Global Container Supply Chain Compendium

Project acronym: SMART Container Chain Management

<table>
<thead>
<tr>
<th>Deliverable No. (use the number indicated on technical annex)</th>
<th>D1.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workpackage No.</td>
<td>WP1</td>
</tr>
<tr>
<td>Workpackage Title</td>
<td></td>
</tr>
<tr>
<td>New requirements and logistics services for global container management</td>
<td></td>
</tr>
<tr>
<td>Task No.</td>
<td>T1.1</td>
</tr>
<tr>
<td>Task Title</td>
<td></td>
</tr>
<tr>
<td>Global Container Supply Chain Management (jointly INTEGRITY)</td>
<td></td>
</tr>
<tr>
<td>Date of preparation of this version:</td>
<td>31/10/2008</td>
</tr>
<tr>
<td>Authors:</td>
<td></td>
</tr>
<tr>
<td>Albert Veenstra (RSM)</td>
<td></td>
</tr>
<tr>
<td>Juha Hintsa (CBRA)</td>
<td></td>
</tr>
<tr>
<td>Gerwin Zomer (TNO)</td>
<td></td>
</tr>
<tr>
<td>Status (F: final; D: draft; RD: revised draft):</td>
<td>F</td>
</tr>
<tr>
<td>File Name:</td>
<td>SMARTCM_D1.1.1_v7.docm</td>
</tr>
<tr>
<td>Version:</td>
<td>1.0</td>
</tr>
<tr>
<td>Task start date and duration</td>
<td>M1-M7</td>
</tr>
</tbody>
</table>
## Revision History

<table>
<thead>
<tr>
<th>Version No.</th>
<th>Date</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>31/10/2010</td>
<td>Final version</td>
</tr>
</tbody>
</table>
List of abbreviations

- SCM: Supply Chain Management
- JIT: Just In Time
- SCEM: Supply Chain Event Management
- LSP: Logistic Service Providers
- VMI: Vendor Manager Inventory
- EDI: Electronic Data Interchange
- SCS: Supply Chain Security
# Table of Contents

1. Supply Chain Management ........................................................................................................... 7  
   1.1 An introduction into Supply Chain Management ................................................................. 7  
      1.1.1 Supply chain management ......................................................................................... 7  
      1.1.2 Supply Chain design and structure ............................................................................ 9  
      1.1.3 Supply chain event management .............................................................................. 12  
      1.1.4 Long term trends ....................................................................................................... 14  
      1.1.5 Security .................................................................................................................... 15  
      1.1.6 Visibility .................................................................................................................. 17  
   1.2 Vulnerability and resilience ................................................................................................. 19  
   1.3 Key supply chain actors .................................................................................................... 29  
   1.4 Bottlenecks in ports and hinterland (and solutions) ....................................................... 34  

2. Supply Chain Risk Management ................................................................................................. 43  
   2.1 Conceptual framework ........................................................................................................ 43  
      2.1.1 Sources of risk ......................................................................................................... 43  
      2.1.2 Supply chain security framework .......................................................................... 45  
      2.1.3 Mitigating risk through supply chain design and structure .................................. 46  
      2.1.4 Security enhancing measures ............................................................................... 48  
      2.1.5 Vulnerability in the chain ...................................................................................... 50  
      2.1.6 Supply chain security management tools ............................................................... 53  
   2.2 Main international security programmes .......................................................................... 55  
   2.3 Comparison of security programmes and measures ......................................................... 78  
   2.4 Comparison of toolkit solutions ....................................................................................... 82  
      2.4.1 The Port of Rotterdam ISPS toolkit ....................................................................... 82  
      2.4.2 IRU security toolkit ............................................................................................... 83  
      2.4.3 Integrated logistics security toolkit ........................................................................ 84  
      2.4.4 ICC Customs security toolkit ............................................................................... 84  
      2.4.5 AIAG Automotive supply chain security toolkit .................................................. 85  
   2.5 Bottlenecks ......................................................................................................................... 85  
      2.5.1 Structural Security Bottlenecks ............................................................................ 86  
      2.5.2 Security awareness ............................................................................................... 86  
      2.5.3 Customs controls ................................................................................................. 86  
      2.5.4 Sealing .................................................................................................................. 86
2.5.5 Warehouse security ................................................................. 87
2.5.6 Loading and stuffing areas .......................................................... 87
2.5.7 Container handling in port/port security ...................................... 88
2.5.8 Personnel related security bottlenecks ........................................... 88
2.5.9 IT-Process security and information flow ....................................... 88

3. The role of Customs ............................................................................ 89
3.1 Customs’ role in the 21st century ....................................................... 89
3.2 Possible implications of changing environment for customs administrations .... 92
3.3 European Customs Regulation and Initiatives .................................. 93
3.4 Security co-operation EU with 3rd countries (US and China) .......... 96
3.5 The World Customs Organization: SAFE Framework of Standards .......... 99
3.6 Other developments: single window, UCR, data models .................... 104

4 Global SCM Technology ...................................................................... 109
4.1 Overview of supply chain management technology ........................ 109
4.1.1 Communication technologies ....................................................... 109
4.1.2 Positioning technology ................................................................. 111
4.1.3 Container security devices and eSeals .......................................... 113
4.1.4 Cargo scanning technology and scanning equipment .................... 115
4.1.5 Terminal access control technology .............................................. 116
4.2 User experiences with security technology ....................................... 119
4.3 Bottlenecks .................................................................................... 123

5 Standardisation .................................................................................. 124
5.1 Standardisation organisations .......................................................... 124
5.1.1 ISO .......................................................................................... 124
5.1.2 CEN, European Committee for standardization ............................. 125
5.2 Standards in the supply chain ............................................................ 126
5.2.1 Container Standards ................................................................. 126
5.2.2 UCR ....................................................................................... 126
5.2.3 Containers numbers standards ...................................................... 126
5.2.4 Seal standards ........................................................................... 126
5.2.5 Pallet standards ......................................................................... 127
5.2.6 Electronic standards ................................................................. 127
5.3 Bottlenecks .................................................................................... 129
5.3.1 Technology standards ............................................................... 130

5
5.3.2 Process standards ......................................................................................... 130
5.3.3 Information standards .................................................................................. 130
5.3.4 Customs standards ....................................................................................... 130
6 Emerging trends ......................................................................................................... 132
   6.1 Emerging trends in ports and hinterland ............................................................ 132
   6.2 Emerging trends in customs/ security ................................................................. 142
      6.2.1 Importance of the security in the supply chain ............................................ 142
      6.2.2 Customs Reorganisation - A dynamically evolving trend ......................... 142
      6.2.3 Security trends for the industry ................................................................. 146
      6.2.4 Conclusions ............................................................................................. 148
   6.3 Emerging trends in technology ......................................................................... 150
      6.3.1 The Container Supply Chain and Technology Applications ...................... 150
      6.3.2 Emerging Trends in Container Supply Chain Technology ......................... 155
      6.3.3 Conclusions ............................................................................................. 161
   6.4 Standardisation ................................................................................................. 164
      6.4.1 Trends related to standards drafting .......................................................... 164
      6.4.2 Trends related to Standards-Harmonization through collaboration ............ 165
7 Concluding remarks and mandate ............................................................................. 169
References ................................................................................................................ 173
1. Supply Chain Management

Information exchange in the supply chain has a long history of research and attempts to build platforms. While research shows that information exchange is beneficial for supply chain performance, in practice, very little real integral supply chain information platforms exist. The cases where they do exist, the supply chain are often managed by a single company that has a strong hierarchical relationship with other partners in the chain.

This chapter introduces some of the main concepts and issues related to business supply chains. The choices we have made are determined to what is relevant for the projects INTEGRITY and SMART-CM. We will describe supply chain structure and design issues in some detail (section 1), and focus in section 2 on vulnerabilities and resilience of supply chains. Section 3 introduces the main actors in the supply chain, while section 4 concentrates on the role of customs. We finish this chapter with bottlenecks in ports and hinterland.

1.1 An introduction into Supply Chain Management

Focus on supply chain management, and supply chain design, with an emphasis on dependencies and sources of vulnerabilities.

1.1.1 Supply chain management

A supply chain is a network of organisations that are involved, through upstream and downstream linkages, in different processes and activities that produce value in the form of products and services in the hands of ultimate consumers (Christopher, 1998). The term supply chain is a simplification of the supply web or network of suppliers, manufacturing plants, retailers, and the myriad supporting companies (Sheffi, 2005). Supply chain management identifies how supply chains should or could be managed. Becker (2001) distinguishes five scopes of supply chain management philosophy. According to him the philosophy develops from the most simple scope called functional chain awareness school (only concerning material flow in the supply chain) to most comprehensive scope – strategic network management (supply chain as strategic alliance and other co-operative relations).

Supply chain management (SCM) is the ‘integration of key business processes (customer relationship management, customer service, demand management, order fulfillment, manufacturing flow management, procurement, product development and commercialization and returns) from original supplier through to the end user that provides products, services and information that add value for customers and other stakeholders’ (Stock and Lambert, 2001). ‘SCM is the management of upstream and downstream relationships with suppliers to deliver superior customer value at less cost to the supply chain as a whole’ (Christopher, 1998). These are two of the more extensive supply chain management definitions.
Simchi Levi et al. (2000) define SCM as ‘a set of approaches utilized to efficiently integrate suppliers, manufacturers, warehouses and stores, so that merchandise is produced and distributed at the right quantities, to the right locations and at the right time in order to minimize system-wide costs while satisfying service level requirements’. This definition incorporates the hierarchy between supply chain management and logistics management. The Council of Supply Chain management defines logistic management as ‘that part of the supply chain process that plans, implements and controls the efficient, effective flow and storage of goods, services, and related information from the point-of-origin to the point-of-consumption in order to meet customer requirements’. Figure 1 illustrates this hierarchical view on supply chain management and logistics.

Figure 1.1: SCM/LM hierarchy

A third approach to viewing supply chains is the network approach. Chapman et al. (2002) argue that the term supply networks is more accurate because “modern supply chains are very complex, with many parallel physical and information flows occurring in order to ensure that products are delivered in the right quantities, to the right place in cost-effective manner.” Ferrin et al. (2001) even introduce the term matrix in this context. In their view supply takes place in a matrix environment where horizontal as well as vertical trade and relationships exist between many suppliers.

Global supply chains

The global context of supply chains is not discussed very much in the literature. In most cases, the term ‘global’ is understood to mean ‘entire’ or ‘complete’ (see for instance the book by Skjott-Larsen et al. 2007 – Managing the Global Supply Chain). Christopher (1998) argues the impact of globalisation on logistics is mainly on cost items such as inventory, materials and transportation. He identifies as main challenges the larger decision space on issues such as transport decisions, intermodality and routing.
Dornier et al. (1998) describe market - global costs - technical - and political and macroeconomic forces as the four dimensions of the globalization process in operations. This encompasses the issues raised by Christopher, but also puts emphasis on broader topics, such as politics and technology. Whybark (1997) on the other hand argues that the global dimension does not necessarily provide any new insight for operations management, but acknowledged that the international focus does help to emphasise the main bottlenecks.

1.1.2 Supply Chain design and structure

Supply chain management is much broader than only the design and structure of the supply chain, but the latter is an essential part of it. As Christopher (1998) states the decision on where to manufacture, assemble, store, tranship and consolidate can make the difference between profit and loss. The supply chain structure should determine how customer demand should be fulfilled, which customer relations should be started and what transportations should be arranged. According to Stock and Lambert (2001) the decision for the logistics structure should be based upon the desired market coverage, product characteristics and customer service objectives. To some extent this of course depends on the number of echelons and number of choices per echelon. Although Peck (2005) proposed a multi-layer framework in the context of identifying risk drivers and risk sources it is also suitable in the supply chain design and structure context. The four levels she identifies are:

- Level 1: value stream/product or process
- Level 2: assets and infrastructure dependencies
- Level 3: organisations and inter-organisational networks
- Level 4: the environment

![Figure 1.2: Multi-layered framework](source: Peck (2005))
The first level deals with the value stream, product and process. This level refers to the three flows logistics management deals with: products, information and money. The second level deals with the assets and infrastructure where the actual workflows and information flows take place. For the supply chain design and structure this layer deals with the choices of fixed assets or mobile assets providing more or less flexibility. The third relevant layer deals with the organisations and inter-organisational network. This relates to issues such as what contracts will be closed and how they will be managed. The fourth level - the environment - is also relevant because governmental restrictions could result in choosing other partners, or other countries for production, sourcing and management. The natural environment, for example, could impose natural “barriers” and influence the choice of one port over another.

The framework of Peck (2005) resembles the supply chain concept approach of Van Goor et al. (1999). The asset and infrastructure level of Peck could be compared to the logistics structure proposed by Van Goor et al., while the organisations and inter-organisations network is similar to their logistics organisation. Where Van Goor et al. (1999) separate the information and operating system these two are combined in Peck’s first level. The advantage of Peck’s multi-layer approach is that it provides a clear separation between what happens at each level and how interdependencies are created.

**Dependencies**

Dependencies focus on the interrelation in supply chains or networks where one company needs other companies in order to achieve its goals (usually customer fulfillment). These dependencies are being accelerated and increased by both business and logistic trends such as Just-In-Time, outsourcing and even globalization. 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.

The literature also recognizes that some of the existing dependencies in the supply chain are the result of adapting logistics concepts over time. Norrman and Jansson (2004) for example state that current logistics and supply chain principles have been influenced by the attempts in the past few decades, first to reduce costs, then time and quality and have lately focused on concepts of responsiveness, agility and leaness. Svensson (2004) discusses how supply chains suffer from high levels of dependencies. Vulnerability in supply chains is a direct result of these dependencies between companies’ business activities (Svensson, 2004). With this statement Svensson argues that as a result of decisions in supply chain management dependencies are created which lead to vulnerabilities. Svensson continues by stating that existing interdependencies create a necessity for co-operation between firms, in order to achieve individual and sometimes mutual goals (Svensson 2000). Spekman and Davis (2005) advocate that to trust is to accept dependence. And trust is a necessary component for co-operation between firms.

When the findings of Hammerkvist et al. (1982) and Mattsson (2000) are combined, one can distinguish the following seven types of supply chain dependencies:

- Technical
- Time
- Knowledge
Svensson (2004) divides these dependencies into three categories: time-, relationship and functional- dependence. The first, time dependence, refers to the fact that there is a chronological or sequential dependence between companies’ business activities in marketing channels (Svensson, 2002b). The second, relationship-dependence refers to other relationship factors that influence the interaction process between companies in marketing channels (Svensson 2002b). And finally, functional dependence includes technical adaptations and coordination (Svensson, 2004). With this view he extends his research of 2002b where he bases his typology of vulnerability scenarios in supply chains on only time and relationship dependencies. Svensson also replace relationship in relational dependence in his later work. His framework only based on time – and relationship dependence is displayed in figure 1.3.

![Figure 1.3: typology of vulnerability scenarios](source: Svensson (2002b))

Svensson (2002b) states that both time and relationship dependence are dependent upon the companies upstream and downstream business activities in supply chains. Svensson further explains that companies would prefer to be in the dynamic vulnerability scenario with respect to its customers, but at the same time they would prefer to be in the static vulnerability scenario with respect to their suppliers. This means supply chain optimisation is difficult to achieve. Uniqueness of the product, limited suppliers, low inbound inventory buffers and a high degree of outsourcing, cooperation, coordination are a few causes Svensson (2002b) mentions for high or low dependence. These statements again make the direct link to supply chain management. Sheffi (2005) emphasises the dependencies on infrastructure connections, such as phone lines, power lines, water lines, gas lines, rail lines, highways and ports connecting companies to
critical service suppliers and customers. Although these fall into Svensson’s functional dependency, the extensive list of Sheffi is worth mentioning because they are all too easily forgotten.

Example

The implications of the design and structure and its role in dependencies will now be discussed with lean manufacturing as an example. In the 1980s Toyota laid the foundations of the Just-In-Time (JIT) concept when it proved that major cost reduction could result from lean manufacturing. Toyota was able to reduce both inventory and the bullwhip effects (Sheffi, 2005). The concept of JIT manufacturing leads to tight supply chains operating with only a few hours’ worth of safety stock, relying on constant communication with components’ suppliers, transportation carriers, and warehousing operators to avoid parts’ stock-out (Sheffi, 2005). The JIT concept thus results in all three dependencies Svensson describes. Because of low inventory, time becomes a crucial dependency. In most cases long term contracts (with only a few suppliers) are involved in JIT supply chains leading to relationship dependencies. Finally, the network communication and coordination required for JIT results in functional dependencies.

The sources of risk that have exposed the vulnerability of JIT system are numerous. Daimler-Chrysler had to stop seven of the company’s plants across North America because their suspension parts production plant was impacted by Hurricane Floyd (Norrman and Jansson, 2004). Toyota had to stop almost all Japanese plants when their brake shoes manufacturer could not supply due to the Kobe earthquake (Sheffi, 2005). Ford had to idle manufacturing because trucks with parts were stuck at the Canadian and Mexican boarder as result of government actions after 9/11 (Sheffi, 2001). These three examples illustrate the vulnerability of such a supply chain concept. Although companies may reduce their everyday costs, they may be increasing certain long-term vulnerabilities (Sheffi, 2005).

1.1.3 Supply chain event management

Along a supply chain, various decisions are continuously being made, from the simple choice, which customer order to be processed next, to the serious question, whether to select a new supplier or to cancel an existing one (Fleischmann/Meyr, 2003). The provision of relevant information supports this decision making.

SCEM describes the fundamental business problem of disturbances and deviations caused by the outside factors, and inter-organizational process failures which result in the inability to meet the requirement of customer orders. 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. These two issues are interrelated since the software solution supports the management concept.

The main purpose of SCEM is managing exceptional events in supply chain. 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). Within the context of
supply chains, Karrer (2003) states that for any deviation between the plans and the actual outcomes, the decision makers in the supply chain have to be informed in a hierarchical sense. A prerequisite to manage these events is visibility through the operation of information technologies and information system.

The traditional enterprise planning systems respond to disturbances by generating a report after the occurrence of an exceptional event. These messages are just an announcement that something did not meet the expected target. Such messages are fairly non-discriminative, there may be many of them (too many to look at), and they often contain little information about the cause of the exception. In a supply chain context, the proper interpretation of a message often requires information from other sources to get the full picture. As conclusion, the traditional enterprise planning systems do not meet the requirement of businesses of visibility in the entire supply chain, with respect to exceptions.

Companies need a system which can monitor the events in the entire supply chain and that provides reports to all stakeholders involved. Driven by such requirement, many software suppliers, such as Tilion, Manugistics and i2, have included SCEM as part of their supply chain suite of B2B applications. Gartner, however, in their IT hype cycle for supply chain management 2006 considered supply chain event management to be around, but . More recently, SCEM has disappeared from the hype cycles altogether.

Much of the current literature describes SCEM as a software solution. However, the business concept of event management is the real basis for SCEM. Observe the following example (Otto 2003): a PC manufacturer receives a large order from a PC distributor. The order management system reads this order and creates time-phased requirements for all related activities like purchasing, assembly, and shipping. An order specific network of processes then has been created. Any deviation will lower the reliability of the supply chain to satisfy client’s needs. As a solution, the order network has to contain inventory buffers in order to avoid the downstream deviations as a result of upstream deviation from the planning (time, quality, quantity, etc).

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 processes is defined as an event and the late 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 to re-plan the milestones for the following 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 works on calculation and proposing to lower priorities of the assembly centers for further orders and give suggestions to insert time buffer in the order network for future plans related to this assembly center, and finally give suggestions to insert an extra event to identify deviations earlier.

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.
This figure combines the triggers that maybe generated by customs (on the left-hand side), with the triggers generated in the supply chain (rhs).

For customs, the event resulting in the ‘actual’ information is a declaration, based on interactions at the transaction level in the supply chain. This is compared with targets from the risk assessment process and the intelligence data gathering by customs. If there is a mismatch, this leads to the trigger of a response. The response will be one of the following data gathering events:

1. Requiring additional information,
2. Scanning the container,
3. Opening the container up and visually inspecting the contents.

In an analogue way, companies have target information that is fed by their performance standards: on time arrival, arrival in full, arrival of the right products, arrival at the right location. Actual information on milestones is compared to those targets, and mismatches will result in triggers of events. These events can be information (messages) and/or corrective action (re-routing containers, speeding up transportation, using buffers in the supply chain).

1.1.4 Long term trends

Bowersox et al. (2000) introduce ten mega-trends which, they argue, will change the face of supply chain logistics. The trends are formulated in terms of developments: from … to … They are:

1. From customer service to relationship management
2. From adverserial to collaborative
3. From forecast to endcast
4. From experience to transition strategy
5. From absolute to relative value
6. From functional to process integration
7. From vertical to virtual integration
8. From information hoarding to sharing
9. From training to knowledge based learning
10. From managerial accounting to value based management

Apart from the exact meaning of these terms, at first instance, they form the perfect context for the development of supply chain visibility platforms. The trends emphasise collaboration, integration, information sharing, knowledge based operation, and individualisation of the service offering (as a result of relationship management and process integration).

Bowersox et al. (2000) also identify several risks associated to adopting these trends. These risks are:

1. Dependence on real time connectivity,
2. Shifting balance of power in the supply chain
3. Vulnerability of global operations
4. Vulnerability from strategic integration, information sharing, and technology investments.

The first of these is well known: more use of IT enlarges the dependency on the same systems to always work. The second has to do with the current balance of power between manufacturer and retailer/seller. Currently, in many chains from China, the power is with the latter party. If, however, the main first data entry is going to originate from the manufacturer, this may change the position of the retailer vis-à-vis inspection agencies, customers, and the manufacturer and other parties in the chain. The other two sources of risk are more generic: globalisation introduces risks of working more in arms-lengths processes, and increased collaboration also increases dependencies and risk related to the performance of the collaboration partners.

### 1.1.5 Security

To all the trends mentioned in the previous section, since 9/11 one more trend can be added: From laissez-faire to secure chains. This trend is enabled by a number of the other trends, such as process integration, collaboration, information sharing.

By end-to-end supply chain security management we mean the combination of all security measures – resources, processes and technologies which are installed, operated and maintained to fight against all types of supply chain crime, by preventing crime, detecting crime, and helping to recover after crime incidents back to normal operational level. By supply chain crime we mean any criminal act coming from outside or inside the supply chain which aims to benefit from and/or cause damage to existing supply chains theft, smuggling, intellectual property violations, sabotage (with blackmailing) and terrorism (with destruction) being obvious samples here where crime can be either of minor or major nature.
If a company invests in security either because of legislation or from a sense of corporate social responsibility, it can provide benefits. Although Rice Jr. and Spayd (2005) correctly point out security investments by nature do not directly increase revenues, they do tend to decrease disruption and brand/franchise destruction. Perhaps the most significant collateral benefit of investment in security is the improved ability of a firm to continue operations – supply chain security – so that it may maintain its economic livelihood in the face of significant disruption (Rice Jr. and Spayd, 2005). Motorola proves that there are firms that are able to make security investments quantifiable. Bullington (2004) reported Motorola had saved $12 Million from theft reduction in 2003. He further claimed that each dollar spent on security reduced losses by 10 dollar. However, the view of Rice Jr. and Stayd (2005) is more realistic, stating that firms deriving collateral benefits from investments in security may very well have a competitive advantage over firms that invest in security but do not do so in a way that creates collateral benefits. Furthermore supply chain security has the potential to become a competitive advantage, because at the moment it is rare and in that sense adds value to the supply chain.

According to the outcome of a PROTECT (2005c) survey, 51 percent of the interviewed companies in the Netherlands consider security as a potential competitive advantage.

![Security as competitive advantage](image.png)

**Figure 1.5: Survey question outcome**

Source: Protect (2005c)

The respondents of the questionnaire are separated into shipper and logistics service providers (LSP). The interviewees were also asked for which underlying reason they consider security a competitive advantage. 41% of the LSP’s consider crime as the main reason for the advantage. This is in glaring contrast to the shippers (10%). Both parties agree on security for both criminality and terrorism (27 versus 28%).

The way to extend security from the main company in the supply chain towards the other supply chain partners is to obtain more insight in the operational performance of
these partners, and collect more information on the security status of these partners (which programs they comply with, and what the outcome of security audits was). In particular, the continuous performance monitoring can help add more information to the data that concerns security status (which, in many cases is determined in annual or bi-annual audits).

Visibility along the chain becomes a requirement to satisfy additional information requirements stemming from security needs. It is this additional visibility that also potentially results in collateral benefits, such as the ones mentioned in Rice and Spayd (2005).

### 1.1.6 Visibility

Many logistics managers describe their transportation system as a “black hole” – shipments disappear when tendered 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.

Haywood and Peck (2004a) but also Svensson (2004) describe visibility in the supply chain beyond the first tier supplier and/or customer as an illusion. Haywood and Peck (2004b) state that companies are confronted with a fog of confusion while navigating across a featureless terrain. In this context the terrain extends beyond the first tier supplier or customer. 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). With an optical fiber supplier as an example, Sheffi (2005) illustrates how difficult it is to have visibility in the entire supply chain, since disruption can be caused by very unexpected/unforeseen participants/events. The optical cable supplier of U.S. West Communications was unable to deliver. As a result Northwest Airlines – customer of U.S. West – was unable to have their communication system up and running which resulted in grounded aircrafts. Even the KLM flights from Singapore were grounded because they were flying under a Northwest flight number. In many cases, a supply chain mapping tool is one of the first steps in achieving supply chain visibility.

Visibility is crucial for increased security in the supply chain. Agility for example cannot be achieved without increased visibility and the same applies for 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 is 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. Logistic concepts such as Vendor Managed Inventory (VMI) can only be successful when information is shared. 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. These two items will be discussed in a bit more detail.

**Known supplier/customer**

The implementation of a known supplier/customer concept can help in gaining more visibility in the supply chain. This means that the members of a supply chain are known by name to the supply chain initiator, but also that they have insight in their financial situation as well as their security enhancing measures. Sheffi (2005) mentions it as one of the ways to become resilient. The introduction of such a concept could result in a reduction in the number of members in the supply chain. This can be either because they are not accepted based on their financial state or their security measures. Another benefit is that it provides a good opportunity to perform audits.

**Traceability**

Security concerns demand a new layer of visibility in the supply chain (APL, 2003). On the one hand this is the visibility described above, on the other it deals with traceability. Smyth and Phillips (2002) mention three definitions of traceability. The most suitable for this context is that of the ISO: the ability to trace the history, application or location of an entity by means of recorded identifications (Smyth and Phillips, 2002). Traceability in the sense of supply chain security should offer the possibility to reconstruct the supply chain until that point in time and generate information to determine the degree of security. This should provide the opportunity to prove its security level and for example gain advantages for example at the border, while on the other hand it provides the shipper with the ability to check if only known members with the right security enhancing measures participate. Traceability in this sense should not be confused with Tracking and Tracing. Traceability has to do with reconstructing the supply chain and checking the history to see who actually has handled the goods. Tracking and Tracing is a service provided by logistics service providers to check where a shipment is at a specific point in time.

The agricultural-food sector, the aircraft industry, the pharmaceutical industry and the automobile industry are examples given by Wilson and Clarke (1998) of industries that have recognized the importance of traceability. Safety is the key word for justifying their efforts. For the food industry, retail products found with unacceptable bacteria levels or intolerable levels of pesticide or chemicals residues need to be quickly and completely removed from store shelves (Smyth and Phillips, 2004). This is only possible with a satisfactory administration levels. Different methods of tracing have been developed. Bartels (2005) mentions bar- coding, RFID, DNA and biometrics as methods used for traceability in the meat industry. Most traceability of meat is mandatory after the outbreak of BSE. Van Dorp (2003) illustrates a simple supply chain with ear tags or bar-coding of cattle. This is registered in a central database. In the slaughter house this information is modified and linked to the end product. Nutreco has already put such a system into practice for their fish, poultry and pig supply chains. They have an internet based warehouse which contains real-time information on the breeding, farming, processing, transport and storage of raw materials, feed and animals
(Joppen, 2003). The Nutreco CEO admits in the article that it only works because Nutreco controls most of the parts in the chain, from feed to egg or embryo to fish steak or pork chop.

That the traceability can be more difficult for a product with 10,000 components is proven by Albright’s paper on the tracing of parts in the automotive industry. U.S. car manufacturers do not have the desired level of traceability. Only engines, air bags and other safety related parts are registered by serial number. The lack of standard part numbering schemes at their suppliers is not particularly helpful. To gain more visibility and improve part quality, manufacturers would need to combine automatic data collection, data analysis tools and text recognition software to scour warranty and accident reports (Albright, 2005). Visibility and traceability are important for supply chain security but that the solutions are still being developed.

1.2 Vulnerability and resilience

While security issues in container supply chain have been well discussed and many security measurements initiatives such as C-TPAT, CSI and ISPS are well developed and valid for years, supply chain resilience as a complement to supply chain security is emerging after the disaster of September 11, 2001. Both of security and resilience are the capabilities of ports operators and hinterlands transport actors to fight against potential threats such as natural hazards or terrorist attack in the supply chain. However, security more focuses on reducing the occurrence likelihood of failures in supply chain, while resilience more focuses on eliminating the impact when failures occur. A report from RAND (www.rand.org) indicated that resilience is one of the key capabilities of modern global container supply chain. The container shipping system should be able to respond to disruptions and failures of isolated components without bringing the entire system to a grinding halt. A well organized container supply chain is resilient insofar as it is able to return to normal operating conditions quickly after the failure of one or more components. For instance, the west coast ports of United State of America locked out and the ECT labour strike at Rotterdam harbour directly disrupted the loading/unloading of containers and other activities at the terminals. Resilience in these cases can be creating backlogs at the port and delaying shipments in other ports. The more resilient the supply chain is, the quicker these backlogs will be cleared, avoiding the resulting delays.

By adapted a concept from Christopher (1998), Meijer (2007) defines container supply chain as:

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

There are two significant flows in container supply chain, physical flow and information flow. The followed figure demonstrates the process among the supply chain actors (the figure in concept states all the actors involved, however only the actors make physical flow and information flow are in the scope of our projects INTEGRITY and SMART-CM.
Both security and resilience are investigating the possible failures inside the above mentioned physical flow and information flow. These failures are called supply chain disruptions. Craighead et al., (2007) define supply chain disruptions as unplanned and unanticipated events that disrupt the normal flow of goods and materials within a supply chain. Materials/products flow and information flow are the main flows in the supply chain. Supply chain disruptions can occur in any node (such as supplier or manufacturer) and link (such as materials flow from supplier to manufacturer) of supply chains. Unplanned and unanticipated events do not occur regularly or periodically and are thus difficult to prevent.

In the literature no clean cut definition of disruptions can be found. Chapman et al. (2002) seem to be discussing disruptions in their article, when they are actually discussing sources of risk. Also Sheffi (2005) does not make a clear separation between vulnerability and disruptions. Instead of disruptions, Svensson (2002b) uses the term disturbance, which he separates into sources and categories of disturbance. He divides the sources of disturbance into a) atomistic and b) holistic. He identifies Qualitative (lack of accuracy, reliability and precision of components and material) and Quantitative (availability or volumes of inbound) as his categories of disturbance. Atomistic refers to direct sources whereas holistic results from indirect sources. Consequently he is also talking about the sources of risk discussed in the previous section.
What are the disruptions could be happened in the container supply chain?

Sheffi and Rice (2005) categorize supply chain disruptions by the matrix of disruption probability (from high to low) and consequences (from severe to light). They name the matrix as the vulnerability framework and provide several disruptions as examples to each category. The framework is based on 20 case studies among supply chain actors (i.e. shippers).

By this framework, they identify high vulnerability disruptions (high probability and severe consequence) and low vulnerability disruptions (low probability and light consequence). They advise companies to make priorities of their supply chain disruptions based on the probabilities and consequences. As their recommendation, companies should treat different supply chain disruptions in a different way.

From the more practical approach in this section, Rice Jr. and Caniato’s disruptions classification is not sufficient. A disruption in transportation for example can also be classified as disruption in supply. As the definition above states, not being able to deliver to the customer or not being able to produce are more appropriate.

The supply chain context sheds a new light on the discussion of disruptions. In a chain, a disruption in one part of the chain will almost certainly lead to other disruptions elsewhere in the chain. This proliferation effect is similar to the well known process that underlies the bullwhip effect. However, a specific supply chain strategy can do much to counter or eliminate the negative effect of local disruptions on the supply chain as a whole.

Figure 1.7: The Vulnerability Framework

Source: Sheffi and Rice (2005)
In order to find out the responses to supply chain disruptions, TNO firstly makes a distinction between terrorist acts and criminal acts. Terrorist acts have the purpose of harming the society, mainly for political reasons. In contrast, criminal acts have the purpose of economic self-interest, or can originate from frustration and aggression.

Three types of terrorist acts that may have an impact on logistics activities are defined:

- **Destructive acts**: acts aiming at the complete destruction of a supply chain node;
- **High casualty / high damage acts**: acts aiming at a high number of casualties (often combined with significant physical damages);
- **Obstruction acts**: Acts aiming at blocking transport flows, not necessarily combined with high damage and/or casualties.

Criminal acts can also be classified into different types. Here four types can be distinguished, again based on the goal of the criminal and the impact of the act on the supply chain:

- **Theft acts**: acts aiming at steeling goods, money or information
- **Vandalism acts**: acts aiming at damaging goods, equipment, or other means without a specific other goal
- **Strikes**: acts linked to personnel strikes, like blocking roads, facilities, etc.
- **Smuggling acts**: acts aiming at illegal transport of goods and/or human beings via ‘legal’ supply chains

Other causes for disruption include damage from spontaneous fire, storm, earthquakes and volcanic eruptions (which are also appearing in the vulnerability framework of Sheffi and Rice 2005).

Eventually a disruption results in some kind loss. This can be either literally the goods, or figuratively money. Harland et al. (2003) separate 5 types of losses:

- Financial
- Performance
- Physical
- Social
- Time

One does not exclude the others. A physical loss can also result in a loss of money and loss of time. Theft of cargo for example means a physical loss, but because additional goods must be produced and/or shipped it costs money as well, meaning a financial loss. If time is a critical part of the supply chain, time loss also exists. Sheffi (2005) states that many natural (and man-made) phenomena follow statistical rank-size laws (called Power law distributions) that relate the size of the phenomenon to the frequency of the disruption. He compares this Power law distribution to the well known 80/20 rule (20 percent of the disruptions will cause 80 percent of the losses). Rice Jr. and Caniato (2003) report that a selected few are actually able to quantify the loss of a disruption. One company surveyed estimated a $50 million to $100 million cost impact for each day of disruption in its supply network (Rice Jr. and Caniato, 2003). Norrman and
Jansson (2004) report that Ericsson suffered a total loss of 400 million dollar as a result of a small, five minute fire.

**Security vs. Resilience**

When observing the physical flow and information flow, what security does is to collecting and categorizing/clustering risks and thus finding out the *preventing* strategies to each category of risks. As the complement, what resilience does is to collecting and categorizing/clustering the potential failures/disruptions (which brought by the risks) and then finding out the *reacting* solutions to each categories of failures/disruptions. Notice that in order to reduce the impact of failures/disruptions, effects can be made at both before and after the occurrence of failures/disruptions. The effects made before the failures/disruptions are not the same as the preventing security. For instance, establishing and maintaining a sub-port available as a backlog to a main-port, when there is a failure/disruption occurring at the main-port, the vessels are able to continue their loading/unloading activities through the sub-port. The impact of the failure/disruption is reduced while the strategy (always a sub-port maintained as backlog to main-port) does not increase the security level of port. Resilience is especially important to container supply chain in the case that the failures/disruptions are very difficult to be prevented through out security measurements. It is because that the global container supply chain is getting more and more complicated, lean and unpredictable. In the extreme circumstances, the failures/disruptions can not be well prevented even though they will certainly occur (for example, the nature disasters).

The same as risk categorization in security, it is also necessary to identify and categorize failures/disruptions according to their impacts in order to find out the resilience strategies. Theoretically, the failures/disruptions can be categorized as different ‘modes’. Rice and Caniato (2003) describe failure modes like this: While there are many different types of risk, there are but a limited set of potential outcomes or impacts from any of the various risks. The term failure modes was used by several firms to connote this limited set of outcomes, effectively the few ways that the system could fail, regardless of the actual source of the risk. Each failure mode could be generated by different causes, but the effect on the supply chain network is nearly the same. Despite the high number of threats and possible sources of risk, the relevant failure modes are just a few, and they will probably remain the same even if new menaces appeared. The table below shows the five failure modes provided by Rice and Caniato (2003)

<table>
<thead>
<tr>
<th>Failure mode:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply</td>
<td>Delay or unavailability of materials from suppliers.</td>
</tr>
<tr>
<td>Transportation</td>
<td>Delay or unavailability of the transportation infrastructure or various modes.</td>
</tr>
<tr>
<td>Facilities</td>
<td>Delay or unavailability of plants, warehouses, office buildings, facilities used in converting products.</td>
</tr>
<tr>
<td>Communications</td>
<td>Delay or unavailability of the information and communication infrastructure.</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Delay, loss or unavailability of human resources to continue operations.</td>
</tr>
</tbody>
</table>

*Figure 1.8: Failure modes in supply chains*
Instead of looking at security threats and relating them to possible supply chain vulnerabilities, the failure mode approach starts at the direct span of control and responsibilities of the manager. That is, the logistics manager is responsible for continuity, and an efficient and effective functioning of (his part of) the supply chain. The failure modes are the mean threat for his objectives. The failure modes are further discussed as:

- **Disruption in supply**
  Supply chain disruptions can result in a delay or unavailability in the supply of raw materials and spare parts from suppliers. This failure mode is particularly relevant to the companies relying on rare raw materials or spare parts; the companies rely on a supplier who has unique technology; and the companies operate on a lean supply/just in time base. The possible causes include breakdown of suppliers’ operations; exhaustion, monopoly or boycott in certain raw materials or spare parts; and also bankruptcy or merger & acquisition of suppliers, etc. Companies that use single sourcing are normally more vulnerable than those use multiple sourcing.

- **Disruption in transportation**
  Supply chain disruptions can result in a delay or unavailability of the transportation of raw materials, spare parts and completed products. In particular, companies that rely on international shipments are more exposed to this failure mode. (International) transportations are threatened by natural hazards such as storms, hurricanes, tsunamis and earthquakes; uncertain (import/export) regulation between countries such as the import/export quota between EU and China; terrorism attack and the responding actions by government such as 9/11 terrorism attack and blockage of ports, coasts and closure of national borders.

- **Disruption in production (internal)**
  Supply chain disruptions can result in a delay or unavailability of plants, warehouses, office buildings, facilities/machines used in converting products. This failure mode is most relevant to companies that own high value assets and run manufacturing activities. Companies’ productions can fail due to an on-site disruption (for example, a fire at the plant), a disruption at a supplier or a disruption in transportation processes. Compared to the first two failure modes, the failure in production could be the consequence of the failure in supply or transportation. It is especially true to manufacturing companies that operate just-in-time or have a single transport mode/route.

- **Disruption in communication/information system**
  Supply chain disruptions can result in a delay or unavailability of the communication and the information system. Besides physical goods flow (raw materials and completed products), information flow is also important in a supply chain. The development of internet technologies has resulted in many new patterns of business (such as e-commerce and Electronic Data Interchange/XML). Information flows and information systems play a critical role to companies that rely on electronic communication and transactions. Adopting/switching to a new information system (such as an advanced ERP system or WMS software) can disturb the existing operation of companies.
Computer viruses can lead to loss of critical information/data or damage of the information system. In 2007 Coca-Cola Netherlands introduced a new ICT-system. After that a problem arises with the physical distribution of goods. During picking and sorting errors occur and as a result wrong orders arrived at customer. Coca-Cola Netherlands made use of other production plants in Antwerp, Gent and Dunkerken to overcome the large demand of Coca-Cola, Fanta and Sprite (www.logistiek.nl, 2007).

- **Disruption in human resource**

Supply chain disruptions can result in a delay, loss or unavailability of human resources to continue operations. The most common failure in human resource is labour strike. Labour strikes can occur at suppliers, logistics service providers, manufacturers, distributors or retailers. One other failure in human resources is unavailability (temporary or permanent) of key personnel, who has specialized knowledge/skills or critical networks/relationships, due to illness or quit/retirement. This is especially true to companies that have intensive labour work or rely on the skilled labours that are rare/short in the labour market.

**Analysis of Failure Modes**

For each failure mode a number of causes can be defined. These can be of a terrorist, a criminal, or another origin. Terrorism is thus not the only concern for the supply chain: businesses are worried also from other sources of risk, like natural disasters, thefts, strikes, utility failures, cyber attacks, bankruptcies, etc. (Sheffi et al., 2003; Chapman et al., 2003).

Without the aim of offering a complete picture but rather with the intention of offering a baseline for further research and analysis within the project an inventory has been done based on practical supply chain expertise of TNO together with Buck Consultants International, also using the information gathered during the SIT project (European Commission, 2003-2004). The starting point for this inventory was the MIT report as mentioned earlier.

- **Causes for supply chain disruptions**

Based on previous research projects, TNO provides a list as demonstration to possible causes for supply chain failure.

**Causes of Disruption in Supply**

- Sabotage of raw material inputs (e.g. food industry)
- Customs control delays
- Fire, explosion or natural disaster at plant of a supplier
- Blocked main transport infrastructure nodes
- Supply disruption because of bad product quality and unclear product origin
- Strikes
Causes of Disruption in Transport

- Theft of goods at supplier DC, or at infrastructure node
- Supply disruption due to manipulated/destroyed information systems

- Theft of trucks or cargo from trucks during transportation
- On purpose manipulation of goods during transportation
- Physical blocking of transportation (borders, road/rail blockage, etc.)
- Sabotage of transport equipment / vehicles
- Bombing or other planned destruction of vehicle, train, plane, etc.
- Weather or other natural events causing delays
- Smuggling of illegal goods together with normal freight flows
- Manipulation of goods during transport (e.g. cold chain disruption)

Causes of Disruption in production (internal)

- Bombing or other planned destruction of production facility
- Sabotage of production equipment
- Fire or other natural disaster at plant
- Energy supply shortage
- Theft of goods from production plant
- Production disruption due to manipulated/destroyed information systems

Causes of Disruption in communication

- Systems failure of ERP, WMS, TMS, etc. systems
- Cyber attack aiming at theft or manipulation of data
- Cyber attack aiming at destruction of system
Causes of Disruption in human resource

- Strikes
- Direct attack at personnel at a facility
- Personnel suffering from attack or disaster in a region (e.g. SARS)

**Creating resilient supply chains**

Christopher and Peck (2003) suggest creating resilience by better managing supply chain risks. They categorize supply chain risks as supply risk, process risk, demand risk, control risk and environmental risk. Supply risk relates to potential or actual disturbances to the flow of product or information upstream of the focal firm. Demand risk is the downstream equivalent of supply risk. Supply risk and demand risk are external to the focal company but internal to the supply chain. Process risk relates to disruptions in product conversion and value addition. Control risk arises from the application or misapplication of rules, procedures or management systems. Process risk and control risk are internal to the focal company. Environmental risk concerns the events outside the scope of the supply chain such as natural disasters, governmental policy and economic regression. They indicate that a resilient supply chain considers risk reduction and business continuity as one of the most significant management objectives. A conceptual framework ‘creating the resilient supply chain’ is provided to minimize the five supply chain risks.

![Conceptual framework](image)

Figure 1.9: Conceptual framework
Adapted from Christopher and Peck (2003)

Supply chains are normally designed to minimize cost or maximize/optimize customer service, rarely to minimize risk. The framework shows four factors toward resilient supply chains.
This framework advocates creating resilient supply chains by categorizing, assessing and managing supply chain risks. It indicates what companies can do to reduce supply chain risks from suppliers, customers, environment and internal to the companies.

- **Responses to supply chain disruptions**

Again, based on the previous research projects, TNO provides a list namely responses to supply chain disruptions which identified supply chain failure modes, actions/responses from supply chain perspective,

<table>
<thead>
<tr>
<th>Failure Mode</th>
<th>Actions / measures</th>
<th>Preventive</th>
<th>Reactive</th>
<th>Main advantage from Supply chain perspective</th>
<th>Main disadvantage from Supply chain perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disruption in Supply</td>
<td>Multiple sourcing x</td>
<td>Spreads risks over multiple sources</td>
<td>Higher supplier management costs; lower economies of scale in purchasing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Single sourcing x</td>
<td>100% guarantee no ‘b Frosty’ product is produced</td>
<td>No delivery to customers could mean loss of market share on longer term</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stop production until product is guaranteed again x</td>
<td>100% guarantee no ‘b Frosty’ product is produced anymore</td>
<td>No delivery to customers could mean loss of market share on longer term</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Strict control at facilities (CCTV, entry control, etc.) x</td>
<td>High prevention effect</td>
<td>High investments</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IT-systems redundancy in the chain x</td>
<td>Supply chain remains ‘running’ in case of an event</td>
<td>High cost of setting up and maintaining redundant systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Large emergency stocks at suppliers x</td>
<td>Supply chain can be fed with supplies for some time after event has occurred</td>
<td>High chain inventory costs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Seapling with industry peers x</td>
<td>Supply chain can be fed with supplies Long-term trustworthy partners</td>
<td>Premium price to be paid</td>
<td>Reduced flexibility in procurement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Certification of ‘known’ suppliers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disruption in Transportation</td>
<td>Container, truck seals (electronic, smart) x</td>
<td>Prevention effect</td>
<td>High costs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Container, truck alarm systems x x</td>
<td>Prevention effect</td>
<td>High costs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Multiple mode and multiple carrier strategy x</td>
<td>Flexibility in transport routing</td>
<td>High (transport management) costs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spot market use in case of disruption in capacity x x</td>
<td>Flexibility in transport routing</td>
<td>Reduced control over partners used</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Single carrier strategy x</td>
<td>Long term, trustworthy, partnership</td>
<td>Reduced flexibility</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Safety stocks close to plant (raw materials) or market finished product)</td>
<td>Plant or customer can be supplied for some time in case of an event</td>
<td>High chain inventory cost of an event</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Training and awareness programs for staff x</td>
<td>Prevention and fast reaction effect</td>
<td>Cost inefficiency of setting up these programs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 1.10: Responses to supply chain disruptions**

Source: TNO (2005)
Concluding remark

When looking at the failure modes and the possible causes for the various types of disruptions, one can draw the conclusion that the different failure modes are sometimes related to each other. That is due to the relationship dependence of supply chain partners. Disruptions in supply may for example lead to disruptions in transportation. Also, when looking at the total supply chain, one finds that disruptions (e.g. in transportation) of company A can lead to disruptions (e.g. in supply) of company B. In the end, this could lead to disruption in delivery to the ultimate customer.

Further research could focus on the exact identification of the causes that lead to supply chain disruptions, their relations, how they affect each other, and the extent in which a cause lead to a certain disruption. The in-depth insights gained may lead to additional research on how to make priorities and decisions in disruption management.

1.3 Key supply chain actors

A supply chain is a network of organizations that are involved, through upstream and downstream linkages, in different processes and activities that produce value in the form of products and services in the hands of ultimate consumers (Christopher, 1998). Since the emergence and development of containers in worldwide civil transportation during the second half of last century, a specific container supply chain has been formed: it is a system of containers, container vessels, container port/terminal facilities, container barges, railcars and trucks that transport cargos in discrete units around the world. In this system, the most concrete process is the physical flow performed by the shipping lines and hinterland logistics service providers. The steering and coordinating of the physical flow are technically supported by the information cluster such as freight forwarders and are regulated and standardized by oversight authorities such as governmental agencies (i.e. U.S. Department of Homeland Security) and world wide organizations (i.e. International Maritime Organization). All these actors play roles in container supply chain form a complex triple-layer system.
The activities in oversight layer has the purpose of controlling and securing cargo flows for social protection reasons. The parties in the oversight layer do not directly involve the routine container transport process. Compare with them, the actors in the are which actually make the containers moving by controlling/initiating two important flows in the container supply chain: physical flow and information flow. The following figure demonstrates the container supply chain process and the two important flows.

There are varies actors play roles in the container supply chain. In practice some big companies such as big shipping lines (i.e. A.P. Moller – Maersk Group) or logistics companies (DHL) play multiple roles and thus have effects/activities over several links in container supply chain. But in general, the container supply chain actors can be identified based on their activities as stated below.
Actor 1 – Shipper/exporter

The merchant (person) by whom, in whose name or on whose behalf a contract of carriage of goods has been concluded with a carrier or any party by whom, in whose name or on whose behalf the goods are actually delivered to the carrier in relation to the contract of carriage. Synonym: Consignor, Sender. The shipper (or exporter) is the party which by contract sends goods from one place to another. (PROTECT, 2005-2008)

Actor 2 – Consignee/importer

The consignee (or importer) is the party to which the goods are consigned. This might be someone else than the final recipient. (PROTECT, 2005-2008)

Actor 3 – Forwarder (merchant haulage)

The party performing the task of organizing the dispatch of goods including the necessary documentation. A forwarder can act as an agent for the shipper or the consignee. A forwarder has to arrange transport, Customs formalities, and insurance of goods during transport, etc. on behalf of a shipper or consignee. (PROTECT, 2005-2008)

Actor 4 – Shipping line agent/logistics service provider (carrier haulage)

In shipping, a shipping line agent is a corporate body with which the shipping line has an agreement to perform particular functions on behalf of the shipping line at an agreed payment. A shipping line agent is either a part of the shipping line’s organization or an independent body. (PROTECT, 2005-2008)

Actor 5 – Ship broker

(Local) representative of shipping companies. They act as an intermediary between the shipping companies and the charterer. One ship broker can represent one large shipping company or can represent different smaller shipping companies.

Actor 6 – Carrier
Carrier (road / barge / rail) that performs the on-carriage from terminal in port of discharge to consignee. (PROTECT, 2005-2008) Carrier (road / barge / rail) that performs the pre-carriage from shipper to terminal in port of loading. (PROTECT, 2005-2008) For export a container goes from a shipper thru a pre-carrier to the sea terminal. From the sea terminal the shipping line takes the container to the foreign port from where the on-carrier takes the container to the consignee. For import the roles are reversed.

- Road carrier/road hauler

Their main interest is the optimal allocation of their fleet by combining runs and preventing “empty runs”. The road carrier is the first or final link in the chain from the shipper to the receiving party and therefore it will be confronted most heavily with waiting times. Communication with the terminals is therefore essential. A number of road carriers have started various inland terminals in order to create thick and frequent flows of containers to be shipped by inland vessels and to have a full occupied road fleet. A road carrier can be a pre-carrier or an on-carrier.

- Rail operator

Operator of rail container transport. Rail operators sometimes have their own rail terminals for loading and unloading of containers onto or from the trains. A rail operator can be a pre-carrier or an on-carrier.

- Barge operator/Inland shipping operator

- Operator of inland shipping vessels. (PROTECT, 2005-2008) - The inland shipping operator is a logistic service provider focused on the broad service offering in container transport between seaports and inland terminals via inland vessels. They aim to offer frequent reliable services with large vessels between the large number of terminals in the seaport and one or more inland terminals in the hinterland, this in conjunction with pre and post transport. They seek for optimal occupancy of their vessels with full load containers. They often rent vessels and sail fixed cycles past the terminals. Fast handling of the vessels and tight tuning of loading and unloading at the seaport and the inland terminals is in the main interest of the captains. A barge operator can be a pre-carrier or an on-carrier.

**Actor 7 – Shipping line/sea carrier**
A company transporting goods over sea in a regular service. (PROTECT, 2005-2008)

Actor 8 – Terminal operator/stevedore

A party running a business of which the functions are loading, stowing and discharging vessels. The terminal operator has to perform the physical handling of the cargo, related to vessels. This means that the terminal operator has to load the goods into a vessel. The vessel, into which the goods have to be loaded, is instructed by the liner-agent. Before any loading can take place, the terminal operator has to be informed of the delivery of the goods at his gate. This is the responsibility of the forwarder: he sends the terminal operator a Pre-Arrival, announcing which pre-carrier will deliver the goods at the terminal operator's premises. The receipt of the pre-arrival is a condition for acceptance of the goods. Given the pre-arrival and the load instruction, the goods can be loaded on the vessel if it is present at the quay. A vessel is either a general cargo vessel or a container vessel and should be loaded accordingly. It is the responsibility of the forwarder to arrange for Customs clearance. (PROTECT, 2005-2008)

- Inland terminal operator

The development of an inland terminal is often related to the presence of a large shipper in the region. The ability to offer high frequency reliable services for the transport of large numbers of containers via inland shipping from and to seaports is for a shipper of main importance. Besides the inland terminal might act as a depot for storing (empty) containers and by flexibly anticipating on the timelines that shippers need their containers.

Actor 9 – Empty container depot

The place designated by the carrier where empty containers are kept in stock and received from or delivered to the container operators or merchants. (PROTECT, 2005-2008)

Actor 10 – Customs
Customs is a regulatory authority for controlling the import, export and transit of goods. Customs performs both administrative and physical controls and is primarily focused on container and bulk transport.

**Actor 11 – Regulatory authorities**

Group of organizations not directly involved in the physical process of transporting containers. These organizations have a supervisor role and (continuously) monitor the physical and/or information flow in order to detect unlawful acts that could harm the security, safety and/or reliability of the supply chain.

### 1.4 Bottlenecks in ports and hinterland (and solutions)

A bottleneck in a container supply chain can be defined as an operation (a fragment in the chain) that has the lowest effective capacity compared with other operations and thus limits the container supply chain outputs, i.e. the container supply chain can only deliver containers as fast as the slowest operation. Bottlenecks can range from physical operations, such as the limited loading/unloading facilities, to information flow and even administrative processes, such as security scanning or customs procedures and ports requirements. A container supply chain contains physical flows and information flows among actors in ports and hinterlands. Identifying bottlenecks helps to build up an efficient, secure and resilient container supply chain. The section starts describing the main bottlenecks, followed by an elaboration on the improvements necessary to overcome these bottlenecks.

**Container traffic growth and terminal capacity growth**

On average, traffic in European ports has increased by 4% a year in the last 20 years (+7% for container traffic). Traffic Asia-Europe grew by 15% a year in the last few years. Although the overall level of congestion is not as alarming as in the U.S., Asian or Russian ports, a number of European ports already find themselves in a difficult situation. All the more if one considers that a port is said to be at full capacity when 80% is used, because there is then very little scope to deal with peaks. When one looks at the prospects, between 2005 and 2011, container traffic is expected to grow by 7.8% per annum while European port capacity should increase by 4.2% a year. The table below shows the forecast container handling supply/demand balance to 2015.
Economies of scale in global shipping

The previous section already shows the strong growth in container traffic, putting pressure on the hinterland transport modes. Another development putting even more pressure on the hinterland transport system of ports is the development of bigger deepsea container vessels leading to bigger call sizes. Bigger container ships will lead to higher capacity requirements and demands in respect to port infrastructure. Currently around 140 ships with a capacity of more than 12,000 TEU (post-panamax) are ordered. The biggest challenges for shipping lines in the future, bunker costs and pollution, have led some even to envisage vessels with a capacity of 22,000 TEU that would mean huge economies of scale. The bigger ships will call only at the bigger ports, leading to more transhipment ship/ship (feeding) and therefore require more capacity and coordination in the port. But although this will already be quite a challenge for the port, the real challenge ahead is the port-hinterland connection.

Terminal efficiency and dwell times

Containers stay too long in terminals and it is mainly due to the congestion at port and its surrounding. It is often that some containers stay at the terminal for 6 to 10 days. The reason of the congestion can be:

- Not enough operating facilities (i.e. cranes, lifting truck) or storage capacity (i.e. stack ground). Lack of flexibility of the rail carrier and lack of rail cars.
- The bill of lading or other documentations of containers are missing. In these cases, the port operator and the custom do not have the information of the containers.
- In some ports such as the port of Rotterdam and the port of Antwerp, parts of the ships ‘out of window’ (can be 60%).

Working conditions in ports

<table>
<thead>
<tr>
<th>mTEUs/year</th>
<th>2005</th>
<th>2010</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>North Continent East</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capacity</td>
<td>12.95</td>
<td>21.70</td>
<td>23.80</td>
</tr>
<tr>
<td>Demand</td>
<td>11.42</td>
<td>17.06</td>
<td>23.63</td>
</tr>
<tr>
<td><strong>Utilisation</strong></td>
<td>88.2 %</td>
<td>78.6 %</td>
<td>99.3 %</td>
</tr>
<tr>
<td><strong>North Continent West</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capacity</td>
<td>24.18</td>
<td>45.64</td>
<td>51.14</td>
</tr>
<tr>
<td>Demand</td>
<td>18.52</td>
<td>25.41</td>
<td>32.89</td>
</tr>
<tr>
<td><strong>Utilisation</strong></td>
<td>76.6 %</td>
<td>55.7 %</td>
<td>64.3 %</td>
</tr>
<tr>
<td><strong>Scandinavia</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capacity</td>
<td>5.13</td>
<td>6.56</td>
<td>6.51</td>
</tr>
<tr>
<td>Demand</td>
<td>3.63</td>
<td>4.71</td>
<td>5.61</td>
</tr>
<tr>
<td><strong>Utilisation</strong></td>
<td>70.8 %</td>
<td>71.9 %</td>
<td>86.2 %</td>
</tr>
<tr>
<td><strong>East Baltic</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capacity</td>
<td>3.13</td>
<td>6.51</td>
<td>8.89</td>
</tr>
<tr>
<td>Demand</td>
<td>2.17</td>
<td>5.04</td>
<td>9.17</td>
</tr>
<tr>
<td><strong>Utilisation</strong></td>
<td>69.2 %</td>
<td>77.4 %</td>
<td>103.2 %</td>
</tr>
</tbody>
</table>

*Source: Ocean Shipping Consultants*

*Figure 1.13: Forecast Container Handling Supply/Demand Balance to 2015 (Source: Ocean Shipping Consultants)*
Non-flexible working conditions in the ports, both as regards calculation of waiting time, idle time, over-time, etc. Non-flexible collective wage agreements, e.g. number of dockworkers in each gang. This issue is actual in BE, DE, DK, SW, FIN, FR, IRL, ES, IT, PT, NL and S. It is a general problem that depends also on the port system in the country.

Peak in vessel arrivals and capacity utilization

In each terminal, the arrival of container vessels are not spread equally during one day, in certain hours the terminal is extra busy (more vessels coming) and in other hours the terminal could be less busy (less vessels coming). For example, 40% vessels arrive in 6 peak hours each day. Part of all arriving drivers is rejected due to incorrect or incomplete information being entered in advance of their arrival.

Waiting times for hinterland modes

The waiting times for trains, ships and trucks at the terminal are too long. Many terminals have the facilities to perform intermodal transportation, such as the crane to load the containers directly to freight trains which stop at the port railway station (or barges in the inland waterways). Due to the capacities such as the handling speed of the crane, containers can be waiting for a long time to be loaded on other transport models. In some ports, inland vessels and deepsea vessels use the same port facilities, priority is generally given to ocean shipping causing negative time and financial implications for inland waterway vessels.

Bottlenecks in information flows

Digitalization is lacking in customs procedures in some member states (such as NL, F, SE, DK & N) and EEC countries. At the ports of these countries, electronic manifests are not accepted and the electronic stamps are not recognized in customs procedures. The bill of lading and other necessary documentations are still handled in the manner of paper work. The transformation of data/information is still rely on labour activities (enter data/information from bills to system) such as reading and typing. These labour activities are normally inefficient and create rooms to transfer faults.

Use of EDI for transmitting data between ports is still not generalized. EDI has been wildly adopted in various industries (such as suppliers and manufacturers; manufacturers and retailers). Due to the complexity of container supply chain regarding various actors, operations and regional factors, EDI is not easy to be generalized among ports in Europe. Without an efficient information/data interchange system, the ports operations can not be integrated. The automated goods managements system are also lacking at the ports in some European countries.

Customs documents have to be issued 24 hours before shipment due to difficult customs’ clearance procedure. With IT this could be done in minutes. However, for the ports do not have qualified IT system, this rule brings extra constrain to container shipping. In some case, containers have to wait at the port and the shipment is delayed because the customs document are issued not in advanced enough (within 24 hours).
Short sea shipping cannot compete with road transport with such expensive and excessive administrative burdens.

Only minority of shipping infrastructures are handled electronically (i.e. customers can only receive the information/state of their containers/cargos through telephone call, but not a completed online information platform). What customers require is a wide range of e-service which integrated in only one channel, even allow tailor-made requirements.

**Types of improvement in port hinterland connections**

The bottlenecks in port and hinterland require five types of improvements in port hinterland connections:

- Development of transport infrastructure to the hinterland
- Efficient use of the hinterland infrastructure
- Coordination of the transport chains
- Increasing need for a sustainable hinterland transport system and
- Improvement of the quality of commercial services (such as terminal services, barge/rail services)

**Improvement of infrastructure - The transport infrastructure to the hinterland needs to be sufficiently well developed**

Infrastructural limitations like the lack of sufficient Trans-European Transport-Networks (TEN-T) should be tackled and bigger investments provide a further boost. In the face of the enormous growth in seaports, hinterland connections have to be especially improved. This growth should primarily be steered to rail and inland waterways wherever possible. Since the power of the EU is limited in this respect Member States have to take on their responsibility and make the necessary investments.

*Capacity constraints* already exist in the main European ports and their hinterland today and their being aggravated by high growth rates in container traffic and the consequential need for handling capacity and hinterland connections. As a consequence, shipping lines are already facing poor schedule reliability, mainly caused by port terminal congestion. On the Far East – Europe trade only 44 percent of the vessels are on time. Among the late arrivals, 50 percent was one day late, 20 percent two days late, roughly 10 percent three days late and the remaining 20 percent four or more days late. Barges are victim of these capacity constraints as well. Since they have to be mainly handled on the same quaysides and cranes as the big sea vessels, quite often they have to wait for the bigger and more profitable vessels.

In the ports itself, rail terminal capacity is only one aspect. In Hamburg for example, the port railway (Hafenbahn) has suffered enormously as a consequence from underinvestment while the number of freight trains is expected to double from around 200 in 2005 to 400 in 2015. Bottlenecks in the ports also concern the problem of waiting times reaching their peak in front of terminal, depots or administrative buildings. These need to be evened-out. However, this requires the willingness of all partners in the chain to change established working practices. This applies especially to the manufacturing and retail industries who should adapt their time windows for receiving and pick-up of goods.
Capacity constraints also result from the high amount of empty container repositioning due to unbalanced flows. They also need to be stored somewhere and available space in ports is limited while the problem is growing bigger. A so called “grey box”, a container without logo could be good tool but is not accepted among the industry since the containers are seen as marketing tools.

As it is now, it seems that North-Western Europe will not see much new major corridor infrastructure developments in the foreseeable future like the Betuweline, a dedicated rail freight corridor with a capacity of a train every six minutes amounting to 400 trains a day linking the Port of Rotterdam and the German hinterland. The major problem of separate fast and slower traffic (mainly passenger from freight) will not be solved in the foreseeable future. However, more sidings/passing tracks should be developed to unmix traffic.

Lacking capacities of the railways are becoming a major bottleneck. Freight trains in the port of Hamburg are expected to double from 200 today to 400 in 2015. Traffic expectations of the German Infrastructure Development Plan for 2015 were already realized in 2015.

A main infrastructure problem for efficient intermodal port hinterland connections is the lack of a network of transhipment terminals and the efficiency of existing terminals. According to a recent study by the International Union of Railways (DIOMIS 2008), the growth of intermodal volumes in the next years will be much higher than what is currently planned in order to increase terminal capacity. What they propose is an international programme on establishing a system of intermodal hub terminals. “They are required as turntables (“dry ports”) for container hinterland traffic in countries such as Belgium, the Netherlands, Germany and Italy, and for integrating small and medium-sized transport areas into continental and maritime combined transport”. The DIOMIS study also calls for more international coordination of terminal development plans which would reduce unnecessary capacity constraints and not impede the extension of intermodal transport services and volumes, as is currently the case.

Intermodal players alone cannot achieve as much efficiency and stretch existing capacity endlessly as it is needed to cope with the growth we are facing. In Germany alone, investment needs for new and extending existing railway infrastructure amounts to 15 billion Euros. Nonetheless, much of the focus will have to be on stretching existing capacity on the corridors via advanced traffic management systems, better coordination among all partners of the supply chain and the implementation of effective cargo bundling and cargo coordination systems.

**Efficient use - The transport infrastructure needs to be used efficiently**

Inland hubs, the so-called extended gates, are increasingly created. Deutsche Bahn and the Port of Duisburg (Germany) are jointly developing the world’s biggest inland port in order to serve as a main inland hub for the ports of Rotterdam, Antwerp and Amsterdam. In order to cope with the massively growing container flows, a new gateway terminal will be developed to allow for direct transhipment from one train to another. All trains coming to Duisburg will have direct connections to DB’s continental network. The new facility will make it possible to move the boxes out of the seaports as quickly as possible, create thereby more capacity within the port, and consolidate the flows for the
railway and inland waterway network. More frequent shuttle trains to the ports and more hinterland destinations like Warsaw or Budapest will be the consequence.

Inland terminal and dry ports are crucial for the further development of hinterland networks under conditions of high-volume growth. However, the possibilities of deploying inland cargo centres to relieve the problems in seaports are not limitless. An increasing number of inland locations are facing strict environmental regulations and a lack of spare capacity.

Rotterdam has also started to develop a container transferium outside the Rotterdam motorways ring to enable carriers to drop off and pick up containers outside the congested ring. The containers then move the final 30 to 50 kilometres by barge.

A solution for the problem of **barges waiting for deepsea vessels at quaysides** would be to develop separated handling areas. ECT has recently developed the “Delta Barge Feeder Terminal” in Rotterdam that is separating the sea and inland traffic. The Euromaxx-Terminal in Rotterdam (opened in its first phase 5 Sep 2008) has also been designed to better reconcile needs of deep sea vessels and barges by installing separate cranes and handling devices for the different needs, the terminal has also been directly linked to the new Betuweline.

**Better coordination - The transport chains need to be well coordinated**

Early information for logistics chain partners is highly important for improving efficiency of transport chains from and to the ports (Conclusion of the 3rd Conference on the Northern ports in Germany, Potsdam, 2 July 2008). Overarching process improvements among the actors can increase reliability and efficiency significantly. Prognosis planning based on consultation among the partners of the transport chain is also important. Bottlenecks that slow down the flow of the whole chain occur if only one actor in the chain does not adapt its capacities on time. However, partners do not easily exchange their data. An anonymous confidential data interchange with a neutral platform is highly important. Reliable and neutral external player might also give advice to the individual players in their planning of capacity and investments in order to avoid bottlenecks in the transport network resulting from different estimations of different market players.

In lack of better coordination among logistics chain partners, bigger shipping lines and global port operators are investing in hinterland terminals and inland logistics operations. Maersk Line wants to push containers into the hinterland supported by its terminal branch APM Terminals and its rail branches. Hutchison (HPH) owned ECT in Rotterdam has followed an active strategy of acquiring key inland terminals acting as extended gates to its deepsea terminals, e.g. a rail terminal in Venlo (the Netherlands), DeCeTe terminal in Duisburg (Germany) and TCT Belgium in Willebroek (Belgium). DP World is following a similar strategy by working in partnership with CMA CGM to streamline intermodal operations on the Seine and Rhône axes. Thus, terminal operators incorporate inland terminals as extended gates to seaport terminals and by introducing an integrated terminal operator haulage concept for the customers. **Customs can qualify an inland terminal as an extension of a deepsea terminal, so custom clearance can be done there.** The terminal operator typically remains responsible en route between the deepsea terminal and the inland terminal. The advantages of the extended gate system are substantial: customers can have their containers available in close proximity to their
customer base, while the deepsea terminal operator faces less pressure on the deepsea terminals due to shorter dwell times and can guarantee a better planning and utilization of the rail and barge shuttles. However, the success of both extended gates and terminal operator haulage largely depends on the transparency of the goods and information flows.

Unfortunately, terminal operators often lack information on the onward inland transport segment for containers that are discharged on the terminal. A close coordination with shipping lines, forwarders and shippers is needed to maximize the possibilities for the development of integrated bundling concepts to the hinterland. More can be achieved through a better data exchange among the supply chain partners. Especially the smaller firms such as trucking companies, which are heavily involved in hinterland transportation, often do not have the financial means to invest in such systems. As a consequence, trucks often arrive at terminals with the wrong information, without pre-notification or to collect containers that are not yet cleared by customs. As a consequence, it does not come as a surprise that the recent Conference on the Northern ports in Germany claimed that more transparency along the logistics chain is most important together with infrastructure improvement.

Customer requirement and behaviour often impede carriers from minimizing inland logistics costs. Shippers often insist on receiving/loading containers early in the morning and at the end of the week. This logistics requirement of the customers leads to money-wasting peaks in inland logistics costs. Currently, it seems that willingness to do is increasing. In Hamburg for example, warehouses around the port have extended opening hours. Customs offices have also done so in the case of Hamburg. However, problems also result from understaffing and in the case of Hamburg also in the unclear situation concerning the status of the Freeport in the future.

Better coordination has also been pushed forward by port authorities that have seen that their hinterland connections are increasingly becoming a main issue. They set up task forces together with various stakeholders (carriers, shippers, transport operators, labour and government bodies) to identify and address issues affecting logistics performance in the port-hinterland-link. This can lead to the bundling of rail and barge container flows in the port area and the development of rail and barge shuttles. For example, a joint project by the Antwerp Port Authority and the cargo handling companies PSA HNN and DP World, with support from the rail track operator Infrabel, the so-called Antwerp Intermodal Solutions (AIS), brought all the parties around the table and led to the introduction of new rail links by market players. The interest of the port authority is clear: more efficient transport chains lead to more throughputs.
Sustainability - An increasing need for a sustainable hinterland transport system

Port authorities are facing a wide array of local constraints like road congestion, lack of available land and increasingly environmental issues. Thus, intermodal players like the Port of Rotterdam have started to develop their ports with ambitious modal split objectives in favour of rail and barge. *Concessions for terminal operators are granted amongst others on modal split* (to be achieved by terminal operators for example through a price structure favouring environmental friendlier modes). Ports must demonstrate a high level of environmental performance and sustainability not only in view of community support, but also in view of attracting new trading partners and potential investors. A large number of port authorities promote already and others will increasingly do so an efficient intermodal system in order to be able to grow in the face of growing environmental concerns and transport political more and more focused on promoting greener modes of transportation.

Quality - The services provided by private firms need to be attractive

Another bottleneck in port hinterland connections consists in the *insufficient reliability of intermodal trains*, which is increasingly important in a logistics system that is based on just-in-time delivery. According to the International Union of combined Road-Rail transport companies (UIRR), in 2007 on average only around 60 percent of the trains were on time, almost 10 percent were even more than 24 hours late.

This shows that a lot of potential to shift transport to more efficient modes on longer distances for port hinterland connections like rail still remains unused for reasons to be
found within the respective mode. Especially the *monopolistic railway undertakings* do not have the best *image among shippers*. In a recent German study of the Bundesverband Materialwirtschaft Einkauf und Logistik (BME) 94 percent of shippers that have 100 percent mode-neutral cargo – goods that can be transported by any mode of transport - said that rail transport does not play any role in their logistics processes, although 81 percent are ready to have their cargo transported by more environmental-friendly service providers. According to the same study, the reasons for not including rail in the logistics processes are to be found in bad customer service (46 percent) and too high prices (31 percent).

Elevated traction cost and the *long preparations and negotiations* with the railway companies needed to install fast direct rail services are also major issues for carriers buying capacity from the different national railway companies.

The *lack of tracking and tracing in the rail sector* is also main bottleneck for higher market reach. According to the Community of European Railways (CER), rail operators are jointly working on the technical specification for telemetric application for freight on rail (TAF/TSI). Implementation of the service shall improve tracking and tracing and also facilitate ordering of train paths. It is due to become operational by 2013, with some features available before.

Another limitation is the *lack of transparency in the market for shippers*. There are numerous players like for example carrier hauliers, railway operators, shipping lines, short sea operators or seaports and each of them has its own strategy for marketing its services and this results in a wide disparity of marketing channels. Customers, however, often prefer one central commercial contact: a one stop shop. *One stop shops* have a full overview of the whole transport process and have the skills and resources needed to obtain information and intervene in the process, at all stages including during the logistics service, should need arise.

The European Commission has tried to *stimulate* the development of *one-stop-shopping* solutions in its policy of promoting intermodal transport by supporting the development of the concept of Freight Integrators. Freight integrators are transport service providers who arrange full load, door-to-door transportation by selecting and combining without prejudice the most sustainable and efficient mode(s) of transportation.

Another *solution* seems to arise from the industry itself. Some larger players increasingly *offer one-stop-shopping* solutions like the German Railways that have bought several railway companies in other countries, like the British EWS last year, and have offered road solutions with its sister company Stinnes. Another example is the shipping line Maersk that invested in rail solutions with its European Rail Shuttle. Thus, we might see in the future that more and more players originating from different sectors are competing with each other to control the whole chain and offer complete door-to-door services and one-stop-shopping services for customers.

**Conclusion**

Given the limited amount of public money available for major infrastructure improvement, better coordination and more efficient use of infrastructure are key issues in respect to solving bottlenecks in port hinterland connections in the near future.
2. Supply Chain Risk Management

This chapter introduces the issue of risk in the supply chain. The way risk is dealt with in supply chains (supply chain risk management) is the main context for security. Since risk management assumes that risks have to be weighted, security management in supply chain will be defined by choices of what risks to eliminate, and what risks to control. In terms of the conceptual framework developed below, supply chain security management is about how to mitigate inherent vulnerabilities.

2.1 Conceptual framework

This section develops a conceptual model of supply chain security. Figure 2.1 illustrates the relationship between sources of risk, disruptions and supply chain security. This model postulates that business can develop a supply chain security strategy to mitigate the influences of sources of risk on eventual business disruptions. First the sources of risk and the disruptions will be discussed. After that supply chain security will be explored.

![Figure 2.1: Supply chain security strategy](image)

This model is created from a supply chain point of view. In principle, the main manufacturer/shipper is the party that requires a secure supply chain. It is usually this party that will initiate security enhancement of the supply chain.

2.1.1 Sources of risk

Sources of risk are all uncertainties on the periphery of the supply chain. Two categories can be distinguished: external to the supply chain and internal (directly related to the supply chain). Sources of risk are random events with negative impact on business operations. If the outcome is predictable or there is no uncertainty associated with the outcome, there will be no risk (Spekman and Davis, 2004). The sources of risk are what make the outcome uncertain and by initiating their existences countermeasures can be taken to ensure the continuity of business activities. The sources of risk taken from the literature will be discussed below.

In chapter 1, the presence of dependencies in supply chains was highlighted. Sources of risk, both internal and external, usually ‘attack’ the dependencies in supply chains. As
such, the dependencies themselves become problematic only when there are additional shocks from sources of risk.

In the literature both Chapman et al. (2002) and Christopher (2005) identify internal and external risk sources. According to Christopher (2005) the risk of business disruptions has many sources, not just the obvious and current threats from terrorism and geopolitical events but also the unexpected impact of particular business decisions. Some literature sources add to these categories the separate category of network related risk. By this they mean the specific risks related to logistics structure decisions.

According to Christopher (2005) however, companies should cope with internal and external sources with their network. This view will be illustrated by two examples.

Example 1 (external source of risk), Foot and Mouth Disease (FMD) in England affected the production of Jaguar and Volvo (Norrman and Jansson, 2004), because they were unable to purchase high quality leather from the infected area in England. Their network structure made them dependent on one geographic leather market.

Example 2 (internal source of risk): a financially distressed Land Rover supplier went bankrupt (Chapman et al. 20002). Land Rover was highly dependent on this supplier and it would have taken six months to start producing with another supplier. Land Rover decided to support its supplier financially in order to keep producing. Again the designed network structure made them dependent on this supplier. The same applies for the fire incident of Toyota’s fluid-brake supplier and Ericsson’s semiconductor supplier (Norrman and Jansson, 2004). Both examples illustrate that the additional network related risk sources are not necessarily the key to vulnerabilities.

![Figure 2.2: Supply chain vision: internal, external and network](image)

Figure 2.2: Supply chain vision: internal, external and network

Adapted from Jüttner (2003)

Figure 2.3 shows the internal and external sources of risk that can be separated.

The human factor is added in both internal and external sources of risk. None of the reviewed literature mentions theft and smuggling as internal human factor. Since fraud could be considered similar to theft and it is a significant source of risk, it is added to the list. Examples of the category diseases are the foot and mouth outbreak, SARS and bird flu. Legislation adapted by governments all over the world regarding security should be categorized under the government imposed legal restrictions. This means companies could be forced to implement these into their security enhancing measures. Interesting additions to the list are the computer viruses as discussed by Sheffi (2005) - Melissa (1999), Love Bug (2000), Code Red (2001) and the Slammer worm (2003). These could be added under human action either internal or external.

The list is not exhaustive, but the table above touches on the most important sources of risk both internal and external. According to Christopher’s (2005) point of view companies are able to influence internal sources of risk with their network, but not the external. Sheffi (2005) also agrees to some extent. He says that acts of God are frequent and statistical models can be used to estimate the likelihood of their occurrence and their magnitude. Section 2.1.3 will provide suggestions as to how internal sources of risk may be influenced and how to cope with the external sources.

### 2.1.2 Supply chain security framework

In a previous section the definition of supply chain security (SCS) was introduced. Supply chain security can be divided into design and structure and security enhancing measures. Both try to influence the vulnerability to sources of risk and the probability of a disruption. The figure below shows the supply chain security framework.
This framework is an adaptation of Jüttner et al. (2003). The more central position of vulnerability is an important addition to that model. Companies can choose a certain balance between design & structure and security enhancing measures to realize supply chain security. Companies should incorporate supply chain security in their broader business strategy to decide on this balance. The eventual result is the extent to which the supply chain remains vulnerable to “sources of risk”. These choices can result for instance in a resilient or an agile approach to security. Although both approaches deal with the supply chain design and structure they are dealt with at a higher hierarchical level and should thus more appropriately be discussed in the larger supply chain management context.

2.1.3 Mitigating risk through supply chain design and structure
We will focus on two critical approaches: resiliencies and agility.

Resilience (re-active)
In material science, resilience is the physical property of a material which causes it to return to its original shape or position after a deformation that does not exceed its elasticity (Rice Jr. and Caniato, 2003). In a business context resilience is an organisation’s ability to react to an unexpected disruption such as one caused by a terrorist attack or a natural disaster and resume normal operations (Coutu, 2002). Smallman (1996) categorizes proactive and re-active risk management where he puts
resilience under re-active risk management. The last words of the definition makes this approach re-active. Also Christopher (2005) states that resilience implies the ability of a system to return to its original or desired state after being disturbed (Christopher, 2005). Restoring after the disruption implies that no backup plans are in place and after the disruption is over the supply chain will be restored in its original design and structure.

According to Rice Jr. and Caniato (2003) resilience can be achieved by either flexibility or redundancy. Flexibility means switching to other suppliers when a disruption occurs, while redundancy means reassigning to other factories, because they are expressly under-utilized for this purpose. According to Rice Jr. and Caniato (2003) flexibility can be achieved by investment in infrastructure and resources such as a multi-skilled work force, a product system designed to accommodate multiple products with real time change and multiple suppliers.

**Agile (pro-active)**

Agility means the ability to respond to short-term changes in demand or supply quickly and to handle external disruptions smoothly (Lee, 2004b). This implies that backup plans are present, other potential suppliers can be selected and the supply chain is redesigned to cope with the disruption. This approach is considered proactive, because measures have already been taken in advance. For agility; visibility, velocity and acceleration are required (Peck and Christopher, 2004). Velocity and acceleration require shorter end-to-end pipelines while visibility reduces uncertainty and enables the reduction of supply chain risk through shared information, both upstream and downstream (Peck and Christopher, 2004). Lee (2004b) points out that companies should pursue agility in order to respond to sudden and unexpected changes in markets. Demand and supply fluctuations should be coped with by agility. But it is also a good remedy for increasing supply chain security.

Methods mentioned by Lee (2004b) to increase agility are: the promotion of flow of information between suppliers and customer, the development of collaborative relationships with suppliers, designing for postponement, building inventory buffers by maintaining a stockpile of inexpensive but key components, having a dependable logistics system or partner, drawing up contingency plans and developing crisis management teams. Although mentioned in the context of redundancy Sheffi (2001) advocates working with known suppliers, managing a central inventory, dual manufacturing (offshore for bulk and local as backup) and the creation of emergency stock. These measures are similar to those mentioned by Lee.

Reviewing both the literature on resilience and agility, this leads to the conclusion that they appear to be similar. Rice Jr. and Caniato (2003) mention issues such as a multi-skilled work force, and multi-sourcing as part of resilience while they are also used to achieve agility. Peck and Christopher (2004) on the other hand identify agility as one of the five principles of supply chain resilience. In this thesis resilience and agility are seen as two separate – re-active and proactive – approaches in considering supply chain security from strategic point of view. The main difference between resilience and agility is that the first restores its design and structure after the disruption has been coped with, whereas the other has options in place to change the design and structure in order to cope with disruptions and lower the vulnerability. Both approaches are part of the
supply chain security strategy of a company and influence the balance between supply chain design and structure and security enhancing measures.

2.1.4 Security enhancing measures

Security enhancing measures enable companies to cope with vulnerabilities created by supply chain design and exposed by sources of risk. This section will be divided in three parts: Measures, Analysis and Visibility. The first will discuss measures companies can implement. Second, Analysis is an important activity in assessing the current state of vulnerability and impending danger of being exposed to sources of risk. Finally the third pillar of security enhancing measures is Visibility, which may generate more accurate information to help mitigating vulnerabilities.

2.1.4.1 Measures

Sheffi (2005) recalls that perimeter fencing, burglar alarms, closed-circuit television monitoring and access control have become commonplace in many corporate locations since 9/11. In addition, gaining admittance to most larger corporate locations requires a pre-arranged appointment and an employee escort while on the premises (Sheffi, 2005). These are a few of the obvious security enhancing measures. The following measures can be identified:

- Physical security
- Personnel security
- Information security
- Freight protection
- Security manager
- Security plans

Some of these are adapted from Rice Jr. and Caniato (2003). Access control, badges, guards and camera systems are mentioned as physical security measures. The measures summed up by Sheffi (2005) at the beginning of the section also belong in this category. Personnel security deals with criminal, credit and background checks on potential employees. The privacy protection legislation of the European Union and The Netherlands hamper this kind of security measure to a large extent. Information security should prevent people accessing information they do not have authorization to. This could be quite simple, by keeping the freight documents behind closed doors, but also by having basic cyber security to prevent hackers gaining access to crucial information and protecting a company against viruses etc. Freight protection implies the use of cargo seals, tracking technologies and sensors. Rice Jr. and Caniato (2003) also propose an employee background check as part of freight protection, but again local legislation prevents this as a main security measure. Appointing a security manager should improve the implementation of the security measures in the organisation as well as in the organizational culture. Finally a company should formulate security plans, which describe what should be done in which circumstances. Ericsson for example has set up a matrix for component supply. If the business recovery time is 9 to 12 months the product should be redesigned to fit in a part from another supplier (Norrman and Jansson, 2004)
Preventive and re-active

Most of the measures described above are of a preventive nature. Especially the physical -, personnel -, information security and security manager belong in this category. The security plans on the other hand have a re-active nature. Freight security has little bit of both. On the one hand, cargo seals are preventive while on the other hand tracking technologies and sensors provide re-active possibilities.

Audits

Sheffi (2005) adds an extra measure: audits. According to him Seagate, IBM, HP, Gillette, Target and many others conduct pre-engagement security audits as well as ongoing (including unannounced) on-site security audits. In an audit, the security measures such as mentioned above are actually checked in practice to see if they are adequate for the circumstances. The ultimate goal is to ensure the right measures are taken to prevent vulnerabilities. In other fields such as ISO 9000 and 14000 the execution of audits is common. This measure is mainly preventive but audits are also deployed after something has happened.

2.1.4.2 Analysis

Using analysis tools can contribute to pro-active actions to prevent disruption to occur or re-active approach by analyzing a past event and avoiding it in the future. When discussing analysis tools in most literature this is described as risk assessment. Risk mapping, Fault tree analysis and Event tree analysis are examples that are briefly mentioned by Normman and Jansson (2004) as tools for risk identification. Michalski (2004) discusses the comprehensive outsource risk evaluation (CORE) as a tool developed by Microsoft and Arthur Anderson. According to Michalski, the Anderson business model identifies 75 different risks. In their paper Harland et al. (2003) define eleven types of risk. Among others these are: strategic risk, supply risk, operations risk, customer risk and reputation risk. Before discussing a few risk assessment tools a fundamental analysis tool will be reviewed, namely supply chain mapping.

The Willis and Ortiz (2004) of the RAND corporation introduces a layer approach, distinguishing a logistic -, transaction - and oversight layer (see figure 2.5). Willis and Ortiz (2004) refer to the logistic layer as a multimodal physical network for the transport of cargo and can be considered similar to the logistics concept described by van Goor et al. (1999). The transaction-based view of the global supply chain can be represented as the union of the interacting networks: information network and a material network (Willis and Ortiz, 2004). It reflects the companies involved in the coordination and payment. The third layer represents the legal and regulatory structure of the global supply chain. Customs, the Treasury Department and also the International Maritime Organisation (IMO) are situated in this layer. Interactions exist between the different layers. The transaction layer coordinates the flow of goods in the logistics layer and the transaction- and logistics layers are limited by regulations from the oversight layer.
The main advantage of the layer approach is the distinction of the different companies involved. For example in the logistics layer, it is difficult to integrate an agent or expeditor because in most cases he does not physically handle the goods himself. In the transaction layer he can be added and his role in the different transactions becomes clear. The same goes for the governmental bodies such as Customs Border Patrol (CBP), World Customs Organisation (WCO) and International Maritime Organisation (IMO). The oversight layer is useful but not all security measures involved in global supply chains are shown in this layer.

### 2.1.5 Vulnerability in the chain

After discussing supply chain management and design and structure it is time to review vulnerability itself. Vulnerability is the potential of susceptibility to risk sources. This potential is determined by the interaction of structures and measures.

The design and structure of a supply chain is a paradox. On the one hand vulnerabilities can be dealt with by the design and structure of the supply chain, on the other hand the trends in supply chain management have resulted in higher dependencies and thus more vulnerabilities.

Security enhancing measures can be implemented to deal with the vulnerabilities created by design and structure. The better the balance between both supply chain security tools, the lower the vulnerability to sources of risk. One should keep in mind
that some sources of risk cannot be eliminated and as a result there will always be a chance of business disruption.

In the literature different authors explain what feeds the vulnerability of the supply chain. The views are similar to the ones discussed in the context of dependencies. The adoption of lean practices, the move to outsourcing and a general tendency to reduce the size of the supplier base can all potentially increase supply chain vulnerability (Christopher, 2005). Svensson (2002b) mentions as the underlying reasons for vulnerability the following: decrease of inventory, reduction of the number of subcontractors used and at the same time increase their sharing or diffusion (partly or totally) of manufacturing, assembling, research and development of new materials and components (e.g. outsourcing). Both Norrman and Jansson (2003) and Svensson (2002b) come to the conclusion that current principles used in supply chain management have led to very vulnerable supply chains. Chapman et al. (2002) come to a similar conclusion, stating that the drive towards more efficient supply networks during the recent years have resulted in these networks becoming more vulnerable to disruptions. Sheffi (2005) adds that the very complexity of global supply networks means that in most cases it is difficult to assess a priori vulnerabilities. The consensus of their views is that the dependencies as discussed earlier mainly create the vulnerability.

Haywood and Peck (2004) conclude that supply chain vulnerability is an important but underdeveloped area of management research. In general four approaches to supply chain vulnerabilities can be identified:

a) Svensson (2000, 2002 and 2004),

b) Harland et al. (2003) and

c) Cranfield School of Management, Cranfield University.

d) Massachusetts Institute of Technology (MIT)

For Cranfield University Helen Peck, Uta Jüttner and Martin Christopher are the major authors on this subject, while Sheffi (2001 and 2005) and Rice Jr. (2003 and 2005) are the researchers from MIT. Peck (2005) integrates both horizontal and vertical approaches in contrast to Svensson’s horizontal and Harland et al.’s vertical approach. Horizontal in this context is described as vulnerabilities within the boundaries of a single firm or between a focal and adjacent firms (Peck, 2005). Svensson himself remarks that supply chains have a vertical emphasis and for this reason his article is limited to the channel theory described by Weld (1916) and Bucklin (1966). Peck (2005) describes the vertical approach as mapping and analyzing of one or more representative product lines. Apart from the discussion of whether a supply chain is vertical or horizontal, the literature describes a fine line between supply chain vulnerability and risk. For example Harland et al. (2003) discuss the subject risk in supply networks while Svensson and Peck discuss frameworks for supply chain vulnerability. This is also the case in the MIT approach: Sheffi (2005) does not make a clear separation between sources of risk, vulnerabilities and disruptions.

In the table below the different definitions of supply chain vulnerabilities as they can be found in the literature are noted.
The first three definitions touch on the intention of supply chain vulnerability. Svensson (2000) emphasises that it has consequences for the manufacturer and its sub-contractors, while the other authors only use the supply chain context. Chapman et al. (2002) emphasise the exposure to serious disturbance, where Sheffi (2005) takes a more strategic approach by directly linking vulnerability to the likelihood and potential severity when it results in a disruption. In a way this is already a step ahead. Jüttner et al. (2003) are the only ones discussing risk mitigating strategies. The security enhancing measures proposed in the conceptual supply chain security framework also try to adverse supply chain consequences.

Although supply chain security has as its goal the reduction of vulnerability, there remains always a chance that it could escalate into a disruption. Christopher (2005) argues that internal sources of risk can be dealt with but not the external sources. To some extent this is true; even with all the measures in place there is still an opportunity for a terrorist attack. Sheffi (2005) advocates that companies should bear in mind that governments will always exaggerate actions after a terrorist attack. Other vulnerabilities that can still happen are the ones resulting from the human factor. With all the security measures in place cargo can still be stolen and fraud will always be attempted. Professional criminals are usually one step ahead of the security measures, getting into the same pace is challenging enough.

Companies cope in different ways with reducing vulnerabilities. Toyota, General Motors (GM), Ford and Chrysler, for example, have (re)engineered their supply chains after 9/11 (Sheffi, 2005). They have chosen to decrease their vulnerability by adjusting the design and structure of their supply chains. Ericsson on the other hand has only introduced an analysis tool as the answer to their dramatic supply disruption. This analysis tool should enable them to handle such incidents more adequately in the future. There are of course companies who do install both. GM has adjusted its structure as well as implemented a “Catalogue of Catastrophes” tool for analysis purposes (Sheffi, 2005). Hewlett Packard (HP) already has secondary suppliers for all critical components (Martha and Vratimos, 2002) and also already uses local sourcing as backup (Sheffi,

<table>
<thead>
<tr>
<th>Definitions of supply chain vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jüttner et al. (2003)</td>
</tr>
<tr>
<td>Supply chain vulnerability is “the propensity of risk sources and risk drivers to outweigh risk mitigating strategies, thus causing adverse supply chain consequences.”</td>
</tr>
<tr>
<td>Chapman et al. (2002)</td>
</tr>
<tr>
<td>Supply chain vulnerability can be defined as: “an exposure to serious disturbance, arising from risks within the supply chain as well as risks external to the supply chain.”</td>
</tr>
<tr>
<td>Svensson (2000)</td>
</tr>
<tr>
<td>“The existence of random disturbances that lead to deviations in the supply chain of components and materials from normal, expected or planned schedules or activities, all of which cause negative effects or consequences for the involved manufacturer and its sub contractors.”</td>
</tr>
<tr>
<td>Sheffi (2005)</td>
</tr>
<tr>
<td>“A firm’s vulnerability to a disruptive event can be viewed as a combination of the likelihood of a disruption and its potential severity.”</td>
</tr>
</tbody>
</table>

Figure 2.6: Definitions of Supply chain vulnerability (Source:?????)
2005). This is an example of a company which deals with supply chain security on the higher strategic level by implementing resilience. The companies above acknowledged the existence of vulnerabilities in their supply chain and made adjustments. In a survey of supply chain progress by Computer Sciences Corporation (CSC), 48% of the respondents indicated that they had implemented a supply chain vulnerability inventory planning and inventory level strategy. This would indicate that companies are willing to adjust their design and structure. 39% of the same respondents had or planned to have such a system for critical trading partner/outsourcing partner vulnerability and 37% on international freight movement. Unfortunately it was not specified which companies already have these kinds of plans and which companies are planning to implement it.

In a Dutch project PROTECT, a survey was done in 2005 among 80 shippers and logistics service providers. An important conclusion from this survey is that 60% acknowledged that vulnerability in supply chains originated from supply chain improvement programs. The PROTECT survey (2005c) indicates that only 8% of the respondent shippers were willing to increase inventory levels in the supply chain to reduce vulnerability. With reference to visibility less then 50% of the CSC respondents agreed that their organisation had an increased visibility of supply chain continuity and protection. Vulnerabilities in the supply chains do exist and companies are to some extent aware of this. Not every company is willing or able to change their logistics design to counter these vulnerabilities.

2.1.6 Supply chain security management tools

Mapping is an useful tool for gaining more insight into the supply chain and offering opportunities to determine any vulnerabilities and dependencies. The following subsections will discuss risk analysis/risk assessment tools.

SAM

Kleindorfer and Saad (2005) developed the so-called SAM (Specifying sources of risk and vulnerabilities, assessment and mitigation).

This framework is based on industrial risk management divided in four steps: 1) specify the nature of the underlying hazard giving rise to this risk, 2) quantify risk through disciplined risk assessment process, 3) fit the risk management to the characteristics and need of the decision environment, 4) integrate ongoing risk assessment and coordination. They also introduced 10 principles that must be understood collectively and simultaneously.

One of them is applying the Total Quality Management (TQM) approach, as also proposed by Lee and Christopher (2004). This has all led to disruption risk management and security in global supply chains, based on an established voluntary security standard, classification of assets/processes, ranking and prioritisation with continuous improvements.
Supply network tool

Harland et al. (2003) have developed a supply network tool for helping to identify, assess and manage risk. The tool is based on their eleven risks categories and thus deals with supply risk.

![Figure 2.7 Supply network risk tool](source: Harland et al. (2003))

The figure shows the tools and steps.

Ericsson contingency planning

In their paper Norrman and Jansson (2004) discuss the Ericsson contingency planning approach adopted by the cell phone manufacturer after fire at Philips semiconductor plant in 2000. Contingency planning is part of risk assessment/analysis encompassing risk identification, risk assessment, risk treatment and risk monitoring. Contingency planning consists of a response plan (the response is the required reaction to an incident or emergency to assess the level of containment and to control activity), a recovery plan (recovery phase actions include the actions that are needed to resume critical or essential business operations, functions or processes) and restoration plan (the process of planning for and implementing full-scale business operations again and to allow the organisations to return to normal service level). The contingency planning of Ericsson is more based on analyses and therefore categorized in this security enhancing section. Secure site location decision process Hale and Moberg (2005) have developed a secure site location tool which will lead to the selection of a minimum number of emergency resource locations that provide logistics managers with quick access to critical resources while minimizing the total costs incurred by the supply chain preparing for future crisis. The tool consists of 1) identifying the emergency resources needed at each secure location, 2) identifying all critical facilities within the supply chain, 3) setting maximum response time goals for access to emergency resources and setting minimum distances at which secure site storage areas must be placed from supply chain facilities and 4) using
the proposed decision model to identify the number and approximate location of emergency resource storage facilities

**Near miss analysis**

In his book Sheffi (2005) explains the “Near Miss” analysis used by the British Civil Aviation Authority and the U.S. Military. The purpose is to identify systemic or latent errors and hazards and to alert industry to them. The near miss pyramid entails: 1) unsafe, hazardous, insecure processes and practices; leading causes; 2) hundreds of accidents without significant property damage or loss; 3) dozens of incidents with property damage; 4) several minor injuries; 5) death or serious injury. Sheffi acknowledges that every industry has different rules on what incidents should be identified and reported as near misses and reported. Sheffi does emphasise that managers should not look for a reduction in the number of reports over time as clear evidence of increased safety. Reporting incidents also results in the employees staying alert.

### 2.2 Main international security programmes

This section provides an overview of the main security programmes that are currently relevant for companies operating in a global arena. We have chosen not to provide lengthy discussions of pros and cons, but report the bare facts on each programme. For more extensive discussion on most of these programmes, we refer to an excellent document prepared by Swedish National Board of Trade (2008): “Supply Chain Security Initiatives” (www.kommers.se). We first summarize the initiatives as follows.

<table>
<thead>
<tr>
<th>Name / abbreviation</th>
<th>Originated Country/ Institute</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. BASC</td>
<td>Latin American trade</td>
</tr>
<tr>
<td>2. C-TPAT</td>
<td>USA</td>
</tr>
<tr>
<td>3. EU-AEO</td>
<td>European Commission</td>
</tr>
<tr>
<td>4. ISO 28000</td>
<td>ISO Technical Committee</td>
</tr>
<tr>
<td>5. TAPA</td>
<td>USA</td>
</tr>
<tr>
<td>6. CSI</td>
<td>USA</td>
</tr>
<tr>
<td>7. PIP</td>
<td>Canada</td>
</tr>
<tr>
<td>8. Stairsec</td>
<td>Sweden</td>
</tr>
<tr>
<td>9. STP (Secure Trade Partnership)</td>
<td>Singapore</td>
</tr>
<tr>
<td>10. Secure Export Partnership</td>
<td>New Zealand</td>
</tr>
<tr>
<td>11. Frontline</td>
<td>Australia</td>
</tr>
<tr>
<td>12. APEC/ STAR</td>
<td>Australia</td>
</tr>
<tr>
<td>13. 24 Hour Rule</td>
<td>USA</td>
</tr>
<tr>
<td>14. ISPS Code</td>
<td>IMO</td>
</tr>
<tr>
<td>15. WCO SAFE</td>
<td>WCO headquarters in Brussels</td>
</tr>
<tr>
<td>16. Golden List Program</td>
<td>Jordan</td>
</tr>
<tr>
<td>17. Operation Safe Commerce</td>
<td>USA</td>
</tr>
<tr>
<td>18. SST (US Smart and Secure Tradelanes)</td>
<td>Strategic Council on Security Technology, USA</td>
</tr>
<tr>
<td>19. EU-China: Smart and Secure Trade Lane Pilot Project</td>
<td>Joint EU-China Customs Cooperation Committee (JCCC)</td>
</tr>
</tbody>
</table>
A summary of the details of each program is provided below.

<table>
<thead>
<tr>
<th>Name/abbreviation</th>
<th>Originated Country/Institute</th>
<th>Start year</th>
<th>Regulating body</th>
<th>Covered route</th>
<th>Transport mode</th>
<th>Participation/Status</th>
<th>Category</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. BASC</td>
<td>Latin American trade</td>
<td>1996</td>
<td>World BASC Organization</td>
<td>Latin America to North America/Europe</td>
<td>Mostly sea (also land and air)</td>
<td>1500 companies</td>
<td>Private voluntary</td>
<td>Supply Chain Security and partnership</td>
</tr>
<tr>
<td>2. C-TPAT</td>
<td>USA</td>
<td>2001</td>
<td>CBP</td>
<td>From any country to U.S.A. (Import)</td>
<td>All</td>
<td>6375 certified, and 3916 validated companies</td>
<td>Government-Voluntary</td>
<td>Supply Chain Security</td>
</tr>
<tr>
<td>3. EU-AEO</td>
<td>European Commission</td>
<td>2008</td>
<td>DG Taxud</td>
<td>Any country to EU import, export</td>
<td>All</td>
<td>192 Companies</td>
<td>Government - Voluntary</td>
<td>Trade facilitation and Supply Chain Security</td>
</tr>
<tr>
<td>4. ISO 28000</td>
<td>ISO Technical Committee</td>
<td>2005</td>
<td>ISO</td>
<td>All</td>
<td>All</td>
<td>157 Member countries</td>
<td>International -Voluntary</td>
<td>Improve Supply Chain Security</td>
</tr>
<tr>
<td>5. TAPA</td>
<td>USA</td>
<td>1997</td>
<td>BoD</td>
<td>Only truck transport routes in USA, Europe, M-E, Africa, and Asia</td>
<td>Truck</td>
<td>207 members</td>
<td>Private - Voluntary</td>
<td>Identify the fields in which members experience losses and share information</td>
</tr>
<tr>
<td>6. CSI</td>
<td>USA</td>
<td>2002</td>
<td>CBP</td>
<td>Applied to sea ports, import to USA</td>
<td>Sea containers</td>
<td>58 ports</td>
<td>Government - Voluntary</td>
<td>Target and prescreen containers for preventing the terrorist threat to cargo destined to the United States</td>
</tr>
<tr>
<td>7. PIP</td>
<td>Canada</td>
<td>1995</td>
<td>Canada Border Services Agency (CBSA)</td>
<td>Import to Canada</td>
<td>All</td>
<td>615 companies</td>
<td>Government-voluntary</td>
<td>To secure the supply chain and facilitate legitimate trade.</td>
</tr>
<tr>
<td>8. Stairsec</td>
<td>Sweden</td>
<td>2003</td>
<td>Swedish ministry of transport</td>
<td>Any country to Sweden (import)</td>
<td>Air and sea</td>
<td>30</td>
<td>Government-voluntary</td>
<td>Quality and Secure from terrorism</td>
</tr>
<tr>
<td>9. STP</td>
<td>Singapore</td>
<td>2007</td>
<td>Singapore customs</td>
<td>Import, export and transit in</td>
<td>Sea</td>
<td>22 partners</td>
<td>Government-Voluntary</td>
<td>Awareness program, establish Singapore as</td>
</tr>
<tr>
<td>Partnership)</td>
<td>New Zealand</td>
<td>2004</td>
<td>NZ Customs</td>
<td>All</td>
<td>Limited information</td>
<td>Government-Voluntary</td>
<td>Protect cargo against crime</td>
<td></td>
</tr>
<tr>
<td>10. Secure Export Partnership</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Australia | 1991 | Australian Customs | Import & export in Australian companies | All | 700 companies | Government-Voluntary | Prevent illegal imports and exports |
| 11. Frontline |  |  |  |  |  |  |

| Australia | 1997 | APEC observers | Pacific Ocean Area | Sea and Air | 21 member countries | International-Voluntary | Economic growth and partnership |
| 12. APEC/STAR |  |  |  |  |  |  |

| USA | 2003 | CBP | Any country to USA (Import) | Sea vessels | Limited information | Government-Voluntary | Advanced information |
| 13. 24 Hour Rule |  |  |  |  |  |  |

| IMO | 2001 | IMO | Worldwide | Ships and ports | 167 member states | International-Mandatory | provide a standardized, consistent framework for evaluating risk, |
| 14. ISPS Code |  |  |  |  |  |  |

| WCO headquarters in Brussels | 2005 | WCO | Worldwide | All | 154 potential country members | International-Voluntary | Standards for supply chain security |
| 15. WCO SAFE |  |  |  |  |  |  |

| Jordan | 2005 | The Jordan customs | Import & export in the companies in Jordan | Pilot phase, can cover all | 15 companies | Government-Voluntary | Securing the supply chain |
| 16. Golden List Program |  |  |  |  |  |  |

| USA | 2002 | Department of Transportation and U.S Customs | Highways and railways in USA | Containers - (pilot project) | Government-driven pilot Voluntary | Identify existing vulnerability in Supply chain |
| 17. Operation Safe Commerce |  |  |  |  |  |  |

| Strategic Council on Security Technology, USA | 2003 | Strategic Council on Security Technology, USA | Imports in USA | Sea | 15 world’s largest ports and tradelanes | Private-Voluntary (supported by US Govt, funded by port authorities) | Enhance visibility of container shipment |
| 18. SST (US Smart and Secure Tradelanes) |  |  |  |  |  |  |

| Joint EU-China Customs Cooperation Committee (JCCC) | 2006 | EU and China Customs | Initially involves Rotterdam (NL), Felixstowe (UK) and Shenzhen (China). | Initially the sea ports | Pilot project | Government-pilot | Mutual recognition of safety and security and smooth and prompt customs clearance |
| 19. EU-China: Smart and Secure Trade Lane Pilot Project |  |  |  |  |  |  |
1. BASC

**Originated country/area**

The BASC was initiated in 1996 by a private North American foundation, Mattel corp, that imported goods from Latin America via the port in San Diego, California. This program is supported by U.S. Customs and Border protection (CBP). BASC refers in the first place to trade with Latin America and the vast majority of its participants are Latin American companies. (http://www.wbasco.org)

**Regulating body**

World BASC Organization is constituted as a non-profit organization under the laws of the state of Delaware (USA).

**Covered Routes**

Latin America to North America/Europe

**Transport mode**

Mostly sea (also land and air)

**Participation/status**

1500 companies

BASC’s members are to be found in the private and public sectors, as well as among international organisations and associations. The private sector is represented by companies in the international supply chain which are active in logistics and other activities in international trade. The public sector is represented by customs authorities and international police organisations. In Europe, France, for example, is a member of BASC since its customs authority has joined the programme. The World Customs Organisation (WCO) and the USA’s Chamber of Commerce are two examples of organisations and associations that participate in BASC.

**Category**

Private-Voluntary

**Goal**

Facilitate and promote world trade by establishing and administrating global supply chain security standards and procedures, in partnership with business, governments, customs, law enforcement agencies and international business organizations.

**Special requirements**

1. Be a company or a person actively involved in logistics, production or service activities related to foreign trade or services.
2. Each company must be legally established and have commercial activities in the country, as well as overseas, that will permit the validation of the integrity of the firm and their partners and directors. Also, the company should not have any criminal record or considered to have by any national or foreign authorities a suspicious person and/or dubious legal or criminal reputation.
3. Comply with the registration process approved by each chapter according to the procedure set by the WBO.
2. C-TPAT

**Originated country/area**

After the September 11 incident the CBP in USA initiated C-TPAT in order to act against the supply chain terrorism especially in the container security.

**Regulating body**

US Customs and Border Protection (CBP) (www.cbp.gov)

**Covered Routes**

From any country to U.S.A. (Import)

**Transport mode**

All (The road transactions from the Canadian and Mexican border has ‘green lane’, where the C-TPAT certified vehicles get priority)

**Participation/status**

In February 2007 more than 10000 companies had applied to participate in the programme and 6375 had been accepted as certified partners. Of these 3916 companies had been validated.

**Category**

Government- Voluntary

**Goal**

CBP’s strategy relies on a multilayered approach consisting of the following five goals:

- **Goal 1**: Ensure that C-TPAT partners improve the security of their supply chains pursuant to C-TPAT security criteria.
- **Goal 2**: Provide incentives and benefits to include expedited processing of C-TPAT shipments to C-TPAT partners.
- **Goal 3**: Internationalize the core principles of C-TPAT through cooperation and coordination with the international community.
- **Goal 4**: Support other CBP security and facilitation initiatives.
- **Goal 5**: Improve administration of the C-TPAT program.

**Special requirements**

C-TPAT members must agree to leverage their service providers and business partners to increase their security practices. In fact, many companies are demanding that their business partners enroll in C-TPAT or adhere to its security guidelines, and they are conditioning their business relationships on these requirements.

If a business partner has been certified and validated in C-TPAT, you do not need to obtain further information from that partner in terms of their compliance with C-TPAT security criteria or guidelines.

The C-TPAT program does not require that C-TPAT certified and validated business partners complete security surveys, disclose internal security audit results, or fill-out other questionnaires regarding implementation of the C-TPAT security criteria or
guidelines. Such programs may be appropriate for non-C-TPAT business partners, but are not appropriate for C-TPAT certified and validated business partners. C-TPAT members should aim to achieve an open dialogue with all business partners, C-TPAT certified and non-C-TPAT certified alike, on ways to improve supply chain security.
3. EU AEO

**Originated country/area**
European commission.

**Regulating body**

DG TAXUD (http://ec.europa.eu/taxation_customs/customs/policy_issues/-
customs_security/index_en.htm#cus_relat)

**Covered Routes**
Any country to EU import, export

**Transport mode**
All

**Participation/status**
192 companies (including three categories of certification, AEOS, AEOF and AEOC)

**Category**
Government-voluntary

**Goal**
Provide reliable traders with trade facilitation measures

**Special requirements** Applications for AEO status may only be accepted from economic operators as defined in Article 1.12 of CCIP, according to which: “Economic operator means: a person who, in the course of his business, is involved in activities covered by customs legislation”.

On the basis of this definition an EU based supplier not involved in customs activities that supplies raw materials already in free circulation to an EU based manufacturer may not qualify to apply for AEO status. Similarly, in this case, a transport operator that moves only free circulation goods within the customs territory of the Community may not qualify to apply for AEO status.
4. ISO 28000

**Originated country/area**

ISO/PAS 28000 was prepared by Technical Committee ISO/TC 8, Ships and marine technology, in collaboration with other relevant technical committees responsible for specific nodes of the supply chain. (ISO/PAS 28000 (2005))

**Regulating body**

ISO

**Covered Routes**

All

**Transport mode**

All

**Participation/status**

ISO is made up of 157 members which are divided into three categories: Member bodies, Correspondent members, Subscriber members.

**Category**

International-Voluntary

**Goal**

According to the guideline ISO/PAS 2008 the ultimate objective of the specification is to improve the security of supply chain.

In another word the goal is to facilitate better controls of flows of transport, to combat smuggling, and to meet the threats of piracy and terrorism, and to create a secure management of the international supply chain.

**Special requirements**

This Publicly Available Specification is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:

a) establish, implement, maintain and improve a security management system;

b) assure compliance with stated security management policy;

c) demonstrate such compliance to others;

d) seek certification/registration of its security management system by an Accredited third party Certification Body; or

e) make a self-determination and self-declaration of compliance with this Publicly Available Specification.

There are legislative and regulatory codes that address some of the requirements in this Publicly Available Specification. It is not the intention of this Publicly Available Specification to require duplicative demonstration of compliance.

Organizations that choose third party certification can further demonstrate that they are contributing significantly to supply chain security.
5. TAPA

Originated country/area

The Transported Asset Protection Association (TAPA) is a non-profit association which was formed in the USA in 1997 (formerly called Technology Asset Protection Association) and which started working in Europe in 1999 and in Asia in 2000. (www.tapaemea.com)

Regulating body

The membership is approved by BoD (currently there are 11 boards of members)

Covered Routes

TAPA covers only the truck transport routes in USA, Europe, Middle East, Africa, and Asia.

Transport mode

As opposed to most other security initiatives in the supply chain, TAPA’s security measures focus on truck transports and do not take up container transports at sea at all.

Participation/status

207 members in the world

Category

Private-Voluntary

Goal

TAPA’s overall goal is to identify the fields in which members experience losses, and to share information on effective

To protect the assets of the high tech industry in EMEA in the supply chain by:

- Exchanging information on a global basis
- Co-operating on preventive security
- Increasing support from the logistics and freight industry and where appropriate, from law enforcement and governments
- Work as a parallel organization with TAPA US/ APAC.

Special requirements

Since the program focuses in its entirety on the transport of high-tech goods, the possibility to become a member of the program is strictly limited for an average company. Initially, only companies that produce or export high tech goods could become members, but this was later extended to include companies producing other high value goods.
6. CSI

**Originated country/area**
In few US ports in 2002.

**Regulating body**
CBP (www.cbp.gov)

**Covered Routes**
CSI is applicable to the containers coming in the US. However there are several ports in the North and South America, Caribbean, Europe, Asia and Africa, which are operating CSI.

**Transport mode**
As it is applied to the ports it covers the sea containers.

**Participation/status**
58 CSI ports, which is about 86% of the total port in the world.

**Category**
US Government- Voluntary

**Goal**
Their mission is to target and pre-screen containers and to develop additional investigative leads related to the terrorist threat to cargo destined to the United States.

**Special requirements**
The countries that want their ports to be CSI ports must fulfil a large number of requirements. Their customs administration must be technically capable of implementing NII (Non-Intrusive Inspection- i.e. inspections are made without having to enter a container physically, which is often costly and can create delays in the flow) inspections of all goods that are imported, exported, in transit, or transhipped through the country in other ways. The port in question must have direct, regular and substantial container traffic to ports in the USA. The port authorities, together with the customs, must undertake to produce a risk management program that can identify possible high risk containers. Furthermore, the country’s authorities must be prepared to share information with the USA and CBP to facilitate a joint focus on high risk objects, and be prepared to introduce an automated mechanism for this exchange of information.
7. PIP

**Originated country/area**

PIP was developed in Canada in 1995 with an objective “on promoting business awareness and compliance with customs regulations”. However after the 9/11 the focus is shifted to the supply chain security (www.cbsa-asfc.gc.ca/security-securite/pip-pep/menu-eng.html).

**Regulating body**

Canada Border Services Agency (CBSA)

**Covered Routes**

Import to Canada

**Transport mode**

All

**Participation/status**

Based on the statistics of 22.08.08 there are about 615 companies have signed the agreement with CBSA.

**Category**

Government-voluntary

**Goal**

To secure the supply chain and facilitate legitimate trade.

**Special requirements**

The applicant owns or operates facilities in Canada that are directly involved in the importation and exportation of commercial goods or the applicant is a U.S. company applying for a FAST (Canada) membership.

If a PIP applicant has been validated by the U.S. Customs-Trade Partnership Against Terrorism within the last two years, a site validation by PIP may not be required. However, each program reserves the right to perform its own site validations.
8. StairSec

Originated country/area
Sweden

Regulating body
Swedish ministry of transport

Covered Routes
Any country to Sweden (import)

Transport mode
Air and sea

Participation/status
30 (Gutierrez and Hintsa, 2006)

Category
Government-voluntary

Goal
This module makes it possible to quality assure operators within the Stairway not only for quality in their customs routines but also for the security measures they have taken to prevent terrorists from using the operators commercial flow of goods for transporting weapons of mass destruction.

Special requirements
According to the Swedish Customs, one requirement in the development of StairSec was that the system should comply with the requirements made by other international security systems such as C-TPAT and CSI.
9. STP (Secure Trade Partnership)

Originated country/area
Singapore

Regulating body
Singapore customs (www.customs.gov.sg)

Covered Routes
Import, export and transit in Singapore

Transport mode
Sea

Participation/status
22 partners.

Category
Government-voluntary

Goal
Through the STP programme, Singapore Customs seeks to:

- create awareness of the importance of adopting a total supply chain approach to cargo security;
- encourage companies to play their part in securing their own processes within supply chains;
- enhance the security of global supply chain and prevent disruptions to the smooth flow of goods;
- profile Singapore as a secure trading hub.

Special requirements
N/A
10. Secure Export Partnership

**Originated country/area**
New Zealand

**Regulating body**
New Zealand Customs

**Covered Routes**
NZ to any country export

**Transport mode**
All

**Participation/status**
Not enough information has been found regarding this topic.

**Category**
Government- voluntary

**Goal**
It is designed to protect cargo against tampering, sabotage, smuggling of terrorists or terrorist-related goods, and other transnational crime, from the point of packing to delivery”. Exporters from New Zealand are eligible and encouraged to participate; especially those moving goods to the US. The program emphasizes that security measures are customizable depending on the applicant’s situation.

**In relation with other Security Programs**
CSI, C-TPAT

**Special requirements**
N/A
11. Frontline

Originated country/area
Australia

Regulating body
Australian customs

Covered Routes
Import & export in Australian companies

Transport mode
All

Participation/status
700 companies

Category
Government- voluntary

Goal
Frontline focuses, in common with Partnership in Protection – PIP, on preventing illegal imports and exports through the collection of information from partner companies.

In relation with other Security Programs
C-TPAT, CSI, PIP, EU AEO.

Special requirements
N/A
12. APEC/STAR

Originated country/area
Australia

Regulating body
Apec observers (the Association of Southeast Asian Nations secretariat, the pacific economic cooperation council and the pacific islands forum secretariat.) (www.apec.org)

Covered Routes
Pacific Ocean Area

Transport mode
Sea and Air

Participation/status
21 member countries

Category
International-Voluntary

Goal
- To develop and strengthen the multilateral trading system
- To increase the interdependence and prosperity of member of economies; and
- To promote sustainable economic growth.

Special requirements
In 1997, APEC imposed a moratorium on new members until 2007. The guidelines for admitting new members as outlined in the Joint Statement of the 1997 APEC Ministerial Meeting include:

- an applicant economy should be located in the Asia-Pacific region;
- an applicant economy should have substantial and broad-based economic linkages with existing APEC members; in particular, the value of the applicant’s trade with APEC members, as a percentage of its international trade, should be relatively high;
- an applicant economy should be pursuing externally oriented, market-driven economic policies;
- an applicant economy will need to accept the basic objectives and principles set out in the various APEC declarations, especially those from the Economic Leaders’ Meeting;
- a successful applicant will be required to produce an Individual Action Plan for implementation and to immediately participate in the Collective Action Plans across the APEC work program;
- the admission of additional members to APEC requires a consensus of all existing members. In 1997, APEC imposed a moratorium on new members until 2007. The guidelines for admitting new members as outlined in the Joint Statement of the 1997 APEC.
13. 24 Hour Rule

Originated country/area
USA

Regulating body
CBP

Covered Routes
Any country to USA (exports)

Transport mode
Sea vessels

Participation/status
Not enough information has been found regarding this topic.

Category
Government-Voluntary

Goal
The rule makes it possible for customs personnel in the USA to make an advance examination of high risk consignments before a container is loaded in a foreign port.

Special requirements
The fact that the advance notification must be made 24 hours before a container is loaded means, in other words, that when the vessel has arrived in the port there is no time for advance notification of new shipments. Last minute shipments cannot be taken on board.

Where air transport is concerned, the information shall be submitted to CBP directly after the departure of the flight.
14. ISPS Code

Originated country/area
The International Maritime Organization (IMO) was established in 1948 in Geneva.

Regulating body
IMO (www.imo.org)

Covered Routes
International

Transport mode
Ships and port

Participation/status
The IMO has 167 member states at the present time.

Category
International- Mandatory

Goal
The purpose of the Code is to provide a standardized, consistent framework for evaluating risk, enabling governments to offset changes in threat with changes in vulnerability for ships and port facilities.

The goal of the ISPS Code is, according to the IMO, to establish an international framework for cooperation between governments, government agencies, local administrations, and shipping and port industries. This framework is intended to facilitate the detection and analysis of threats to security and the introduction of preventive measures to meet security incidents that affect ships or port facilities used in international trade. With the aid of the Code the roles and responsibilities of all parties shall be defined, at both national and international level, for ensuring maritime security.

Special requirements N/A
15. WCO SAFE

Originated country/area
At the June 2005 annual Council Sessions in Brussels, Directors General of Customs representing the Members of the World Customs Organization (WCO) adopted the SAFE Framework of Standards by unanimous acclamation.

Regulating body
WCO (www.wcoomd.org)

Covered Routes
Worldwide

Transport mode
All

Participation/status
154 countries have expressed their intention to implement the program. (Situation in 9/6/2008)

Category
International-voluntary

Goal
International organizations aiming to establish supply chain security standards that can be generalized for the entire trading community.

The SAFE Framework aims to:

- Establish standards that provide supply chain security and facilitation at a global level to promote certainty and predictability.
- Enable integrated supply chain management for all modes of transport.
- Enhance the role, functions and capabilities of Customs to meet the challenges and opportunities of the 21st Century.
- Strengthen co-operation between Customs administrations to improve their capability to detect high-risk consignments.
- Strengthen Customs/Business co-operation.
- Promote the seamless movement of goods through secure international trade supply chains.

Special requirements
N/A
16. The Golden List Program

Originated country/area
Jordan

Regulating body
The Jordan customs

Covered Routes
Import & export in the companies in Jordan

Transport mode
Pilot phase, can cover all

Participation/status
15 companies

Category
Government-voluntary

Goal
It is a program that has the aim of securing the supply chain. One important idea behind the program is to attract foreign investors by creating a more secure investment climate.

Special requirements N/A
17. Operation Safe Commerce (OSC)

Originated country/area

U.S.A

Regulating body

Department of Transportation and U.S Customs (www.dot.gov).

Covered Routes

This initiative will ensure the security of the containers that will pass through our ports and on to America's highways and railways.

Transport mode

Containers

Participation/status

Pilot

Category

Government-driven pilotVoluntary (this initiative is set up by U.S government, shipping industries and private business)

Goal

Operation Safe Commerce will provide a test-bed for new security techniques that have the potential to increase the security of container shipments. DOT and Customs will use the program to identify existing vulnerabilities in the supply chain and develop improved methods for ensuring the security of cargo entering and leaving the United States. Those security techniques that prove successful under the program will then be recommended for implementation system-wide.

Special requirements N/A
18. SSTL (US Smart and Secure Trade Lanes)

Originated country/area

Regulating body
Strategic Council on Security Technology

Covered Routes
Imports in USA

Transport mode
Sea

Participation/status
15 world’s largest international ports and trade lanes have participated in the initiative.

Category
Private (Supported by U.S Government and initially funded by the port operators) - Voluntary

Goal
The initiative’s ultimate goal is to enhance the visibility of each container shipment as well as the transparency of those shipments within the overall supply chain, improve the physical security of containers and their contents and create an audit trail that enables the system to analyze, learn and adjust to dynamic changes.

Special requirements
N/A
19. EU-China: Smart and Secure Trade Lane Pilot Project

**Originated country/area**
During the 2nd session of the Joint EU-China Customs Cooperation Committee (JCCC) session on 19 September 2006, EU and China reached to an agreement to initiate this pilot project.

**Regulating body**
EU and China Customs

**Covered Routes**
Initially involves Rotterdam (NL), Felixstowe (UK) and Shenzen (China).

**Transport mode**
Initially the sea ports

**Participation/status**
Pilot project

**Category**
Government-Pilot

**Goal**

**Special requirements**
None
2.3 Comparison of security programmes and measures

The existing voluntary security programs have been created for different purposes and by different agencies or organizations. Four types of programs have been identified: i) Customs compliance programs to which the security layer has been added; ii) Government origin, pure security programs; iii) International organization origin, security standards programs; and iv) Private origin, pure security programs. Table 1 summarizes the main motivation and philosophy for each type and provides examples of programs belonging to each group (Gutierrez X. and Hintsa J., 2006).

Table 2.1. Identified types of voluntary supply chain security programs (Source:???)

<table>
<thead>
<tr>
<th>Type of Program</th>
<th>Examples</th>
<th>Main motivation and philosophy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customs compliance programs to which the security layer has been added</td>
<td>PIP (Canada), StairSec (Sweden), ACP &amp; Frontline* (Australia), AEO (EU)</td>
<td>Customs administration aiming to streamline Customs processes (e.g. accounting, payment and clearance) for compliant importers/exporters. Due to new security concerns these programs have added a security layer. This implies that importers/exporters eligible for border crossing facilitation benefits should not only be Customs compliant but also low risk.</td>
</tr>
<tr>
<td>Government origin, pure security programs</td>
<td>C-TPAT(USA), Secured Export Partnership (New Zealand)</td>
<td>Governments and border agencies motivated by recent terrorist attacks. Security measures aiming to transfer some of the customs control responsibilities to importers/exporters, in order improve the capacity to detect illegal activities. These programs have become prerequisites for participating in other Customs compliance programs.</td>
</tr>
<tr>
<td>International organization origin, security standards programs</td>
<td>WCO framework of standards, ISO (International organization for standardization)</td>
<td>International organizations aiming to establish supply chain security standards that can be generalized for the entire trading community.</td>
</tr>
<tr>
<td>Private origin, pure security programs</td>
<td>BASC (Latin America), TAPA (technology companies)</td>
<td>Private companies exposed to high risk of suffering from illegal activities in their cargo management operations. Security measures targeting the protection of cargo from being tampered or removed illegally.</td>
</tr>
</tbody>
</table>

In order to carry out a systematic comparison of the selected security programs the security measures that companies must fulfil in order to be considered security compliant were reviewed. There is high variability regarding the level of detail in which these measures are presented. While some programs provide a complete list of activities, processes, controls and technologies that need to be implemented, others just provide a small list of what could be called “security musts” putting the onus on each company to enforce the security measures that they consider necessary given their own constraints. Despite of these differences, it can be observed that most of the programs promote security measures which target one or more of the following security goals:
• Facility management: Guaranteeing the security of the facilities where cargo is stored and handled.
• Cargo management: Protecting cargo during all steps of shipping and transport processes.
• Human resources management: Guaranteeing trustworthiness and security awareness of all personnel in direct and indirect contact with cargo and other company assets.
• Information management: Protecting critical business data and exploiting information as tool for detecting illegal activities and preventing security breaches.
• Business network & Company management systems: “Building security in” into internal and external organizational structure and company's management systems.

Each of the previous goals can be achieved in different ways. For instance, Information management is a combination of capturing high quality cargo information, storing it adequately, sharing it with the pertinent partners and protecting it from unauthorized access and usage. At the same time, high quality cargo information can be achieved by implementing error-proof documentation processes, increasing the quantity of data, integrating the data and many other related measures. In order to create a common supply chain security management framework, with an appropriate level of detail but still general enough to be able to compare the different programs, it was decided upon that a classification of the security measures belonging to each of the previous five goals, into five sub categories was necessary. Figure 2.8 summarizes the resulting framework.

Even though this framework covers most of the security measures suggested by the current leading supply chain security programs, it is important to note that there is no exact formula to establish an adequate supply chain security management system. The
security measures that constitute the framework are not all-inclusive; meaning that implementing them all does not necessarily mean that the security system will be complete, and that implementing only part of them does not necessarily mean that the security will be inadequate. However, this framework provides a better understanding of the concrete measures suggested by each program and can be used to evaluate how similar or dissimilar these programs are. Table 2.2 shows the security measures within the general framework that are present in each of the studied programs (data from year 2005).

Table 2.2. Comparison of security programs (source:????)

<table>
<thead>
<tr>
<th>Security measures / Security Initiative</th>
<th>WFO</th>
<th>BASC</th>
<th>TAPA</th>
<th>C-TPA</th>
<th>BSI</th>
<th>ISO 27001</th>
<th>ECSEL</th>
<th>PIP</th>
<th>BASC TAPA C-TPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Facility management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1 Warehouse/terminal layout design</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2 Inventory management and control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>67%</td>
<td></td>
</tr>
<tr>
<td>1.3 Facility protection (fences; locks; walls; minimization of exit and entry points etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1.4 Facility monitoring (24hr camera system, security guards, filming activities of loading containers, picking etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1.5 Access/Presence control processes and technologies (id / badges; smart cards; biometrics etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2. Cargo management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1 Prevention, detection and reporting of shipping process anomalies (routes and schedules continuous review; alerts management, detection and follow-up of overages and shortages etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2.2 Inspections during the shipping process (in points where liability changes, to packaging materials and vehicles before getting in contact with cargo, reporting of shortages overages etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2.3 Exploitation of cargo inspection technical solutions (use of various scanners; nuclear/chemical/biological weapon sensors/detectors etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2.4 Exploitation of cargo tracking technical solutions (bar codes, RFID, satellite tracking, etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2.5 Exploitation of cargo and vehicle anti-tampering technical solutions (use and control of high security seals; vehicle immobilisation devices; etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3. Human resource management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1 Employee hiring / exit process (background checks; interviews for leaving or fired employees etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3.2 Personal training process (continuous training on security issues; risk awareness etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3.3 Information dissemination process (internal and external publication of the company security policies)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3.4 Organizational roles and responsibilities (establish security goals, assign security responsibilities to personnel, identify security required skills etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3.5 Security culture development (motivation and incentive programs targeting for cooperation and engagement with security issues)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4. Information management systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1 Quality information/data management (manage more complete and accurate shipment information, establish error-proof documentation processes, data integration etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4.2 Protection of business information/data (management procedures and storing methods design to protect information from unauthorised access and usage)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4.3 Recordkeeping of shipping information for potential security audits (maintenance of complete records of the custody of cargo, improved recordkeeping methods; quality control of records, errors correction etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4.4 Data exchange with Customs administrations (readiness to provide complete and on-time information as required; in particular compliance with Advance cargo information schemes etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4.5 Use of international standards for data management (WCO Customs Data model, Unique Consignment Reference, digital signatures, digital certificates etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5. Business network &amp; Company management systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 Company security management system (defined and documented security processes, defined and controlled security indicators; internal and external audits, etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5.2 Logistics system designed to reduce risks (Evaluation of scenarios of natural risks, accidents, intentional human acts, terrorism etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5.3 Logistics system designed to guarantee quick eventual disaster/failure recovery, contingency plans, additional capacity, alerts management etc.)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5.4 Business partners evaluation system (selection of low risk and high security compliant suppliers, clients and subcontractors)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5.5 Establishment of collaborative relationships with Customs administrations and other border agencies with control or security functions; Procedures for the notification of anomalies or illegal activities. Consultation customs regulations and security matters.</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Degree of similarity to the general supply chain security framework 48% 60% 58% 56% 60% 24% 76% 60% 64%
It is clear from the table that there are no two programs suggesting the exact same set of security measures. In contrast, it can be observed that each one targets the same security objectives but suggests different ways to achieve them. In spite of this apparent incompatibility between the programs it is possible to observe/see that there are several voluntary security measures that are suggested by most of the studied programs. Figure 2.9 shows the security measures organized by the percentage of programs that suggest them.

**Figure 2.9. Security measures organized by percentage of programs suggesting them (Source:???)**

It can be observed that there is a group of five security measures (Facility protection, Access/presence control process technologies, Personnel training process, Employee hiring process and Protection of business information/data) that are present in more than 80% of the studied voluntary security programs. Following this group, it is possible to identify six measures that appear on average in 70% of the existing programs (see details in Figure 2.9). It can be noted that they mainly refer to collaboration with government and other business partners, and to internal company security processes. It can be argued that while the five most common security measures target the security of the human, physical and information resources itself, the second most frequent group of measures deals with the internal and external processes that interconnect these resources during daily operations. On the other hand, measures targeting quick recovery after disaster and those suggesting the use of specific data or technological standard were found to be the least common measures among the analyzed programs.
2.4 Comparison of toolkit solutions

Since 9/11, a great number of security initiatives have been launched and implemented. Some of these are compulsory and have been laid down in legislation or government directives. Others are commercial initiatives, and, in principle, non-compulsory. Some examples of the latter are C-TPAT, ISO28000 and TAPA.

To help especially small and medium sized enterprises to find out what is required from them in terms of security measures, and which existing measures qualify them for which security certificate, a number of toolkits have been developed over the years. This section will give a brief description of some of these toolkits, and their use.

2.4.1 The Port of Rotterdam ISPS toolkit

The IMO ISPS code was launched as chapter XI of the SOLAS convention towards the end of 2002 and became effective July 2004. It contains a number of required measures for the securing of ships and port facilities. The most important of these are the designation of ship and port facility security officers, and the development of a security plan based on a security assessment, for each ship and port facility (i.e. port terminal).

To assist the terminals in the Port of Rotterdam area, the Port of Rotterdam, together with several partners (among which a large insurance broker, Aon), developed a toolkit that can assist the terminal operators to perform the security assessment and develop the security plan.

This toolkit was later introduced in other ports in The Netherlands, Belgium, and several countries around the world. The Worldbank has also adopted the toolkit.

The toolkit applies to a slightly larger area than is originally intended by the ISPS code. The port facility only refers to the quay side of a terminal. However, in most cases, the terminal as a whole will fall under the ISPS security assessment and security plan.

Toolkit elements are:

1. risk assessment support
2. action plan
3. standardised security plan

The toolkit provides support for the risk assessment through a Threat and Risk Analysis Matrix. This analysis is supported by questions on over 400 topics from the ISPS code. It results in the threat and risk analysis matrix and an assessment.

The action plan is a gap analysis between the answers to the questions in the risk assessment and ISPS benchmarks. This plan indicates where further action by the terminal operator is required.

The security plan is generated by the toolkit on the basis of the risk assessment and the action plan. The security plan also contains an overview of the procedures that need to be followed for the various security levels.
2.4.2 IRU security toolkit

In the IRU Goods Transport Council Yokohama meeting in April 2004, a Task Force on Security (TFS) was established with the objective to elaborate voluntary security guidelines for road transport operators. Representatives of 8 IRU Member Associations took part in the drafting of the guidelines: AFTRI, ANTRAM, ATRH, DTL, FEBETRA, RHA, TLN and ZMPD.

The guidelines (published in 2005) contain voluntary measures for:

- Managers,
- Drivers,
- Shippers,
- Operators carrying dangerous goods and,
- Customs-related guidelines.

The IRU guidelines should be seen in relation to other standards of supra national bodies, such as ECMT, and other related initiatives within IRU, among others, on customs matters and dangerous goods.

In part, the toolkit is basically a list of recommendations that serves more as a check list than as an active tool to support company security policy.

In addition to these recommendations, the toolkit also contains predefined structures for a company security plan, an operational review, incident reporting, and ‘what to do in
case …’ lists. For the dangerous goods, the guidelines incorporate the security chapter from the ADR rules (chapter 1.10). ADR is mandatory, and for certain types of dangerous goods, the security rules are therefore also mandatory.

2.4.3 Integrated logistics security toolkit

The transport and logistics sector is at the receiving end of most of the security regulation and programmes: they are the service providers (either logistics services or transportation and related services) that bear the brunt of the rules to which shippers have committed themselves in programs such as TAPA and CTPAT. As such, many SME logistics service providers are confronted with rules and regulations from many different angles, and experience great difficulty to find out if what they have is sufficient, and what additional measures they should take, and which program that qualifies them for.

In the Netherlands, the Dutch Transport and Logistics Netherlands Industry Association has launched, together with insurer AON and others, an initiative to develop an integrated toolkit that contains all relevant security regulation and programs for the transport and logistics section. The aim of the toolkit is to help businesses address the issues mentioned above.

The toolkit is currently under development, and includes:

- ADR 1.10
- EC 648/2005 AEO
- EC 622/2003 Air freight; regulated agent
- EC 725/2004 ISPS code
- EC 251/2006 secure operator (currently put on hold)
- TAPA FSR and TSR

The toolkit will have the same web-based approach as the Port Facility Toolkit, such as a smart questionnaire (that skips questions that are not relevant for the particular user) and a reporting module that can generate standard security management plans.

The toolkit is not only targeted at businesses, but also at various authorities (Customs, Harbour Master, Water Police) to enable the quick verification of compliance, and offer planning support.

2.4.4 ICC Customs security toolkit

The ICC has long been involved in international trade and trade facilitation. As such, it has developed a host of guidelines on Customs procedures and operations. In light of the heightened attention for terrorism, ICC has put together the most relevant of these guidelines in a ‘toolkit’ in order to facilitate the rapid assessment of the security management of Customs organisations, and the ways in which internal company procedures can help customs detect risks.

This toolkit overlaps to some extent with another ICC toolkit in customs and other officials’ integrity. Also, there is strong reference to the role of WCO in coordinating
Customs initiatives, to avoid unilateral security initiatives by individual customs organisations.

The topics in the guidelines included in the toolkit are:

- Strategic Plan and an internal Annual Management Plan as set out in Guideline 1.
- Quality of the Customs Workforce (Guideline 3),
- Automated Information (Guideline 35) and Automated Risk Assessment (Guideline 36) systems. Internal Security Unit (Guideline 4)
- Staff Identification (Guideline 5)
- Fraud Investigation (Guideline 6)
- Pre-arrival Entry and Post-entry Audit (Guideline 9)
- Compulsory port or airport warehousing (Guideline 13).
- Automated risk-assessment (Guideline 14)
- Non-intrusive Inspection equipment (Guideline 17)
- Convergence of Official Controls (Guideline 20)
- Transit measures (Guidelines 25 and 26)
- Consultation with the Trade (Guidelines 29)
- Customs Trade Memoranda of Understanding (Guideline 30)
- Support for WCO (Guideline 49)
- Mutual assistance (Guideline 50)

2.4.5 AIAG Automotive supply chain security toolkit

AIAG (the automotive industry action group) has many members who are early adopters of the CTPAT scheme of the USA. This program has evolved in the sense that some parts have become mandatory in order to obtain customs benefits. One of these measures is the risk based assessment of suppliers, vendors and service providers. Many major auto industry OEMs and Suppliers are now facing the task of how to implement these measures in an acceptable and certifiable way. Importers and their foreign suppliers and transportation providers will have to perform assessments based on risk criteria to evaluate which measures are appropriate in which part of the chain.

AIAG has developed an extensive toolkit to support this process and help companies align the security measures throughout the entire chain.

2.5 Bottlenecks

This section names and describes current security bottlenecks along the supply chain. It includes a description of hampering effects of the bottlenecks, and also possible measures towards a solution. Most security issues concern the prevention of the theft of goods or information and of terrorist attacks, therefore this section focuses on links in the supply chain that are crucially exposed to these risks.
2.5.1 Structural Security Bottlenecks

Security in the supply chain is a matter that concerns all actors within the chain. A publication of the OECD argued that “transport authorities must address weak links of the container supply chain.” If one link of the chain is weaker than the other it compromises the security of the whole chain. (ECMT/OECD 2005)

In fact many of the actors along the chain are small- and medium-size companies, one major problem is that security standards of the companies in the chain differ. It is often a matter of cost that smaller companies cannot guarantee for the same security-quality as the larger actors in the supply chain. Therefore transport authorities must address week links of the container transport chain. Up to date bilateral and international security initiatives had their main focus on security assurance of the larger supply chain actors, in future the scope will lie on the assurance of security for the smaller inland carriers, which will be difficult due to the fact that these small actors are numerous and disparate in nature (ECMT/OECD 2005).

2.5.2 Security awareness

As mentioned earlier in a supply chain every actor is responsible to ensure the security of the goods. That includes the physical security of the goods, but also data security. The supply chain is only as strong as its weakest link. Currently, security issues are not always taken seriously by all supply chain actors. Measures should focus on the creation of security awareness. The C-TPAT certification for example includes security awareness trainings (http://www.cbp.gov/).

2.5.3 Customs controls

Customs controls also play a vital role in the security chain, and can also represent a security bottleneck. In practice customs controls differ in quality from country to country. The OECD claims that, in general, land-side border crossings bear a higher risk than the sea-side entry into a country (ECMT/OECD 2005).

The reason is that customs controls for land-side entries often have lower standards, and in addition, delays in the customs control process result in a high risk exposure while the goods are standing still. Measures of ensuring higher security could focus on ensuring minimum standards for customs controls and avoidance of delays due to inefficient processes. Security measures that focus on customs site security have to be taken seriously in a similar way as for the container stuffing sites.

2.5.4 Sealing

Another bottleneck in supply chain security concerns sealing standards for containers. A container is generally sealed by the shipper after the goods have been loaded into the container. The purpose of sealing is to prevent the goods from being stolen or manipulated. There are different types of seals that include mechanical seals and electronic seals. Also, there are three types which can be distinguished, according to the level of protection they offer. These types are: indicative seals, security seals, and high security seals.
The purpose of the first one is to indicate if a container had been opened after sealing. It just gives an indication whether the container remained closed during the entire journey. The security seal serves the same purpose, but they also have a unique seal number for identification and a stamp of the seal owner which makes this type slightly safer compared to the first seal type. The third type is the “high security seal”, which aims to physically protect the container from being opened by unauthorized persons (ECMT/OECD 2005).

In practice a major problem is the heterogeneity of sealing standards and practices of various shippers. Since there are numerous types and forms of seals and stamps, it is hard for the opener to proof if the seal is still the original one. Therefore in practice the seal number double check with the shipper is not always taken seriously by the seal openers. In order to grant a higher level of security, minimum standards should be defined. It also should be considered that the sealing process is a factor for the overall security. The quality sealing process could be guaranteed, for example, by proper documentation, seal use training, correct application of seals, recording of anomalies, identification of the persons and parties involved in the process, etc (ECMT/OECD 2005).

2.5.5 Warehouse security

The physical security of the goods is not only at risk during the actual transport process but especially at the links of the chain where the goods are not moving. “Containers are most vulnerable to being tampered with when they are at rest and least vulnerable when they are in motion. This means that security measures are especially important at those nodes in the network where the container is handled and/or stored” (ECMT/OECD 2005).

As a consequence of this, warehouses plays a vital role for the security in the supply chain. The physical security of the goods has to be assured by the warehouse operator. Warehouse security measures can include warehouse access control, video surveillance, security trainings for personnel, additional security personnel, etc. Access control can be achieved by electronic ID-cards and security personnel. TAPA TSR rules have helped a lot in achieving this. Since the introduction of TSR by large logistics service providers, they have observed marked decline in robbing in warehouses, and a shift of crime to the transportation parts of the chain.

2.5.6 Loading and stuffing areas

The areas where containers are loaded and stuffed are very crucial points from the security perspective, because the goods are exposed to a higher risk. Stuffing areas are also the last part on the export side where the goods can be physically identified, before the container gets sealed. There are generally no further visual checks of the goods before the containers are reopened by the customs at the country of destination. Therefore the risk of theft of the goods or manipulation of the container is very high at the stuffing location. In order to guarantee security, the shipper has to take appropriate measures to prevent the numerous security threats. The main activities to achieve this are: ensuring site security (e.g.: fences, surveillance, etc.) and proper stuffing procedures, and compiling an accurate inventory of the shipped goods. In view of the
importance of this chain link, an adequate share of security expenditures should be dedicated to security measures at stuffing areas.

2.5.7 Container handling in port/port security
The handling of containers in port potentially bears a high risk since the major container ports in the world are large in size and the containers are standing still for a certain time. On the other hand, the areas are usually under the control of a single port authority, the handling terminals are usually protected by fences, but also video surveillance, and well trained security personnel and other security systems are common. The international standard for port security is the IMO/ISPS code, which has been adopted in all major ports in the world.

2.5.8 Personnel related security bottlenecks
Personnel, relevant for the supply chain security, includes all persons that have physical contact with the container or with the goods in any form, as well as personnel responsible for the information flow that goes along with the physical cargo transport. The use of unqualified personnel can compromise the security of the chain. Secure processes have to be carried out by qualified and reliable personnel, otherwise the processes and measures are useless or even counterproductive (ECMT/OECD 2005).

Therefore personnel related security measures have to focus on recruiting reliable personnel, especially for sensitive parts of the supply chain, but also on trainings and monitoring procedures. Some of the current security certification also focus on personnel related security issues, and try to improve security awareness.

2.5.9 IT-Process security and information flow
In recent years IT-supported information flow in the supply chain has constantly increased. This leads to a need for higher security standards for IT-processes and information transmission (Kummer/Schramm 2004).

In general, information can be divided in three categories: trade contracts, regulatory compliance, and operational details. Currently data related harmonization problems among supply chain actors are still very common, and different message structures are continuous challenge (ECMT/OECD 2005).

New security concepts include the carriage of data on the container (e-seal, smart container). This information should be distinguished in two groups: security relevant information and information relevant only for the forwarder and or consignee which have no security relevance. For data security reasons only the security relevant data should be carried on the container (ECMT/OECD 2005).
3. The role of Customs

This chapter is about the role of customs agencies in international trade and supply chains. We will first review the role of customs in the 21st century. We then discuss implications of the changing environment of trade and supply chains for customs. After that we review some of the main regulatory developments for customs in recent years, such as the customs security program and AEO. We also discuss the development of international cooperation, with the EU-China cooperation as the main example. The fifth section deals with the role of the WCO and the SAFE framework of standards. We finish this chapter with a brief introduction of some further developments, such single window, UCR and data models.

3.1 Customs’ role in the 21st century

Most of the material for this section is taken from the report by the World Customs Organization (2008) ‘CUSTOMS IN THE 21ST CENTURY - Enhancing Growth and Development through Trade Facilitation and Border Security’.

The role of Customs is to control the movement of goods and thereby secure the states interests and safeguard revenue collection. The key aims have been to ensure compliance with state policies and laws applicable to the cross-border movement of goods, to combat smuggling, and to secure borders, whilst ensuring the facilitation of legitimate trade. Although much of this role will remain the same in the future, some responsibilities will be broadened, and some focus points will be refined and sharpened. In this chapter, we explore the changing global trade landscape; the changing state responsibilities; key objectives for Customs to respond to the changing environment; and building blocks for new strategic direction for Customs administrations worldwide.

The global trade landscape is complex, fluid and highly sensitive to external drivers, including the following ones:

(a) Increased volumes (8% a year, 2002-2006) and complexities of international trade, e.g. complex preferential rules of origin.
(b) New business models and requirements; e.g. Just-in-time distribution; multi-modal transport; protection on IPR infringements etc.
(c) Increased security threats and organized crime; e.g. cross-border fiscal fraud; the smuggling of drugs, dangerous, harmful and prohibited goods.
(d) A new approach to the “border”: New measures are emerging for the end-to-end management of the movement of goods across borders such as the WCO SAFE.
(e) Demands from society: regarding smuggling of prohibited and dangerous goods, such as weapons and narcotics; quality and safety standards; and public health, and the environment;
(f) New trading patterns: approximately 50 % of world trade takes place between connected parties; and
(g) Increase in revenue fraud: including duty and tax evasion and avoidance.

The strategic drivers and new trans-national and national challenges have increased the demands on, and the responsibilities of, states in the 21st Century. According to the UN,
globalization does not reduce but rather redefines the role of the state and the necessary state responses at the national, regional and international levels. Some of the key responsibilities of states – where Customs would have natural roles to play – include the following:

(a) Promoting socio-economic development: Ensuring the proper management of social and economic development by developing and implementing appropriate socio-economic policies;
(b) Creating the conditions for economic growth: Ensuring a level playing field and nurturing an efficient international trading system, which is critical to economic growth and the collection of state revenues;
(c) Controlling borders: Ensuring secure borders is one of the oldest functions of the state. Carrying out this responsibility in a very open world is more important and challenging than ever. States are recognizing that international trade and economic integration raise new global security challenges that have to be addressed internationally so that common solutions can be developed;
(d) Providing security: The concept of providing security, also one of the core functions of the state, has expanded from the traditional notion of military and political national security to also include national economic security; and
(e) Protecting citizens: Protecting citizens against threats such as contaminated food, unsafe toys and consumer products, fake medicines and other counterfeit products also provide new imperatives for Customs.

The common globally accepted mission of Customs is to develop and implement an integrated set of policies and procedures that ensure increased safety and security, as well as effective trade facilitation and revenue collection. This is achieved through efficient and effective use of tools and information in dealing with the international movement of goods, conveyances and people connected with the goods. The objectives that underpin the mission are:

(a) Promoting certainty, predictability and security of the international movement of goods and people accompanying goods by establishing clear and precise standards;
(b) Eliminating duplication and delays in international supply chains such as multiple reporting requirements and inspections;
(c) Supporting the international trading system by creating level playing fields for business at global, regional and national levels;
(d) Strengthening cooperation between Customs administrations as well as between Customs and business and Customs and other government agencies by creating meaningful and beneficial partnerships; and
(e) Providing Customs administrations with the capacity to promote regulatory compliance in a manner that facilitates legitimate trade.

Globalization and the other strategic drivers necessitate a new approach to managing the movement of goods through international trade supply chains and across borders. This requires the development of a New Strategic Direction for Customs. The building blocks for the New Strategic Direction are:

(a) Globally networked Customs: The new challenges of the 21st Century demand a new concept of Customs-to-Customs cooperation.
(b) Better coordinated border management: This entails coordination and cooperation among all the relevant authorities and agencies involved in border
security and regulatory requirements that apply to passengers, goods and conveyances that are moved across borders.

(c) Intelligence-driven risk management: The expanding responsibilities and opportunities facing Customs administrations require a more sophisticated understanding of the risk continuum.

(d) Customs-Trade partnership: Customs in the 21st Century should enter into strategic pacts with trusted economic operators.

(e) Implementation of modern working methods, procedures and techniques: Demands regarding the rapid movement of goods, combined with complex regulatory requirements, require modern innovative approaches.

(f) Enabling technology and tools: Customs must take advantage of new and emerging technologies to enhance, amongst others, processing, risk management, intelligence and non-intrusive detection.

(g) Enabling powers: In order to address these challenges, Customs administrations require appropriate legislative provisions that strengthen enforcement powers, the provision of advance information and the sharing of information domestically and internationally.

(h) A professional, knowledge-based service culture: The future orientation of Customs requires moving towards a knowledge-based and customer-orientated model.

(i) Capacity building: Customs administrations need to ensure that they have the capacity and skills across all dimensions of the operating model to perform all Customs functions most efficiently and effectively.

(j) Integrity: The fight against corruption remains an important task that should be undertaken over the years to come.

To conclude: The challenges Customs are facing, are many: the globalization of business and trade; development and poverty reduction; complex new governance rules; international terrorism; environmental protection; and the increase in trans-national threats. Equally, the opportunities for bold, proactive and innovative responses are just as numerous: a global Customs network; better management of borders; a strategic framework with globally beneficial objectives; a deepening Customs understanding of supply chains and their management; leveraging new technology; and the strengthening of Customs partnerships not only with trade but also with other border, law enforcement and other relevant government agencies.

Finally, the fast-changing global environment demands that governments and Customs leaders respond to these changes. The challenges are formidable and it is imperative for the international trading system that they are addressed. This visionary statement by global Customs leaders is aimed at meeting the requirements of governments, citizens and other stakeholders. The New Strategic Direction for Customs in the 21st Century foresees Customs administrations playing a new and dynamic role in providing their governments with a unique set of capabilities to achieve their respective programmes. For decades to come, Customs will remain a vital force for security and the enhancement of the economic well-being of nations.
3.2 Possible implications of changing environment for customs administrations


Upon request of the World Customs Organization, the Cross-border Research Association team developed a “21st century supply chain model”, following the Delphi methodology. This study aimed to answer the question: What are the possible impacts of the 21st century supply chain model(s) to customs administrations on worldwide basis? Which supply chain aspects are likely to have a connection to customs long-term planning for resources, skills, technologies, facilities etc.? The main points from the 21st century supply chain model are discussed one by one, on their possible impacts on customs operations.

**Customers having more weight in international supply chain systems.**

It is a challenge for international supply chain operations to keep satisfying the customers on shipment by shipment level by delivering the right product, in right condition, at right place, on right time. Any delays in the process, such as extra cross-border waiting times, are likely to introduce customer relationship management problems in the future.

**Manufacturing taking place in new countries/regions, and raw material sources and focused factories serving more global markets.**

This can lead into increase in the amount of international trade transactions, both in trade value and in number of import/export events. New export-import country combinations might also emerge, including possible increase in south-to-south trade.

**Product variety increasing while product life cycles becoming shorter.**

This can lead into more complexities in product classification systems. Keeping up to date on new consumer and industrial products and defining correct duty rates may require more focus on product aspects in customs operations in the future.

**Business-to-business and business-to-government networking and collaboration increasing in the future**

This is an opportunity for customs to gain deeper relationships with various business actors operating in international supply chains. Networking and collaboration can be exploited to create transparency and trust between customs and businesses, as well as operational efficiencies for both customs administrations and for businesses.

**Supply chain service providers increasing their service offerings in logistics, technologies and finance**

This trend can lead into the emergence of “trusted 3rd parties”, e.g. companies which specialize in secure portals data management between all supply chain business and governmental actors, including customs administrations.

**Consolidation and mergers in increasing in logistics markets**

This partially connects to the previous argument on increasing service provider roles. In the future there will be a smaller number of large logistics service companies taking
bigger role in international supply chains. Obviously customs should have a special focus on managing relationships with these big players.

*Sea freight growing possibly faster than air freight.*

This can obviously lead into a situation where customs needs to direct more resources on sea ports and inland operations dealing with sea freight imports and exports.

*International trade, logistics and customs data standards increasing their role*

This is a key requirement for complete automation of cross-border operations and transactions. Customs should do their best to promote the usage of these standards within their business communities.

*Risks and vulnerabilities increasing in international supply chains*

International supply chains, with Just-in-time and lean management principles, are vulnerable for all types of disruptions, caused e.g. by security incidents or by government regulations and countermeasures. Thus customs should take a proactive role in designing and implementing such security standards which support supply chain operations both under normal situations as well as high risk / post-incident situations.

### 3.3 European Customs Regulation and Initiatives

The relevant EU customs regulations that will be discussed below are the proposed security amendments (regulation 648/2005) to the Community customs code, the customs security program, and AEO. This is admittedly a brief selection, but these are relevant for the current projects.

**Customs related security initiatives of the EU**

At the end of July 2003, the European Commission presented to the Parliament and Council a series of measures to address security issues. These measures can be found in [two communications and a proposal for amending the Community Customs Code](#).

This package brings together the basic concepts underlying the new security-management model for the EU’s external borders, such as a harmonised risk assessment system.

The security amendment to the Community Customs Code ([Regulation (EC) n° 648/2005 of 13 April 2005](#)) has been published in the Official Journal of the European Union on 4 May 2005.

With this amendment the European Union introduces a number of measures to tighten security around goods crossing international borders. The measures will mean faster and better-targeted checks. The results are positive for customs authorities, the public and industry.

The measures cover three major changes to the existing Customs Code:

- require traders to provide customs authorities with information on goods prior to import to or export from the European Union (see [Pre Arrival / Pre Departure Declarations](#));
• provide reliable traders with trade facilitation measures see Authorized Economic Operator (AEO);

• introduce a mechanism for setting uniform Community risk-selection criteria for controls, supported by computerised systems.

EC Regulation 648/2005 and its implementing provisions

The follow-up to EC Regulation 648/2005 is the publication of the implementing provisions which set out the operational details in the customs processes for the above mentioned measures. The implementing provisions Regulation 1875/2006 (see also Press Release IP/06/1821 and MEMO/06/495) entered into force on 26 December 2006 and applies within the following timeframe:

Since early 2007, a common risk management framework has been used to support improved risk based controls by customs authorities. The risk management system will be fully computerised by 2009.

On 1/1/2008 the provisions for the Authorised Economic Operator programme (AEO) entered into force. The AEO programme strikes a balance between increasing security requirements and facilitation for compliant traders.

On 1/7/2009 it will become mandatory for traders to provide customs authorities with advance information on goods brought into, or out of the customs territory of the European Community.

Additionally a non-security related measure is introduced with the entering into force of the implementing regulation: Customs authorities are enabled to exchange information electronically on exports between the customs offices involved in the procedure, allowing Community exporters to receive the proof of export immediately after the exit of the goods (Export Control System). The above measures have been developed in close co-operation and consultation with trade. Legislation and guidelines are laying down details for the implementation in practice with a view to uniform application and a level paying field for economic operators within the European Union.

Customs Security Program (CSP)

The EU Customs Security Program covers activities supporting the development and implementation of the above mentioned measures. CSP supports the balanced approach:

Introduce proper security controls to ensure the protection of the internal market and, in close cooperation with major trading partners in the world, secure the international supply chains; and

Provide facilitation to those traders which demonstrate compliant efforts to secure their part of the internationals supply chains
Authorized Economic Operator (AEO)

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 of the Community Customs Code, Member States are entitled to grant the AEO-status to any economic operator that meets common criteria relating to the operators' control systems, financial solvency and compliance record. The status of the authorised economic operator granted by one Member State is recognized by the other Member States, but does not confer the right to benefit automatically in the other Member States from simplifications provided for in the customs rules. However, the other Member States should grant the use of simplifications to authorised economic operators provided they meet all the specific requirements for the particular simplifications.

In considering a request to use simplifications, the other Member States do not have to repeat the evaluation of the operator's control systems, financial solvency or compliance record, which will already have been completed by the Member State that granted the operator the 'status of authorised economic operator', but should ensure that any other specific requirements for use of the particular simplifications are met. The use of simplifications in other Member States may also be coordinated by agreement between the customs authorities concerned.

A project-group with experts from EU Member States and the European Commission has been working on the details of this concept. The project report laid down proposals for the detailed criteria that the AEO has to meet, the authorisation process and benefits for AEO. The Implementing Provisions on AEO have been drafted on the basis of the result of the project-group.

A pilot action involving 11 Member States' customs authorities and 11 companies was organised between January and July 2006 with a view to assisting implementing the AEO concept in the best manner and test the audit and authorisation procedure. The objective of the pilot action was to check the applicability of the AEO guidelines and to
give a more precise idea of the way to proceed with AEO application, audit and authorisation, and to assist the Customs Code Committee in the drafting of the implementing provisions of regulation (EC) 648/2005. The 11 companies have been audited to determine whether or not they were meeting the criteria and conditions to become AEOs. The pilot action gave both customs authorities and companies experience on how to best proceed with the auditing and the authorisation process and provided the legislators with important information.

*Commission Recommended Model on AEO Self-Assessment*

The abovementioned document provides a practical tool for an economic operator to perform a self-assessment and can form part of the process of applying for the AEO status. It follows on from the legislation, EC Regulation 648/2005 and 1875/2006 and the related AEO Guidelines.

This model on self-assessment was recommended by the AEO Pilot group working on the AEO Guidelines. The Commission services recommend its use as a model for self-assessment to facilitate the AEO application process.

It should be noted that there may be some instances where specific national provisions may require additional information or necessitate adaptation of the model.

*Data base on AEO (Authorised Economic Operators)*

The database of economic operators who hold a valid AEO certificate and gave their prior agreement to the publication is available on the Commission website under "Online databases".

### 3.4 Security co-operation EU with 3rd countries (US and China)

**Agreement with the United States of America on intensified customs co-operation on Container Security**

On 22 April 2004, an agreement with the United States on container security within the scope of the existing EU/U.S. customs co-operation agreement was signed (see also [Council Decision 2004/634/EC](#) and press release: [IP/04/525](#)) by the then Irish Minister of Finance, C. McCreevy and U.S. Secretary of Homeland Security, T. Ridge, in presence of European Commission's Director General for Taxation and Customs Union, R. Verrue and CBP Commissioner R. Bonner.

The agreement will improve security on a reciprocal basis for both the EU and the U.S. It will also guarantee the right balance between trade facilitation and security by:

- ensuring that general customs control of legitimate trade takes due account of security concerns; and
- creating equal levels and standards of controls for U.S. and EC operators.

The agreement establishes a working group that will elaborate the necessary operational elements of expanded co-operation, such as minimum standards for CSI ports, common risk criteria and trade partnership programmes.
Results of the EU-US co-operation

Following the 2004 agreement, two expert working groups were established with specific agendas; one group focused on furthering joint efforts in security standards, and the other focused towards the comparison of trade partnership programmes. In pursuit of the agreements' objectives, a series of meetings were held to identify and define programmes and activities that would achieve these objectives (see press release IP/04/1360).

The outcome of these meetings is a joint list of recommendations for the initiation of a series of measures and actions that concerns, amongst other things, the establishment of minimum standards for risk-management techniques, agreed operating procedures for customs controls and CSI requirements for EU ports.

The in-depth comparison of the customs to business partnerships programmes provided on both sides a complete overview of the EU Authorised Operator Concept (AEO) and the US Customs and Trade Partnership Against Terrorism (C-TPAT) programme. The comparison serves as a basis for further development of reciprocal standards and systems for securing and facilitating legitimate trade on both sides of the Atlantic. The developments and the results of the EU-US customs cooperation in this field are closely monitored by other international organisations (WCO, OSCE) and will certainly have an impact on the work in the latter international fora (i.a. the future work in connection with the WCO Framework of Standards (SAFE).

In the 7th EU-US JCCC meeting held in Brussels on January 31, 2006, CBP's Acting Commissioner Ms. Deborah Spero and EC's Director General Robert Verrue endorsed the results of the working groups. They also agreed on the recommendations proposed by the working groups, e.g. to merge both working groups to one Steering Group and to further elaborate activities supporting a reciprocal implementation of the operating procedures and standards developed by the experts.

In the 8th EU-US JCCC meeting, which took place on 22 January 2007 in Washington, CBP Commissioner Ralph Basham and EC's Director General Robert Verrue took note and endorsed the results of the second phase of the EU-US expanded customs cooperation on transatlantic supply chain security and inter alia agreed on focusing in a third phase of the cooperation on three priority actions (Initiate a pilot to test the feasibility of the CSI concept at EU feeder ports, Customs-Trade Partnership Initiatives and Joint Risk Rules).

The roadmap towards mutual recognition of Customs-Trade Partnership programmes

Mutual recognition is an important element in securing the transatlantic supply chain on an end-to-end basis. Based on this common understanding and with a view to the meanwhile adopted EU legislation (see Commission Regulation (EC) No 1875/2006 of 18 December 2006; OJ L 360 of 19 December 2006), the JCCC agreed in its meeting in January 2007 that, in the interim to the formal implementation of the AEO programme on 1 January 2008, a roadmap towards mutual recognition should be developed by US and EU customs experts on trade cooperation issues. The work on the road map, including a pilot exercise, will be taken forward by the EU-US JCCC Steering Group with the inclusion of the appropriate subject matter experts.
Co-operation on supply chain security with China

The European Community has concluded an Agreement on Customs Co-operation and Mutual Administrative Assistance in Customs Matters with the People's Republic of China that entered into force on 1 April 2005. In order to take co-operation on supply chain security forward and work towards mutual recognition and reciprocity of security measures, the EC and China agreed on the occasion of the Joint Customs Co-operation Committee on 19 September 2006 launching as a starting point for strengthened co-operation a pilot project on smart and secure trade lanes that initially involves the ports of Rotterdam (NL), Felixstowe (UK) and Shenzhen (China), with particular emphasis on sea containers.

The customs administrations of the United Kingdom, of the Netherlands and of China exchange as of 19 November 2007 electronic information on sea containers leaving their territory through the ports of Rotterdam, Felixstowe and Shenzhen. This is an important step in our customs cooperation with China and paves the way for reciprocity and mutual recognition of security measures, which the European Community has always favoured.

This operation took place in close cooperation with the European Commission in the framework of the secure and smart trade lanes pilot project launched in September 2006 (see IP/06/1206) by the Commission and the Customs administration of China. The purpose of the project is to test and ensure security from the point of stuffing containers throughout their journey until their final destination.

Both sides agreed in the context of co-operation on security to exchange experience and develop best practices in order to better understand and prepare the implementation of the WCO Framework of Standards to Secure and Facilitate Global Trade. They also agreed to pursue the objectives of reciprocity and mutual recognition of measures for security and facilitation to be implemented between the General Administration of Customs of the People's Republic of China and the Customs authorities of the European Community.

In the short term, the co-operation on the Smart and Secure Trade Lane Pilot Project (SSTL) will allow, among other,

- testing end to end supply chains from the point of stuffing through the entire container movement to the point of final destination;
- agreeing and testing criteria for economic operators to be granted authorised economic operator status with a view to agreeing mutual recognition of AEO concepts on both sides;
- agreeing and testing data requirements for pre-loading security clearance towards "door to door" supply chains;
- defining and agreeing minimum risk rule set (profiles) and minimum control standards for customs clearance and
- testing and evaluating IT and technical solutions that enhance security and control systems while facilitating legitimate trade.

After a testing period of 9 months, it is expected that the pilot will be extended to other ports in the EU and China. This strengthened cooperation should in the long term lead
to increased security and trade facilitation between the EC and China through mutual recognition of security measures, control results and AEO.

3.5 The World Customs Organization: SAFE Framework of Standards

The World Customs Organization (WCO) is an intergovernmental organization that helps Members (Governments usually represented by Customs administrations from 173 countries) communicate and co-operate on customs issues. It was established in 1952 as the Customs Co-operation Council; it adopted its current name in 1994.

![Figure 3.2: Members of the WCO](image)

Headquartered in Brussels, Belgium, it develops agreed rules on customs procedures and provides advice and assistance to customs services. It has established an international standard classification of commodities called the Harmonized Commodity Description and Coding System, which is used to classify goods for tariff purposes the application of tariffs. The WCO has 174 members; see World Customs Organization member states. The current Secretary General is Michel Danet (1999-2008) from France.

In June 2005, the WCO adopted the Framework of Standards to Secure and Facilitate Global Trade ("SAFE"),[1] an international instrument containing 17 standards that promotes security, trade facilitation, anti-corruption, and revenue collection.

On 28 June 2008, Kunio Mikuriya from Japan was elected Secretary General of the organisation and will take office on 1 January 2009. Martyn Dunne from New Zealand was elected Chair of Council replacing Tapani Erling of Finland (2006-2008).

There is a need for a World Customs Organization (WCO) endorsed strategy to secure the movement of global trade in a way that does not impede but, on the contrary, facilitates the movement of that trade. Securing the international trade supply chain is only one step in the overall process of strengthening and preparing Customs administrations for the 21st Century. Accordingly, to strengthen and go beyond existing programmes and practices, WCO Members have developed a regime that will enhance the security and facilitation of international trade. This is the WCO SAFE Framework of Standards to Secure and Facilitate Global Trade (hereafter referred to as the "SAFE WCO Framework" or “Framework”). This WCO Framework to secure and facilitate
global trade sets forth the principles and the standards and presents them for adoption as a minimal threshold of what must be done by WCO Members.

**Objectives and principles of the SAFE Framework**

The Framework aims to:

- Establish standards that provide supply chain security and facilitation at a global level to promote certainty and predictability.
- Enable integrated supply chain management for all modes of transport.
- Enhance the role, functions and capabilities of Customs to meet the challenges and opportunities of the 21st Century.
- Strengthen co-operation between Customs administrations to improve their capability to detect high-risk consignments.
- Strengthen Customs/Business co-operation.
- Promote the seamless movement of goods through secure international trade supply chains.

The Framework consists of four core elements.

First, the Framework harmonizes the advance electronic cargo information requirements on inbound, outbound and transit shipments.

Second, each country that joins the Framework commits to employing a consistent risk management approach to address security threats.

Third, the Framework requires that at the reasonable request of the receiving nation, based upon a comparable risk targeting methodology, the sending nation's Customs administration will perform an outbound inspection of high-risk containers and cargo, preferably using non-intrusive detection equipment such as large-scale X-ray machines and radiation detectors.

Fourth, the Framework defines benefits that Customs will provide to businesses that meet minimal supply chain security standards and best practices.

**Two Pillars of the SAFE Framework**

The Framework, based on the previously described four core elements, rests on the twin pillars of Customs-to-Customs network arrangements and Customs-to-Business partnerships. The two-pillar strategy has many advantages. The pillars involve a set of standards that are consolidated to guarantee ease of understanding and rapid international implementation. Moreover, the Framework draws directly from existing WCO security and facilitation measures and programmes developed by Member administrations.
Pillar 1: CUSTOMS-to-CUSTOMS Standards

Per pillar WCO sets different standards to follow in order to accomplish the goals of the pillar.

**Standard 1 – Integrated Supply Chain Management**

The Customs administration should follow integrated Customs control procedures as outlined in the WCO Customs Guidelines on Integrated Supply Chain Management (ISCM Guidelines).

**Standard 2 – Cargo Inspection Authority**

The Customs administration should have the authority to inspect cargo originating, exiting, transiting (including remaining on board), or being transhipped through a country.

**Standard 3 – Modern Technology in Inspection Equipment**

Non-intrusive inspection (NII) equipment and radiation detection equipment should be available and used for conducting inspections, where available and in accordance with risk assessment. This equipment is necessary to inspect high-risk containers or cargo quickly, without disrupting the flow of legitimate trade.

**Standard 4 – Risk-Management Systems**

The Customs administration should establish a risk-management system to identify potentially high-risk shipments and automate that system. The system should include a mechanism for validating threat assessments and targeting decisions and identifying best practices.

**Standard 5 – High-risk Cargo or Container**

High-risk cargo and container shipments are those for which there is inadequate information to deem shipments as low-risk, that tactical intelligence indicates as high-risk, or that a risk-scoring assessment methodology based on security-related data elements identifies the shipment as high-risk.

**Standard 6 – Advance Electronic Information**

The Customs administration should require advance electronic information on cargo and container shipments in time for adequate risk assessment to take place.

**Standard 7 – Targeting and Communication**

Customs administrations should provide for joint targeting and screening, the use of standardized sets of targeting criteria, and compatible communication and/or information exchange mechanisms; these elements will assist in the future development of a system of mutual recognition of controls.

**Standard 8 – Performance Measures**

The Customs administration should maintain statistical reports that contain performance measures including, but not limited to, the number of shipments reviewed, the subset of high-risk shipments, examinations of high-risk shipments conducted, examinations of high-risk shipments by NII technology, examinations of high-risk shipments by NII and physical means, examinations of high-risk shipments by physical means only, Customs
clearance times and positive and negative results. Those reports should be consolidated by the WCO.

**Standard 9 – Security Assessments**

The Customs administration should work with other competent authorities to conduct security assessments involving the movement of goods in the international supply chain and to commit to resolving identified gaps expeditiously.

**Standard 10 – Employee Integrity**

The Customs administration and other competent authorities should be encouraged to require programmes to prevent lapses in employee integrity and to identify and combat breaches in integrity.

**Standard 11 – Outbound Security Inspections**

The Customs administration should conduct outbound security inspection of high-risk containers and cargo at the reasonable request of the importing country.

---

**Pillar 2: CUSTOMS-TO-BUSINESS Standards**

**Standard 1 – Partnership**

Authorized Economic Operators involved in the international trade supply chain will engage in a self-assessment process measured against pre-determined security standards and best practices to ensure that their internal policies and procedures provide adequate safeguards against the compromise of their shipments and containers until they are released from Customs control at destination.

**Standard 2 – Security**

Authorized Economic Operators will incorporate pre-determined security best practices into their existing business practices.

**Standard 3 – Authorization**

The Customs administration, together with representatives from the trade community, will design validation processes or quality accreditation procedures that offer incentives to businesses through their status as Authorized Economic Operators.

**Standard 4 – Technology**

All parties will maintain cargo and container integrity by facilitating the use of modern technology.

**Standard 5 – Communication**

The Customs administration will regularly update Customs-Business partnership programs to promote minimum security standards and supply chain security best practices.

**Standard 6 – Facilitation**

The Customs administration will work co-operatively with Authorized Economic Operators to maximize security and facilitation of the international trade supply chain originating in or moving through its Customs territory.
WCO Authorised Economic Operator (AEO)

At WCO level the Authorised Economic Operator concept is also elaborated. The SAFE Framework incorporates the concept of the Authorized Economic Operator (AEO), and the Council directed the WCO to develop more detailed implementing provisions for the AEO concept. The conditions and requirements of the AEO at WCO level are nearly equal to the AEO that we know from the EU legislation:

A. Demonstrated Compliance with Customs Requirements
B. Satisfactory System for Management of Commercial Records
C. Financial Viability
D. Consultation, Co-operation and Communication
E. Education, Training and Awareness
F. Information Exchange, Access and Confidentiality
G. Cargo Security
H. Conveyance Security
I. Premises Security
J. Personnel Security
K. Trading Partner Security
L. Crisis Management and Incident Recovery
M. Measurement, Analyses and Improvement

Benefits to the Authorized Economic Operator

The SAFE Framework is premised upon four core elements, the last of these relating to benefits that Customs will provide to businesses meeting minimum supply chain security standards and best practices (SAFE Framework, Section 1.3). Further, Section 3.3 of the SAFE Framework offers certain specific examples for consideration. Ultimately, effective implementation of the SAFE Framework will best be realized by striking a balance between trade security and trade facilitation. Tangible benefits for Authorized Economic Operators are a measure of such balance.

Due to possible limitations imposed by national legislation, any benefits within Customs control must necessarily be defined and offered by individual Members. Pillar 2, Standard 3 of the SAFE Framework provides that such benefits be tangible and documented. These benefits should be enhancements above and beyond the normal procedures utilized when working with non-Authorized Economic Operators and not result in a loss of access to normal procedures already in place.

Benefits should be meaningful, measurable and reportable. The examples of benefits included in this section are separated into categories and offered for consideration by administrations. These do not establish a required set of benefits that all administrations must offer - they are an indicative list of example benefits that are subject to specific Customs consideration, offering and approval. These examples are drawn from several
sources including WCO studies, Conventions, certain operational programs of WCO
Member administrations, the regulations of the European Union, and input from the
trade community. The three categories are: (1) Measures to expedite cargo release
reduce transit time and lower storage costs, (2) Providing access to information of value
to AEO participants, (3) Special measures relating to periods of trade disruption or
elevated threat level and (4) First consideration for participation in any new cargo
processing programs.

3.6 Other developments: single window, UCR, data models

This section describes other important developments for customs, such as the development of
single windows for importers and exporters, the unique consignment reference and various
customs data models.

Single Window

The WCO defines a ‘single window’ as follows:

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”, explaining that “the single window is
clearly a trade facilitative measure. It permits the trader or transporter to submit all the
data needed for determining admissibility of the goods in a standardized format only
once to the authorities involved in border controls and at a single portal. This concept
places the onus on the authorities to manage the Single window and to ensure that the
participating authorities or agencies are either given access to the information or are
actually given the information by the managing authority. It eliminates the need for the
trader or transporter to submit the same data to several different border authorities or
agencies.

Key Elements of Single window are following:

- Fully integrated front- and back-office processes
- Electronic processing from end-to-end
- Services that span government agencies and jurisdictions
- Improved and more accessible business management information

Key to these improvements is how next-generation e-government systems embraces
existing workflows, business rules and legacy systems, leveraging and making use of
current investments.

The single window concept will provide economic operators with the following benefits:

- Easier access to information through better co-ordination between all authorities
  involved– leading to time savings when looking for information and increased
  compliance due to better understanding;
- Improved efficiency when submitting information through exchange of data
  between authorities involved allowing economic operators to give the same
information only once to these authorities – faster processing, more rapid clearance, greater accuracy of data and increased compliance;

- Fewer delays, less uncertainty, and more targeted inspections through better coordination between authorities involved;
- Lower barriers to trade, which makes it possible for new traders to focus on strategic and commercial considerations as opposed to regulatory regulations.

The single window concept will provide Member States and the Community with the following benefits:

- Improved service to customers improving the competitiveness of EU business;
- Reduced levels of inadvertent non-compliance, leading to better ability to focus on those traders that actively try to avoid regulations;
- Better quality of information by increased sharing of information between government agencies – leading to improved security, better ability to target consignments to be inspected;
- Improved efficiency when moving from paper-based to electronic applications, licenses etc. – reduced re-typing, faster processing;
- More joined-up government.

**Developments with UCR**

Unique consignment reference number has been discussed as a trade facilitation tool starting from late 1980s. One long-term bottleneck has been the non-mandatory nature of the instrument. According to the results of the most up-to-date information from WCO (Report of 3rd UCR correspondence group meeting-PV0033E1a) recent developments and discussions could be summarized as follows:

- Some member administrations have showed enthusiasm about exchange of export-import data among them. This will probably lead to single submission of data. (see: Single window)
- It is thought that one of the main rational behind UCR is allowing customs to be more focused on account-based controls rather than physical ones. Account-based controls are basically post-release and use accounting and auditing methodology. UCR will help associated with auditing will enable customs authorities to navigate through all trade transactions by taking UCR as reference.
- Thus, UCR will improve the security level of supply chain and its visibility. As a result, it is expected that integrity of trade data will increase and the establishment of an “audit trail” from origin to destination would be possible.
- It has been suggested to members that acceptance level of UCR should be promoted and these administrations take measures to impose it.
- One of the most challenging questions on the agenda is whether UCR should be mandatory or not. WCO encourages that this issue to be discussed in a wider level such as SAFE and other Supply Chain Management Guidelines.
Another important issue is how to finance the cost with the implementation of UCR system, since this will potentially load more cost to corporate world. As a remedy for that, it has been observed that Korean Government already decided to bear the costs instead of the industries due to the comparative financial weakness of SMEs in this country to carry any additional costs coming from international trade operations.

There is also another suggestion that the UCR become a binding instrument as HS or as an annex to Revised Kyoto Convention.

Also there are ongoing discussions for some time related numbering issues of UCR. There are ideas claiming that these numbers should be random, while opposing side saying that company identifiers should be the essential part of the numbers. The consensus has been reached on the idea that final structure should be based on company identifier, follows the rational in existing prototypes and be as simple and neutral as possible.

In conclusion, this will create hopefully some positive externalities by paving the way for the implementation of more efficient risk management tools because of the improved visibility and traceability of data.

The initiative supported by Korean Customs to promote UCR has been showed as an important model for global application. Also a China-EU project and Wine/Spirit Project could be mentioned in terms of the implication of UCR.

Data models (WCO, SSTL, 10+2)

The main objective of a customs data model are the introduction of common data sets and uniform electronic messages for cargo report, import, and export declarations. The data model enables maximum data requirements for the routine exchange of information between customs and the trader, while countries to require as little information as necessary for customs control purposes.

Basic components of WCO data model are the following (www.customs.gov.au/-webdata/resources/files/wcopres.pdf):

- Data sets in line with UNTDED
- UML class diagrams using CCTS data types
- EDIFACT and XML message specifications
- International code sets
- WCO (HS, UCR)
- ISO (3166 country, 4217 currency, 6346 container, etc.)
- UN Rec’s (5: Incoterms, 16: LOCODE, 20: units of measure, 21: types of packages, 28: modes/means of transport, etc.)
- Others (IATA, ITU, IMO, EAN.UCC, D&B)

WCO Data Model : Version 2 comprises:

- Data sets for import/export manifest, goods declarations & conveyance report
- EDIFACT message implementation guidelines
- International code sets
- Customs and Trade review
- Guidelines on how to compose an XML message


- Complex process of incorporating Other Governmental Agencies (non-trade or customs related) Agencies data;
- Scope is “single window” domain;
- Increased scope for transit
- Considers the implications of XML.

In addition to the data models, there are agreed upon (or enforced) data sets that play a role in some of the current and new customs initiatives. For instance, in the EU-China SSTL project, the agreed upon list of data elements that is exchanged between customs is:

1. Transport document number
2. Conveyance reference number
3. Exit date
4. Customs office of exit, coded
5. Place of loading, coded
6. Tariff code number (Customs)
7. Number of packages
8. Brief cargo description
9. Unique consignment reference number
10. Exporter, Coded
11. Identification of means of transport crossing the border
12. Equipment identification number
13. Seal number
14. Date and time of goods release
15. Customs remarks

By 1/1/2009, the following data elements will be added:

- Consignor
- Consignee
- Person lodging the summary declaration
- Carrier
• Notify party

In the new US 10+2 regulation, the following data elements are mandatory

1. Manufacturer (or Supplier) Name and Address
2. Seller Name and Address
3. Buyer Name and Address
4. Ship to Name and Address
5. Container Stuffing Location
6. Consolidator (Stuffer) Name and Address
7. Importer of Record/Foreign Trade Zone (FTZ)
8. Applicant Identification Number
9. Consignee Number(s)
10. Country of Origin

11. Commodity Harmonized Tariff Schedule of the United States (HTSUS) Number

These are general data elements for all importers. On foreign cargo remaining on board, the following five data elements need to be reported: Booking Party Name and Address, Foreign Port of Unlading, Place of Delivery, Ship to Name and Address, HTSUS Number.

The additional ‘+2’ elements are the ship stowage plan and the container status messages. Especially these two will put a burden on carriers to deliver this information to US Customs.
4 Global SCM Technology

This chapter provides an overview of technology developments in supply chains, with a particular emphasis on security. The first section introduces the various technologies. A second section reports on a brief survey among technology users into their user experiences. The final section lists bottlenecks for further development and adoption.

4.1 Overview of supply chain management technology

Technologies for supply chain management often make use of communication technologies and positioning technology. The very basic concept of these general technologies will first be discussed, then three technology application areas in supply chain security will be discussed in more detail, being:

- Container Security devises and eSeals
- Cargo scanning technologies
- Terminal access technologies

4.1.1 Communication technologies

Communication technologies are being applied in Logistics and Supply Chain Management. Below, an overview is given of the main communication technologies, being:

- Satellite communication
- GSM
- RFID
- WLAN
- Mesh Networking
- Zigbee

Satellite

A communications satellite (sometimes abbreviated to comsat) is an artificial satellite stationed in space for the purposes of telecommunications. Modern communications satellites use a variety of orbits including geostationary orbits, Molniya orbits, other elliptical orbits and low (polar and non-polar) Earth orbits.

For fixed (point-to-point) services, communications satellites provide a microwave radio relay technology complementary to that of submarine communication cables. They are also used for mobile applications such as communications to ships, vehicles, planes and hand-held terminals, and for TV and radio broadcasting, for which application of other technologies, such as cable, is impractical or impossible.
GSM
GSM is the most popular standard for mobile phones in the world. GSM also pioneered a low-cost, to the network carrier, alternative to voice calls, the Short message service (SMS, also called "text messaging"), which is now supported on other mobile standards as well.

RFID
Radio-frequency identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. The technology requires some extent of cooperation of an RFID reader and an RFID tag.
An RFID tag is an object that can be applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves. Some tags can be read from several meters away and beyond the line of sight of the reader.
Today, RFID is used in enterprise supply chain management to improve the efficiency of inventory tracking and management. However, growth and adoption in the enterprise supply chain market is limited because current commercial technology does not link the indoor tracking to the overall end-to-end supply chain visibility. Coupled with fair cost-sharing mechanisms, rational motives and justified returns from RFID technology investments are the key ingredients to achieve long-term and sustainable RFID technology adoption.
About 90% of the world’s trade is transported in cargo containers according to USA customs administration. Because of piracy (Strait of Malacca in Southeastern Asia for example), terrorism or involuntary losses, the need to enhance tracking and tracing of containers has emerged globally. Pundits and operators have come out with the solution of Radio Frequency Identification tag to put on freight containers.

WLAN
A wireless LAN or WLAN or wireless local area network is the linking of two or more computers or devices using spread-spectrum or OFDM modulation technology based to enable communication between devices in a limited area. This gives users the mobility to move around within a broad coverage area and still be connected to the network.

Mesh Networking
Mesh networking is a way to route data, voice and instructions between nodes. It allows for continuous connections and reconfiguration around broken or blocked paths by “hopping” from node to node until the destination is reached. A mesh network whose nodes are all connected to each other is a fully connected network. Mesh networks differ from other networks in that the component parts can all connect to each other via multiple hops, and they generally are not mobile. Mesh networks can be seen as one type of ad hoc network. Mobile ad hoc networks (MANETs), and mesh networks are therefore closely related, but MANETs also have to deal with the problems introduced by the mobility of the nodes.
Mesh networks are self-healing: the network can still operate even when a node breaks down or a connection goes bad. As a result, a very reliable network is formed. This concept is applicable to wireless networks, wired networks, and software interaction. The animation at right illustrates how wireless mesh networks can self form and self heal. For more animations see History of Wireless Mesh Networking

Wireless mesh networks is the most topical application of mesh architectures. Wireless mesh was originally developed for military applications but has undergone significant evolution in the past decade. As the cost of radios plummeted, single radio products evolved to support more radios per mesh node with the additional radios providing specific functions- such as client access, backhaul service or scanning radios for high speed handover in mobility applications. The mesh node design also became more modular - one box could support multiple radio cards - each operating at a different frequency.

**Zigbee**

ZigBee is the name of a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4-2006 standard for wireless personal area networks (WPANs), such as wireless headphones connecting with cell phones via short-range radio. The technology is intended to be simpler and cheaper than other WPANs, such as Bluetooth. ZigBee is targeted at radio-frequency (RF) applications that require a low data rate, long battery life, and secure networking.

ZigBee is a low-cost, low-power, wireless mesh networking standard. The low cost allows the technology to be widely deployed in wireless control and monitoring applications, the low power-usage allows longer life with smaller batteries, and the mesh networking provides high reliability and larger range.

The ZigBee Alliance is a group of companies which maintain and publish the Zigbee standard. The ZigBee Alliance also publishes application profiles that allow multiple OEM vendors to create interoperable products.

**4.1.2 Positioning technology**

One of the main application areas of positioning technology is supply chain management. Identifying the position of cargo in the chain (tracking and tracing) enables the planning and execution of several upstream activities in the supply chain. The following basic satellite positioning technologies are discussed:

- GPS
- GALILEO
- GLONASS
- COMPASS
- IRNSS

GPS
The Global Positioning System (GPS) is a Global Navigation Satellite System (GNSS) developed by the United States Department of Defense. It is the only fully functional GNSS in the world. The Russian GLONASS is a GNSS in the process of being restored to full operation. The European Union's Galileo positioning system is a GNSS in initial deployment phase, scheduled to be operational in 2013. China has indicated it may expand its regional Beidou navigation system into a global system. India's IRNSS, a regional system is intended to be completed and operational by 2012.

GPS uses a constellation of between 24 and 32 Medium Earth Orbit satellites that transmit precise microwave signals, that enable GPS receivers to determine their current location, the time, and their velocity (including direction).

A GPS receiver calculates its position by carefully timing the signals sent by the constellation of GPS satellites high above the Earth. Each satellite continually transmits messages containing the time the message was sent, a precise orbit for the satellite sending the message (the ephemeris), and the general system health and rough orbits of all GPS satellites (the almanac). These signals travel at the speed of light (which varies between vacuum and the atmosphere). The receiver uses the arrival time of each message to measure the distance to each satellite, from which it determines the position of the receiver (conceptually the intersection of spheres - see trilateration[5]). The resulting coordinates are converted to more user-friendly forms such as latitude and longitude, or location on a map, then displayed to the user.

**GALILEO**

Galileo is a global navigation satellite system currently being built by the European Union (EU) and European Space Agency (ESA). The €3.4 billion project is an alternative and complementary to the U.S. Global Positioning System (GPS) and the Russian GLONASS. On November 30, 2007 the 27 EU transportation ministers involved reached an agreement that it should be operational by 2013.

When in operation, it will have two ground operations centers, one near Munich, Germany, and another in Fucino, 130 km east of Rome, Italy. Since 18 May 2007, at the recommendation of Transport Commissioner Jacques Barrot, the EU took direct control of the Galileo project from the private sector group of eight companies called European Satellite Navigation Industries, which had abandoned this Galileo project in early 2007.

Galileo is intended to provide more precise measurements than available through GPS or GLONASS (Galileo will be accurate down to the metre range), better positioning services at high latitudes and an independent positioning system upon which European nations can rely on even in times of war or political disagreement, since Russia or the USA could disable use by others (through encryption). Like GPS, use will also be free for everyone.

**GLONASS**

GLONASS is a radio-based satellite navigation system, developed by the former Soviet Union and now operated for the Russian government by the Russian Space Forces. It is an alternative and complementary to the United States' Global Positioning System (GPS) and the planned Galileo positioning system of the European Union (EU).
Development on the GLONASS began in 1976, with a goal of global coverage by 1991. Beginning on 12 October 1982, numerous rocket launches added satellites to the system until the constellation was completed in 1995. Following completion, the system rapidly fell into disrepair with the collapse of the Russian economy. Beginning in 2001, Russia committed to restoring the system, and in recent years has diversified, introducing the Indian government as a partner, and accelerated the program with a goal of restoring global coverage by 2009.

**COMPASS / Beidou-2**

The Compass system (also known as Beidou-2) is a project by China to develop an independent global satellite navigation system. Compass is not an extension to the previously deployed Beidou-1, but a new GNSS system similar in principles to GPS and Galileo. The new system will be a constellation of 35 satellites, which include 5 geostationary orbit (GEO) satellites and 30 medium Earth orbit (MEO) satellites that will offer complete coverage of the globe.

**IRNSS**

The Indian Regional Navigational Satellite System (IRNSS) is an autonomous regional satellite navigation system being developed by Indian Space Research Organisation which would be under total control of Indian government. The requirement of such a navigation system is driven by the fact that access to Global Navigation Satellite Systems is not guaranteed in hostile situations.

The government approved the project in May 2006, with the intention of the system to be completed and implemented by 2012. The first satellite of the proposed constellation, developed at a cost of Rupee 1,600 crore (16 billion rupees), is expected to be launched in 2009. A goal of complete Indian control has been stated, with the space segment, ground segment and user receivers all being built in India.

It is unclear if recent agreements with the Russian government to restore their GLONASS system will supersede the IRNSS project or feed additional technical support to enable its completion.

The following paragraphs deal with three specific technology application areas in supply chain security:

- Container Security devises and eSeals
- Cargo scanning technologies
- Terminal access technologies

**4.1.3 Container security devices and eSeals**

Container security devices (CSD) play a crucial role in ensuring the integrity of the container along the supply chain and facilitating trade and customs processes. These devises not only ensure the integrity of a container during transportation, but also allows communicating status messages along the chain. Some of the commercially available (on the shelf) CSD are listed below.
The characteristics and technological differences are listed in the table below.

### Table: Comparison of Container Security Devices

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Global Sentinel</th>
<th>CommerceGuard</th>
<th>EDC</th>
<th>SensorTags</th>
<th>GlobalTrak+</th>
<th>CSB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need of LandInfrastructure</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Mounting Time</td>
<td>&gt; 60 sec</td>
<td>&gt; 60 sec</td>
<td>&gt; 60 sec</td>
<td>&gt; 60 sec</td>
<td>&gt; 60 sec</td>
<td>&gt; 60 sec</td>
</tr>
<tr>
<td>Communications:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Satellite</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>GSM (SIM/GPRS)</td>
<td>Quad (SIM &amp; GPRS)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Z225</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>B-SIM (ZigBee, SMS)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ZigBee (5Ghz)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Positioning (GNSS)</td>
<td>12 Channel</td>
<td>12 Channel</td>
<td>12 Channel</td>
<td>12 Channel</td>
<td>12 Channel</td>
<td>12 Channel</td>
</tr>
<tr>
<td>Storage Temperature (Range)</td>
<td>-20°C to +70°C</td>
<td>-5°C to 45°C</td>
<td>-5°C to 45°C</td>
<td>-5°C to 45°C</td>
<td>-5°C to 45°C</td>
<td>-5°C to 45°C</td>
</tr>
<tr>
<td>Temperature Limit (High-Low)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Acceleration</td>
<td>10g</td>
<td>10g</td>
<td>10g</td>
<td>10g</td>
<td>10g</td>
<td>10g</td>
</tr>
<tr>
<td>Humidity Range</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Location</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Wireless remote sensor interface</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Key Switch</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>False Alarm Rate (Certifier)</td>
<td>1% (US Sandia Lab)</td>
<td>1% (US Sandia Lab)</td>
<td>1% (US Sandia Lab)</td>
<td>1% (US Sandia Lab)</td>
<td>1% (US Sandia Lab)</td>
<td>1% (US Sandia Lab)</td>
</tr>
<tr>
<td>Certifications (Certifier)</td>
<td>R4</td>
<td>R4</td>
<td>R4</td>
<td>R4</td>
<td>R4</td>
<td>R4</td>
</tr>
<tr>
<td>Safety Act Certification</td>
<td>IP65</td>
<td>IP65</td>
<td>IP65</td>
<td>IP65</td>
<td>IP65</td>
<td>IP65</td>
</tr>
</tbody>
</table>

**Figure 4.1: Comparison of Container Security Devices (Source:???)**
4.1.4 Cargo scanning technology and scanning equipment

Cargo scanning or non-intrusive inspection (NII) refers to non-destructive methods of inspecting and identifying goods in transportation systems. It is often used for scanning of intermodal freight containers. In the US it is spearheaded by the Department of Homeland Security and its Container Security Initiative (CSI) trying to achieve one hundred percent cargo scanning by 2012 as required by the US Congress and recommended by the 9/11 Commission. In the US the main purpose of scanning is to detect special nuclear materials (SNMs), with the added bonus of detecting other types of suspicious cargo. In other countries the emphasis is on manifest verification, tariff collection and the identification of contraband. As of 2007 less than 5% of US incoming containers are scanned. In order to bring that number to 100% researchers are evaluating numerous technologies, described in the following sections. Important to notice is that 100% security is not possible, not even with 100% scanning. This is a consequence of the fact that the focus with container scanning is only on one particular link in the logistic supply chain.

Generally, two types of scanning variants can be distinguished:

- Active scanning: A system making images of the content of a container based on gamma or Rontgen radiation.
- Nuclear detection; a passive system detecting radio-active materials based on their radiation levels

Active scanning using Gamma-ray radiography

Gamma-ray image of a shipping container showing two stowaways hidden inside. Gamma-ray image of a truck showing goods inside a shipping container. A truck entering a gamma-ray radiography systemGamma-ray radiography systems capable of scanning trucks usually use cobalt-60 or caesium-137 as a radioactive source and a vertical tower of gamma detectors. This gamma camera is able to produce one column of an image. The horizontal dimension of the image is produced by moving either the truck or the scanning hardware. The cobalt-60 units use gamma photons with a mean energy 1.25 MeV, which can penetrate up to 15-18 cm of steel. The systems provide good quality images which can be used for identifying cargo and comparing it with the manifest, in an attempt to detect anomalies. It can also identify high-density regions too thick to penetrate, which would be the most likely to hide nuclear threats.

X-ray radiography

X-ray radiography is similar to Gamma-ray radiography but instead of using a radioactive source, it uses a high-energy Bremsstrahlung spectrum with energy in the 5-10 MeV range created by a linear particle accelerator (LINAC). Such X-ray systems can penetrate up to 30-40 cm of steel in vehicles moving with velocities up to 13 km/h. They provide higher penetration but also cost more to buy and operate. They are more suitable for the detection of special nuclear materials than gamma-ray systems. They also deliver about 1000 times higher dose of radiation to potential stowaways.
Nuclear detection

Recent years it has become clear that Nuclear Detection of containers in ports will become common practice. Only as recent as September 2006, an amendment was proposed for the US SAFE port act in which Nuclear Detection will become mandatory for US-bound containerised cargo. Many of the largest ports in Europe, Asia and the USA are in the process of installing Detection Portals. Almost all these programs take place under responsibility of Customs.

4.1.5 Terminal access control technology

Bar Code Technology

A bar code is a series of alternating dark and light stripes that are read by an optical scanner. The organization and width of the lines is determined by the bar code protocol selected. There are many different protocols but code 39 is the most popular in the security industry. Sometimes the digits represented by the dark and light bars are also printed to allow people to read the number without an optical reader. The advantage of using bar code technology is that it is cheap and easy to generate the credential and it can easily be applied to cards or other items. The disadvantage of this technology is that it is cheap and easy to generate a credential making the technology susceptible to fraud and the optical reader can have reliability problems with dirty or smudged credentials. One attempt to reduce fraud is to print the bar code using carbon-based ink and then cover the bar code with a dark red overlay. The bar code can then be read with an optical reader tuned to the infrared spectrum, but can not easily be copied by a copy machine. This does not address the ease with which bar code numbers can be generated from a computer using almost any printer.

Optical Character Recognition

Optical Character Recognition, usually abbreviated to OCR, is the mechanical or electronic translation of images of handwritten, typewritten or printed text (usually captured by a scanner) into machine-editable text. OCR deals with pattern recognition, artificial intelligence and machine vision.

The OCR technology is more than 99.99% accurate for Latin- script and typewritten text. Recognition of hand printing, cursive handwriting, a text printed text in other scripts (especially those with a very large number of characters)-are still the subject of active research.

In container terminals, OCR is increasingly used to either capture data on container number or truck license plate, or to verify data upon arrival that was already entered in the system before the arrival of the container and/or truck.

Magnetic Stripe Technology
Magnetic stripe technology, usually called mag-stripe, is so named because of the stripe of magnetic oxide tape that is laminated on a card. There are three tracks of data on the magnetic stripe. Typically the data on each of the tracks follows a specific encoding standard, but it is possible to encode any format on any track. A mag-stripe card is cheap compared to other card technologies and is easy to program. The magnetic stripe holds more data than a bar code can in the same space. While a mag-stripe is more difficult to generate than a bar code, the technology for reading and encoding data on a mag-stripe is widespread and easy to acquire. Magnetic stripe technology is also susceptible to misreads, card wear, and data corruption.

**Wiegand Card Technology**

Wiegand card technology is a patented technology using embedded ferromagnetic wires strategically positioned to create a unique pattern that generates the identification number. Like magnetic stripe or bar code, this card must be swiped through a reader to be read. Unlike those other technologies the identification media is embedded in the card and not susceptible to wear. This technology once gained popularity because of the difficulty in duplicating the technology creating a high perception of security. This technology is being replaced by proximity cards because of the limited source of supply, the relatively better tamper resistance of proximity readers, and the convenience of the touch-less functionality in proximity readers.

**Proximity Card Technology**

The Wiegand effect was used in early access cards. This method was abandoned in favor of other technologies. The new technologies retained the Wiegand upstream data so that the new readers were compatible with old systems. Readers are still called Wiegand but no longer use the Wiegand effect. A Wiegand reader radiates a 1" to 5" electrical field around itself. Cards use a simple LC circuit. When a card is presented to the reader, the reader's electrical field excites a coil in the card. The coil charges a capacitor and in turn powers an integrated circuit. The integrated circuit outputs the card number to the coil which transmits it to the reader.

A common proximity format is 26 bit Wiegand. This format uses a facility code, sometimes also called a site code. The facility code is a unique number common to all of the cards in a particular set. The idea is that an organization will have its own facility code and a set of numbered cards incrementing from 1. Another organization has a different facility code and their card set also increments from 1. Thus different organizations can have card sets with the same card numbers but since the facility codes differ, the cards only work at one organization. This idea worked fine for a while but there is no governing body controlling card numbers, and different manufacturers can supply cards with identical facility codes and identical card numbers to different organizations. Thus there is a problem of duplicate cards. To counteract this problem some manufacturers have created formats beyond 26 bit Wiegand that they control and issue to organizations.

In the 26 bit Wiegand format, bit 1 is an even parity bit. Bits 2-9 are a facility code. Bits 10-25 are the card number. Bit 26 is an odd parity bit. Other formats have a similar
structure of a leading facility code followed by the card number and including parity bits for error checking.

Smart Card

There are two types of smart cards: contact and contactless. Both have an embedded microprocessor and memory. The smart card differs from the card typically called a proximity card in that the microchip in the proximity card has only one function: to provide the reader with the card’s identification number. The processor on the smart card has an operating system and can handle multiple applications such as a cash card, a pre-paid membership card, and even an access control card. The difference between the two types of smart cards is found in the manner with which the microprocessor on the card communicates with the outside world. A contact smart card has eight contacts, which must physically touch contacts on the reader to convey information between them. A contactless smart card uses the same radio-based technology as the proximity card with the exception of the frequency band used. Smart cards allow the access control system to save user information on a credential carried by the user rather than requiring more memory on each controller.

PIN

A personal identification number (PIN) falls in the category of what you know rather than what you have. The PIN is usually a number consisting of four to eight digits. Less and the number is too easy to guess. More and the number is too difficult to remember. The advantage to using a PIN as an access credential is that once the number is memorized, the credential cannot be lost or left somewhere. The disadvantage is the difficulty some people have in remembering numbers that are not frequently used and the ease with which a PIN can be observed and therefore used by unauthorized people. The PIN is even less secure than a bar code or magnetic stripe card.

Biometrics

Biometrics refers to two very different fields of study and application. The first, which is the older and is used in biological studies, is the collection, synthesis, analysis and management of data in biology. Biometrics in reference to biological sciences, or biostatistics, has been studied since the early twentieth century. More recently and incongruously, the term's meaning has been broadened to include the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioural traits.

A biometric system can provide the following two functions:

- Verification; Authenticates its users in conjunction with a smart card, username or ID number. The biometric template captured is compared with that stored against the registered user either on a smart card or database for verification.
- Identification; Authenticates its users from the biometric characteristic alone without the use of smart cards, usernames or ID numbers. The biometric template is compared to all records within the database and a closest match score
is returned. The closest match within the allowed threshold is deemed the individual and authenticated.

An interesting project on the benefits of RFID in sea terminals is the EU-FP6 project CHINOS (Container Handling in Intermodal Terminals – Optimal and Secure). This project identifies three sets of challenges: A commercial challenge is the rapidly increasing container volume; legal/security drivers concern the actual security of the containers as well as regulatory compliance and technical drivers are related to the new technologies employed in container transport and, especially, RFID. CHINOS focuses on introducing new technologies into intermodal nodes, accompanied by an event management module and information exchange.

4.2 User experiences with security technology

The purpose of this section is to establish the current state of the art in the use of security technology. For this purpose, we have performed a mini survey among some of the partners of INTEGRITY, with questions on various technologies, and their current experiences.

We focused on the following technologies/solutions:
- Optical Character Recognition (OCR)
- Container Scanning (Gamma Ray/X Ray)
- Nuclear scanning
- Damage scanning
- Container (e-)seals, CSDs (container security devices) (RFID based)
- Biometrics in access (pass) systems
- GPS tracking and tracing
- Sensor technology: Chemical, biological, radiation, nuclear, explosives
- Advanced information exchange platforms (pre-arrival notification, data capture, information provision, …)

Questions included:
- Which technologies/systems are used in daily operations? Since when? Provided by whom? Who is the main operator? What is its main purpose?
- What type of information do these technologies/systems typically generate?
- Which other party is using/needs this information?
- How reliable is the information in general? What is the false alarm / false-positive rate, in case of any detection technologies?
- Where are the technical bottlenecks, i.e. which features lack behind the user needs (battery life, device size, etc.)? Is the technology working properly? Major breakdowns, major revisions?
- How is the standardization situation?
- Is there lack of common standards / are there competing standards?
Is the lack of standardisation standards a bottleneck for broader adoption of the technology?

What is the price level of the technology? What is the operational cost? Balpark figure or as cost per container?

Has the technology led to operational improvements? Which ones? Measured by which variable?

What type of technology is missing/is being developed?

Below, we will discuss the various technologies, and, in a separate section, review use and the impact on operations.

**Technology review**

OCR is used in the gates of terminals to quickly read data from the truck and container and, possibly, take images of the container to verify for damage. Customs uses OCR in Rotterdam to collect information on empty trucks and trailers leaving the terminal. In the future this may extend to trucks leaving with unblocked containers. The data that is read is license plate, container nr, IMO labels and ISO code. This information can be checked against pre-information obtained from the trucking company or freight forwarder. In most cases, a physical inspector is present, who checks and augments the information, such as with the seal nr. Reliability of the equipment is above 90-95%, but sometimes grime or location of numbers influences the data capture.

**Container Scanning (Gamma Ray/X Ray)**

One of the earliest applications of container scanning as part of the operational process was in Hong Kong, where at several terminals, SAIC gamma ray scanners together with OCR and nuclear scanning portals were installed in 2005. In the meantime, technology has advanced, and these type of non-intrusive scanning streets are now based on low radiation x-ray technology, which gives a better image. The best image, however, is still obtained with high radiation X-ray scanning in a stand alone facility. This is, however, intrusive to the operational process at the terminal.

The scanner collects a complete x-ray image of the container, which can be checked against the expected pattern on the basis of documents. In most cases, scanners are owned and/or operated by Customs agencies, who have the most use for the images. In container terminals and depots, the scanners could also be used to verify the emptiness of the container.

**Nuclear scanning**

Nuclear scanning has been introduced in terminals since several years (2005 in ECT). These portals are also operated by Customs. The terminals do not get information on the scanning results.

**Damage scanning**
Although damage scanning technology exists, it is not widely used in container terminals or anywhere else. Current damage assessment is based on visual inspection at gate-in (YICT), or by taking a complete set of pictures from all sides of the container (ECT).

**Container (e-)seals, CSDs (container security devices) (RFID based)**

Several pilot projects have been launched since 9/11 to test and develop RFID based tagging and sealing solutions. Savi Technology is one of the pioneers in this area, together with several others. Container terminals seem to be the main location to install RFID infrastructure (readers). There are several important moments in a container terminal process that are relevant for logistics planning further down the chain: gate-in, (container in stack), container loaded on ship, container unloaded, gate-out. These moments can be captured by reading RFID tags. As part of INTEGRITY, Savi will build a web based interface with SICIS to transfer data on RFID reads.

Much of the insight in the performance of RFID based technology is present at Savi Networks (the company that is developing and operating the RFID network in HPH terminals, and around the world). Savi’s container security device is called the Savitrak. The current insight is that the technology works well and that mis-reads, false positives and false negatives are reaching acceptable levels.

While Customs is involved in a number of RFID based pilots, for the moment, this technology is not an integral part of Customs operations.

**Biometrics in access (pass) systems**

Biometric access passes (cargo card) have been used in Rotterdam for a decade. It is based on a handprint that connects to relevant information that the truck driver and terminal need to exchange to pick up and deliver containers (container nrs, locations on terminal, driver id, transport company id). Reliability of the system is close to 100%.

**GPS tracking and tracing**

GPS tracking and tracing is used in Shenzhen between the Hutchinson owned container depot and the terminal. Also, the crane locations are tracked with GPS. A problem seems to be the connection between the GPS system and the terminal operator system, which results in less than real-time information about crane locations.

**Sensor technology**

Sensor readings are used for various purposes: to check if containers are empty, contain people, or gasses, and in the case of ECT, sensors are an integral part of the automated equipment. In general, the sensor technology to ‘read’ the contents of the containers is quite sensitive. It requires much maintenance, and the readings take time. As such, there does not seem to be much scope for sensor technology to become data capture technology for SICIS.

**Advanced information exchange platforms**
The terminals are extensively using web-based services to make information available to users of the terminal and parties that have to interact with the terminal to fulfil their role in the logistics chain (trucking companies, freight forwarders). These web services contain information services on vessel arrivals, container status (loaded, unloaded), customs and commercial blocks, as well as arrival booking and information capture for trucking companies. This last service is augmented with voice recording, where truck drivers can enter the last information bits by phone while they are driving.

These platforms mostly interact with other parties through EDI and through data entry via internet. Information can be sent by EDI, email, sms, and can be retrieved through lookup interfaces via internet. Terminals are looking at these systems to eventually completely replace manual gate handling.

In the Netherlands, pre-arrival notification of trucks can also run through the port community system. This is not entirely real-time, but standard messages are used, and the pre-arrival notification is increasingly used for various modes (truck 50%, barge 70%, rail 90%).

Customs is also building new information systems, with new ways of data collection and exchange. These are required to enable the future changes in Customs interaction with companies, such as the single electronic access point, which will eventually allow companies to interface with Customs in one location in Europe only. These developments are described in more detail elsewhere in this report.

Currently, 99% of Customs declarations are done electronically. However, many other required documents (certificates of origin, agricultural certificates, etc) are often still paper-based. Customs obtains the declaration information directly, based on EDIFACT messages or via the two community systems (Port Infolink and Cargonaut).

**Other technology**

Other security technology present includes CCTV, personnel identity cards based on RFID technology, access gates with cards for visitors and (service) suppliers, and, in Yantian, the PCC card, which identifies the truck, and, recently, is starting to be used as an e-payment device.

**Impact**

The impact of the above technology on, especially, terminal operations varies. Most of the technology (id cards, OCR, X-ray scan, nuclear scan, web services, PCC card) is meant to automate gate entry or exit, and/or is non-intrusive. Most of the technologies employed today are quite successful in reaching this objective (of automating gate processes) although the full potential may not be used yet. For instance, restrictive slot booking for trucks is technically a possibility, but is not used by terminals.

Some technology is still being tested, and its operation is disconnected from operations. As such there is no impact to measure yet. This holds mostly for the RFID infrastructure to run e-seals and container integrity devices on.

The technology, in most cases, seems to be quite robust. Bottlenecks are reading conditions (dirty trucks, unexpected movement and weather), and data transmission, which can be slow, either by design or due to limited data exchange capacity.
Preliminary conclusion

In the context of the development of supply chain information exchange platforms, several features that now exist can be used: pre-arrival notification at terminals of the land side modes and RFID reads at gate and quay. These information elements are available, although not always directly through the terminals systems.

4.3 Bottlenecks

One important observation from the above description and user experience survey is that most of the technology performs well under reasonable conditions. The technology does not fail a lot, does not break down a lot, and results in few fault readings or misreading.

One bottleneck for the container security devices is that this is the newest type of technology that has only been proven to work in pilot projects. For all available systems, performance under full scale application is unknown. This performance is not so much determined by the technology, but by the information processing that goes with the exchange of information to stakeholders along the chain.

This bottleneck is also valid for some applications of tracking and tracing technology, where information exchange takes time (for a variety of reasons), and therefore, the tracking and tracing information is not available in real-time.

Bottlenecks arise in the application of the container terminal access technology under difficult weather conditions, such as heavy wind, snow, and rain. In these circumstances, readers do not work well, and misread much more than under normal weather conditions. Furthermore, the physical state of trucks and containers (scratches, dents, location of the numbers) also influences the readability of numbers and plates.

Finally, a bottleneck for the performance of the scanning technology is the speed with which trucks, or other transportation modes, are driving through the scanning portals. This does not hold for the heaviest X-ray scanners, where the truck is pulled through by a pulley system. For all non-intrusive scanners, however, the quality of the image, which is already poorer than for a higher frequency scanner, is almost completely determined by the speed through the portal.
5 Standardisation

A standard provides a model to follow in setting up and operating a management system. This model incorporates the features on which experts in the field have reached a consensus as being the international state of the art. The main international body that delivers standards is the ISO organization, International Organization for Standardization).

Alternatively, the European standardisation organization CEN defines a standard as a document established by consensus, and approved by a recognized body, that provides, for common and repeated use, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

5.1 Standardisation organisations

The main standardization bodies are: International Standards Organisation (ISO) and European Committee for Standardization in Europe (CEN). In addition, there are national standards (BS; DIN, NF, AS).

5.1.1 ISO

ISO was created on February 23rd 1947 in Geneva, Switzerland. The organization was designed to facilitate the international coordination and unification of industrial standards. It is a non-public organization that is composed of national institutes of standards from 157 member countries.

Industry or Business sectors can bring requests for standards to the ISO. The standard must be relevant to a special need in that industry or business sector. They submit their need to their national standardization institute. The latter sends the proposal to ISO. If an agreement is reached, the work item is transferred to an existing technical committee.

Proposals may also be made to set up technical committees to cover new scopes of activity. The final phase comprises the formal approval of draft International Standard (the acceptance criteria stipulate approval by two-thirds of the ISO members that have participated actively in the standards development process, and approval by 75% of all members that vote), following which the agreed text is published as an ISO International Standard. International standards should be reviewed every five years at the latest.

The ISO system had 3 041 technical bodies, including 193 ISO technical committees. Furthermore, ISO has three general policy development committees that provide strategic guidance for the standards' development work on cross-sector aspects. These committees ensure that the specific technical work matches up with broader market and stakeholder group interests. They are:

Conformity assessment (CASCO) members work on conformity assessment for products, processes, services and management systems to appropriate standards or other technical specifications.
Consumer policy (COPOLCO)’s services are available to ISO members worldwide. It supports its members in developing consumer participation in standards-making, it studies how consumers can benefit from standardization, promotes the positive role of standards in consumer protection, encourages the exchange of experience on standards work of consumer interest and channels consumers’ views into both current standards projects and proposals, for new work in areas of interest to consumers.

The role of the developing country matters (DEVCO) committee is to raise the awareness of international standards in developing countries, in order to foster business.

The ISO body had published 17,000 international standards and there are 1100 new ISO standards.

5.1.2 CEN, European Committee for standardization

CEN was created in 1961, combining the European Community ISO national institutes and national institutes from European Free Trade Association (EFTA) countries. voluntary technical standards which promote free trade, the safety of workers and consumers, interoperability of networks, environmental protection, exploitation of research and development programs, and public procurement.

CEN is a non-profit making technical organization set up under Belgian law. It provides European standards for the single market. Along with CEN, there are CENELEC and ETSI. CENELEC is the European Committee for Electro-technical Standardization. ETSI is the European Telecommunications Standards Institute.

The objectives of CEN standards include:

- Developing standards for a sustainable world economic growth
- Promote interoperability of products and services
- Help manufacturers comply with European legislation
- Promote ecological safety
- Promote energy efficiency
- Improve quality of air, soil & water
- Help achieve social equity
- Consumer and worker protections
- Health services
- Disseminate innovation

CEN standards cope with industries that are related to chemistry construction, consumers, energy, environment, food, healthcare, health and safety heating, cooling, ventilation, information society, material and mechanical engineering.
5.2 Standards in the supply chain

5.2.1 Container Standards

A container is an intermodal system for freight transport cargo transportation. It can be carried by ships, railroad cars, plane and trucks. Container capacity is expressed in Twenty-Foot Equivalent Units (TEU). There are three ISO containers (ISO 668/ISO 1496 international standards). They are used worldwide.

5.2.2 UCR

To facilitate information exchange in the supply chain, especially with Customs agencies, the concept of a unique consignment reference number was launched through the WCO. The idea is that all trade consignments should be accompanied by a Unique Consignment Reference for Customs purpose. The UCR is based on ISO 15459-1 international standards. It should be used in all relevant communications, as an access key for audit, consignment tracking and information, or for reconciliation purposes. UCR numbers are unique at both national and international levels. A UCR number must be issued as early as possible in the supply chain, and is required to be reported to Customs at any point. It provides information on carriers, on commercial data and on destination of goods. The Serial Ship Container Code is a subset of the ISO/IEC 15459 standard. It is a non-significant fixed-length 18-digit number. It is constructed from a GS1 company prefix assigned to a company, from serial number and extension number designated by a company, and Check digit. This number can be used as an UCR.

5.2.3 Containers numbers standards

ISO 9897 standard: ‘Freight Containers – Container Equipment Data Exchange (CEDEX) – General Communication Codes’. This provides information on the owner, the country (ISO 3166), and location of the company. It is a means to identifying interchanging parties and location at which the container is physically residing at time of transaction. It is used in 70 countries and by operators representing 50% of the world container fleet.

ISO 6346 standard: ‘Freight Containers - Coding, Identification and Marking’. This standard is aimed at encoding information on the owner and on the unit (dimensions, size…). It is useful as a reference number for the company’s database. It enables international circulation and temporary admission for customs purpose. It is used in 150 countries and by 1700 operators that represent 90% of the world container fleet.

5.2.4 Seal standards

Container seals are provided by shipping lines and serve as locks for securing the container. Each seal has a unique number and the shipper should also record this number on all documentation pertinent to the shipment. The World Customs Organization (WCO) recommends ISO PAS 17712 seals and electronic seals to improve security and safety of the supply chain as far as containers are concerned.
Indeed, as e-seals are equipped with Global Positioning System (GPS) or other positioning solution, containers can be located throughout the supply chain. ISOPAS 17712 seals are not electronic, but for bolt seals. These are usually solid and of high quality. They are set to be reliable. Indeed, they cannot be easily removed.

5.2.5 Pallet standards

Pallets are flat transport devices for goods. The purpose is to ensure stability and protection of goods, easy transportation and rapid unloading. There are wooden pallets, plastic, metal and paper pallets as well. They can charge up to 1000kg, approximately 2000lb. A specific kind of pallet is used for planes: it serves for mail, luggage, and freight. The ISO Standard for pallets is ISO 6780. This standard prescribes the dimensions of the ISO pallet, which are 1 x 1.2 meter.

5.2.6 Electronic standards

Bar code standards

Supply chain standards for codification are the Global Standards 1 (GS1). These are used to create bar codes (useful to identify boxes). GS1 operates in more than 20 industries and sectors in 104 countries, and addresses all aspects of supply chain, enabling a million of companies of all sizes to execute more than five billion transactions a day.

These are international standard for bar codes:

EAN UPC (European Article Numbering Universal Product Code) bar codes are commonly used in the world. They fit for retail Point of Sales because they are designed for high volume scanning environment. They can only carry GS1 numbers.

GS1 (Global Standards 1) data bar can be scanned at Retail Point of Sale. They are smaller than EAN/UPC. Furthermore, they can carry additional information such as serial numbers, lot numbers of expiry dates. They can also be used for healthcare products as far as they do not cross Point of Sale (POS).

[http://www.gs1.org/productssolutions/barcodes/technical/bar_code_types.html](http://www.gs1.org/productssolutions/barcodes/technical/bar_code_types.html) - GS1-128 (UCC/EAN-128) bar codes can carry all GS1 data but they cannot be used for items crossing Points of Sale.

[http://www.gs1.org/productssolutions/barcodes/technical/bar_code_types.html](http://www.gs1.org/productssolutions/barcodes/technical/bar_code_types.html) - ITF-14 bar codes can only carry GTINs (Global trade Item Numbers). There is a possibility to print them directly on corrugated cartons. They cannot be used to identify items that cross POS.

GS1-Serial Shipping Container Code (SSCC): The most important GS1 Identification Key for logistics units. It identifies items of any composition established for transport, storage or distribution, which needs to be managed through the supply chain. This number uniquely identifies transport unit for the entire life cycle, and can be used for identification of pallets, crates, containers. Upon emerging from the manufacturing or preparation process, the logistics unit is created and identified with SSCC. The SSCC is a subset of the ISO/IEC 15459 standard.
GS1 Data Matrix is the only “2 Dimension Matrix” symbol for GS1. It is widely used for healthcare products. To read a GS1 Data Matrix bar code, camera based scanner is needed. It cannot be used for items crossing POS and direct part marking.

Composite Component is the only "2D linear" symbol specified by GS1. It is called a component because it is only used with a linear bar code like GS1-128 or Reduced Space Symbology (RSS).

Furthermore, GS1 standards have developed standards for items: Global Trade Item Number. They can be 12, 13 or 14 digit (GTIN 12, GTIN 13 or GTIN 14).

**RFID tag**

There is a specific RFID tag standard for pallets and containers, which is the EPC Global Gen 2 UHF [Ultra High Frequency] RFID. It is specifically designed to prevent radio frequency interference or absorption of signals by liquids on board ships. This standard is part of GS1 (Global Standards 1) Supply Chain standards.

**EDI**

EDI stands for Interchange of Electronic Data. Basically, it is a computer-to-computer exchange of formatted messages. This is a set of specific standard syntax, security and confidentiality rules for electronic business data transmission, defined by the International Organization for Standardization standard ISO 9735 EDIFACT. (Electronic Data Interchange for Administration, Commerce and Transport) It prevails outside of Northern America.

EDI documents are widely used between and within business organizations. Since they were developed before the internet, they do not require the Internet to work.

The latest version of ISO 9735 is the syntax version number 4. These are normative provisions for the conformance of the structure, given by the United Nations Economic Commission for Europe website. Ensuring security of data and authentication procedures (Public Key Infrastructure, PKI) for users are critical to avoid diversion of sensitive information concerning the supply chain.

Secondly, the other IT language that is used to deal with data from the supply chain is the XML language.

**eXtensible Markup Language (XML)**

It is a specific language developed by the World Wilde Consortium (W3C). XML format is a way of sharing information on the Internet (contrary to EDI format) regardless of operating systems. The United Nations Center for Trade Facilitation and Electronic Business (UN/CEFACT) has adopted the XML Schema Definition (XSD). As the UN/CEFACT put it: “it provides a way to identify, capture and maximize the re-use of business information expressed as XML schema components to support and enhance information interoperability across multiple business situations.”
When developing XML schemes, attention has to be drawn on the Core Components Technical Specifications (CCTS) which have been standardized as ISO 15000-5 ebCCTS ebXML. The following structure shows how it works:

![Diagram](http://www.unece.org/cefact/xml/XML-Naming-and-Design-Rules-V2.0.pdf)

The advantages of using UN/EDIFACT (for EDI) or UN/CEFACT standards (for XML) are that they save time and money. There is much less human interaction (it reduces the probability of human errors) and it cuts down use of paper. In addition, they ease information exchange at the international level because data is exchanged on the same standards (scale economies). Organizations such as WCO recommend the use of EDI and XML standards for interchange data between operators and customs administrations.

### 5.3 Bottlenecks

The current section on standardisation bottlenecks discusses issues that are relevant for an efficient supply chain and problems that can occur because of inhomogeneous process-, technology-, and information-standards.
5.3.1 Technology standards

Different technology standards among supply chain actors can be regarded as a bottleneck in international transport. It is often the case, that some technologies and devices are not available in all regions of the world.

As mentioned in previous section, there are different types of container seals in use. For the proper utilization of e-seals there are certain technical requirements in order to read and process the recorded data. Not only for the use of e-seals, but also for smart containers differences in technology standards are capable of causing bottlenecks. The technological requirements will have to be met by all partners of the supply chain in order to achieve satisfying results and exceed current standards in order to justify the additional costs caused by the introduction of new devices and applications. The cost factor could be one of the main challenges for smaller members of the supply chain, regarding implementation of new standards.

5.3.2 Process standards

There are several bottlenecks concerning process standards in international transport management. An average supply chain consists of numerous heterogeneous actors, of different size and background in various countries and regions. As a consequence certain processes vary among those actors, which can cause difficulties and inefficiencies.

5.3.3 Information standards

Regarding the quantity of information that goes along with the physical movement of standards, common information standards are vital in order to provide an efficient communication process. For the purpose of an Electronic Data Interchange (EDI), it is necessary to implement common data formats and communication standards. This can be facilitated by an independent platform that is neutral to the hardware and software of the companies and communication partners.

Bottlenecks arise out of the fact that these standards are often not used by small and medium enterprises (SMEs) due to the complexity of most of these messaging standards. The use of the named standards is therefore often limited to the “core”, and communication with the outer reaches of the chain has to be performed in different ways.

5.3.4 Customs standards

Customs standards are not homogeneous in all countries worldwide. Each country has different legal requirements in terms of documentation, customs procedures (VAT rules) and import and export regulations. E.g. for cargo destined to South American countries it is not allowed to issue a sea way bill. Especially Eastern European countries have a lot of VAT rules which have to be taken into account when issuing transport invoices. Countries like Australia and Canada request fumigation certificates for import cargo. For particular goods, some countries demand a certificate of origin or other certificates.
Specifications are not commonly used in all countries, e.g.: PLT = pallets must not be used in cargo descriptions for cargo to the US, since it is not regarded as package unit.

Due to the various requirements, enormous efforts have to be taken to arrange customs clearance (customs experts). Further related standardization bottlenecks concern pre-registration of containers in European ports, and manifest filings. For the registration in ports there are different forms for the various European ports, and harmonization would grant benefits to the exporters. Regarding manifest filings it should be pointed out that slightly different data is required in the various countries, and the format is often slightly different. Given this format/data diversity, it causes difficulties to apply to the 24-hour rules and there is a probability of a high error rate. Failure to file the cargo manifest or to file in time and correctly in the USA, lead to fines starting at 5000 USD. The incorrect application of the 24-Hour rule leads to delays and slowdowns in the supply chains. Additionally it is very cost-intensive to adapt IT-systems to the requirements of all the countries introducing the 24-hour rule.

In the near future, the US will request for cargo imports an even more sophisticated filing, called 10+2, that will not be asked by other countries.
6 Emerging trends

This chapter introduces the trends that determine the changing landscape of global supply chains. These trends encompass developments in the hinterland, customs, technology and standardization. These areas will determine to a large extent how supply chains will look in the future.

6.1 Emerging trends in ports and hinterland

Ports and inland terminals play more and more a new decisive role in the supply chains and terminal operators are gradually imposing new operational challenges to their customers (e.g. berthing windows, dwell time charges, truck appointment slots) with a view to increase capacity and productivity of their operations. At the same time their customers seek to attain service commitments from the terminal operators (e.g. service windows and guaranteed productivity. This process of increased role of the terminal operations in the supply chains is called “supply chain terminalization” (Rodrigues and Notteboom, 2008) and it is anticipated to further strengthen in the future. At the same time, supply chain managers base their port choice decisions increasingly on reliability and punctuality considerations along with cost considerations. Since supply chain managers seek to minimize warehousing capacities at distribution centres, they often apply a hybrid inventory strategy of “inventory in transit” coupled with “inventory at terminal” (Rodrique and Notteboom, 2008). In this way, the terminal becomes the main buffer, instead of the distribution centre, in the supply chain.

On the other hand, shipping lines apply more and more yield management strategies1 to their operation, borrowed from the airline industry, and therefore they seek to minimize the number of the empty containers not being used by either increasing their own container fleet or by applying innovative leasing concepts (Theofanis and Boile, 2008).

Furthermore, port terminals are entering a tendency to extend the traditional captive hinterlands of the ports through a system of networked inland terminal. The term “port regionalization” has been introduced to describe this tendency (Notteboom and Rodrigue, 2005).

Among the previous developments the concept of “extended distribution centres” is gaining momentum. Inland terminals are considered as buffer terminals for certain distribution centres of major consignees (e.g the TCT Belgium and JVC Belgium Distribution Center) (Rodrigue and Notteboom 2008). Dwell times are very tight at the port terminals, while they are much more prolonged and flexible at the inland terminals. Therefore, the inland terminal and the distribution centre act as a storage and inventory cluster.

---

1 Yield management considers revenue on the basis of the container unit (TEU) instead of the vessel round trip.
This approach provides for better flexibility in ensuring backloads for empty containers and minimizing unproductive empty container distance travelled (Theofanis and Boile, 2008).

Both “agile” port and “extended warehouse” concepts have not yet been applied fully into practice, mainly due to business practices the business partners are used to nowadays (shipping lines, port operators, inland terminal operators, 3PL, shippers and consignees).

The “Extended Gate Concept”

Port terminals and inland terminals are increasingly working together in a seamless way. As indicated by Rodrigue and Notteboom (2008) “...For satellite terminals in the vicinity of port terminals the degree of synchronization is high with a propensity of the extended distribution centre to use dwell times at both the gateway and the satellite terminal as buffer”.

![Figure 6.1: The extended Gateway concept](http://people.hofstra.edu/geotrans/eng/ch4en/conc4en/agileport.html)

The extended gate approach can take two forms:

1. The synergy between inland terminals and port terminals, as indicated earlier (see figure 6.1) and the role of the inland terminal as an extended warehouse, and
2. The so called “agility concept”\(^2\), where port storage is extended to inland locations through the use of dedicated or satellite inland terminals. Containers

\(^2\) http://people.hofstra.edu/geotrans/eng/ch4en/conc4en/agileport.html
are fast (un)loaded at the port terminal and are either directly or after a short
term storage transferred to an inland terminal, where can be further stored,
cleared and delivered/received. Delivery and receipt can be accomplished in a
more customer oriented way (e.g. on call delivery) (Fig. 2). Thus container dwell
time reduces dramatically at the port facility, while increasing cargo throughput
capacity.

Figure 6.2: Inland Terminals and Terminalisation of Supply Chains
Source: Rodrigue and Notteboom (2008)

According to these trends, Notteboom & Rodrigue (2006) have introduced this concept
as port regionalization, which is the interaction between seaports and inland locations
that would lead to the development of large scale logistics poles in several logistics
zones around the main seaport Gateway. The concept adds dynamics to both the
logistics poles and the seaport. The seaports hinterland is expanded in the hinterland
through a number of strategies linking it more closely to inland freight distribution
centres preserving its attractiveness as sea gateway, while the logistics poles around the
vicinity and catchment area of the port ensure regular freight flows and consolidated
shipments for further processing. This fact brings the perspective of port development to
a higher geographical scale, i.e. beyond the port perimeter.

Port authorities are in an excellent position to play a leading role in such initiatives as
the pivotal location for international movements. Their interest concerns generally the
overall efficiency and the growth of trade rather than the performance of particular
sectors. In the regionalisation phase port authorities can play an important role in
shaping regional load centre networks and logistics poles.

Examples of Port regionalisation

1. The Tioga group
Container sorting is done exclusively at the satellite terminal (The Tioga Group, 2006). Transfer between the port terminal and the satellite terminal is accomplished mainly through rail (see Figure), although in some cases dedicated out of peak truck transfer has been proposed (Truck Fed Inland Terminals – TFIT). In certain cases, satellite terminals are considered as an extension of the port terminal from a Customs point of view (e.g. TCT Venlo in Netherlands has a bonded warehouse C license and when containers are shuttled from ECT Delta Terminal in Rotterdam they do not need the issuance of a clearance document). From the technology side of the concept, automated rail transfer has been proposed, though technology solutions have not yet been applied. Operational as well informational integration between the various components of the system is a prerequisite. The concept has not yet been fully applied for reasons mainly owing to current port and transfer terminal business practices.

The port agility and the extended warehouse concept can also be combined, i.e. containers are (un)loaded at the port terminal, where they are stored for a very limited period of time (e.g. 24 hours) uniform for all containers and they are shuttled to a satellite terminal via rail. The satellite terminal may belong to the port terminal operator, a shipping line or a 3PL company. No separate customs document is issued when containers are shuttled to the satellite warehouse. Extended storage dwell time may be applied for each customer and the satellite terminal may act as an inventory buffer. Container sorting and clearance takes place at the satellite terminal. In a more complicated approach, each port terminal is supported by several satellite terminals, although in this case some kind of sorting should take place at the port terminal.

A practice similar to the later extended warehouse pattern is applied by Dell in the USA. Suppliers of Dell are obliged to develop and operate their own warehouses near port locations and orders placed by Dell have to be executed within a very short period of time (e.g. 24 hours). In this way, the suppliers have to cater for the demand uncertainties and the required level of parts inventory, instead of Dell.
2. Port regionalisation in Flanders

Another example of port regionalisation and improvement of port-hinterland connections and interfaces is the Extended Gateways of Flanders, a study conducted by VIL. The rationale for the study was the scarce location of gateways that could not exploit their full potential without coordination activities. A regional study consisting of several plans for the optimal location of these gateways was considered essential, and the concept was implemented. The aim of this concept is to provide fast, frequent, reliable and efficient multimodal connections with the gateways in order for the hinterland locations to have the same opportunities for logistics activities as the original prime locations in the gateway (Van Breedam and Vannieuwenhuyse, 2007). The Extended Gateway idea can be considered as a practical application of the port regionalisation concept. The implementation of the idea of the Extended Gateway has received top priority status in Flanders in view of preserving or even increasing the pace of logistics development. Still, prerequisite to the success of the concept is to achieve an integrated multimodal approach of transport, strong partnerships among logistics actors and continuous search for innovation in logistics concepts and technologies.

Rodrigue and Notteboom (2008) argue that through this strategy of collaboration among companies in the different links of the supply chains, a reduction of the costs and concentration of high volumes could be achieved. Vertical collaboration among partners in the chain can be achieved through intensive information sharing, this is becoming more and more common practice. Horizontal collaboration results for example in a bundling of freight flows with an increased utilization of the transport network and the used equipment as consequences.

3. Extended gateway ECT –Venlo

ECT is the operator of most of the container terminals in the Port of Rotterdam. The company was established in the late 1960s, and grew in parallel with the growth of
containerised trade. In 1988, ECT started cooperation with the shipping line SeaLand to build the world’s first automated container terminal. This terminal commenced its operations in 1993. Two other terminals at the Maasvlakte now also use this automated concept.

ECT, together with other major European container terminals has experienced considerable growth in recent years, mainly due to the economic development of China. While expansion plans are being executed, most of the new capacity was not ready early enough. As a result, most of the European container ports were severely congested in the period 2003-now. The result for the terminals is that the stacks become very full, which slows down the productivity of the stacking cranes, the quay to stack system and, ultimately, the quay cranes.

To benefit from the relationship between terminal (i.e. quay crane) productivity and stack fill rate and dwell time, ECT is developing the so-called extended gate concept. The key to this concept is the possibility to send large volumes of containers from the deepsea terminal to inland terminals immediately after arrival on the deep sea ship. This clears up the stack, and allows the terminal operations to work without delay.

ECT happens to own three inland terminals, one in Belgium (Willebroek), one in the Netherlands (Venlo) and one in Germany (Duisburg). While these terminals operate in different ways, they are all well connected with the deepsea terminals. There is a daily container barge shuttle to Duisburg, for instance, and both Venlo and Willebroek have a barge and a rail link with Rotterdam.

There are a number of issues involved in the extended gate concept. These are:

- Liability: who contracts whom, and who is responsible for the goods?
- Charging: who send who an invoice and what is on this invoice?
- Information: who informs who of what, and when?
- Customs clearing: who decides when a container can be moved or not?

The extended gate system started operation late 2007. It has been running for a year, and operationally it works well. Currently, ECT is contemplating a wider role-out of this system, and a different way of planning the hinterland transport within the extended gate network.

Towards Global Port Operators

The globalisation of shipping and trade has lead to a new trend in the ports organisational profiles over the last decades increasing pressure on ports to reduce container terminal costs and improve operational efficiency. With the intention of the big shippers or Logistics service providers to have the total control of the chain these stakeholders seek for single supplier contracts looking for carriers that can provide efficient and cost effective services. In turn, the shipping lines and the carriers look for reduction of their operational costs and receive efficient port services, being keen on having single sourcing across ports in terms of port terminal operations. Therefore, in response to this and in order to fulfil the need for integration in the global supply chain, the expansion of the Global Port Operators (GPOs) has emerged. A limited number of GPOs manage an increasing number of the world’s ports. This development has been
pushed by port deregulation and changes in ownership in many countries (Mangan, Lalwani, 2008).

These players dominate global port operations and are particularly involved in the SMART-CM and INTEGRITY projects. The competitive advantage of the GPOs relies on the following:

- Composition an extent a network of terminal around the world covering the needs for integrated global chains
- Exploitation of state-of-the-art know-how in port terminal management and services
- Achievement of the economies of scale in supplying with sophisticated IT management tools, handling equipment, etc

The acquisitions of container terminals at ports around the globe by GPOs is a trend that is expected to continue and will influence the global logistics chains structure and port governance schemes, with yet unknown consequences for the Port Authorities and their position in the global supply chains (Theofanis, Boile, 2007)

In addition, the shipbuilding industry trends are posing also new challenges for ports development and operations. Vessel size has increased dramatically in recent years and the introduction since 2006 of the Emma Maersk, currently the world’s largest containership with a capacity of about 12,500 TEU and a crew of only 13 is a specific example of this “gigantism” trend. Such a generation of containerships can be accommodated by a limited number of high capacity port terminals worldwide creating specific business models and special conditions in the ports. Still, in order to cope with this pressure the container terminals are expected to assign large number of cranes to insure a standard level of service. For example in some Chinese container ports up to 9 cranes are assigned to the transhipment. The impacts of a fleet of new generation ships
on global container port operations are not well known and are likely to reinforce only a few hubs (Rodrigue, 2007).

An important consequence of the trend of bigger container vessels is the growing traffic concentration at certain ports. Increasingly, many mid-sized ports are playing a feeder role to the very large ports, emerging towards hub and spoke networks. In these networks, the larger vessels ply between the major transhipment hubs, with the result that the prosperity of the smaller ports is increasingly dependent on the route strategies of the major shipping lines (UNCTAD, 2008).

Another trend for ports to increase efficiency due to the need for high performance is the need for automation of port operations and becoming less reliant on the human factor. High demand in big ports have resulted in investments in automated guided vehicles and container handling equipment in order to reduce labour costs, especially in ports with high personnel rates. Moreover, in order for ports to increase their gains they continue to seek for advanced terminal layouts, more efficient IT-support and improved logistics control software systems, as well as automated transportation and handling equipment.

Considering the above mentioned facts, it could be also said that the competition among the ports, even though not a contemporary trend, has changed and now rely on being flexible, adapting quickly to changing opportunities and following an integrated approach to logistics chains, minimising costs and increasing efficiency.

Emerging trends in shipping and hinterland transport

1. Increasing transport costs

One of the key factors that determine the trends in freight transport is the increasing transport costs. Transport costs consist of a combination of factors including geography, trade volumes, economies of scale, infrastructure and administrative processes. However, one of the most determinants factor influencing the transport trends is the increasing fuel and oil prices, representing 63% of the operating costs of an 8.000 twenty-foot-equivalent-unit (TEU) container ship (Dynamar BV 2007). Also the bunkering costs at the major ports of Europe increase the shipping prices.

At over US$140 a barrel in June 2008, some trade observers are suggesting that globalization may be hindered and trade patterns changed, with China’s comparative advantage according to some analysts, soon coming to an end. This, in turn, would affect transportation strategies, global production plant locations as well as the underlying logic of current global trade flows (UNCTAD, 2008). Still, there are also scenarios for a stabilisation of the oil prices at a lower rate that would not affect the gains from the global trade operations of the oil producing countries and Asia. In any case, despite the increasing oil prices and overall transport costs, the demand side has not slowed (yet?), which preserved the trade volumes with Asia at a high level without heavy losses for the industry or even modest profits.

But how do the stakeholders react in this boom in transportation costs? According to UNCTAD there is anecdotal evidence that some major shippers are considering adapting their inventory policy to reflect higher transport costs which have as base the high demand and absorb the increased transport costs. Such strategies followed by big shippers, carriers and logistics services providers are
to increase the utilization rates by moving of full container and truck loads through cross docking operations,
• turning from road transport to alternative modes of transport such as rail,
• reducing sailing speeds and reorganising maritime services,
• investing in fuel efficient technologies for shipping (hull design, propulsion, engines), and
• applying inventory optimisation strategies like optimal locations of warehouses and distribution centres. Concepts like the extended gateways and the agile warehouses are among those strategies.

Still, these strategies are not measures to offset only the energy costs but that would add sustainability to the global supply chains and ensure the development and growth of the companies in a long term basis.

2. Moving towards rail freight operations

After a period of neglect, rail is currently receiving more attention particularly because of the following.

• The increasing international trade flows have increased the importance of the gateways for providing an interface between global supply chains and national distribution. The inland flows from the gateways carried out by trucks tend to be better served in terms of quality of service (punctuality, capacity, volume, costs etc) by rail.

• New concepts already described such as the extended gateways have contributed towards this direction since the capacity constraints for the trucking industry are not easily manageable. Thus, intermodal rail offers an opportunity to ship freight in and out of major port facilities to inland distribution centres.

• Major shipping lines are “moving inland” in order to gain control on the entire supply chain either by buying other companies or creating new ones. Already, Maersk owns the rail freight operator European Rail Shuttle, which mainly operates from the ports of Rotterdam and Antwerp towards a variety of destinations inside Europe. It carried in 2005 more than half a million TEUs. Also, MSC and Hapag Lloyd operate rail services in specific segments of the European hinterland. (Rodrigue, 2007).

Still, even if worldwide rail freight have been flourishing and being over 40%-50% of the total freight transport flows, (Australia, China, Russia, US) this is not the case in Europe, where the road networks have for decades received a larger share of public investments and existing technical barriers have caused that the rail freight market share in the EU 27 today is just 16.8% (Eurostat, 2007).
Still, revitalising the railways comes from a combination of policy and business aspects that are currently moving on scene of the European freight transport.

At a policy level measures for rebalancing the transport modes have led to improved competitive equality between the road and rail, therefore providing more incentives for using the environmentally friendly and efficient railways. The directive on charges on HGVs (Eurovignette Directive), the electronic tachograph and the new Directive on drivers’ hours are all a step in the direction of increasing the rails freight competitiveness. The liberalisation of rail freight traffic in Europe enabled single companies to offer cross-border services and will make it easier for train operators with new ideas to enter the market. On a national level, several countries are investing in terminals for private railway sidings and combined traffic has been successful. For instance, the German program for subsidising railway sidings has proved to be highly efficient. Subsidies totalling 15.5€ million, granted up to the end of 2006, mean that annual performance of around 760 million tonne-kilometres was shifted onto the railways. These developments make it clear that rail freight industry’s potential for growth has not been fully exploited (CER, 2008).

Concerning business trends, as discussed also in the previous paragraphs of this chapter, the internationalisation of the flows, the long haul of the shipments, containerisation, increase of transport costs and the trend of large logistics service providers taking control of the global supply chain (also inland branches of the chain) have all worked for the benefit of the railway corridors. This fact has improved the investments in terminals as well, a precondition that was required for achieving efficient maritime/rail integration for intermodal flows.

However the level of integration of freight rail is still very diversified in Europe, as rail freight has high share mostly in countries with extent logistics networks, big port gateways and dense railway network (Germany, Netherlands, Sweden, UK) while railway is still losing its market share in the South Eastern Europe. Even so companies like K+N, PROODOS, Railcargo and others, continuously invest and operate rail freight corridors along countries in Southeast and Central Europe, where rail freight is still
underdeveloped, implying that also in these regions there potential for further improvement.

6.2 Emerging trends in customs/ security

6.2.1 Importance of the security in the supply chain

Developments in the last decade have increased the need for enhanced supply chain security. There are three drivers that affect the supply chain security:

- The increasingly global economy and global production networks depend on and generate the free flow of people, goods, and information.
- Businesses increasingly depend on efficient supply chain operations.
- Increased terrorist threats result in significant implications for global supply chain security.

These factors have created significant challenges for public authorities involved in the global supply chain (countries, customs), for safeguarding global trading itself and global economy and relationships. More than ever the industry has to implement continuous improvement in processes that enhance both supply chain execution and security.

These improvements must go beyond the limits of individual stakeholders (port/terminal authorities, carriers, logistic service providers, etc) and be extended throughout the supply chain as a system. At the same time, governmental agencies responsible for the movement of goods and people across borders must continuously review and update security procedures with the goal of enhancing both security and efficiency in an as rational as possible way. This includes balancing the essential governmental obligation to protect citizens with the critical role of promoting economic viability through trade.

In addition the globalisation trends are likely to further continue and thus special emphasis is placed upon the global perspective and the goal of the industry to expand the number of “trusted” partners. Still, a balance between efficiency of global supply chain and enhanced security must be met and this could be achieved only by international cooperation and ICT integration. An elaborate overview of where we stand with regards to security regulations has been presented in a previous chapter of this compendium. This section focuses on the one hand on the trends observed in the customs procedures i.e. to the public authorities and on the other hand on how increased need for along the chains is viewed by the industry. It is to be mentioned that trends in container security are mostly related to technology developments. This will be examined in the next section.

6.2.2 Customs Reorganisation - A dynamically evolving trend

Global environment is characterised by global economic competition and physical mobility but also terrorists’ threats are affecting at a high level the domain of customs procedures worldwide.
Customs and container movement through the nations experience tremendous pressure to respond to this rapidly changing environment. Though the intensity may vary from nation to nation, most countries are facing three major demands vis-à-vis supply chain efficiency:

- Global economic competitiveness. For most nations, political and economic stability depends on participation in a complex international trade network.

- National security. The reality of recent terror attacks has magnified this concern in the minds of citizens and governments alike. Terrorism is no longer confined to regional hotspots, but has erupted on five continents, threatening all major markets.

- Operational efficiency of the supply chains. Despite the importance of achieving national economic and security goals, border management operations are the critical nodes in the entire global chain and face significant pressures for improving their performance.

In order to achieve a balance between these main demands a series of measures/initiatives are put in place that continuously evolve and aim at the rationalisation of the customs operations and the collaboration with the global supply chain industry. These measures/initiatives are presented in the following paragraphs.

**The Single window Concept**

Governments usually have separate and different processes for managing exports and imports. The high priority given to export facilitation often results in reduced controls at departure. With clear revenue and security incentives to control incoming cargo, imports are more rigorously managed. Risk assessment for import cargo clearance is commonly performed after goods arrive at their port of entry. The WCO, as the main body for customs reconfiguration, leads the nations for adopting a different perspective in order to achieve this balance. Supply chains are viewed as a system in which the customs cannot be involved in isolation but as being part of the system. This “system” approach calls for integrated processes from point of manufacture to final delivery destination. In this context (referred as an “elastic border” model), customs in the arrival country expands its formal control horizon beyond physical borders – back to the shipment’s origin and forward to the ultimate delivery location. In order to enhance this procedure and facilitate international and public/private sector integration, the WCO has established standards for mutual recognition, certification and risk management the WCO SAFE Framework of Standards.

This need has also emerged from the global trend of the industry to integrate in everyday business ICT solutions, e-commerce solution for transactions with the other partners of the supply chain and internet based application for monitoring and managing the supply chain. As shown in Figure 6.7 below, international standards now mandate “single window” clearance processing at the border as key “node” in order to rationalize information flow and to expedite legitimate trade.
Figure 6.7: The Single Window (SW) concept

Source: UNECE

Customs around the world are penetrating in the e-business world by providing their services with the industry and providing the incentives for an efficient public/private cooperation. The following table provides an overview of current initiatives in the trend of the SW systems implemented worldwide including attempts for the Global SW. (Nowak, 2006).

<table>
<thead>
<tr>
<th>Stage</th>
<th>Geographic Scope</th>
<th>Cases Studied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Window Portals</td>
<td>National</td>
<td>Australia (Tradegate); Finland (PortNet); Germany (DAKOSY); Ghana (GCNet);</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guatemala (SEADEX); Hong Kong (DTTN); Jamaica (TradePoint); Japan (NACCS);</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Korea (KTNet); Malaysia (Dagong Net); Mauritius (TradeNet); Netherlands</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(VIPPROG system); Singapore (TradeNet); Sweden (VCO); Thailand (TradeSiam);</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tunisia (TTN); United States (ITDS); New Zealand; Jordan</td>
</tr>
<tr>
<td>Regional, Multi-nation Portals</td>
<td>Multi-nation, Regional</td>
<td>ASEAN Single Window initiative; The European Commission’s Single Window initiative</td>
</tr>
<tr>
<td>Global Portal</td>
<td>Global</td>
<td>Bolero.net</td>
</tr>
</tbody>
</table>

The advantage of this trend is that building on this expanded operational view; governments that are well progressing on these issues are establishing trading partner certification programs that streamline processing for known and authorised entities, focusing limited resources on the “unknowns.” In parallel private stakeholders are more freely investing in increased physical security in supply chain facilities and using advanced information, certification programs and digital seals to safeguard a container’s
contents and integrity throughout its trip, thereby strengthening control while maximising the efficiency of the supply chain. Supported by a wealth of electronic information, automated processes help stakeholders reduce chances of error, theft and fraud. Governments and regions in particular (e.g. EU) are adopting these new approaches and rapidly disproving the popular notion that national security and government efficiency are mutually exclusive goals.

**The EU AEO and other certification initiatives**

In an effort to increase supply chain security for goods crossing international borders, the European Commission has implemented various security measures. These measures, referred to as the Customs Security Program (CSP), impact all importers, exporters, logistic service providers and other companies involved in moving goods in international trade. The CSP controls are designed to secure the international supply chain and protect European Union (EU) member states and markets and have been already described in previous chapters.

The most significant on-going trend for Europe is the Authorised Economic Operator (AEO) concepts which have already been described in earlier sections of this Compendium. The first observation is that AEO seems to have different levels of integration at different countries. Industrial partners from the Netherlands, Sweden, UK and Germany acknowledge the benefits of trade facilitation and are keener to invest in becoming an AEO thus comprising the vast majority of the European AEOs certified. In other European countries, preparatory work for the integration of the concept is still going on, or implementation is even completely absent (e.g. Italy, Greece, Poland).

Regarding the type of certifications, the vast majority of the submitting companies aim at obtaining the entire package of Customs Simplifications/ Security and Safety (AEOF) except Sweden where the AEO certified are mostly aiming at customs simplifications (AEOC). The fact that few AEOs aiming only at security and Safety have been certified until now indicates that the major priority for the companies is to achieve a better level of customs’ services rather than a vertical security and safety approach.

Besides the certification of secured traders, alternative approaches are also under examination and will be further assessed in the future. Indicatively the Horizontal supervision, as supported by the Dutch customs authorities through their Business plan (2006-2010) is an initiative of transferring supervision and enforcement tasks to the private parties and social organisations. It is expected that this organisational model would be the link between the custom authorities and the private companies (public/private cooperation) to realize self-regulation by means of certificates, quality-guarding institutes, codes of conduct, etc, leaving the time and place for the customs to look after higher risk inspections and tasks.

**The bilateral international cooperation of EU**

For European and Third countries governments and government agencies, the traditional focus has been on the control of trade, ensuring the collection of taxes and fees, restricting the flow of illegal items, with sampling inspections of imports for security. The contemporary focus, however, is shifting to trade facilitation with security concentrated on earlier stages in the supply chain and the identification of trusted
partners to increase security through export inspection and information trails. For this reason several initiatives are undergoing or planned for bilateral (trans-regional) cooperation for achieving secure trade lines. An overview of these initiatives can be found in chapter 2.3 of the Compendium.

**The WCO views**

The WCO SAFE Framework identifies the need for countries to adopt common definitions and criteria for determining high-risk cargo and for sharing risk assessment results. It also calls for mutual recognition of trading partner “certifications” (e.g., low-risk participants). Sharing alerts and lookouts across agencies and governments is a prime example of such integration. This increased standardisation also enables automation; the WCO standard for automated risk assessment has been widely adopted by customs departments.

The latest thoughts and ideas put on the table from the Belgian customs to the WCO is the creation of “the SWIFT of customs” aiming at strengthening the role of the customs in the global trade field (Colpin, 2008). The bilateral agreements are considered for the time efficient but as the members of WCO grow and these continuous increase, there is high probability that these schemes may not be efficient in the future. The SWIFT, as proposed, should integrate a single electronic window and incorporate paperless transactions for making WCO a Single Access Point for trade to customs information exchange. In other words, what is the aim to be achieved in this concept is the interoperability between the customs-to-customs systems (based the WCO standards) as well as customs to business systems and integrating information sharing services for customs and security issues. These requirements should be taken into account by the SMART-CM and INTEGRITY service platforms.

6.2.3 Security trends for the industry

Given the global nature of supply chains, the industry is dependent on the procedures, laws, and regulations of countries across the globe, and decisions about suppliers are likely to increasingly depend on the “trusted partner” status of the supplier country. The global trends like outsourcing, just-in-time deliveries, etc also increase the risk of fraud, losses, thefts etc. Due to increasing competition and security standards, supply chain managers become more engaged in self-appraisal of supply chain security and contingency planning. Cross-functional teams develop crisis management plans that include planning, mitigation, detection, and response and recovery components.

For example, the loss of a key supplier can critically disrupt a supply chain, and industrial partners are dependent on the security procedures of their origin points (suppliers) in order to ensure their own security and to maintain trusted-partner status with government agencies. The other stakeholders, carriers, freight forwarders, port authorities, and terminal operators are also in charge of performing critical operation towards security along the supply chain and their operational environment, thus affecting the security of the entire system. Regarding each of the different parties of the supply chain, there are different regulations, standards and private interest for achieving security that have been already identified and described in previous section of the compendium.
As the security of the supply chain equals the security of its weakest link or node, the ports as intermediary points and in the same extent the ocean carriers are regarded as high importance points in the chain. Special emphasis has been placed on the maritime industry through the ISPS and other IMO initiatives. The use of ICT for monitoring and assessing security standards are introduced starting from a container (or loading unit) level security measures, to infrastructure, safeguarding, monitoring, achieving transportation visibility and inspections level. Still the cost of the compliance investments required is creating distortions in the market that affect in particular SMEs in all industries involved (ports, carriers LSP, etc).

As concerns hinterland carriers, the security is ranked as a lower priority compared to the other members of the chain and they tend to react on security driven regulation rather than initiating any measures. However, quality carriers would introduce security related services in the market. Transport managers may select routing directions that avoid insecure segments (with the purpose of avoiding smuggling and thefts) or select parking places that are monitored and secured (fenced, camera surveillance available, guards, etc). Theft and fraud are still considered as number one security issue for hinterland transport.

Looking at the holistic approach, one of the most important security related services to the SC partners is the provision of visibility services, while tracking and tracing of the goods becoming a competitive advantage. Still, interoperability with the LSP and/or shipper is an issue, since tracking and tracing technologies of the cargo type may not be compatible.

Therefore, the industry trends in security monitoring and assessing are changing to incorporate supply chain management (Closs, 2004). This is depicted in Figure 6.8 below.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Security</td>
<td>Cross-Functional Team</td>
</tr>
<tr>
<td>Theft Prevention</td>
<td>Theft Prevention and Anti-Terrorism</td>
</tr>
<tr>
<td>Inside the Company</td>
<td>End-to-End Supply Chain</td>
</tr>
<tr>
<td>Vertically Integrated Supply Chain 1st Tier Suppliers</td>
<td>Outsourced Business Model 2nd, 3rd Tier Suppliers</td>
</tr>
<tr>
<td>Country or Geographic Focus</td>
<td>Global Focus</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>Contingency Planning and Crisis Management</td>
</tr>
</tbody>
</table>

**Figure 6.8: Corporate responses to changing supply chain security requirements**

Source: Closs (2004)
The Eye for Transport Forum has undertaken a survey on the industry appraisal on security related priorities and investments of industrial actors (Eyefortransport, 2006). The survey indicates that the main concern for the companies (41%) is to reduce the theft along the supply chain, rather than safeguard against terrorism (22%). In particular regarding theft the main measures that the companies are keen on implementing for mitigating the risk are the development of a complete security system (56%) and integrating it along the entire (40%) chain, while there is particular concern about the organisation and new trends in the in cargo theft (56%). Finally, as regards the future for the security in the supply chain and the improvement of security core measures the tracking devices (RFID, CSD, etc) (52%) and smart containers (35%) are considered priority for improving the visibility of the cargo, while other measures like, x-ray screening, infrastructure surveillance, physical security locks etc, are ranked lower as priority, not passing the 30%.

Still, beside the issue of security in terms of thefts, losses and frauds, supply chain managers also face other disruptions and demanding requirements to recover quickly from incidents thus improving their chains resilience. The vulnerability of the supply chain is generally faced by the managers by focusing on conventional disruptions which tend to create company specific resilience strategies for increasing their competitiveness. These resilience strategies are not a sound answer to the disruption risks of today. One of the investments made for achieving the flexibility required to avoid disruptions is visibility of the cargo and collaboration with the partners of the supply chain for sharing information for efficient event management.

6.2.4 Conclusions

The most important challenge for supply chain security is system complexity and the need to combine productivity and performance with security. Supply chain security can only be achieved through practical solutions and effective collaboration between public and private sector stakeholders and this is where the global trade market is heading. The initial steps are to fully understand the operational complexities, understand the related economic impacts, and to participate in ongoing dialogue.

With regards to the role of the customs and governments in general, the trends for accomplishing the new challenges of global supply chain can be summarised the following:

1. Provision of advanced clearance service: Modernizing clearance service delivery is a key goal to support trade facilitation and enhance compliance. A number of “e-service” (“e-Government”) improvements such as electronic document submissions via the Internet are augmenting traditional Customs processes.

2. Creating strategic Partnerships and enhancing voluntary participation Schemes: Seamless data exchange among all stakeholders, regardless of role – supplier, administrator or financier – is the future vision emerging for the global supply chain. Existing community-based “e-logistics” models now require active participation and investment by Customs agencies.

3. Investment on Information Technology: Customs agencies have access to a plethora of technology to address tactical operational priorities. Non-invasive inspection and tracking devices are being widely adopted to promote safer,
quicker cargo clearance. Knowledge-based technologies are empowering decision support and risk management. Customs agencies are also beginning to participate in the electronic transaction flow between traders and Customs agencies.

As for the industry and in all likelihood, globalisation will continue and intensify. It is not unlikely that this will make completely new demands on security work with the risk that there will be further strains on trade, increasing operational costs of the companies. The security issue will remain topical disaggregated into the different partners of the chain and security standards will be also required for enhancing business. This means that measures to secure the flows of goods and people between countries will continue to remain high on the agenda and thus also affect the possibility of achieving effective trade.

There is always a thin line between the reliability of the measures to be proposed and introduced and the cost of implementing these measures, especially for SMEs. The trend of extending the security would decrease the efficiency of the small and medium industries and different stakeholders responsible for a specific segment of the chain. This fact would distort the market not only regarding the size of companies but also regarding country development and trade performances.

Therefore, it is now additionally important to develop the capacity to construct effective and efficient methods and systems that do not distort trade but allocate the costs of security in an effective way and provide clear rules for secure trade. In addition to this there is a risk that security initiatives may be used in the future for protectionist purposes and as technical trade barriers.

Possible requirements emerging from the trends regarding security and customs can be summarised in the following way:

1. There is a need for enhancing Public-private cooperation for data sharing. Still, open issue are the standards to be used as well as the concrete information to be shared through a communication platform
2. Compliance with international WCO standards for B2A and C2B information sharing should be considered base on the SAFE standards
3. Specific security standards for the users of service supporting platforms could be introduced (in relation to AEO criteria)
4. Interoperability requirements would be required not only between technology providers for container surveillance, but also between e-customs applications available
5. Interfaces with current single windows and/or customs management system participating to the pilots should be examined for the efficient integration and information exchange processes
6. Data sharing requirements should be in the position to efficiently support the risk management for the dynamic re-configuration of the supply chains improving the global chain resilience
6.3 Emerging trends in technology

Logistics is the central competitive factor of companies in supply chain networks. The efficient adapting of electronic data transfer, information processing systems, data networks and identification and tracking technology is in a central position in the development work of the logistics. Automatic identification and tracking systems aid in the optimisation of the delivery process. The need for intensification of supply chain operation requires large systems, which cover different parties and commodity groups through all levels of the supply chain.

The technologies used for container tracking have been presented in previous chapter of this report. In this section we summarize their main characteristics & shortages that impact the trends in technology development.

New technology applications span from advanced forecasting that comes under the label of advanced planning and scheduling systems (Drew 2003) to e-commerce applications (electronic marketplaces, e-procurement etc.) to the use of equipment for automatic identification, item visibility, vehicle tracking and security scanning of transport units.

Certain practices like the collaborative planning, forecasting and replenishment (CPRF) are exclusively based on the use of internet connectivity between partners to share information and coordinate operations (Bowersox et al. 2000). Some companies require direct access to contract manufacturers’ databases to monitor production and inventory (Drew 2003).

The so called next generation internet applications have spread all over the supply chain and they have created virtual supply chains along with the physical supply chains.

In addition IT solutions applied in supply chain management are discussed in the context of highlighting the trends in transaction systems development for efficient management of intra and inter company information sharing related to transport chain operation and visibility increase.

6.3.1 The Container Supply Chain and Technology Applications

Functional Needs and Technology Applications

Although technology applications span through the overall supply chain, our approach is focused on the container transport supply chain and issues associated to visibility, productivity, security and collaboration between partners involved or associated to container transport.

This area of supply chain technologies include the wide spectrum of IT applications, radio frequency identification, the use of satellite technology for geo location and
Radio Frequency Based Technologies

The most important identification techniques for goods are barcode and RFID (Radio Frequency Identification). Barcode is currently the most widely used method, but RFID is better suited for automated identification since it allows to handle larger reading distances, has the possibility to identify multiple items in a single reading, and can identify the target in motion. RFID has also the possibility to change the information stored on the parcel or handling unit, does not require visual contact and is less susceptible to environmental conditions. There is a wide range of RFID techniques: from small inductive tags for animal identification with a few centimetres reading range to active microwave or UHF active transponders with 100 meter reading range. The lack of widely industrially accepted standards has however delayed wide deployment of RFID techniques. Hence, there have not been affordable interoperable products, limiting as such the use of RFID systems to closed systems.

Tags can either be active or passive. Active tags allow for higher reading ranges, in some cases more than 100 meters, but are more expensive (> 20 €) than passive tags, which cost less than 1 Euro. The most popular form of passive RFID tags is the "smart label", in which the tag is laminated between different layers of material. This allows e.g. to combine barcode and RFID tag in the same label. RFID can use different frequencies, from which 13,56 MHz (inductive technology) and UHF (860-960 MHz) are the most important for passive tags. UHF systems allow longer reader ranges and higher transmission speeds and lower costs, but cannot penetrate well through non-metal materials. As a basic guideline, UHF is hence better for vehicle and pallet level identification, which demands for free-flow identification at the entry gates of distribution centres and shops; inductive systems are more useful for item level identification, where long detection ranges are a disadvantage, e.g. when it is needed to distinguish between products placed near to each other. Whereas the 13.56 MHz frequency can be used globally, there is not a single UHF frequency which can be used globally: In the USA 915 MHz is used, in Europe 865-870 MHz.

Also the allowed transmission power differs in the different areas: in the USA 4 W eirp can already be used for a long time, but Europe allows only from the end of 2004 a transmitting power of 2 W e.r.p. (about 3.2 W eirp), which guarantees sufficient reading range (i.e. over 2 meter) for logistics purposes. The regulations, which came in 2004 into force in Europe require also readers to implement a frequency hopping mechanism, and to "listen before talk", i.e. detection of a free transmitting channel.

Large efforts have been made in standardisation of RFID systems during the last years, but standardisation is not yet finished and there are still some open points. Two major organizations are developing standards: ISO and EPCglobal. EPCglobal is a joint organisation of EAN and UCC.

Another market that has not yet emerged is container tags, often referred to as electronic license plates. These electronic plates would be a permanent tag associated with the container that can be read electronically at all times. Port operators and shipping lines...
may want to have this additional visibility. Another possible solution would be if shipping lines begin tagging containers. E-Plates can also provide additional visibility within ports. Although it is undetermined whether an e-plate will be active or passive, speculation is favoring the latter. This will allow for a tag that is manageable throughout the life of the container as well as having a low cost. With this assumption, it is clear that carriers would be more interested in passive tags than in tags that relate more to security.

**Satellite Based Technologies**

Satellite based technologies are used either for geo location (GPS of the GNSS, Galileo Satellite System etc.) or for communications. Satellite-based communication systems are preferable to cellular communications, though more expensive, when dealing with wide area applications not necessarily covered by wireless networks. Satellite communications based on Low Orbit

In general, there are two broad categories of GPS satellite systems. The first and most widely known is geostationary or a high orbit satellite that is in equatorial orbit and appears to be stationary. These satellites are approximately 36,000 kilometres or 23,320 miles above the earth and rotate along with the earth. The second is a low earth orbit (LEO) satellite system that is approximately 800 kilometres or 496 miles above the earth and does not rotate with the earth.

The advantages for LEO applications include inexpensive narrow-band data transmission in frequencies similar to FM signals. Some LEO systems allow for voice and visual signals. Regardless, both LEO and geosynchronous systems offer logistics advantages by tracking, and identifying the location of containers and trailers throughout the supply chain. However, the LEO systems allow for fewer dead spots, and for the use of non-protruding antennas that are especially good for security applications. Additionally, a firm like Orbcomm (a LEO constellation owner) provides 24-hour communication service at multiple Gateway Control Centers (GCC) that receive, manage, and forward communications from their satellites to locations worldwide.

**Data Handling and Information Platforms**

IT solutions in Supply Chain management have undergone tremendous progress during the recent years, spanning from intra-organizational issues (e.g. web-enabled ERP) to inter-organizational transactions (e.g. IOS, interorganisational information systems). The real issues in global IT are mostly of organizational nature (Akkermans et al.).

There is a clear tendency for network platforms with open access to stakeholders, as an evolution from isolated applications and proprietary systems and standards (Bask et al. 2001). Web-based systems have replaced in most cases the EDI systems. Web-based systems are fundamentally different from traditional EDI systems. The later were based primarily on the idea of locking in customers and suppliers, while Web technologies and systems are relatively inexpensive and highly flexible; and therefore, they have reduced substantially the switching costs of suppliers and customers (Ranganathan 2004).
Handling and processing the volume of data collected through RFID readers (Angeles 2005) and satellite systems is a major challenge, though data collected from active RFID tags for container visibility have a substantially lower volume, as compared to that of the RFID tags attached to cartons or individual items.

Secure data transmission led to the adoption of strong cryptographic techniques in electronic commerce (Transportation Research Board 2003).

Furthermore, over the past two decades, many companies have invested significant capitals to enhance their information systems. A centrepiece of this investment has been in Enterprise Resource Planning capabilities, or ERP systems, to manage their customer orders, billing, accounting & financials, inventory, procurement and human resource management transactions. Many companies have also added Customer Relationship Management (CRM) systems, Transportation Management Systems (TMS), Warehouse Management Systems (WMS), Manufacturing Execution Systems (MES) and other transaction systems to better manage different aspects of their businesses. Generally these systems have provided good value, adding efficiency, more timely information and control (compliance) to their operations.

However, most users of these transaction systems yearned for deeper and better analytics and reporting. Users could not easily customize reports. In addition, they found it very difficult to extract data and conduct deeper, more insightful analysis, especially if it required tapping data from more than one module of their ERP system or data from multiple transaction systems. They also lacked the ability to quickly and easily combine customer, operating and financial data to gain new insights into their businesses. This need for better analytics and reporting has been amplified over the past decade as more managers became more analytically oriented and data driven.

Furthermore, from a business perspective, enterprises tend to organise their organisational and operational environment (in all kind of business and not just in the global supply china industry) through Service Oriented Architecture (SOA) driven applications. The benchmark report of Aberdeen Group March 2007, Management and Governance: Planning for an optimised Application life highlighted that in the increasingly comparative and fluid global market, the need to develop new business capabilities or new products and services and reduce cost through the re-use of application Web Services are the top factors driving organisations to invest in SOA. Successfully implemented and governed, SOA offers the potential for significant business improvements through increased agility, efficiency and productivity. However, many organisations struggle to effectively manage the SOA lifecycle, thus not realising any business advantages from their SOA initiatives because of ineffective sometimes non existent, governance. In fact Aberdeen’s March 2007 report identified the top challenge in managing a SOA lifecycle as establishing a comprehensive governance framework.
The establishment of a SOA governance framework is vital to realise in the optimal benefits of a SOA deployment. In fact, as a direct result of their SOA governance initiatives, well positioned enterprises organisations were able to substantially decrease operating costs (18%) by reusing existing services; an average reduction in costs that is 127% greater than all other organisations.

Aberdeen’s most recent research illustrates that the need to achieve such business improvements are the top factors driving organisations to implement SOA governance strategies which is also applicable for supply chain management solutions.
As figure 2 depicts beyond improvements in business agility and cost reductions, organizations are increasingly viewing SOA governance as a vehicle to optimize the alignment between business and IT units. Governing the lifecycle of a SOA implementation can significantly reduce the likelihood of the SOA initiative failing due to two frequently encountered problems:

1. The tech-intensive nature of SOA deployments and solutions ineffectively translated/explained to business units and upper management budget holders in terms of top-of-mind business benefits.
2. Inefficient scope/timing of deployment due to the lack of communication from the business side to the IT side of needs, goals, and results sought.

6.3.2 Emerging Trends in Container Supply Chain Technology

**RFID Trends**

Cost reduction for the active RFID tags is a research and development priority. Though the price of the passive tags has reached an acceptable level, the price of the active tags is still very high, particularly when these devices are combined with environmental sensors. One key line of research is the further development and implementation of low cost cryptographic primitives. These include hash functions, random number generators and both symmetric and public key cryptographic functions (Sarma et al. 2003).

Alleviating vulnerability issues mentioned earlier, such as spoofing, eavesdropping, skimming attacks, counterfeiting, signal jamming and illegal traffic analysis is another line of research. It is envisaged that these problems will be resolved in a way within the next five years of R&D.

Apart from overcoming limitations of the existing RFID technology mentioned earlier, future trends in RFID will include, the introduction of the following technology variations:

- Chip-less tags (these tags are expected to surpass the limitations of the existing active tag technology, e.g. cost, power consumption, difficulties of operation in metal and liquids)
- Flexible semi-active tags to work on irregular surface texture objects
- Use of conducive ink (to print antennas)
- Development of micro sensory tags of new generation

Significant advances are expected also with the development of the so-called “agile” RFID readers. These readers will have the ability to support multiple tag protocols and will have increased level of intelligence and processing capability. Therefore, they are expected to work with several brands of tags. Apart from the core technology issues this approach needs adoption of common communication standards between tags and readers by equipment developers, a rather slow process currently.
A challenging, yet very important trend is that of developing interoperability of networks for active and passive RFID tags. Readers may read both active and passive tags and through middleware ensuring interoperability, information to be exchanged. Active tags can be attached to containers and passive to cartons contained into the containers.

Permala (2005) presents an initiative in Finland, where a national freight transport telematics architecture has been developed, which describes open interfaces between the actors without binding them to specific technologies and without intervening in the internal systems of companies. The viewpoint of the architecture is the freight and related information flowing through the logistics chain from sender to receiver. The architecture focuses on the processes that are directly related to the transport of goods and on the information flows of these processes. The architecture contains role definitions for the sender, the receiver, the logistics service providers and the public administration. The described process areas of the freight transport are planning, management and control, supply chain operations, and tracking and tracing. The information flows comprise management data, track and trace data and other data related to the goods order, transport agreement, transport order, dispatch note and load specification.

Figure 6.11: Different tracking levels ion Supply chain (Permala 2005)
When the objectives defined in the freight transport telematics architecture have been reached:

- Real-time information about the location, contents and conditions of identified shipments, goods items, parcels and transport vehicles can be collected in a controlled manner.
- The collected information can be combined with planning information and refined appropriately to be used during various parts of the process and distributed efficiently and timely to actors.
- By collecting, refining and distributing information efficiently organizations can improve the efficiency of their goods transport logistics processes, lower their operational costs and improve their portfolio of logistics services.

The following drivers help the implementation of RFID through the whole supply chain:

- "Power shifts within the supply chain". During the last decades the decision making has been moved to the end of the supply chain along with the intensification of the stores themselves. Big players such as Wal-Mart have started to demand changes in the supply chains.
- "Supply chain inversion" - the logistics systems control is changing from push to pull
- Pressure to decrease inventory levels
- Increasing legislation and directives, such as tracking of food from the individual farms or even animals
- Pressure to decrease logistics costs
- Pressure to automate
- Demand for visibility through the supply chain and communication needed for that
- Identification and tracking of the origin of a product
- Reduction of shrinkage (stealing, minimising losses)
Based on the implementation plans from Wal-Mart, Metro and the US Department of Defence, a following timetable for the implementation of RFID can be expected:

- **2001-2004:** use of RFID in closed systems, due to the lack of standardised and interoperable systems. Most implementations use inductive technologies.
- **2005-2008:** use of RFID on transport unit (pallet) level, under impulse of the big retail chains.
- **2009-2013:** use of RFID on product packages. If the price of tags decreases significantly, under 5 cents, the retail chains will demand to put tags on single items.

Also the price of readers has to decrease considerably (under 100 €), and readers could be embedded in e.g. mobile phones.

**Combination Approaches**

Basic passive radio frequency identification (RFID) tags can, when interrogated, improve the control and security of the international supply chain by providing information on the integrity of the container or trailer with respect to door openings. Now, active RFID devices placed inside the container, when combined with satellite, can do more. These technologies have direct application in identifying unauthorized breaches into sealed containers anywhere served by satellite coverage in virtual “real-time.” Together they provide asset management of the container/trailer and report the condition of the cargo. Add to that the identity of a real person who becomes part of the technological system, and one has a “smart container.” Therefore, the use of RFID and satellite communications combined with a responsible human agent enhances logistics efficiency and reduces the probability of using a container or trailer as an implement of terrorism.

**Satellite and RFID combination** approaches seem to provide a great potential for the future, since the combination can alleviate shortcomings associated with the exclusive application of either the radio frequency or the satellite technologies. The system can be integrated with other status and environmental sensors to provide complete information along the supply chain. The system can be either integrated, attached to the container, or a combination of a RFID unit attached to the container and a satellite technology unit associated with the vehicle (truck, vessel). Communications can be either exclusively satellite or a combination of cellular and wireless mesh data communications on the land part of the container transport, along with satellite communication, in case that cellular infrastructure is not accessible. Geo location information can be also provided through a GPS device. Different sensors can be also combined, provided environmental information (temperature, humidity etc.) as well as information about nuclear, biological and chemical threats. A major challenge for the wireless sensors supporting the combination approaches is the application of the so called “pervasive sensing”. According to this technology approach, the wireless sensors will self configure when located into wireless networks or mesh communication networks.

Prototypes of these approaches have already been developed and there are several developers’ designs and proprietary brands, but they need full scale application. These devices fall within the broader category of Container Security Devices (CSD).
Cost has to be reduced substantially, along with improvements in the system design and reliability. Massive production and installation of these devices can lead to a ten fold price reduction within the next few years. Low energy consumption and long battery life of the RFID component will be a prominent feature of this combination technology.

Communication and technology standards for these devices are rather diverse and often conflicting and in most cases of proprietary vendor specific or partnership specific type. The development and adoption of these standards, along with widespread interoperability (in terms of protocols, frequencies etc.) and cost is the most challenging issue for the widespread adoption of these technologies.

**Middleware**

Middleware technologies can be categorized into three levels (Asif and Mandviwalla 2005):

- software applications which solve connectivity problems and monitoring in specific vertical industries
- application managers that connect disparate applications within an enterprise,
- device brokers that connect applications to devices like shop-floor machines and RFID readers

Middleware development for information processing both between tags and readers and between readers and information centres is a very important issue. Future developments will include enhanced multitasking. Anti-collision protocol design has been already considered as an R&D priority. Encryption challenges still also persist.

In the case of the combination solutions referred to earlier, an important research issue is to integrate communication with the tag into the satellite communication equipment software via the tag reader and the middleware platform and incorporate advanced decision making capabilities through the middleware.

**Information Sharing Platforms**

The introduction of the XML messaging as an alternative to the EDI messaging, along with implementation of multi-tier architecture and service oriented architecture decisively advanced the scope and spectrum of the information sharing platforms. Several ports have developed Port Community Systems that prove in practice that the achievement of neutral open information platforms is not a matter of technology limitations, but rather a matter of institutional challenges and business relationships.

Information sharing platforms about container supply chains, often called Container Integrity Systems (CIS), are so far platforms developed by business and vendor coalitions and they share information among their partners. Most of these efforts have a demonstration character in a wider scope to support the full scale application of container visibility monitoring equipment. Shipping lines collaborative systems have a similar function and recently they try to extend the scope of their services, by providing a similar spectrum of asset visibility functions.
There is a clear trend to transform the tracking and tracing platforms to full status visibility platforms through incorporating the sensing and pacing concept.

The real challenge in the future will be to combine these information sharing platforms gradually to a uniform globe wide platform, independent of developer specific standards and technology solutions, able to share information, both in “pull” and “push” mode. Another challenging issue to be faced is that of choosing between a centralized and a decentralized information model. Proprietary information sharing systems, falling in the class of CIS, are almost entirely of a centralized information model type.

In looking at the 3PL space, as derived from experts opinions, it seems that optimization will continue to be an ongoing goal for the technology providers and their clients. Many are beginning to use solutions from vendors like Xelocity, for example, to model their entire logistics network and develop their technology background. In the same logic there is an emerging trend in custom logistics providers using this type of simulation software to set up their contracts and by using this process, the 3PLs aim at do pre-execution using a fairly accurate model that helps them understand the level of optimization necessary to go into the contract bid.

Finally according to the experts from the SCMR (Mc Crea, 2008) it seems that for the supply chain software the following trends are under development and expected to become a reality on the years to come:

- Data management mastering coming to the forefront of supply chain applications through of multi-architecture services
- More SOA oriented applications especially for transport management systems for controlling and synchronising the disparate systems across the supply chains as there is a need for the creation of globally-integrated supply chains, with all trading partners (suppliers, customers, shippers and carriers alike) functioning as part of a single, large supply chain, rather than a bunch of individual ones.
- Integration of voice applications into the management systems
- Integration of services for scheduling capabilities based on user-defined business tools such as optimization as well as dynamic routing guides for solving the clients operational problems

**Container Scanning Equipment**

Container scanning equipment emerging trends are associated with introducing new technologies that can detect substances beyond the capabilities of the well established X rays and gamma rays devices.

Neutron scanning technologies are mostly promising, since they can scan a broad range of materials (Orphan et al. 2005). This technique uses neutrons to excite gamma rays from nuclear reactions. These next generation devices will automatically differentiate among materials, based on their elemental composition. Many elements can be directly detected, including carbon, nitrogen, oxygen, silicon, chlorine, aluminum and iron.
Another important feature of the next generation scanners is the enhanced spatial resolution for low attenuation objects. High resolution will be an important feature of the next generation devices.

According to another source (Hardin 2004), a complete next generation scanning device will leverage on various scanning techniques and will ideally comprise of neutron and x-ray scanning abilities; bio-agent and chemical trace detection and a gamma ray detector for plutonium.

**Other Issues**

The issue of trends in wireless sensor systems deserves a special attention. There is a constant direction towards development of wireless sensors networks (Fuhr 2004).

A very important, yet challenging, issue is also wireless network security. As indicated again by Fuhr (2004) “Wireless networks use a variety of techniques to enhance security, such as spreading and interleaving. These techniques can make the signal virtually undetectable without prior knowledge about the network. This can improve the security of the network by orders of magnitude”.

**6.3.3 Conclusions**

Technologies developed so far and being currently at an early stage of full scale application will continue to evolve. It is unlikely that totally new technologies will be developed and applied during the next five years or so.

The main development trends regarding technology application can be summarized in the following:

- Research to alleviate existing drawbacks and limitations of both the radio frequency and satellite technologies, including interoperability and standardization.
- Development of cost effective combination solutions that will booster existing strong points of the technologies to be combined and overcome or leverage drawbacks.
- Further development of the strengths and cost effectiveness of the terrestrial communications
- Wider application of true open access information sharing systems, not by addressing technology challenges, but mainly by solving institutional and business limitations.
- Research to expand the spectrum of the substances scanned by the scanning technology, mainly by further development of the neutron scanning applications.

**Technology trends in fulfilling security requirements**

From the information provided in this chapter and from the technological state-of the art review presented in a previous chapter of the deliverable, it is obvious that technology
implementation in global supply chains has experienced since the 90s high rhythms of
development triggered by the objective to achieve increased security along these chains.
The more developing technologies are those of satellite, cellular technology based
container devices, the RFID technology and the combination of RFID & Satellite
technologies.

So far, there are varying claims of benefits to the private sector for using the one or the
other containers security associated technologies and systems. Although the specifics of
what to detect vary by the type of shipper, there is some general agreement achieved.
The first order of business is to detect any unauthorized breach through any part of a
container—not just through the doors. Second: it’s necessary to detect the container’s
internal environment for the safety of the product being carried. And third, one must
detect the presence of cargo such as weapons, illegal drugs, and human beings.

Sensors that can detect and report a breach or change in container status in real time or
almost real time exist. It would be easy to think that today’s technology is more than
sophisticated enough to handle the detection situations described, but that’s not so.
Here’s what is possible now. In most cases, basic detection is available and inexpensive.
We can detect reaches into containers using magnetic switches, light, vibration,
temperature, and more. Companies such as General Electric and GlobalTrak offer
systems that use a combination of sensors, RFID (radio frequency identification), and
satellite technologies to detect unauthorized breaches. Detecting a container’s position
is also quite simple and low-cost. However, we still lack the sensing technologies
needed to adequately detect biological agents, chemical agents, shielded enriched
uranium, humans, explosives, and drugs—the issues that governments are likely to
consider the most important. The technologies are still in the early stages of
development. Moreover, when appropriate sensors do become available, the cost will be
high.

RFID has no global protocols or standards. For instance, RFID on which the data ride in
the U.S. will not work anywhere else. For instance, a transceiver in Shanghai or Cape
Town cannot trigger data transmission on the tag on a container shipped from Boston or
Jacksonville. In short, RFID for container security is applicable only to those areas of
the world that have agreed on the same frequency. Therefore, only a combination of
RFID and satellite communication integrally linked to a human agent provides both
security and logistics value in a global supply chain, and by its nature becomes the
“smart container.” ABI Research anticipates that a mix mainly of three technologies —
RFID, satellite, and cellular — will be explored for container tracking solutions (CTS).

However, containers technology development focuses not on solutions to the problem of
security, but on the sensors and communication hardware that are part of the solution. In
practice, a truly effective security solution requires a complete system of end-to-end
coverage—from a container’s origin to its destination.

A container security system, then, is much more than just a locked door. It should be
considered as a complete system that must:

- Electronically identify the authorized personnel stuffing and securing the
  container, and accept and report information such as container/trailer number
  and booking data.
- Detect a breach in any part of the container.
• Report the breach in real time (or close to real time).
• Track the container through the supply chain.
• Identify authorized personnel unsealing container.
• Be software-friendly to accommodate disparate logistics programs in communicating critical data

**Unpredictable Future for Container Tracking technologies due to requirements diversification**

It is difficult to determine where the container tracking technology market is headed due to the uncertainties in place. The determining in the shift of the market is whether or not a set of requirements or mandates will be provided to the shippers and who will place these requirements, the governments or the World Customs. For the time being pilots and tests are being done by governments, Customs and by commercial companies in the sector.

The defence sector is interested in securing and having visibility of its goods for obvious reasons. The commercial sector has also seen companies investing in solutions that provide as ensuring decreased pilferage of their goods. Big logistics companies ask for additional visibility along the container transport chain for increasing efficiency and minimize risk of their operations.

Closed loop supply chains are talked about as potential markets for dedicated container tracking technologies & solution, but outside of the military been known no major potential are identified. Open loop supply chains with many players need a set of standards for achieving successful implementation of container tracking technologies. Another interest in visibility and security is expected for those shipping containers with high valued assets, or containers coming from suspicious origins that are looking to gain quicker entry into the EU. United solutions utilized in the future will be those aimed at tracking containers as opposed to securing them.

**Future technology challenges for supply chain visibility**

RFID, satellite, and cellular technologies each provide a different level of visibility for the container while it is in-transit. Also limits are identified regarding the ability of global implementation of each technology due to lack of standardization. A very expensive and highly redundant solution would be a combination of RFID, cellular, and satellite messaging capabilities built into a container. This would provide the highest level of in-transit visibility, as the container’s whereabouts would be known wherever appropriate RFID readers exist, wherever cellular coverage exists, and if there is no cellular network coverage, satellite messaging systems can be utilized to transmit container status.

The high hardware/communication costs of combined real time monitoring solutions will most typically appeal to those transport market segments with high requirements on container visibility like refrigerated cargo or hazardous materials that need a real-time constant monitoring approach. On the other side RFID based technology requires to deploy costly infrastructure of RFID readers and software networks throughout the major hubs and high container traffic areas. The tendency recorded is the development
of hybrid container devices and the high priority for investing in interoperability of solutions.

**Development of Data sharing and service platforms**

As technology continues to evolve, so do too the supply chain applications that companies are using to increase visibility, optimize operations, streamline transportation channels, and increase their bottom lines. Studies show that these applications will be driven by customer demands, heightened global competition, and regulatory compliance among other issues. In this context and with the technology available for accessing information quickly enough for being used, by the global supply chain actors, in decision making, it is expected that the timely visibility into critical processes in global chains will be enhanced. Thus the development of new business capabilities and the reduction of cost through re-using application & information via Web services will become top factors driving the organizations to invest in data & service sharing platforms complying with Service Oriented Architecture (SOA). The establishment of SOA convergence framework will be vital for realizing optimal benefits from technology implementation and platforms operation.

### 6.4 Standardisation

Standards provide a vital part of the infrastructure necessary for sustainable economic growth in synergy with wider societal needs. A technical standard is an established norm or requirement. It is usually a formal document that establishes uniform engineering or technical criteria, methods, processes and practices. They promote confidence in products, processes and services to consumers and assist both in the creation of new markets and opening up of existing ones. They facilitate certification. The operation of the Single Market and the European Union is heavily dependent on European Standards. Moreover, they play an important role in supporting policy objectives of the Community, including the competitiveness of enterprises, innovation, the protection of health and safety, consumer interests and environmental protection.

#### 6.4.1 Trends related to standards drafting

Many high quality harmonisation documents already exist for containers and for risk assessment in supply chain security, providing also data interpretation and data evaluation, leading to better risk management. CEN, the European Committee for Standardization and ISO (International Standardization Organization) can ensure a wider dissemination of these documents, but also their maintenance and their larger use, also as reference in legislation and guides of good practice. The platforms offered by CEN and ISO guarantee that new standards are produced in a democratic and efficient and coordinated way by the interested experts and stakeholders. Current standards are as much as possible “performance based” and therefore do not inhibit innovation.

A practicable approach towards standardisation and the drafting of workable standards, and one which is more and more applied, is the so-called ‘standard integrated approach’. In this approach, the first step is awareness-building: the goal is to identify common
difficulties or weakness of current practice relevant for a group of stakeholders and state these problems explicitly. Once the group of stakeholders is aware of overlapping deficiencies of current practice, these can be prioritized to form objectives. The next step is to decide by consensus on the most efficient ways to reach these often complex objectives. This is typically done by a thorough analysis of a repertoire of components which typically contribute to a successful implementation of standardized procedures. For the efficient movement of containers, these may include research and development, extra legislation, standardisation of procedures for decision-making on hazards and risk, and other assorted complementary measures, including education and standardised training.

6.4.2 Trends related to Standards-Harmonization through collaboration

The trends concerning global container transport chain standards are not about identifying the next standardisation packages from the international and regional associations (ISO, CEN, IMO, etc) for technological components, containers, port equipment and so on, but about understanding the need for new standards. Beside these standard features of the global container chain management there is an implication of a variety of standards and parameters that need to be understood in order to consolidate the standardisation requirements. These standards are indicatively the following:

1. Physical Processes standards
2. Digital processes standards
3. Communication Standards (software standards, documents, data sharing, e-commerce standards)
4. Security standards (physical and virtual)
5. Technology standards (hardware)
6. Trade standards
7. Standards for customs

As explained in previous paragraphs of this compendium, as a dynamically changing and complex environment the business of global container transport calls for standards and standardisation frameworks that should comply both with legislative/regulatory requirements and business requirements. There is plethora of standards that are existing in the market, which still are driven by the need of the market (or individual sector e.g. customs) determining specifications, processes and profile. Therefore according to these drivers of existing standards and business needs, more a challenge than a trend for the global chain management is the harmonisation of the standards available for achieving seamless communication, eliminating information gaps and operational incompatibilities for all members of the chain.

A typical example of harmonisation of standards in the global supply chain is the UN/CEFACT for international trade set of standards harmonising the different aspect of a supply chain for efficient integration into the e-business world.
This necessity/initiatives of the data and standards harmonisation is not a new story but it illustrates the trend of continuous standards harmonisation required in the global industry, combining regulatory and business needs.

As regards the integration of e-business solutions and public authorities (i.e. customs), the Single Window concept addresses standards information exchange requirements in the way as depicted in figure 6.9, where standard exchanged information and document structures for trading, transport, insurance etc, would be combined for electronic business transactions with governmental entities.

However, it is not only a matter of combining the standards from the different international organisations and achieving supply chain efficiency but also to match
these standards with commercial standard solutions that are widely implemented by the industry for inbound and outbound operations and transactions with their partners.

A significant example of such a harmonization of standards for achieving maximum efficiency along the supply chain is the SSCC-UCR Project (2006-2007) held by GS1 and the customs authorities of Australia and the UK along with other chain partners. The objective of the project was to validate use of the SSCC (Serial Shipping Container Code) as the UCR number for Customs purposes as the unique identification code for audit, consignment tracking, information consolidation and reconciliation purposes. The project aimed to address the post-transaction (import and export) assurance of the UCR, and to prove and test the benefits of the SSCC as the UCR used by other participants in the supply chain.

In this particular example a collaboration among the parties of a supply chain would harmonise the standards set from the top-down approach coming from the WCO for enhancing customs procedures (UCR) for the sake of reliable business operations along the chain using separate standards (SSCC) aiming at successful public/private cooperation. Of course this particular procedure met the requirements of the ISO15459 (Information technology - Unique identifiers)

6.4.3 Trends related to technology adoption along the supply chain

Seeking for increased efficiency along the supply chain the main actors have implemented technologies and systems for achieving cost effective operations. The vast technology development and implementation creates “paradoxes” that in order to be efficiently faced requires further standardisation efforts.

From local standards to global standards

Supply chain partners will meet the standards required or provide solutions that comply with local standards. Successful global suppliers have established with buyers or markets the compliance standards required, and have or will have the appropriate accreditations. They do not seek to convince buyers of alternative standards or designs unless the requirement invites alternatives and successful suppliers are fully familiar with the risks and benefits of alternatives.

It is evident that standards are a key for collaboration. Collaboration will demand greater use of standard communications and messaging to ensure its success.

Global data synchronisation will become fundamental, and for many organisations this will lead to a review of existing business-to-business infrastructures, and their e-business strategies.

There are many dangers ahead if organisations within the supply chain fail to collaborate. Poor service to customers and consumers, reduced performance levels, loss of sales, imbalances between demand and supply, excess stock levels and increased conflict will all increase costs in the supply chain and reduce business profitability.
From hierarchical business organizations to open business structures

Adoption of sophisticated enterprise systems & tracing technologies also has a direct, and often paradoxical, impact on a company's organization and culture. On the one hand, by providing universal real time access to data, the systems allow companies to streamline management structures, creating latter, more flexible, and more democratic organizations. On the other hand, they also involve centralization of control over information and standardisation of processes, which are characteristics of hierarchical organizations with uniform culture.

From de-facto technology standards to interoperable technologies

As technology is advancing core “mechanical” aspects of container movement and security have already been addressed (mechanical and electronic seals, physical dimensions, etc) but also management issues, in particular with the ISO 28000 series. The “missing links” in standardisation are more of a “niche” nature. In that context, RFID should be expanded; hybrid container technologies & interoperable solutions for container monitoring should be adopted. The mandated results of recently started EU funded research project like GRIFS (Global RFID Interoperability Forum for Standards), where GS1 and ETSI are Core Partners. (www.grifs-project.eu) should be taken into account.

6.4.4 Concluding remarks

There is considerable work pursued in the standardisation issue that would need also to be reflected in the SMART-CM and INTEGRITY projects. Different standardisation parameters should be taken under consideration such as standardisation in processes; information and communication messages; technology and interoperability; and custom processes. The workshop to be organized with the contribution of CEN will be a decisive point in the standardisation research and requirements of the project. The achievement of standardized application for efficient operation ion security and logistics would be determined at a high rate by the definition of the appropriate standards introduced.
7 Concluding remarks and mandate

This chapter reviews the main insights from this Compendium, and formulates the main mandates of the two projects SMART_CM and INTEGRITY.

Global trade Management

The global trade landscape is complex, fluid and highly sensitive to external drivers, including the following ones:

- Increased volumes (8% a year, 2002-2006) and complexities of international trade, e.g. complex preferential rules of origin.
- New business models and requirements; e.g. just-in-time distribution; multi-modal transport; protection on IPR infringements etc.
- Increased security threats and organized crime; e.g. cross-border fiscal fraud; the smuggling of drugs, dangerous, harmful and prohibited goods.
- A new approach to the border crossing: new measures are emerging for the end-to-end management of the movement of goods across borders such as the WCO SAFE.
- Demands from society: regarding smuggling of prohibited and dangerous goods, such as weapons and narcotics; quality and safety standards; and public health, and the environment;
- New trading patterns: approximately 50% of world trade takes place between connected parties; and
- Increase in revenue fraud: including duty and tax evasion and avoidance.

This results in new requirements for managing such growing complexities. One of these requirements is to deal with the growing number of dependencies in Supply Chain Management. These dependencies are being accelerated and increased by both business and logistic trends such as Just-In-Time, outsourcing and even globalization. This requires not only an internal enterprise focus, but demands looking beyond the company boundaries in order to synchronise activities across suppliers, logistics providers, and customers. Important enablers for this are coordination, cooperation and visibility.

Global supply chain visibility

Companies demand better transparency of orders status, inventory, and shipments across their extended supply chain. In the supply chain, visibility is a precondition to adequately manage events.

Supply Chain Event Management (SCEM) attempts to identify, as early as possible, the resulting deviations between the plan and its execution to trigger corrective actions according to predefined rules. Tracking events in the supply chain is a necessary means for SCEM.

However, companies that do track events often suffer from poor data quality and factual inaccuracies in forecasts and reports. There are three main obstacles to achieving visibility:
• Organisational: it is difficult to address responsibility for visibility since it surpasses different organisational functions and regional boundaries all benefiting from improved visibility.

• Technology: Visibility systems have to gather information from multiple internal and external systems; that requires many interfaces to other systems. However, web services, B2B hubs, and transportation carrier portals are now making interfaces more manageable.

• Managing visibility information: how to drive strategic business improvement from visibility information. Additional technology and organizational capabilities are needed to achieve this. Companies need a system which can monitor the events in the entire supply chain and that provides reports to all stakeholders involved.

Another issue in achieving supply chain visibility is related to the strategic importance of information. Information is power and actors in the supply chain may gain strategic advantage by information ownership. On the other hand industry is convinced by the benefits information sharing and visibility can bring to the whole chain, as witnessed in advanced logistic concepts such as Vendor Managed Inventory. A major dilemma for companies is to decide to share information or not to.

Global supply chain innovation

The efficient adoption of electronic data transfer, information processing systems, data networks and identification and tracking technology is central to efficient and effective logistics. Automatic identification and tracking systems aid in the optimisation of the delivery process. The need for intensifying the supply chain operation requires large systems, which cover different parties and commodity groups through all levels of the supply chain.

One of the emerging trends in supply chain technology is the deployment of RFID applications. In principle, RFID makes it possible to capture data are strategic points in the chain (stuffing, loading, unloading, stripping), in real time, anywhere in the world. The capture of data, and the uplink to centralised data storage facilities, where more extensive data descriptions and other relevant information, such as previous exceptions, and security measures, are stored provides a continuous information flow that moves together with the container through the chain.

Obviously, there is a clear need to extend SCEM with a combination of technology and more pro-active information exchange in order to increase visibility and to be able to react to event related information in an effective and efficient way.

Enterprises tend to organise their organisational and operational environment through Service Oriented Architecture (SOA) driven applications. Successfully implemented and governed, SOA offers the potential for significant business improvements through increased agility, efficiency and productivity. However, many organisations struggle to effectively manage the SOA lifecycle. This highlights the need for a carefully guided development of information exchange platforms based on SOA along the supply chain.
Global trade facilitation requirements

Facilitating global trade is a crucial element of the mission of Customs agencies. One of the objectives to achieve this is by eliminating duplication and delays in international supply chains such as multiple reporting requirements and inspections. This process of simplification, however, should also adequately reflect the requirements of increased security. This has resulted in a series of measures:

- the proposed Community customs code security amendments (regulation 648/2005)
  - require traders to provide customs authorities with information on goods prior to import to or export from the European Union (see Pre Arrival / Pre Departure Declarations);
  - provide reliable traders with trade facilitating measures (see Authorized Economic Operator AEO);
  - introduce a mechanism for setting uniform Community risk-selection criteria for controls, supported by computerised systems
- the customs security program to harmonise control standards and facilitate trade by the AEO programme.
- the AEO programme. AEO certified traders can obtain simplified customs procedures.

The benefits of these programmes are often covered under the all encompassing term of ‘creating green lanes’. This means that import cargo, upon arrival, is already viewed, verified, and found secure before entry, and can pass across the border unhindered by Customs, or other inspection agencies. In many cases, such green lanes already exist, or are being developed, by removing bottlenecks in information exchange with customs, and improving information exchange along the chain, both between business involved, and between customs agencies in different countries.

The main challenges for simultaneously realising increased security as well as trade facilitation are:

- Mutual recognition of green lanes and trusted partners
- Harmonised risk management and assessment approaches
- Acceptance and trust in AEO benefits by industry

Mandate for SMART-CM & INTEGRITY

Visibility requirements in the supply chain are not new. In fact, many businesses already have solutions in place, and many global freight forwarders and logistics service providers spend considerable effort on reporting container, package and consignment status to their clients.

However, much of the relevant data is not readily available to users, although it is available in the chain if one knows where to look for it, and the data is not exchanged automatically. As a result, much of the data gathering is really done through human intervention, through on-off systems interfaces, and through platforms that cover only part of the chain. The consequences are information delay, errors, and, in general, unreliability of data.
It is at this point that the mandate of SMART-CM and INTEGRITY can be formulated with clarity. The information exchange platforms that will result from these projects aim to fill the gap between data availability and data need, by offering information capture and exchange throughout the chain. One critical element in this effort is to capture information as early as possible in the chain, preferably at the point of stuffing the container.

The overview in chapter 1 and 2 explain the structure of supply chains, the inherent dependencies and vulnerabilities in chains and networks, and underline the need for visibility above all else. Chapter 3 then described the complex environment of customs for global trade, and emphasises a number of important developments that have a bearing on information exchange in the supply chain, even if customs is not directly involved. The adoption of the UCR, for instance, will be a necessary element in developing information exchange platforms, and as such, the aims of improving information exchange in global supply chains and facilitating communication with customs are aligned. Technology will be an important requirement to capture data, and technology will result in data that can be added to the flow of information along the chain. One critical technology is the e-seal, which will help capture information early in the chain, and allow the monitoring of the secure pipeline while the container is in transit. Other technologies can progressively be added to the mix to augment the capabilities of the platforms, as well as provide new and enhanced visibility in the supply chain. Finally, standardisation, in terms of using UCR, but also in terms of data structures, messages, technology and procedures will be paramount to ensuring interoperability of the platforms.


References


Bartels, T. (2005), Factors influencing the adoption of traceability in the veal industry, RSM Erasmus University Master Thesis


Bullington, R. (2004), Presentation Motorola Inc., Eyefortransport conference, Washington DC, USA, October 18

Bullington, R. (2004), Presentation Motorola Inc., Eyefortransport conference, Washington DC, USA, October 18


CER Publications, “From Truck to Train” Thirteen examples of successful modal shift in European freight transport, June 2008;


Dornier, P.P., Ernst, R., Fender, M., Kouvelis, P. (1998), Global operations and logistics – text and cases, John Wiley & Sons, New York, USA

Dornier, P.P., Ernst, R., Fender, M., Kouvelis, P. (1998), Global operations and logistics – text and cases, John Wiley & Sons, New York, USA


Hallström (2004): Organizing International Standardisation, Cheltenham


http://www.bearingpoint.com/portal/site/bearingpoint


Joppen, L. (2003), “Nutreco rolls out NuTrace; living food safety”, food engineering & ingredients, April

Joppen, L. (2003), “Nutreco rolls out NuTrace; living food safety”, food engineering & ingredients, April


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

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


Sheffi, Y. (2005), The resilient enterprise, the Massachusetts Institute of Technology press, Cambridge/Massachusetts, London/England

Sheffi, Y. (2005), The resilient enterprise, the Massachusetts Institute of Technology press, Cambridge/Massachusetts, London/England


William Copacino - Better Supply Chain Collaboration Through Business Intelligence - Supply Chain Management Review, 7/31/2008


World Customs Organization, Framework of Standards to secure and facilitate global trade, SAFE, Brussels, June 2005