards] compliance monitoring; and
• Provide open, cost-free deployment of standards.”

Interoperability tools have been shown to be useful means to enable trading partners to comply to the (internationally) agreed standards in a specific situation and to enable, when needed, the local mapping of the standards to the specific situation (Ulankiewicz et al., 2011). In relation to Single Window and the data pipeline, it is important to realize that these two principles are fundamentally different from the existing SW in the sense that, when allowed by the future MCC, no transaction data has to be delivered at border-crossing. All data would reside within the companies’ databases and could be pulled at any time, when deemed relevant. Moreover, rather than having a regulatory perspective, the principles allow for a comprehensive perspective on visibility, safety, and security in the global supply chain (see also Chapter 7).

10.4.2 The Living Lab approach

The ITAIDE project applied the so-called Living Laboratory (Living Lab) approach, a research methodology that builds upon action research. The key characteristics of the Living Lab approach are (Higgins and Klein, 2011, p. 33):

• “Real-world setting, involving multiple stakeholders from multiple organizations and their interaction;
• Active role of users as co-innovators; exposing technology to the creative & destructive energies of the users; facilitating dynamics of collective action;
• Multi-disciplinary research teams actively involved in the research settings, confronted with the technical, social and political dynamics of innovation, at times even driving the agenda;
• Joint collaboration to create a desired outcome.”

In a Living Lab, public and private actors from different organizations collaborate with a multidisciplinary research team to together realize innovative solutions for the problem at hand. The Living Labs provide a real-life, experimental setting in which to develop and pilot IT innovations.

The ITAIDE project designed the Living Lab approach in such a way that each Living Lab had on the one hand the same overarching goal and vision – “solving the trade facilitation and control dilemma with the use of IT innovation” – and on the other hand, each had a particular focus (in this case, industries, namely Beer, Paper, Food, and Drug) which allowed for additional issues and contexts to be taken into account (like excise, VAT, certification, and cold-chain) next to export, transit and import, and which led to the development and piloting of alternative solutions. In each Living Lab, there were different stakeholders involved: the industry partners were the focal point and they were located in different countries. There were partial overlaps in the timing of the Living Labs in order to facilitate the feedback and learning processes. The overall research team shifted somewhat over time due to changes in personnel, but there was a substantial amount of team members that were involved in multiple Living
Specific lessons learned from previous related European projects

Labs. Again, this is important for the learning processes and to capitalize on cross-case comparison and fertilization.

During the ITAIDE project, researchers that focused on the theme of network collaboration have investigated both the Living Lab approach (as it is a relatively new approach and had not been applied in this way yet) as well as network collaboration in relation to adoption of the solution. Understanding the network of stakeholders, with their different interests and interacting in different contexts is imperative for the success of not only the Living Labs but the application of the proposed solutions in real-life as well (cf. Rukanova et al., 2007; Rukanova et al., 2009; Van Stijn et al., 2009). The Living Labs can be seen to go through several stages, from initiation – analysis – redesign (development/innovation) – pilot – evaluation during the design-time of the Living Lab (Rukanova et al., 2011b). During the initiation and coalition building, the key task is to bring the actors of the Living Lab together. It is important to be highly aware of the tensions and different interests in the stakeholder network: as one sets out to change the ways of information sharing, control, and trade facilitation in the international supply chain, the underlying business and revenue models of the stakeholders may also change. This means that new business opportunities may arise, but also that some actors may foresee challenges and obstacles. It is essential during the initiation phase to align the interests, find a common ground for collaboration, and to gain commitment, which has to be sustained throughout the other phases, where it is important to produce tangible results. We have observed that the Living Lab – through the key involvement of academics – provides a neutral ground where the real-life actors from companies and institutions are willing to set aside differences, overcome obstacles, and focus on creative cooperation to come to innovation (Tan et al., 2011). In addition to this, it has been demonstrated that a Living Lab goes beyond mere piloting. The collaboration within the Living Labs lays the foundations for collective action, focusing on network collaboration and consensus-building and adoption of the innovation afterwards (Rukanova et al., 2007; Van Stijn et al., 2009). The Living Labs can provide a solid basis for public-private partnerships, which are not only essential for the successful development of the solutions, but also are at the core of actually implementing and running them. In that case, the Living Labs will fulfil a different function, and may involve different public-private partnerships that are directed towards the investments in and exploitation of the innovation. One of the tasks in the CASSANDRA project will be to come to a public-private governance model (PPGM) for creating the right economic incentive structures and the alignment of interests of the different parties.

10.5 Other past European projects

EU has founded a number of projects devoted to trace and track container; these projects are part of the many building blocks for enhancing visibility that already exist. Cassandra enables and facilitates the combination of those existing information sources in supply chains into new and better visibility, Cassandra does not envisage the development of new tools, hardware, visibility platforms or technical solutions.

This is a list of the most relevant finished projects related to Cassandra’s scope:
10.5.1 Promit
Promoting Innovative Intermodal Freight Transport (European Commission DG TREN, FP6 Coordination Action)

End date: 2009-02-28

Promit is the European Coordination Action (CA) for intermodal freight transport. PROMIT initiated, facilitated and supported the coordination and cooperation of national and European initiatives, projects, promotion centres, technology providers, research institutes and user groups related to this more complex transport form. The strategic PROMIT objective was to contribute to a faster improvement and implementation of intermodal transport technologies and procedures and to help promoting intermodal logistics and mode shifted by creating awareness on innovations, best practices and intermodal transport opportunities for potential users as well as for politicians and for the research community.

Promit contained a collection of highlighted applications and innovative ideas applied within the intermodal supply chain from all over Europe including Switzerland, all of them are contained in the Best Practices Handbook:

http://www.promit-project.net/UploadedFiles/Deliverables/PROMIT_BPH3_April09_cp_MSR.pdf

Cassandra should consider Promit’s results and cross-check if Promit’s best practices are being taken into account in the set-up of Living labs.

10.5.2 D2D
Demonstration of an integrated management and communication system for door-to-door intermodal freight transport operations (European Commission DG TREN, FP5 RTD project)

End date: 3/1/2002

D2D demonstrated how to build and use (in a number of real cases) integrated management and communication systems for door-to-door intermodal transport chains.

These chains were also enhanced with "smart" technologies and equipment for further improvements. The aim was to show solutions that could be used by any operator (shipper/forwarder) responsible for an intermodal chain or parts of it, without having to make major changes to relevant information systems already in use. The goal was to provide a tool for managing intermodal transport chains on a European as well as on a global level and to design a supporting tracking and tracing system, which can be commercially exploited in different settings.

D2D project helped to provide cargo tracing and tracking technologies for operators, these tracing and tracking technologies constitute today one of the information sources that Cassandra has to interconnect into new and better visibility that allows the assessment of risks by business and government.
10.5.3 CHINOS

Container Handling in Intermodal Nodes – Optimal and Secure! (European Commission DG RTD, FP6 RTD project)

End Date: 2009-03-31

Chinos addressed the topic of RFID in container transport (container tags for container identification and electronic seals combining the benefits of classical bolt seals with RFID capabilities) as well as automatic damage documentation. Both stationary and mobile RFID readers were developed together with a system, which collects and stores the acquired data. Tests were performed at several terminals and inland hubs in Europe, indicating how the new technology can improve the processes within the terminals. Furthermore, a methodology was developed how to deal with new security rules and regulations for fighting against terrorism and the change of responsibilities in the chain.

Chinos has developed RFID readers in logistics and supply chain security, this technology was essentially developed for defence purposes previously, the general consensus among observers seems to be that none of these devices (RFID devices, e-seals) have a broad application, that costs are still too high, and that the visibility they generate only partially fulfils the requirements of business and customs offices alike. More specifically, most of these technologies offer visibility at the container level, and not at the cargo or consignment level.

Cassandra is not as specific as Chinos; Cassandra addresses this problem as well and integrates many different sources, combines different technologies: container tracking and localization, tamper proof sealing, container-integrated sensor technologies, statistical methods and data available on the container to provide a holistic approach. Also concerns of data security and data transmission between authorities is addressed.

10.5.4 FREIGHTWISE

Management framework for intelligent intermodal transport, FP6 RTD project

End date: 2010-04-29

Freightwise supported the modal shift of cargo flows from road to intermodal transport using road in combination with short sea shipping, inland waterways and rail. It achieved this objective by means of improved management and facilitation of information access and exchange between large and small, public and private stakeholders across all business sectors and transport modes.

Cassandra can learn from Freightwise the improvement of the management of the supply chain information flows, and technically bridges the gaps between visibility solutions in supply chains. The access to information is a key element in any competitive intermodal chain which requires some degree of interoperability between the systems of the organisations involved in the chain, but also with authorities which requires reporting functionalities e.g. customs, coast guard and bodies which provide traffic information.

Small and Medium-sized Enterprises (SME) often find the threshold for using advanced Information Technology (IT)-based management tools still too high in term of costs and necessary know-how.
Specific lessons learned from previous related European projects

Standards are too wide or inadequate for small enterprises and do not support the interaction of all parties involved. Software tools and IT-services to support the management are needed and, in this sense, Cassandra and Freightwise have similar objectives, but the activities of both projects are different, Freightwise promotes EU-policies encouraging the development of open and interoperable systems, which meet the requirements of cargo owners, transport operators and intermodal freight integrating services. The aim is to support the Commission in formulating future legislation and in developing initiatives that can provide a platform on which the industry can develop management solutions thus helping to increase the competitiveness of intermodal transport.

10.5.5 MarNIS

Maritime Navigation and Information Systems, FP6 IP Project

End date: 2008-11-03

MarNIS addressed the need for a more pro-active management regime of vessel traffic in all EU waters, there was also a recognized need to achieve this without increasing the burden placed upon the vessel itself, i.e. through increased reporting. In fact it has long been understood that the burden on the master should decrease from present day levels in order to allow the master to concentrate on the primary function, i.e. that of the safe navigation of the vessel.

Marnis aimed to:

- Improvement of safety and the protection of the environment;
- Improvement of the efficiency of maritime transport
- Improvement of efficiency and reliability of information flows;
- Develop proposals for administrative, organisational and procedural changes
- Develop proposals for new legislation

MarNIS developed a Single Window architecture for Maritime Safety, based on National Single Windows. CASSANDRA will develop an architecture for Trade & customs Single Window. The challenge is to explore the synergies between the two SW architectures.

10.5.6 KOMODA

Co-modality - towards optimised integrated chains in freight transport logistics FP7 Small or medium-scale focused research Project

End: 12/31/2009

KOMODA’s objective was to produce a roadmap, with associated action plans, to nurture an integrated e-Logistics platform by and between modes of freight transport across Europe. Such platform complied with a series of basic requirements: based in open standards, usable by any concern, able to communicate freely between existing applications and allow the integration of legacy systems and future development.
Specific lessons learned from previous related European projects

Komoda and Cassandra share the vision of a Europe wide e-logistics system supporting co-modality i.e. optimal use of the transport resources in terms of expenses and environmental impact.

10.5.7 GLOBE

Global Border Environment (GLOBE) was a Coordination and Support Action project in FP7, addressing the Integrated border Management System topic

End date: 2009-06-30

Global Border Environment (GLOBE) was a Coordination and support Action project in FP7, addressing the Integrated border Management System topic. The GLOBE project aimed to define a comprehensive framework in which an integrated global border management system must be developed to ensure security European level framework. The work covered the sea and land borders environments, with identification of people, vehicles and goods.

The goal of defining an Integrated Border Management System was achieved with the study of existing and emerging technologies and border management policies and procedures. Close involvement of end-users and institutions such as FRONTEX granted a direct way to tackle the problem of securitizing the vast and diverse borders in the EU. With a consortium of 13 partners the project finished in June 2009, after 12 months of work.

Border crossing is a part of the supply chain, chains that also include manufacturing, distribution and other core business processes. The direct involvement of governments in these chains is currently rather limited: mainly in business licensing in various countries, and in supervising border crossing traffic. Cassandra will have an impact on trade facilitation between European Member States and third countries that are in the stage of developing their business environment and international trade viability.

10.5.8 M-TRADE

Multimodal TRAnsportation supported by Egnos. Completed

End date: 2007

M-TRADE’s main goal was to explore and to promote GNSS (EGNOS / Galileo) use in the Freight Multimodal Transport market. M-TRADE developed an end-to-end solution that combines GNSS (EGNOS) with RFID and GPRS commercial-off-the-shelf components; it was demonstrated in real-life operations and evaluated in Customs and Border Control applications.

A common vision with Cassandra is that intelligent transport systems (ITS) can play a key role. Advanced solutions based on GNSS, coupled with other technologies such as RFID, can contribute towards reaching an optimal and sustainable use of resources. Services for remote localisation of cargo in all modes allow a reliable tracking of both journey and goods, thus decreasing the need for individual controls, and contributing to an efficient and safe management of supply chains.
10.5.9 LOGSEC

Development of a strategic roadmap towards a large scale demonstration project in European logistics and supply chain security

End date: March 2011

The goal of the LOGSEC project was to develop a strategic roadmap for a large scale demonstration project in European logistics and supply chain security, characterized by adequate security for the benefit of business and governments, on low time-delay and other cost implications.

There is currently a limited number of Supply Chain Security solutions implemented in the different scenarios involved in the Supply Chain Security. Gradually, however, the development and deployment of different methods is being undertaken. It should also be noted that there are significant differences between some scenarios and others.

Cassandra has to consider LOGSEC’s roadmap, and the evaluation (in general) of the different solutions actually working in the different scenarios of the supply chain involved (maritime, road, rail transport, warehouses et). LOGSEC shared with Cassandra the vision of an adequate security for the benefit of business and governments, on low time-delay and other cost implications.

10.6 Relevant parallel projects

In this section, current ongoing European projects are analysed, it is important take them into account during the development of Cassandra in order to explore the synergies between the different projects:

10.6.1 EURIDICE

European inter-disciplinary research on intelligent cargo for efficient, safe and environment-friendly logistics, FP7 collaborative project.

Ongoing project, End Date: 2011-10-31.

EURIDICE establishes the most advanced information services for freight transportation in Europe. EURIDICE goal is to build a services platform centred on the individual cargo item and on its interaction with the surrounding environment and the user, allowing cargo objects and devices to perform basic interactions on their own and to involve the users’ information systems if and when needed. Outputs of this project:

- Euridice concepts- Intelligent cargo:
  - Self-identification means
  - Context-detection, cargo relates in every moment to the surrounding environment
  - Context-based access to services
  - Automated status monitoring will allow to detect changes in the goods conditions
Specific lessons learned from previous related European projects

- Cargo will be able to act independently, e.g., alerting the logistic planner that its current position is incompatible with the planned route. This might include a degree of distributed intelligence, enabling the cargo to take autonomous decisions.

- Hardware devices associated to the cargo. Compliant devices shall be able to interact whenever they come into each other’s range, even without human intervention.

- Services provide self-contained functionality to support a broad range of logistics functions and processes. These services are easily combined with each other as well as with users’ system services, to develop customized functions and to support multi-user and multi-organization processes.

- EURIDICE platform: hosts services for the different stakeholders (operators, cargo owners, infrastructures and authorities) and different levels of functionality, from data acquisition to automated transactions, to intelligent data analysis and decisions support.

Eight pilot scenarios have been selected to test the EURIDICE infrastructure and technologies on real cases, with the aim of demonstrating the Intelligent Cargo concept and its advantages.

Cassandra and Euridice have a similar objective, both of the projects try to get a better visibility of the cargo that allows the assessment of risks by business and government, as an answer to the new global needs. But the concept is different, Cassandra does not envisage the development of new tools, hardware, visibility platforms or technical solutions, Cassandra integrates systems that already exist for information sharing between business and customs offices, and Euridice develops hardware devices associated to the cargo, devices that contribute with more valuable information for the different actors. So, for Cassandra is very important to consider Euridice outputs, as these two projects can be complementary and compatible in a single chain.

10.6.2 SECTRONIC

Security system for maritime infrastructures, ports and coastal zones. FP7 Collaborative project.

Start date: 2008-02-01, Ongoing project End date: 2012-01-31.

The SECTRONIC initiative addresses observation and protection of critical maritime infrastructures; Passenger and goods transport, Energy supply, and Port infrastructures. All accessible means of observation (offshore, onshore, air, space) of those infrastructures are exchanged via an onshore control centre.

The overall objective of SECTRONIC is to develop tomorrow’s safety and security system for the commercial maritime world. This system will provide end users with:

- A small area 24 hrs surveillance system
- Intelligent early warning security alert system
- Effective deterrence and protective measures against external threats

Both projects, Sectronic and Cassandra enhance the importance of cargo security; Cassandra investigates how to develop service-oriented architectures as a possible solution for system integration issues in container security, so Cassandra and Sectronic are also complementary projects as Sectronic
Specific lessons learned from previous related European projects

addresses specifically security in critical infrastructures. This will be another additional source of information for Cassandra development.

10.6.3 iCargo

Intelligent Cargo in Efficient and Sustainable Global Logistics Operations. FP7 Collaborative project.

Ongoing project, Start Date: Oct 2011.

The iCargo project aims at advancing and extending the use of ICT to support new logistics services that:

- Synchronize vehicle movements and logistics operations across various modes and actors to lower CO2 emissions
- Adapt to changing conditions through dynamic planning methods involving intelligent cargo, vehicle and infrastructure systems
- Combine services, resources and information from different stakeholders, taking part in an open freight management ecosystem.

To achieve these targets, iCargo will design and implement a decentralized ICT infrastructure allowing real world objects, new planning services including CO2 calculation capabilities and existing systems to co-exist and efficiently co-operate at an affordable cost for logistics stakeholders. The iCargo infrastructure will facilitate reactive decision-making and to integrate information obtained from on-going execution (all modes) into planning processes to optimize environmental performances, including real-time information about traffic and transport infrastructure conditions.

Cassandra and iCargo are parallel projects in time, both of the projects have similarities, as both combine information from different stakeholders, facilitate reactive decision-making and integrate information obtained from on-going execution (all modes), but iCargo goes further with the services and tools, planning processes to optimize environmental performances, including real-time information about traffic and transport infrastructure conditions, however Cassandra will be focussed on the availability of more and better data covering entire supply chains.

10.6.4 PROPS

Promotional platform for short sea shipping and intermodality. FP7 Collaborative project.

Start Date: 2008-07-01. FP7 Ongoing project.

The PROPS project builds on previous EU and national activities undertaken to promote and develop short sea shipping. In particular, PROPS aims to work closely with the Short Sea Promotion Centres (SPCs) to develop a workable and replicable methodology that will enhance their practical promotion activities in the fields of legislative, technical, and operational actions and to extend their operations to encompass inter-modal and co-modal transport.

Props and Cassandra cover different areas of the supply chain, but both projects try to promote and facilitate the use of the inter-modal and co-modal transport.
Both projects are complementary as they work in a different way. Props focus on the methodology enhancement and Cassandra focus on an integrated visibility of the cargo in a supply chain.

10.6.5 TRACKBOCS

Tracking and security system with built-in energy generation for containers, FP6 RTD project.

Start Date: 2009-06-01 FP6 Ongoing project.

The idea is to develop a tracking and security system with energy source and energy generation to be retrofitted in containers to enable tracking and security independently of fixed check point installations and satellite navigation systems. The supply chain will enjoy benefits from lower shrinkage and increased efficiency. The system will meet demands for increased security in the supply chain and provides location information and protection against crime. The system will increase security against terrorist attacks as it will sense and report tampering attempts before arriving to any crowded place and the container can be halted to reduce potential impacts. The aim of the project is to develop a system utilizing a combination of commercial transmitters and cell phone base stations for low power, low cost positioning. The navigation will be based on signal parameters and IDs from commercial transmitters and GSM base stations combined with information in a central data base.

Trackbocs and Cassandra will enhance the security issues related to containers transport. Trackbocs will develop a new security system that will provide new valuable data to the decision makers and Cassandra will interconnect the information come from different sources and systems to support the activity of the authorities.

10.7 Conclusions and implications for CASSANDRA

Considering research on previous projects, we could summarize the following key points that could be of use in the Cassandra project.

From the ITAIDE research:

- Context: trade control and facilitation, AEO, SW, pan-European interoperability
- Importance of embedding the research in such programmes/initiatives, also for consensus-building
- Piggy-backing and data pull
  - Further application and development/data pipeline concept and risk-based approach
  - Importance of data standardization and interoperability
- ITAIDE solutions
  - New models of government border inspections based on the System-based, Risk-based approaches and Trusted Trader concepts (e.g. Authorized Economic Operator). Active collaboration with Dutch Customs, DG-Tax & Customs and UNCEFACT.
  - Models to implement System-based approach with Piggy-Back principle (reuse business data for government control purposes) and Data-Pull principle.
Specific lessons learned from previous related European projects

- Models to implement Coordinated border management; coordinate and harmonize border controls of other inspection agencies (e.g. food/product safety)
- Determine ways how to integrate new models of government border inspections in cross-border IT innovations such as the data pipeline
- Models of public-private partnerships between customs administration, trade and IT providers to develop e-customs innovation

**Adoption:**
- Further integration of System-based approach, Trusted Trader/AEO, Coordinated Border Management in IT innovation for e-customs.
- Scale and diversity of involved and affected stakeholders
- Understanding interests and tensions in the stakeholder network
- Shifts towards extensive collaboration and public-private partnerships
- Further research needed in the Living Labs to come to blueprints

**Living Lab**
- Usefulness of the approach
- Living Lab as “neutral grounds” for creating stakeholder collaboration regarding public-private partnerships
- Set-up of the Living Labs

From the **INTEGRITY** research:

- The main goal of the project is the creation of supply chain visibility, but with some limitations, that are going to be performed in Cassandra

**Core developments**
- Methodology
- SICIS IT system: Shared Intermodal Container Information System
- Tracking and tracing of purchase orders
- Real-milestones on container level
- Messages and exception reports
- Data exchange with customs on secure status of parties and container custom status
- Data availability for analysis and risk assessment
- SICIS data interchange is focused at the container level, Cassandra can extrapolate this concept and experience to the whole supply chain level

**Cooperation with parallel initiatives, as the European Commissions’ funded INTEGRITY project and EU-China customs project SSTL (Smart and Secure Trade Lanes)**

**Concept**
Specific lessons learned from previous related European projects

- Integrity, as Cassandra, is an integration project
- Win-win situation for the “administrative world” and “logistics world” with the combination of existing technologies and new business processes together with legal and administrative agreements

From the SMART-CM research:

- Development of a Single Window interoperability platform main block of the architecture of Cassandra
  - It is a neutral an open platform
  - Promotes data exchange between public administrators and market players
- Easy access to services, just using the Single Window concept
- Collateral security benefits done in conceptual work
- Use of Smart-CM Neutral Layer visibility system

From the PROMIT research:

- Awareness on innovations, best practices and intermodal transport opportunities

From the D2D research:

- Documentation of five demonstrator business models including a description of current business processes with respect to roles, actors, responsibilities, activities, decision points, transport documents, information systems and flows.
- Re-engineered demonstrator business models describing how the future business processes may be organized and performed. The re-engineered models include the new role termed the Transport Chain Manager and a description of how the new D2D systems may be used in order to support management of the chain.

From the CHINOS research:

- Knowledge of security regulations
- Experience with RFID technology in container transport and how to implement a new system in a commercial scenario

From the FREIGHTWISE research:

- Recommendations for standardization, for a future EU policy, requirements for intermodal shift, rules, guidelines and interfaces to assist the intermodal transport actors to establish integrated intermodal chains, bridging organizational gaps.
- It brings in the intermodal business environment aspects such as security, customs, legal requirements, Tracking & Tracing, insurance, managing systems.

From the MARNIS research:
Specific lessons learned from previous related European projects

- Heavy engagement of Global bodies (e.g. IMO, WCO, UNCEFACT) and strong EU policy support (Directives, policy papers/communications).

From the KOMODA research:

- Current state of the European e-logistics: very fragmented, unevenly developed, almost inaccessible for the great number of logistics market stakeholders.
- Proposed e-logistics system and action plan to accelerate the development of the e-logistics system enabling the European Commission better co-ordination of its co-modal transport policy.
- Wide Delphi survey amongst the logistics chain stakeholders to obtain a comprehensive picture of available e-logistics applications used in transport operations, their sources, availability, functionality and use by companies.

From the GLOBE research:

- Swift, rich and integrate-able customs data sharing is needed inside EU/Schengen space.
- End user training is fundamental to assure policies are effectively applied.
- Regulations must be harmonized, better risk assessment implemented.
- Normalization of documents info contents and technology (smartcards e.g.) will ease implementation of common border systems.

From the COSI research:

- The widespread governmental responsibilities within intermodal transport were researched and appropriate knowledge could be applied within Living-Lab Europe - USA via Bremerhaven.
- The same applies to the trial using RFID-based container security devices in one tradelane from Bremen, DE to Miami, USA.

From the M-TRADE research:

- Remote asset and the tracking and tracing of goods through EGNOS Commercial Services.
- Development of an end-to-end solution, demonstration in real-life operative scenarios and evaluation of its introduction in customs and border control applications.
- Friendly service access and benefits in operations.

From the LOGSEC research:

1. Work divided into SCS Clusters, as follows: ‘A. Security awareness and risk management’; ‘B. Authentication, certification and data protection’; and ‘C. Physical transportation security and cargo monitoring’.
2. Clusters were comprehensively found to be relevant to the current and future evolution of supply chain security, and able to address the issues (gaps) raised by those public (governmental) and private industry representatives questioned.

From the TRACKBOCS research:
Specific lessons learned from previous related European projects

1. Development of a system utilizing a combination of commercial transmitters and cell phone base stations for low power, low cost positioning
11 Proposal for the CASSANDRA scope

Based on the outcomes of the previous chapters of the Compendium, following four key CASSANDRA tenets have been derived, as the main conclusions for the Compendium (note: term “CASSANDRA” refers here to the complete set of procedures and solutions delivered as the outcome of the full project):

Tenet 1. Innovative system-based and risk-based approach in the whole project – CASSANDRA project will design, implement and evaluate a set of system-based and risk-based approaches to supply chain management, based on exploitation of information and data existing in the supply chain. Multiple types of risks are included explicitly, based on the actor priorities, (indicator) data availability in the supply chain, and so forth.

Tenet 2. Open, inclusive approach in the supply chain – CASSANDRA is open for the participation of all relevant supply chain actors and public authorities, operating in a variety of supply chain systems, in terms of different supply chain configuration and typologies, start and end points, and so forth.

Tenet 3. Facilitating the implementation of governmental policies and regulations – CASSANDRA is in line with all relevant governmental policies and regulations, while proposing innovative ways to enhance trust in the supply chain, including through public-private partnerships approaches.

Tenet 4. Avoiding reinventing the wheel - CASSANDRA exploits existing data elements, standards and technologies in the supply chain to the maximum extent. CASSANDRA also takes lessons learned from previous relevant research projects seriously into consideration.

Specifics for the CASSANDRA risk-based approach to supply chain management include the following:

CASSANDRA does not exclude up-front any specific supply chain risk categories; instead, both supply chain operator and public authority concerns and requirements are taken into full consideration (WP200)

Priority will be given to those risks, which are of high relevance to all four main actor types of consortium partners with vested interests in the issue, i.e. logistics companies, cargo owners, customs administrations and police.

Prevention and detection of deliberate violations of customs enforced regulations – precise subset to be defined in WP200 – has a special priority in the project.
CASSANDRA also explores the functioning of System Based Control in supply chain environments. This includes process control, chain control and the ability to guarantee complete, reliable and qualitative data are crucial elements to materialize the trust relationship between government and business. The trust partnership builds upon the idea of governments making use of the already existing process controls in supply chains for all kinds of commercial purposes, also referred to as ‘piggy backing’. This enables a much more effective risk analysis and assessment and can be the base for facilitations like green lanes, pre-clearance and even declaration free trade, assuming a legislative framework that supports this.

CASSANDRA also explores the options for decoupling information flows and the physical flow, by pushing the decoupling point as much as possible upstream the supply chain, to the point of packing or consolidation and sharing the reliable source data information with governments as soon as possible. Then, data validation, risk assessment and trade compliance verification can be performed long before the goods physically enter the European Union, so there is time to provide additional information needs. Other administrative processes, like fiscal controls should as much as possible be pushed downstream in the supply chain, typically long after the actual border crossing, and performed on a periodic basis afterwards.

**Other specifics about CASSANDRA scope and approach** include the following:

2. CASSANDRA Pipeline approach, as introduced in Chapter 2 of the Compendium, will be exploited in the project.

3. Relevant data standards, especially UN/CEFACT and WCO data model, will be exploited in the project.

4. New technologies and standards will be proposed regarding CASSANDRA risk based approach, as necessary.

5. Updates and enhancements to governmental policies and regulations will be suggested, as necessary.
12 Disclaimer and acknowledgement

12.1 Disclaimer

Use of any knowledge, information or data contained in this document shall be at the user's sole risk. Neither the CASSANDRA Consortium nor any of its members, their officers, employees or agents accept shall be liable or responsible, in negligence or otherwise, for any loss, damage or expense whatever sustained by any person as a result of the use, in any manner or form, of any knowledge, information or data contained in this document, or due to any inaccuracy, omission or error therein contained.

The European Commission shall not in any way be liable or responsible for the use of any such knowledge, information or data, or of the consequences thereof.

12.2 Acknowledgement

This deliverable results from the CASSANDRA project, which is supported by funding 7th Framework Programme of the European Commission (FP7; SEC-2010.3.2-1) under grant agreement no. 261795. The CASSANDRA project addresses the visibility needs of business and government in the international flow of containerised cargo. It does so by developing a data-sharing concept that allows an extended assessment of risks by both business and government, thereby enabling enhanced supply chain visibility and cost-efficient and effective security enhancement. Ideas and opinions expressed by the [author(s) / reviewer(s)] do not necessarily represent those of all partners.
13 References


INTEGRITY & SMART-CM project report (2008), *Global Container Supply Chain Compendium*.


References


Additional Literature chapter 2:


Veenstra et al. (2009) Detailed User requirements Analysis, Integrity deliverable D2.1


References Chapter 3


References


Tang, O., Musa, S. “Identifying risk issues and research advancements in supply chain risk management”, Int. J. Production Economics 133 (2011) 25-34


WCO SAFE Framework of Standards, June 2007


References Chapter 6:

Ahokas, J, and Hintsa, J. (2010), Assuring Supply Chain Continuity in Industrial Supply Chains and Complying with Authorised Economical Operator AEO Europe, BIT Research Centre.


References Chapter 4, 7 and section 10.4:


