# THE EFFECTS OF SECURITY ON TRANSPORT PERFORMANCE

*Urciuoli, Luca, Dept. Industrial Management and Logistics, Engineering Logistics, Lund University. luca.urciuoli@tlog.lth.se*

*Sternberg, Henrik, Div. Transportation and Logistics, Chalmers University of Technology. henrik.sternberg@chalmers.se*

*Ekwall, Daniel, School of Engineering, University of Borås. daniel.ekwall@hb.se*

## ABSTRACT

The purpose of this investigation is to emphasize the negative effects of security on transport performance. The methodology is based on the analysis of a large workshop with security experts and multiple case studies, where data is collected by means of observations, and unstructured and semi-structured interviews. The findings from the empirical data seem to demonstrate the initial hypothesis that security measures affect efficiency in terms of lower operational performance. Therefore, this paper discusses the importance of developing security capabilities to be integrated in existing logistics information systems. Only in this way will transport companies develop the capability to fully realize wins in terms of both security and efficiency.

**Keywords:** transport security, transport efficiency, transport, supply chain security.

## INTRODUCTION

The introduction of security in transportation networks is fundamental to preserve the integrity of cargo moved around the world and thereby to avoid disruptions and fear and havoc to our communities. For this reason, security regulations are being pushed forward by authorities together with other stakeholders and threaten to burden transportation chains with new costs related to physical implementation, administration and security auditing. Examples of security initiatives issued by the authority are the C-TPAT (Customs-Trade Partnership Against Terrorism), the AEO (Authorized Economic Operator), the ISPS (International Ship and Port Facility Security code), the SOLAS (Safety of Life at Sea) chapter, etc. (CBP, 2008; European Parliament, 2004; European Parliament, 2005; European Parliament, 2007b). In addition, specific transport security programs and initiatives are being developed within the food and pharmaceuticals sectors and aim to protect consumable products from counterfeiting and from contamination threats (EU Commission, 2008).

Obviously, the fear of many logistics and transport operators is that the new security measures could jeopardize their existing operations. Loss of efficiency could stake a competitive advantage on the marketplace and result in consistent economic losses. In addition, too restrictive of security measures could make transport chains less flexible and reliable, implying the loss of their capability to quickly respond to demand volatility. Therefore, the need for more research and to discover the impact of security on logistics and transport efficiency is crucial.

Previous literature outlines the correlation between security and efficiency as factors that can be easily and beneficially combined. These investigations have mainly a normative character and often lack empirical data. Rice and Spayd (2005) state that security enhancement can also bring "*collateral benefits*" such as trade facilitation, asset visibility and tracking, faster standard development, etc. The same concept of "*collateral benefits*" is similarly sustained by Sheffi (2001), Peleg-Gillai et al. (2006) and Closs and McGarrell (2004). Haughton (2007) demonstrates the economic and competitive advantages for large and small shippers becoming FAST-approved (Free And Secure Trade, a Canadian security certification similar to C-TPAT and AEO). Powanga (2006) adds that only large companies may have the possibility to trade-off the security costs with benefits related to supply chain transparency (Powanga, 2006). Willys and Ortiz (2004) emphasize that efficiency and security in supply chain transport are closely interrelated, since higher security may reduce customs delays so as the higher transparency of information of goods flows may reduce shipping costs and time. Lee and Whang (2005) demonstrate the beneficial effect of electronic seals placed on containers entering port terminals in US. According to the authors, savings range between $1,000 and $4,000 per container.

Yet, too little previous research explores how the introduction of security may negatively affect logistics efficiency. In Mazeradi and Ekwall (2009) it is shown how the implementation of the ISPS-code may increase paperwork and slow down processes. Likewise, Stevenson (2005) claims the negative impact of the ISPS code on costs and the efficiency of port terminals.

Security measures are required to be built upon existing efficiency and quality processes that today are the top priority areas of transportation companies. It is well known that these actors, especially the carrier operators, face costs and time pressures from their customers and are demanded to efficiently manage products' demand volatility. At the same time, wasting time and costs, caused by infrastructure bottlenecks as well as by the high complexity of transport chains in which multiple actors with conflicting goals interact have to be avoided. Besides this, security routines constitute an additional mandatory work for terminal, manufacturing or transport operators, whose personnel are forced to learn and apply new procedures on top of their duties (Rolandsson and Ekwall, 2008). Moreover, existing security tools are too complex and expensive to be implemented and necessitate qualified operators as well as top management commitment to be truly effective in a transport company. As a consequence, it can be hypothesized that the performance of logistics and transportation services may be seriously compromised by the upcoming security regulations.

Therefore, the linkage between security and efficiency remains unclear and more empirical research is needed to discover the negative impact of security on transport operations.

By means of observations carried out in occasion of a large security workshop and multiple case studies carried out within the frames of four Swedish national and European projects related to secure transportation, this work sets out to deeply analyze the effects of security on transportation performance. More specifically, we aim to demonstrate the hypothesis that security measures have, in the first place, a negative impact on transport efficiency. However, by carefully de-coupling security and transport operations as well as by exploiting specific hi-tech solutions, efficiency may be restored or even improved.

This article is made of three main sections: first of all, the frame of reference is outlined and classified according to literature inherent to transport security and efficiency. Next, the methodology and the three cases used in this investigation are presented. Finally, the analysis of the cases is carried out and results are discussed.

# FRAME OF REFERENCE

This frame of reference contains the topics that need to be involved to explain the researchers' thoughts. A central definition for this article is transportation, defined as the physical movement of a product (Ross, 1996), which also covers activities involved in modal shift, e.g., loading and unloading in ports and terminals. The literature related to transport security often uses terms such as distribution security, logistics security and supply chain security. Even though using different terminology, generally the literature on distribution, logistics and supply chain security actually focuses on studies of transport activities, the authors of this paper decided, for sake of clarity, to use the term *transport security*.

## Transport Security

Antagonistic attacks have been widely studied within the criminology discipline. In addition, present research has pointed out the correspondence between criminology theories, such as *the elements of crime* and *the crime displacement theory,* and transport security (Ekwall, 2009). In few words, this means that attacks against supply chains take place whenever the perpetrator, the target and the absence of proper security converge (*elements of crime theory*). Increasing security implies that criminals will rationally choose weaker targets (*crime displacement theory*). This phenomenon has been clearly observed in freight transport where the securing of terminals in transport chains has caused the increase of incidents in the links between the terminals (Ekwall, 2009; Purtell and Rice, 2006). Hence, many authors agree on the statement that "*a supply chain is as weak as the weakest of its links*" (Rice and Spayd, 2005; Willys and Ortiz, 2004; Closs and McGarrell, 2004).

While security has always been a crucial problem for logistics and transport operators, the aftermath of the terrorist attack at the World Trade Center on September 11, 2001 brought much more attention to security in today's trade. The reasons are more than just terrorist

attacks. According to Closs and McGarrell (2004), three factors can be outlined. First, the globalization of the world trade, which depends on and is generated by the free flow of people, goods and information. Second, the increasing demands from businesses for efficient transport operations. Third, the increasing threats of terrorist attacks. The third factor can be reformulated as illegal and antagonistic threats, of which terrorists are one type.

Other transport security research outlines four concepts related to the integration of security in a transport chain. First, transport security should incorporate not only theft prevention but also anti-terrorism. Second, global issues should be addressed instead of local or national issues (Sweet, 2006). Third, when conducting contingency planning, the concept of crisis management is to be included to obtain better resilience. Last, security is no longer an internal corporate question but an issue for all actors within the entire supply chain (Closs and McGarrell, 2004).

The need for security during transport is to prevent unwanted negative disruption in the flow of goods (Sheffi, 2001). Transport security is the combination of preventive measures and human and material resources intended to protect transport infrastructure, vehicles, systems and workers against intentional unlawful acts (EU, 2003). In Urciuoli (2009), physical transport security is categorized as a combination of measures for preventing, detecting and recovering:

1. **Prevention**. Preventive measures concern the ability to be a step ahead of the antagonists, scare them and to provide security analysts with key information to predict threats.

2. **Detection**. Detection measures register an attack taking place and send this information to personnel in charge.

3. **Recovery**. Finally, recovery measures are all solutions that support managers in recovering from an attack and reduce its consequences (i.e., detect, identify and capture the antagonists or the processes to recover stolen cargo or to set up a new shipment, etc.).

In Europe, security certifications like the Authorized Economic Operator (AEO) and the International Ship and Port Facility Security code (ISPS) are at the disposal of logistics and transport operators to enhance the degree of security of their assets and operations.

## Authorized Economic Operator

The Authorized Economic Operator (AEO) is a concept integrated in the SAFE framework of standards designed by the World Customs Organization (WCO) to disseminate around the world the security requirements issued in the US and to facilitate global trade (CP3 Group, 2006). Hence, the scope of the AEO initiative is to detect high-risk cargo as early as possible in the supply chain and in a resource-efficient way (CP3 Group, 2005). The AEO interpretation of end-to-end supply chains includes manufacturers, exporters, freight forwarders, warehouse keepers, customs agents, carriers and importers (Figure 1).


**Figure 1:** End-to-end supply chain (EU Commission, 2007).

To categorize the economic operators joining the AEO, Customs assesses the operators' administrative organization and its internal control system, including business processes, procedures, measures taken to reduce fiscal and non fiscal risks, etc. (EU Commission, 2007). Existing relevant standards for safety and security are taken into account and recognized by the AEO as compatible (i.e., ISO 9001, 14001, 20858, 28000, 28001, 28004 and the ISPS code) (*ibid*). More specifically, to gain the AEO certification, organizations have to comply with a set of four main criteria (CP3 Group, 2006; EU Commission, 2007):

1. **Appropriate Record of compliance with Customs requirements.** Prospective members have to furnish a listing of information to the Customs authority. This information includes the volume of business (annual turnover, profits and losses, stock capacity, etc.) and statistics on Customs matters (tariff classification, % of import duties, % of VAT, origin of goods, Customs VAT value, etc.).

2. **Appropriate Record-Keeping.** Operators are required to maintain and store import and export operations in an accurate, complete, timely and verifiable manner. In addition, information has to be carefully protected (i.e., by continuous data back-up and recovery). This is necessary to allow easy and appropriate Customs controls of fiscal and non-fiscal irregularities as well as keep track of other committed infringements over the last 3 years.

3. **Proven Financial Solvency.** Financial solvency for the past three years has to be proven. This is necessary in order to ensure the commitments of operators applying to the certification.

4. **Security and Safety Standards.** The operators have to show a high level of awareness on security and safety measures. A self assessment to identify risks and threats and measures in place may be performed by the operators. Recommendations about 1) physical security of buildings (including entry and access), cargo units, 2) procedures for incoming goods, 3) storage production and loading of goods, 4) personnel security, 5) security requirements imposed on business partners and policies about the hiring of external security services, are provided in the AEO guidelines.

Finally, the supply chain companies that are AEO granted can be further classified into three categories depending on what AEO criteria are fulfilled and what benefits are earned (EU Commission, 2007):

1. **AEO-C (Customs Simplifications).** This certificate is given to operators that fulfill the criteria of customs compliance, appropriate record-keeping and financial solvency. The benefits of this certificate are easier admittance to customs simplifications (Customs authorities don't need to re-examine the conditions

examined when granting the AEO status), fewer physical and document controls, priority treatment and the possibility to choose the place for control.

2. **AEO-S (Security and Safety).** To obtain this certification, the operators have to show that they are able to maintain appropriate safety and security standards. Benefits of this certification include prior notification of inspection (Customs may notify the AEOS operator when the cargo has been selected for further physical control), a reduced data set for summary declarations, fewer physical and document based controls, and the possibility to request a specific place for the control.

3. **AEO-F (Customs Simplifications/Security and Safety).** To obtain this status operators are requested to fulfill the criteria for customs compliance, appropriate record keeping, and financial solvency, and maintain proper security and safety standards. The benefits will be all those related to AEO customs simplification and AEO security and safety certifications.

## ISPS and SOLAS

The ISPS is a framework to ensure the safety and security of ports and vessels. Guidance to support compliance to the mandatory security requirements specified in the ISPS code is provided in the SOLAS chapter XI-2 (special measures to enhance maritime security) and includes the following main recommendations (IMO, 2009):

1. Role of the Master in security decision making.

2. Ship security alert systems. In particular, this system should be able to initiate and transmit security alerts to a competent authority. Messages have to include ship ID, location and threat condition.

3. Security requirements for port facilities. These include the identification of responsibilities of officers, security plans, and security equipment. In addition, the regulation enshrines that security assessments in port facilities have to be carried out while security plans are developed, implemented and reviewed (auditing) in accordance with the ISPS code.

4. Specifications concerning provision of information to IMO (International Maritime Organization).

In SOLAS, Code Contracting Governments, three security levels are defined (IMO, 2009):

1. **Security Level 1, normal.** No action is taken.

2. **Security Level 2.** This level lasts for the period of time when there is a heightened risk of a security incident.

3. **Security Level 3**, lasting for the period of time during which there is the probability of an imminent risk of a security incident.

## Transport Efficiency

The transport network, made of links and terminals where the goods are respectively moved and stored, affects costs and throughput time, and if used smartly it can even increase the value of the product (Lambert and Stock, 1993). Previous research offers a vast collection of metrics to measure the performance of transport networks, with the common principle to ensure that customers are satisfied by guaranteeing that the utilities of time and space are generated persistently by transport companies (Lumsden, 2006; Coyle et al., 2000). Gunasekaran et al. (2004) point out the use of these metrics to constantly monitor organizational performance and thereby contribute to the success of an organization from a strategic, tactical and operational viewpoint. In the context of this study the following performance indicators will be considered:

1. **Quality.** Quality concerns whether the goods delivered conform to specifications. Thus, the right quantity is delivered free of damage or defect (Lumsden, 2006).

2. **Transit Time.** Transit time is the lead time of goods flows needed to arrive at a destination or to enter and exit a temporary storage warehouse or intermodal terminal (Rodrigue et al., 2006; Stewart, 1995).

3. **Costs.** Costs, usually distinguished as fixed and variable costs, relate to the monetary value of the resources (i.e., vessels, personnel, infrastructure fees, fuel, etc.) needed to move the flows of goods (Coyle et al., 2000; Hesse and Rodrigue, 2004).

4. **Reliability.** Transport reliability is the capability of organizations to deliver at the time demanded (also indicated as just-in-time or demand utility) (Coyle et al., 2000). In other words it corresponds to the capacity to fulfill customers' orders according to the agreed specifications (Hesse and Rodrigue, 2004; Stewart, 1995).

5. **Flexibility.** Finally, flexibility is the capacity to quickly respond to freight demand changes or to specific customers' requirements (i.e., technological, packaging specifications, etc.) (Hesse and Rodrigue, 2004; Gunasekaran et al., 2004).

It is important to keep in mind that the above dimensions have a consistent high degree of mutual dependency, which implies for instance that higher flexibility may result in higher costs or transit time, or *vice versa*. Likewise, quality can also be interpreted as a function of costs. This is a direct consequence of the multifaceted and complex nature of logistics and transportation systems. Hence, to enhance the clarity of this investigation, the analysis performed will focus on qualitatively evaluating these indicators independently from each other. While the investigation will have some conceptual limitations, it is still believed that results will not be greatly affected and that the above dimensions will faithfully represent the efficiency degree of logistics and transport companies.

# METHODOLOGY

The methodology followed in this article is based on a literature review, a workshop and three case studies: a DSV warehouse terminal and two transportation setups.

The literature reviewed is within the fields of supply chain and transportation security, as well as transportation efficiency. The material gathered has been used to outline the frame of reference of this paper as well as to enhance the understanding of the topic and the data collection phase.

Workshops employ an iterative process of summarizing and evaluating the respondents' views on a consensus view (McKinnon and Forster, 2000). The method consists of focus interviews, to be followed by a workshop. Ideally, the people interviewed should also attend the workshop. This kind of two-phased process enables the evaluation and prioritization of the preliminary findings. Face-to-face conversations foster interactive communication, which is a precondition for knowledge creation and new innovations (Nonaka and Takeuchi, 1995). Previous research has identified the task-orientated, interaction-centered focus groups (workshops) as an ideal methodology for exploring professionals' experiences and for describing that experience.

A focus group discussion was held in correspondence with a workshop held in Gothenburg in March 2007 in cooperation with the Swedish governmental agency for innovation systems (Vinnova), the Swedish Civil Contingencies agency, the Swedish Defense and representatives from the automobile industries. A total of nearly 60 attendees representing public and private interests were gathered. The workshop started with a set of presentations concerning port security and it followed focus group discussions. Supply chain stakeholders were uniformly represented in each of the groups. The discussion was oriented to collect the stakeholders' views on the topic of supply chain transport security and efficiency. The focus group used in this investigation was made of 12 security experts whose backgrounds include transportation carriers, manufacturers, law enforcement agencies, etc. Afterward, unstructured interviews were performed with other experts that were selected within organizations inside of or related to the Port of Gothenburg. These experts did not overlap with those used in the focus group discussion.

This investigation also exploits a multiple case study approach since this methodology is particularly suitable for explorative studies as well as to identify casualties (Eisenhardt, 1989; Yin, 2003). This approach was preferred by the authors since in the context of this investigation there was not a sufficient amount of data to make a statistical analysis. In addition, the research variables could not be controlled by the authors and it was somewhat difficult to establish their relationship to the study context (Yin, 2003; Arbnor and Bjerke, 1997). Therefore the multiple case studies methodology was believed to be the most appropriate, despite being highly complex.

The data in the case studies are gathered by means of non-participant observations, and unstructured and semi-structured interviews. The exploitation of diverse data collection

methodologies may both enrich the level of detail of the investigated system as well as enhance the validity of the findings by data triangulation (Eisenhardt, 1989; Yin, 2003). The data in the three case studies were collected from a convenience sample extracted from diverse security research projects carried out between 2006 and 2009. In addition, for all the three cases, further secondary data as companies' reports, practitioners' journals and legal frameworks have been examined. The data collected had predominantly a qualitative nature, and to enhance the validity and reliability of the findings it was recorded, transcribed and sent to respondents to confirm the content of the text. In addition, notes from interviews and observations were written down and adequately stored in physical databases to allow the authors easy monitoring and access. More specifically, the data collection techniques, used within each of the three case studies, are the following:

1. **CASE A – DSV Warehouse Terminal.** Within this case study the data were collected by means of non-participant observations and unstructured interviews. During the non-participant observations the researchers had full access to documents and processes. They also had the capability to examine trucks, containers and goods transported to evaluate the degree of security. Finally, five unstructured interviews were carried out with managers working at the facility and with responsibilities related to security and logistics operations.

2. **CASE B – Stora Enso Transportation Setup.** Within this case data were collected by means of non-participant observations and unstructured interviews. During the observations, the researcher had access to the Stora Enso manufacturing plant and storage warehouse. Finally, two unstructured interviews with managers working for Stora Enso were performed.

3. **CASE C – Schenker Transportation Setup.** The case data was collected through non-participant observations, a focus group and semi-structured interviews. Notes were taken in occasion of the observations and the focus group discussion, while the interview sessions were voice recorded, transcribed and sent to the respondents for confirmation.

The most important part of the methodology has been the analysis of the qualitative data that required being systematic and well structured to avoid ambiguity due to the myriad of interpretations that could be given to words (Miles and Huberman, 1994). Therefore, to increase the reliability of the analysis process, content analysis and constant comparative analysis have been exploited (*ibid*; Glaser and Strauss, 1967). By means of comparative case studies in which multiple cases are compared it is possible to discover generalization patterns (Eisenhardt, 1989). In addition, multiple researchers joined the data collection and analysis to increase the reliability and validity of the study (Miles and Huberman, 1994).

# ANALYSIS

This section aims to provide background information about the workshop held in March 2007 and the presentation of the cases studied in this paper. Finally, the findings from the empirical data collected are reported.

**Workshop**

The workshop in Gothenburg was mainly focused on the security of the port of Gothenburg. From a transportation viewpoint, the Swedish Port of Gothenburg offers optimal access to both road and rail infrastructure. The road infrastructure, constituted by two motorways and two national highways, allows the connection of the port to the hinterland of the country (North, East and South access). Rail access to the hinterland is also ensured by means of single and double-track railway lines. Finally, the waterway channel, Göta, allows hinterland transportation as well as a further intermodal connection to both road and rail (Port of Gothenburg, 2009a). In 2008, the Port of Gothenburg handled 22.8 million tons of oil, a total of 862,500 TEUs (Twenty-foot Equivalent Unit), 625,300 RoRo units, and 271,500 cars. About 40% of the TEUs were handled on the rail shuttles (Port of Gothenburg, 2009b). The area on which this study will focus consists of the RoRo (Roll-On-Roll-Off) traffic and unitized cargo handled together with the related security restrictions to be introduced by the Port of Gothenburg (specified in the SOLAS chapter XI-2).

**Case A – DSV Goods Warehouse**

DSV is a global transport and logistics provider working with worldwide transport solutions and cross border logistics services. In Sweden, the company is constituted by three main business units: DSV Road, DSV Air and Sea and DSV solutions (DSV, 2009). This investigation will focus on DSV Road and more specifically on the operations driven at one of the Swedish goods terminals owned by DSV. The security operations evaluated will be those specified in the AEO guidelines.

**Case B – Stora Enso Transportation Setup**

Stora Enso is a Swedish global manufacturer of paper products like newsprint, book paper, magazine paper, industrial packaging, wood products, etc. (Stora Enso, 2009). Despite the low value of these products and the scarce attractiveness for thieves, the examination of the security of the Stora Enso's transport chain is still of great interest from a smuggling and/or trafficking viewpoint. More specifically, the case of interest concerns the transport of paper from the production site in Nymölla, one of Stora Enso's larger manufacturing sites, to the Port of Gothenburg where the goods are shipped overseas to the US and Canada (Figure 2). This study will merely focus on the transport operations, excluding the production site in Nymölla, and the receiving port terminal in Gothenburg. The transportation setup is carried out by a road transport carrier contracted by Stora Enso. The security guidelines of interest are those specified in the AEO-S certification.


**Figure 2:** the Stora Enso transportation setup.

**Case C –Schenker Transportation Setup**

The transport case analyzed consists of a shipment from Sweden to Great Britain in which five different actors are involved (

Figure 3): Schenker (a Logistics Service Provider), the "Bäckebols Åkeri," a road carrier executing the transportation from Schenker's terminal to the Port of Gothenburg, the Port of Gothenburg that receives the shipment, stores it and consigns it to the sea carrier, Customs, which is responsible for inspecting the integrity of the semi-trailer, and finally, the DFDS Tor Line Shipping company, taking care of the sea transportation to Great Britain (Nyquist et al., 2008). The case of interest for this investigation will merely focus on the transportation setup within Sweden enacted by Schenker and the Bäckebols road carrier.

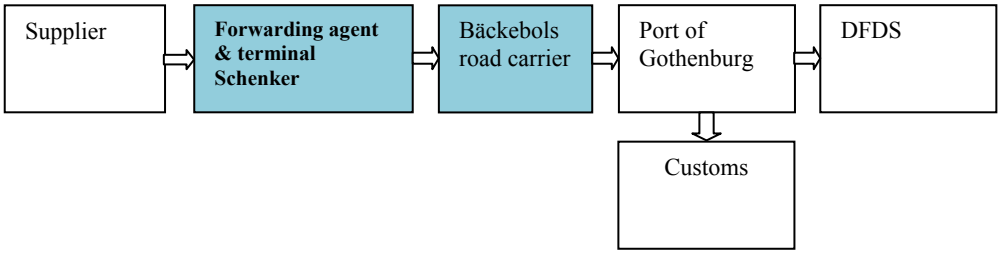


**Figure 3:** the Schenker transportation setup (adapted from Nyquist et al., 2008).

## Findings

Regarding the port of Gothenburg, security measures concern mainly those specified in the ISPS code and SOLAS chapter XI-2. Hence, these include the identification and monitoring of personnel, goods and unit loads passing through the area (IMO, 2009). The main objective of these measures is to detect the smuggling of people, weapons or hazardous substances as well as to prevent unauthorized access to the terminal of potential criminals. The identification of personnel and goods passing through the area is also important for recovery purposes to identify insiders as well as cargo liabilities. According to one of the interviewed respondents:

> "*In the port of Gothenburg it works in this way; you use your personal ID card to enter the terminal area. The oil port is closed for some employees. Those who have access can still move* freely *between the ports."*

According to the analysis of the data collected, the introduction of these procedures has a noticeable negative impact on the costs, transit time, reliability and flexibility of the terminal. Costs will be higher because the organization needs to assign personnel and determine routines to learn security procedures and systems and thereafter control, monitor and inspect personnel and goods passing through the area. In addition, according to the ISPS code the developed security plans need to be assessed by the authority. Therefore, the organization's new costs related to training, auditing and inspection procedures have to be accounted for.

> "*We execute training several times per year under the supervision of the shipping inspection… in addition, auditing and inspection procedures have to be accomplished to ensure our compliance with the security certification.*"

As a consequence, it appears that variable and fixed costs of the organization increase respectively in terms of salaries and technical systems to be purchased, installed and maintained at the terminal.

Transit time also increases since it may be estimated that the identification routines will require more time to enter and exit the protected area of the port. The transport reliability indicator may also be affected if the operator does not consider the time required for the identification routines in the terminal or if the cargo is selected for inspection by the Customs authority. Finally, the flexibility may also be affected from an operational and technical viewpoint. Due to the security constraints it becomes more complicated to make unexpected changes in shipment size or transport assets. Hence, responses to demand volatility may become more cumbersome.

In Case A, where a warehouse terminal is studied, the storage recommendations of AEO-S are considered. Hence, according to these guidelines, goods have to be stored in areas protected from external intrusion. Security measures have to be applied to avoid unauthorized access to the goods (i.e., authorization level for staff categories). In addition, personnel have to be instructed and trained to follow internal control procedures to take proper actions in case irregularities are discovered. The examined warehouse fully follows these recommendations. Security systems installed at the terminal include perimeter fences, access control, alarm systems and a CCTV system for monitoring purposes.

> *"51 cameras monitor all the doorways, but also a part of the main corridor. Alarm goes into four lines that take all* the *doors. Entry is done using a chip card that has been already provided to about 100 trusted drivers. The alternative way to enter the port area is through the intercom."*

Hence, from a security perspective the installed protection measures may support prevention and detection of criminal acts but also recovery operations. The presence of fences as well as of cameras, the alarm and the control systems are a good deterrent to attackers (at least the opportunistic ones). In addition, the CCTV (Closed Circuit TeleVision) system is optimal to monitor and detect security anomalies. Finally, the combined access control and CCTV systems may support recovery operations to identify potential insiders as well as cargo liabilities. As in the previous case, it appears that the security systems have a negative impact on transit times, costs, and flexibility of the transport chain. For the same reasons expounded on in the port case, the access control increases the access time to the terminal. Costs become much higher because the security systems require personnel to be allocated and new technologies to be purchased, installed and maintained. In this case, we don't find any significant impact on the reliability of the transport assignment. On the contrary, we believe that flexibility issues are still to be considered. This becomes more apparent in this case since, due to security requirements, access to different parts of the terminal is restricted to a limited number of operators. As a respondent commented:

> "*Security is going to be successively increased in the future, which means that the average area accessible to* personnel *will be drastically restricted.*"

Hence, this increases the interdependence between the cargo and the terminal operators and, consequently, the degree of flexibility may be negatively compromised. For instance, the absence of key personnel may make it difficult to access cargo and make any changes in labelling or packaging to chance delivery destination or schedule.

Cases B and C concern two transportation setups where trailers and containers are delivered to the Port of Gothenburg. Hence, the security measures of interest for these cases are those issued in the AEO-S guidelines to monitor logistical processes and the integrity of the cargo unit under transportation. First of all, by following the AEO-S specifications, security requirements for the transport carrier have to be specified in the contract agreement stipulated between the owner of the goods (in this case Stora Enso) and the transport operator. This will mostly increase the administrative costs for transportation, since human resources have to be allocated to find certified operators and agree on the security requirements to be put into the contract. Other recommendations that are required by the AEO-S to secure transport assignments concern routines and technical systems to avoid intrusion to the container by unauthorized personnel, as well as procedures to ensure: 1) the inspection of cargo integrity when loading and transporting the goods into the container, 2) the inspection of the container structure, 3) fast recovery in case of an incident, and 4) performed maintenance of containers.

Findings from the case show that, to avoid unauthorized access to the container or to check the integrity of the cargo or of the container, the direct involvement of the truck driver is required. This means that he or she has to learn specific routines to prevent access to the cargo or to inspect the goods' integrity. If specific technologies, like e-seals, mechanical locks, fingerprint or eye scanning, etc. are applied, drivers have to be properly trained to use these systems. While security is certainly enhanced, this will result in new costs for transport companies, both in terms of human resources and technology investments. In addition, limiting access to the cargo may become a constraint in the distribution planning phase. For instance, if a logistics service provider wants to make use of several transport carriers to optimize transportation costs, or to quickly change delivery routes or transport capacity, access to the cargo has to be provided to all of them. Hence, if security is not adequately standardized across all the actors of the distribution chain, and common security practices and technologies are not used, flexibility may be negatively affected. Finally, inspections and maintenance operations may delay transit times and increase costs. Inspections, when cargo is loaded and unloaded as well as when the truck and the container have stopped at a parking place will require additional time. Likewise, maintenance operations will cost the organization in terms of money and time whenever the container is taken out from the distribution network. In addition, subtracting resources from a distribution network for maintenance purposes will imply a reduction of flexibility and reliability in the transport assignment.

# DISCUSSION

Summing up, the purpose of this paper is to discover, by means of a multiple case study, whether security measures may have a negative impact on transport efficiency. The results

of each of the case studies are reported in the table below and show a clear negative implication on the efficiency of transport operations (Table 1).

**Table 1:** effects of security on transport performance indicators ("0" indicates no effect, "+" an increment and "-" a decrement).

| | Quality | Transit Time | Costs | Reliability | Flexibility |
|---|---|---|---|---|---|
| **Workshop** | 0 | + | + | - | - |
| **CASE A** | 0 | + | + | 0 | - |
| **CASE B** | 0 | + | + | - | - |
| **CASE C** | 0 | + | + | - | - |

Hence, this paper highlights the fact that enhancing security within an organization implies an increased workload and costs borne by terminal and transport operators. Implementing security measures concerns introducing routines, practices, or technologies that could go into conflict with the existing assets and operations. Thereafter, the efficiency of an organization may be seriously penalized.

As it is illustrated in Table 1, in all the cases the quality of the transportation appears to be unchanged, and transit times and costs are subjected to an increment, while flexibility is inevitably reduced. Reliability is reduced for both the transportation cases, while storing goods in warehouses where security is enhanced doesn't seem to have any significant effect. An exception is made for the port of Gothenburg where Customs may inspect high-risk containers and thereafter cause transport delays.

The intent of this investigation is not to discredit the usefulness or efficaciousness of security solutions in transportation. Likewise, we don't want to debate the importance of introducing security into logistics and transport companies. On the contrary, we are strongly convinced of the necessity to speed up the process to secure the global transport chain and ensure the security and safety of our communities. However, since this process often negatively affects existing assets and operations in transportation, it is essential to find out how to circumvent such situations and find smart approaches to restore and even improve the efficiency of transport networks.

Previous research has a systematic focus on the beneficial combination of security and efficiency. However, as it is demonstrated in this paper, negative impacts may not be neglected and must be taken into account in any future analysis. Hence, this paper, by means of empirical data, contributes to the scientific community by providing instances in which costs and transit times are increased, and reliability and flexibility of transportation decrease when introducing security measures. From a practical viewpoint this paper offers

practical examples concerning how the application of security contained in certifications like the ISPS code and the AEO may impact existing transport operations.

Hence, future research should be oriented first of all by providing more empirical data to demonstrate the negative impact of security measures on transport efficiency. Moreover, research concerning security investments may take advantage of the findings of this study to develop tailored quantitative models that may accurately compute the impact of security on transport assets and operations.

Finally, the greatest challenge for the research community concerns the integration of security measures into distribution assets and operations. As is shown in Figure 4, according to the findings of this study, the enhancement of security may determine in the first place a loss of efficiency in the transport network.

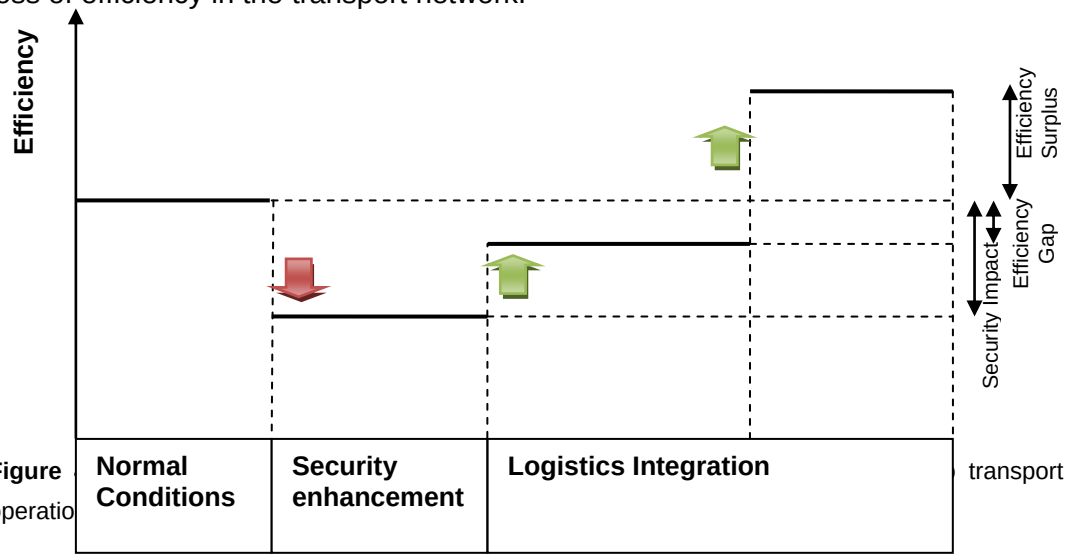


**Figure** transport assets and operatio

However, there may be cases in which the original efficiency, or part of it, may be restored if security is smartly integrated into existing assets and operations of logistics and transport companies (Figure 4).

A clear example is the exploitation of track and trace systems in which security capabilities like time- and geo-fencing may be built upon existing tracing services that have already been proven to increase visibility and thereby improve the efficiency of transportation. Hence, we believe that to accomplish this task, future research as well as future industrial initiatives should focus on the development of security routines and technologies built upon logistical needs of transportation actors. At the same time, standardization of security and collaboration among stakeholders must be enhanced. As has been shown in the cases, if security is not correctly standardized across all the actors of a transport network, flexibility and reliability may be negatively affected. In addition, collaboration among these stakeholders is crucial to ensure the integration of the new systems in the existing ones.

# REFERENCES

Arbnor, I. and Bjerke, B. (1997). Methodology for Creating Business Knowledge, 2nd ed., Sage, Thousand Oaks, CA.

Belzowski, B., Flynn, M., Londal, G., DiBernardo, M., Cole, D.E., Smith, B., Jimenez, T. (2000). Forecast and Analysis of the North American Automotive Industry, Delphi X, For 2004 and 2009.

CBP (2008). C-TPAT: Customs Trade Partnership Against Terrorism, http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/, March 2008.

Closs, D. and McGarrell, E. (2004). "Enhancing Security Throughout the Supply Chain." IBM Centre for the business of government.

Coyle, J.J., Bardi, E.J., and Novack, R.A. (2000). *Transportation*, Fifth Edition, South-Western College Publishing, United States of America.

CP3 Group (2005). Benefits from implementation of the WCO framework of Standards to Secure and Facilitate Global Trade, http://www.cp3group.com/attachments/WCO_benefits.pdf (accessed April 2005).

CP3 Group (2006). AEO Guidelines, http://www.cp3group.com/attachments/AEO%20guidelines.pdf (accessed 2006).

DSV, (2009). DSV Global Transport and Logistics, available at http://www.dsv.com/irj/go/km/docs/documents/DSV_DFDS%20Transport/Integrated%20Internet/External%20Web%20Site%20Repository/SE/SE/Om%20oss/Ekonomi/DSV_eko_fakta2008.pdf (accessed December 2009).

Eisenhardt, K.M. (1989). "Building theory from case study research," The Academy of Management Review, Vol. 14 No. 4, pp. 532-50.

Ekwall, D. (2009). "Managing the Risk for Antagonistic Threats against the Transport network," Division of Logistics and Transportation, Chalmers University of Technology: Göteborg.

EU (2003). "Freight Transport Security," Consultation paper, European Commission, Brussels.

EU Commission (2007). "Authorized Economic Operators – GUIDELINES," TAXUD/2006/1450 (accessed 29 June 2007).

EU Commission (2008). Public Consultation in preparation of a Legal Proposal to combat counterfeit medicines for Human Use - Key Ideas for better Protection of Patients against the risk of Counterfeit Medicines, http://ec.europa.eu/enterprise/pharmaceuticals/pharmacos/docs/doc2008/2008_03/consult_counterfeit_20080307.pdf, Brussels, 11th March 2008.

European Parliament (2004). Regulation (EC) No 725/2004 of the European Parliament and of the council of 31 March 2004, On enhancing ship and port facility security, Official Journal of the European Union, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:129:0006:0091:EN:PDF , 29 April 2004

European Parliament (2005). Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005, On enhancing port security, Official Journal of the European Union, http://eur-

lex.europa.eu/LexUriServ/site/en/oj/2005/l_310/l_31020051125en00280039.pdf , 25 November 2005

European Parliament (2007a). Security - Protection of persons, of assets and the facilities, http://ec.europa.eu/dgs/energy_transport/security/intermodal/, 22 August 2007

European Parliament (2007b). Organised theft of commercial vehicles and their loads in the European Union - Rep. No. 610, Directorate General for Internal Policies of the Union, Brussels: ACEA, June 2007.

Glaser, B.G., and Strauss, A.L. (1967). *The Discovery of Grounded Theory: strategies for qualitative research*, Aldine Transaction, New York.

Gunasekaran, A., Patel, C. and McGaughey, R.E. (2004). "A framework for supply chain performance measurement," International Journal of Production Economics, Vol. 87 No. 3, pp. 333-47.

Haughton, M.A. (2007). "Examining the business case for shipper participation in Canada-USA trade security programmes," *International Journal of Logistics Research and Applications*, 10 (4), 315-331.

Hesse, M. and Rodrigue, J-P. (2004). "The Transport Geography of Logistics and Freight Distribution," Journal of Transport Geography, No3, Vol. 12, pp. 171-184.

IMO, (2009). International Maritime Organization – Safe, Secure and Efficient Shipping on clean oceans, available at http://www.imo.org/, accessed May 2009.

Lambert, D. and Stock, J. (1993). Strategic logistics management, Richard D Irwin Inc, US.

Lee, H.L. and Whang, S. (2005). Higher Supply Chain Security with lower cost: lessons from Total Quality Management, *International Journal of Production Economics*, Vol. 96, N °3, pp. 289-300

Lumsden, K., (2006). *Logistikens Grunder*, 2nd Ed., Studentlitteratur, Poland.

Mazeradi, A. and Ekwall, D. (2009). "Impacts of the ISPS code on port activities – A case study on Swedish ports." *World Review of Intermodal Transportation Research*, *Vol. 2, No. 4,* pp. 326-342.

McKinnon, A., Forster, M. (2000). European Logistical and Supply Chain Trends 1999-2005: The Results of a Delphi Survey.

Miles, M.B., and Huberman, A.M. (1994). *Qualitative Data Analysis*, Second Edition, Sage Publications, London.

Nonaka and Takeuchi (1995). Knowledge Creating Company: How Japanese Companies Create the Dynamics of Innovation, Oxford University Press, New York, NY.

Nyquist, C., Sternberg, H., Nilsson, A., Lumsden, K. (2008). "Combining improved security and efficiency through using information in trailer ports," Chalmers, Gothenburg.

Peleg-Gillai, Barchi, Bhat, Gauri, and Sept, Lesley (2006). Innovators in Supply Chain Security - Better Security Drives Business Value, *Stanford University - The Manufacturing Institute*, The Manufacturing Innovation Series.

Port of Gothenburg, (2009a). Port of Göteborg AB (Gothenburg) – Göteborgs Hamn AB, available at http://viewer.zmags.com/publication/69ea5a62 (accessed December 2009).

Port of Gothenburg (2009b). Annual Report, available at http://viewer.zmags.com/publication/69ea5a62 (accessed December 2009).

Powanga, Luka (2006). A business perspective of US International Seaborne Security Measures: Impact on Importers, *Journal of Global Business.*

Purtell, D. and Rice, J. B. (2006). "Assessing cargo supply risk," *Security management*, November, 2006, pp.78-87, ASIS international.

Rice, J.B.Jr. and Spayd, P.W. (2005). "Investing in Supply Chain Security: Collateral Benefits," IBM Center for Business of Government.

Rolandsson, B. and Ekwall, D. (2008). "Frames of Thefts at Work – Security Culture and the Organisation of responsibility in Transport Networks." *Security Journal advance online publication*, November 17, 2008; doi:10.1057/sj.2008.4.

Ross, D. F. (1996). *Distribution Planning and Control*, Boston, MA, Kluwer Academic Publishers.

SETIF (2007). Secure and Efficient Transportation and Information flows in large ports, pre-study report, Doc. No. 2007:001.

Sheffi, Y. (2001). Supply Chain Management under the Threat of International Terrorism, *The international Journal of Logistics Management*, Vol. 12, N°2, pp. 1-11.

Stevenson, D.B. (2005). "The impact of ISPS code on seafarers," *International Conference Security of Ships, Ports and Coasts*, Halifax/Nova Scotia/Canada.

Stewart, (1995). Supply Chain performance benchmarking study reveals keys to supply chain excellence, Logistics Information Management, Vol. 8, No. 2, pp. 38-44.

Stora Enso, (2009), Stora Enso, available at http://www.storaenso.com/ (accessed December 2009)

Sweet, K. (2006). *Transportation and Cargo security*, Pearson Prentice Hall, New Jersey.

Urciuoli, L. (2009). Supply Chain Security – mitigation measures and a logistics multi-layered framework, *International Journal of Transportation Security*, DOI 10.1007/s12198-009-0034-3.

Willys, H.H. and Ortiz, D.S. (2004). "Evaluating the Security of the Global Containerized Supply Chain," RAND Corporation, Santa Monica, CA.

Yin, R.K. (2003). Case Study Research, Design and Methods, 3rd ed., Sage, Thousand Oaks, CA.