Number 2, Volume VII, July 2012

# CURRENT SUPPLY CHAIN SECURITY TECHNOLOGIES IN CONTEXT

Martina Lánská[1], Tomáš Horák[2]

*Summary: The main aim of this paper is to summarize current most important technologies dealing with Supply Chain Security (SCS). In 2009, The World Bank issued useful Supply Chain Security Guide describing worldwide SCS projects and SCS technologies. We focused on SCS technology part of the Guide and prepared comprehensive overview of the SCS technologies that we found to be used in current EU and US SCS-related projects. The projects were selected based on our first-hand experience from January 2012 workshop on SCS organized by EU and held in Brussels. The last chapter of this paper focuses on different approaches of EU and US to SCS research.*

*Key words: supply chain, security, logistics.*

## INTRODUCTION

This paper is focused on current Supply Chain Security related technologies. In the first and second chapters it gives summary of the technologies that were (a) published in Supply Chain Security Guide by The World Bank in 2009 and were (b) identified as technologies used in the current Supply Chain Security related projects, i.e. projects, that are (a) funded by the 7th Framework Programme of the European Union (EU) and those that were (b) presented on the latest workshop on  Supply Chain Security held in January 2012 in Brussels.

The third and the last chapter offers brief insight into the way the Supply Chain Security projects are handled in the United States (US) through summary of one of the workshop presentations made by the US Department of Homeland Security (DHS) representative followed by a short comparison with EU funded SCS projects.

We would hereby like to underline the fact that the information in chapters one and two was extracted from the Supply Chain Security Guide published by The World Bank in 2009 making it the primary source (1) for those chapters. Further useful information on SCS agenda through the prism of The World Bank can be found on its dedicated website[3].

## 1. SUPPLY CHAIN SECURITY TECHNOLOGIES

[1] Ing. Martina Lánská, Ph.D., Czech Technical University in Prague, Faculty of Transportation Sciences, Department of Logistic and Transportation Processes, Horská 3, 12803 Praha 2, Tel.: +420-22435-9160, E-mail: lanska@fd.cvut.cz

[2] Ing. Tomáš Horák, Czech Technical University in Prague, Faculty of Transportation Sciences, Department of Logistic and Transportation Processes, Horská 3, 12803 Praha 2, Tel.: +420-22435-9169, E-mail: xhorak@fd.cvut.cz

[3] The World Bank. Supply Chain Security Guide: Introduction. Available at: <http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTTRANSPORT/0,,contentMDK:22312099~menuPK:337122~pagePK:148956~piPK:216618~theSitePK:337116~isCURL:Y~isCURL:Y,00.html>

The supply chain requires the use of technologies. This chapter will review emerging and existing technologies; container integrity (CI), track/trace efforts, Advanced Inspection (AIT). Due to space constraints, information and communications technology (ICTs), and technologies used to actualize data models, and two other collaborative tools, Electronic Single Windows (ESW) and Port Community systems (PCS) used in the supply chains. They are here only mentioned, they are not core to SCS.

## 1.1 Emerging trends in technology

Most consider the container to be the main focus of security. Approximately 85% of loss within the supply chain occurs during hinterland transport. As world trade volumes continue to multiply and borders become more open, criminal and terrorist networks have become more organized and sophisticated.

One avenue explored to combat the increased technology use in the modus operandi of criminal elements; so-called “smart containers” have been developed. Today’s “smart containers” include a navigation and routing guidance system, satellite location, interior sensors, and radio frequency identification to secure the box from origin to destination.
“Smart containers” sensors can detect anomalies such as:

- Door opening or removal.
- Cutting of holes in the roof, sides or floor.
- People or animals inside, e.g. by using passive infrared sensors.
- Dangerous chemical, biological or radiological material, e.g. by using CBRNE (chemical, biological, radiological, nuclear) sensors.
- Location, e.g. using GPS or Galileo– for track and/or trace applications.

The sensors would be connected to some form of central data logger. Sensor data from the logger could either be read at a port or border crossing point equipped with a compatible seal reader, or is sent by a long range communication system, e.g. satellite or GSM, to a monitoring point.

## 1.2 Biometrics

Biometrics is also being introduced to the supply chain. Driver identification and verification is an essential function at cargo pickup points, intermediate delivery terminals, and even at destinations. Biometrics can improve the effectiveness of the function, reducing the risks of theft and terrorism while facilitating gate and reception processes, especially for drivers who make frequent pick-ups and drop-offs at the terminal. Biometric identification tools, such as fingerprint and iris recognition, may be incorporated in smart identification (ID) cards and integrated with on-line access to manifest, vehicle, and driver databases. Looking ahead, the Transportation Security Administration (TSA) Transportation Worker Identity Card (TWIC) aims to deploy a common biometric smart ID card for all US transportation workers.

## 2. EXISTING TECHNOLOGIES

The following sections will provide a brief overview on the different types of technology used in SCS and how they are applied:

- SCS Technologies for Container Integrity: Container security devices and seals
- SCS Technologies for Container Integrity: Track/Trace or Positioning technologies
- Advanced Inspection Technologies (AIT)

### 2.1 SCS Technologies for Container Integrity: Container security devices and seals

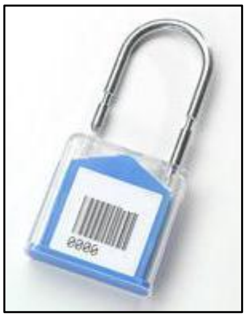
Container Security Devices (CSD) play a crucial role in ensuring the integrity of the container along the supply chain and facilitating trade and Customs processes. Cargo security can be enhanced through the use of both mechanical and electronic seals. Both mechanical cargo seals and e-Seals act as barriers against pilferage, smuggling, and sabotage of cargo within containers and trailers en route to their destination. If either type of seal is found to be broken or if its identification (ID) number is different from the one on the cargo document, this is an indication that the container or trailer door might have been opened by an unauthorized person at some point in the transportation route. The unique ID numbers on both mechanical and e-seals provide tracking information. It is expected that the ID number on either type of seal will be recorded at each handoff in the chain of custody to provide information about when and where the container or trailer was handed over and the seal status at that time.

Ideally, seals should only be placed on containers by the party directly responsible for stuffing and/or visually verifying the contents of the container. In this respect, it should be stressed that the party responsible for stuffing and sealing the container is the first, and most important, link in a “secure” container transport chain. One must however remember that even high-security mechanical seals are only as good as the procedures in place to affix, monitor and document them at each transfer of responsibility.

#### *2.1.1 Mechanical Seals*

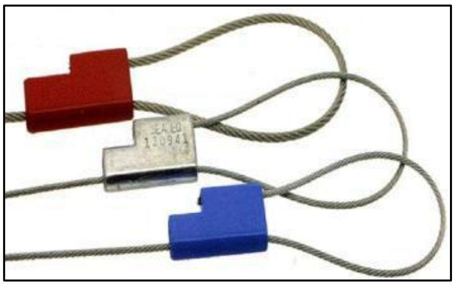
A mechanical seal is a device marked with a unique identifier and is often marked by the seal owner’s or issuer’s stamp and/or color. It is externally affixed to the container doors and designed to evidence tampering or intrusion through the doors of a container and to secure closed doors of a container. In addition, depending on its construction, the seal provides varying degrees of resistance to an intentional or unintentional attempt to open it or to enter the freight container through the container doors. Even if a tampered seal were to be replaced with a similar unit after entry, the seal’s unique identification number might not match with the one that was recorded when the original seal was affixed. The sealing process for security seals is as important if not more important than the seal itself.

There are six types of high security seals used in SCS:padlock seals, cable seal, bolt seal, barrier seals, security seals, indicative seals.



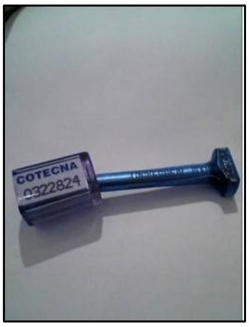
Source: (1)

Fig. 1 – Padlock seal



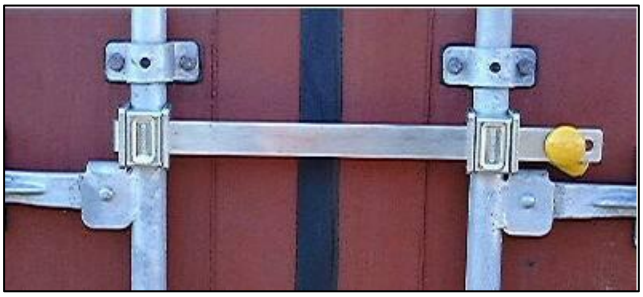
Source: (1)

Fig. 2 – Cable seal



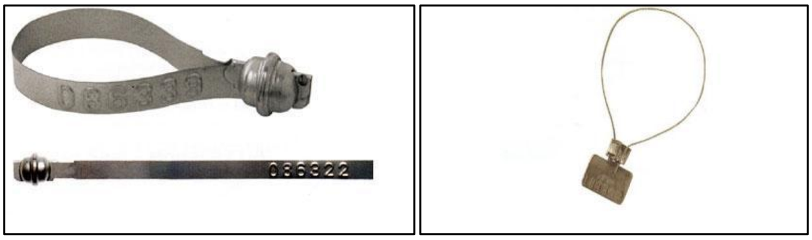
Source: (1)

Fig. 3 – Bolt seal



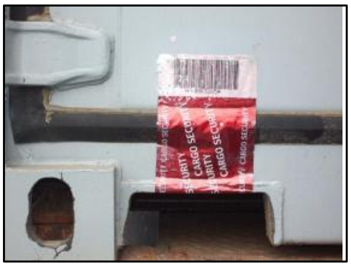
Source: (1)

Fig. 4 – Barrier seal



Source: (1)

Fig. 5 – Security seal



Source: (1)

Fig. 6 – Indicative seal

### *2.1.2 Electronic Seals*

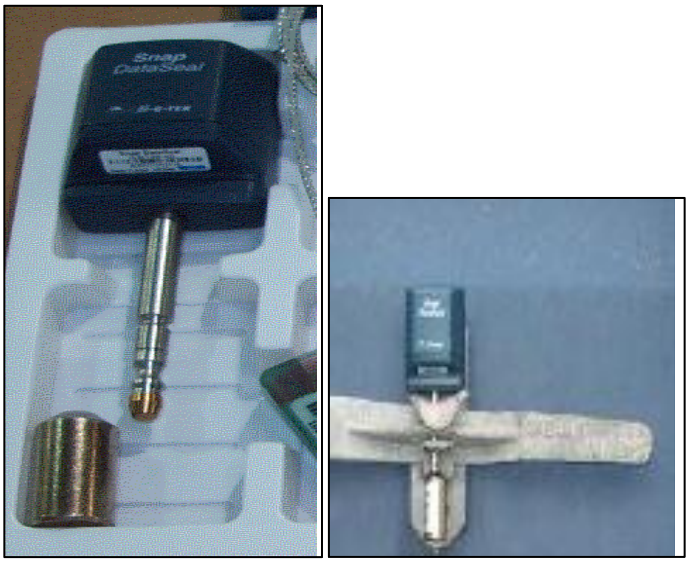
The need to further secure containers containing high value goods has led to the development of several types of so-called “smart” seals. These types of seals have integrated physical security and information management capabilities. It is the latter functionality that sets these aside from their mechanical counterparts since they can transmit data regarding their status as well as the information regarding the contents of the container. At a minimum, an electronic seal system combines a physical sealing device with a data chip capable of recording and restituting basic information regarding the container contents, such as an electronic cargo manifest, and a mechanism for reading the information recorded on the chip. A higher level of functionality is added by systems capable of electronically communicating whether the seal has been broken or otherwise tampered with. These seals use radio frequency (RF), infra-red (IR) or fiber optics to transmit data. In their most advanced iterations, electronic seals can be coupled with a variety of sensors (e.g., radioactive, radiological, chemical, biological, light, $CO_2$, etc.) that can record and communicate data regarding the in-container environment. In combination with a global positioning system (GPS) transceiver, alerts or status messages regarding the container can be transmitted in real time to a central processing system that can pinpoint the container's location.

E-seals only monitor the seal's status and that of any sensors connected to the seal – they do not monitor the condition inside the container. This nuance is important. A container's integrity can be compromised without compromising the integrity of the seal. Even when sensors are attached, the seal records sensor events which may or may not reflect what is actually happening within the container environment. "False-positive" readings from sensors are a particular concern but one should not overlook the possibility that sensors can be defeated by more or less sophisticated means.

E-seals cannot provide detailed information on the contents of a container. What they do provide is information regarding what the party responsible for sealing the container said was in the container. If that party was an originating shipper, one might assume that the information is more or less correct. However, if that party is once or twice removed from the originating shipper like in the case of a carrier placing an e-seal on a container that arrived at the terminal with a non-conforming mechanical seal, then the shipping documents loaded into the seal's memory only reflect the e-seal-affixing party's best available information as to the contents of the container. In a worst case scenario, a conforming e-seal on a container containing illegitimate cargo might actually facilitate the transport of that cargo, rather than prevent it. Non-declaration or mis-declaration of goods is not an unknown phenomenon in international transport, and the catastrophic outcomes of certain incidents such as mislabeled calcium hypochlorite or fireworks-containing containers, highlights both the reality and the risk of such situations.

For e-seals to be an effective part of a global container security strategy, they must be accompanied by a host of reading devices/scanners, computer hardware and a suite of underlying information management software systems capable of properly processing the seal data. Today, these requirements are far from being met, and their fulfilment throughout the container transport chain is not at all assured in the near future. It is likely that major terminal operators will be the first to place e-seal readers at strategic locations within their container terminals and to use such systems to monitor and track the status of such seals. Some of the major maritime carriers might start to deploy e-seal readers as well. However, it is not at all sure that smaller ports will be able to deploy and effectively manage such systems in the medium term. Furthermore, while it is feasible that major railroads and barge operators might also be able to deploy the underlying infrastructure and hardware necessary to support e-seals, it is highly unlikely that small road carriers and smaller barge/rail operators will be in a position to do so any time soon – if ever. What is likely to emerge is uneven support for e-seals across the container transport chain with certain high security nodes capable of processing e-seal data punctuated by areas of low or no e-seal functionality. Properly identifying the boundaries of these zones and developing appropriate container transfer protocols among these zones are necessary components of a comprehensive container security plan.

There are four types of e-seals, classified by the four different communication systems used between the seal and its "reader:" Radio frequency identification (RFID). Infrared (IR), Direct contact and Mobile GSM or satellite.



Source: (1)

Fig. 7 – The RFID bolt seal

## 2.2 SCS Technologies for Container Integrity: Track/Trace or Positioning technologies

It seems evident that if authorities are concerned about the potential misuse of containers by criminals or terrorists, they should have the ability to track containers throughout the transport chain. This is not only important so that containers identified as risky can be found and inspected, but also so that containers that have gone missing like in the case of a hijacked container, can be identified and possibly found.

There are two ways containers can be tracked. The first involves recording the passage of containers through "choke points" in the container transport chain and managing the location data via database systems. The second involves utilizing a transponder or satellite-based system to deliver real-time data on the location of the container, cargo, or transport.

### *2.2.1 GPS*

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

### *2.2.2 GALILEO*

Galileo is a global navigation satellite system currently being built by the EU and European Space Agency (ESA). The €3.4 billion project is an alternative and complementary to the US 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[4].

### *2.2.3 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' GPS and the planned Galileo positioning system of the EU. Development on the GLONASS began in 1976, with a goal of global coverage by 1991.

Beginning on October 12, 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. In 2001, Russia committed to restoring the system, and in recent years, with the Indian government as a partner, has diversified, and accelerated the program with a goal of restoring global coverage by 2009.

### *2.2.4 COMPASS / Beidou-2*

The Compass system (also known as Beidou-2) is a Chinese project 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 includes five geostationary orbit (GEO) satellites and 30 Medium Earth Orbit (MEO) satellites that will offer complete coverage of the globe.

## 2.3 Advanced Inspection Technologies (AIT)

Before inspection technologies can be further discussed, a baseline definition must be established for the three types of inspections that are commonly used when discussing the container and its contents:

1. Screening: described as the targeting and risk management process. Customs should screen information on 100 % of import containers. Each and every container identified as high risk is subsequently scanned and, if needed, physically inspected.
2. Cargo scanning or non-intrusive inspection (NII) is a method of inspecting and identifying goods in transportation systems without a time intensive unloading process. It is often used for scanning of intermodal freight containers. NII and the physical inspection of a container’s contents are conducted in order to provide Customs officials with the ability to verify the accuracy of information provided by shippers on a container’s contents and the effectiveness of container integrity measures. Scanning is important because it can help identify dangerous cargo when the originating shipper, or the party responsible for stuffing and sealing the container, appears to be legitimate but has actually been infiltrated

[4] According to GALILEO Project Factsheet, the Full Operational Capability of GALIELO should be reached in 2020. The Factsheet is available for download as PDF from European Space Agency website: <http://download.esa.int/docs/Galileo_IOV_Launch/Galileo_factsheet_20120321.pdf>

by a criminal group. In these cases, other layers of security may provide a false sense of security because the shipments appear to be outwardly “legitimate” when in fact it is illegal.

Generally, two types of scanning variants can be distinguished:

- Active scanning: A system making container images based on X-rays or Gamma ray beams.
- Nuclear detection: A passive system detecting nuclear and other radioactive materials based on their radiation levels.

3. Physical Inspection: Based on the results from screening and/or scanning the container is opened and unstuffed for a visual verification of contents. This generates extra-costs and delays.

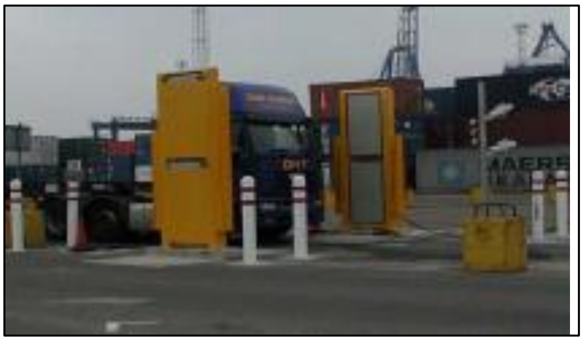
Screening, scanning, and physical inspection of containers, while complementary, are not the same. 100% container screening is possible, should an administration choose to do so – 100% scanning and inspections, on the other hand, are not viable due to the backlog at Customs in ports, nor is it economically feasible for all countries. Screening can be improved with additional sensor-based or information-based inputs. Additional data, whether from the container, i.e. tamper indication, from the facility infrastructure, i.e. radiation detection portals, or from information systems, additional shipment detail, could be used to improve the screening/targeting processes.

### *2.3.1 Nuclear detection*

In September 2006, an amendment was proposed for the US SAFE port act in which Nuclear Detection will become mandatory for US-bound containerized cargo. Many of the largest ports in Europe, Asia and the US are in the process of installing radiation detection portals. Almost all these programs take place under responsibility of Customs.

However, adding to the predicament of the decision-makers, recent tests of the new generation of radiation detection portals, the Advanced Spectroscopic Portal (ASP), developed under the aegis of the US Government, have cast doubts on its ability to detect radioactive material significantly better than the existing generation. On the other hand, the estimated lifecycle cost for one of the new generation ASP exceeds US$ 800,000 or almost the triple of the cost of existing radiation scanners.

While the continuous research and development of NII technologies are needed to detect hazardous cargo without interrupting the flow of goods, one technology cannot detect everything. Thus, the combination of technologies and attentive human operators is necessary. In order to justify the eventual installation of scanning devices, it can be noted that multiple benefits and objectives might result from a good scanning system. Improving scanning ability could serve not only to detect Nuclear or other WMD weapons (weapons of mass destruction) but also to reduce smuggling, to improve tax collection and to earn the trade community’s trust to attract more trade.



Source: (1)

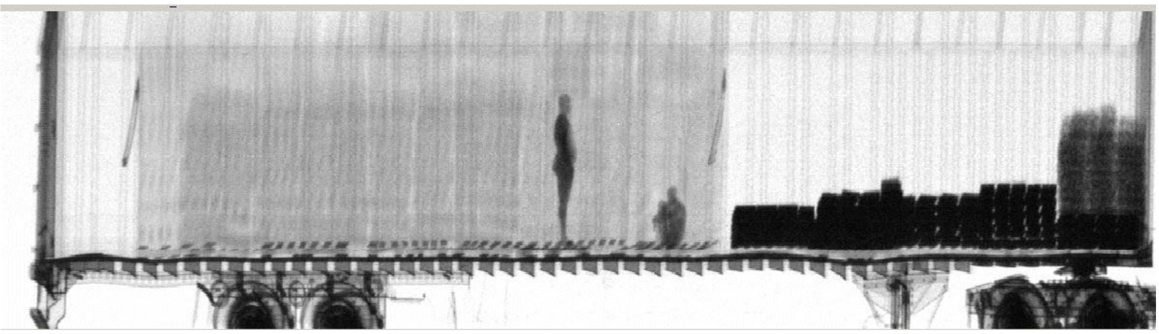
Fig. 8 – Radiation Portal Monitors installed at Port of Felixstowe (UK)

### *2.3.2 X-ray and Gamma – ray radiography*

Advanced Inspection Technologies (AIT) first gained prominence for manifest verification, allowing countries to better enforce import tariffs. Authorities also found that the image quality achieved with X-ray scanning allowed them to interdict contraband, including drugs, cash, weapons, and other illicit materials. X-ray radiography 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. During the last few years, attention has shifted to security concerns, where X-ray screening is expected to become a major tool in prohibiting the smuggling of weapons of mass destruction. X-ray inspection systems for cargo containers have now become a more familiar feature in numerous ports. This rapid adoption has been accelerated by the needs of port security, but made practical by the systems' unique ability to penetrate entire containers and generate images of the contents in just a few seconds. Even at this large scale, the resulting images are comparable to those obtained through traditional baggage scanning at airports and capable of identifying objects smaller than a baseball.

The inspection layer also allows for Customs administrations of both the originating and importing ports to conduct inspections on the same container and can require the container to pass through different types and increasing levels of inspections. The following highlights the built-in layers of a scanning operation.

Gamma-ray radiography is an alternative to X-ray but uses a radio-active source for the radiation.



Source: (1)

Fig. 9 – Gamma-ray image of a truck with two stowaways in a container of Styrofoam trays entering US from Canada at Buffalo, N.Y. image taken using 1, 25 MeV photons

As X-ray cargo scanning becomes more common at ports and border crossings, its impact on container traffic is frequently discussed. This is essentially a question of system throughput, which varies by the type of X-ray system chosen and how it is operated within a port facility. X-ray cargo screening has been adopted at ports and border crossings throughout the world because this technology has solved a number of important problems.

Customs continues to increase the rate of discrepancies that capture revenue that would have otherwise been lost to importer error or deception. From a security stand point one can imagine what some of these discrepancies revealed.

The human side of the scanning process should also be examined so that the inspectors are well trained to interpret the x-ray images and other indicators. Experts argue that better training of Customs staff on analyzing scanned images, the digital revolution and related efficiency gains, diffusion of innovation, as well as growth and specialization in the scanning manufacturing sector will enhance security and efficiency.

### *2.3.3 The dual role of scanning*

Scanning can serve two clearly distinct purposes:

- Assist in detecting and counter illegal material movements by organized crime, be it contrabandist or terrorist in nature.
- Assist Customs to protect and enhance tax collection against fraud and mis-declaration by the trade or their representatives.

The two functions sometimes overlap, often through the use of the same technology, facilities and/or operating personnel. Having one scanner in one port to inspect imports to protect or enhance tax revenue should not normally be considered as fully addressing supply chain security per se. In fact, improved monitoring of possible smuggling of weapons, explosives and similar, an important objective of SCS, is actually a collateral benefit of tax-related scanning.

### *2.3.4 Fast scanning*

One of the clear future directions of scanning is “fast scanning”. Fast Scanning implies that the shipment container could be scanned while in motion at a reduced speed in the port. It is in a way similar to the automated prepaid highway toll principle. This type of scanning is already undergoing investigation by a number of major ports due to their concern in addressing the US 100% scanning requirement.

There are some limitations however to fast scanning. First, as the cargo is in movement and as conveyance vehicle operators are often involved, the scanning beams have to be of relatively low power and penetration. With this type of lower penetration scan, the images do not provide the same capability to discern the container contents to the full level of detail. Second, due to this less detailed image, secondary inspections will be required on a more frequent basis in order to address this weakness.

Fast scanning is in the early stages of development – early systems include road and rail portals that are either planned for testing or currently undergoing testing by ports that are “early adopters” of technology who want to ensure their competitiveness in the current and future supply chain security environment.

In general fast scanning consists of three integrated technology elements, more specifically:

- Identification of the goods/container (RFID, optical character recognition of the container number or other similar technologies).
- X-ray scanning of the container.
- Radioactive threat detection.

## 3. US AND EU PERSPECTIVE

In the United States, government projects related to SCS are administered by the Department of Homeland Security. Further, within DHS, Science & Technology Directorate and its Borders & Maritime Security Division deals with research and deployment of new SCS technologies (2). In European Union, SCS projects run within the 7th Framework Programme (7FP) and follow the common EU model of project funding, i.e. projects are prepared by international consortia and apply for funding through irregular calls (3).

On January 31, 2012, workshop “Towards an R&D Demonstration Programme on Logistic and Supply Chain Security“ organized by the EU Directorate of Enterprise and Industry was held in Brussels. The aim of the workshop was to identify roadmap and priorities of the new, upcoming, FP7 European R&D demonstration programme (large scale research project) on “Logistic and Supply Chain Security“ (4).

Besides this principal goal, current SCS related projects were presented as well. Most of these projects were those prepared by consortia composed of mostly EU-based public institutions and, in less extent, private companies. The most prominent overseas guest present at the workshop was Mr David Taylor, DHS State Chief Information Officer and Executive Director, Agency for Enterprise Information Technology, Florida. Along with him, in total six representatives of EU SCS-related projects presented ongoing or recently finished projects funded within 7FP. Most of the EU projects presentations, besides recently successfully concluded project INTEGRITY (Intermodal Global Door-to-door Container Supply Chain Visibility) (5), failed to attract our full attention due to their inability to show concrete outputs. This was in striking contrast with the presentation of DHS research projects conducted by Mr Taylor. Of course, the problem could be more presentation-conduct oriented than project-content related, however, we fear that the latter is more probable. We have decided to let the reader see the differences for himself. Below, we present summary of Mr Taylor’s presentation and further below links to presentations and websites of currently running or recently concluded EU projects funded within 7FP.

### 3.1 DHS presentation on current SCS research

At first, Mr Taylor presented the core of the new US National Strategy for Global Supply Chain Security, that was adopted on January 25, 2012. This Strategy says that international trade is the engine of the global economic growth including the US and that this trade is made possible by the very existence of global supply chains. This, in turn, means that the supply chain is the key element of working economy and therefore also security of any country, including the US. Smooth operation of the global supply chains is vital. Given these facts, the Strategy has two main goals (6) (7):

**Goal 1: Promote the Efficient and Secure Movement of Goods**

- Resolve threats early to expedite the flow of legitimate commerce. By integrating security processes into supply chain operations, we can identify items of concern and seek to resolve them as early in the process as possible.
- Improve verification and detection capabilities to identify those goods that are not what they are represented to be, are contaminated, are not declared, or are prohibited; and to prevent cargo from being compromised or misdirected as it moves through the system.
- Enhance security of infrastructure and conveyances in order to protect the supply chain and critical nodes, through limiting access to cargo, infrastructure, conveyances, and information to those with legitimate and relevant roles and responsibilities.
- Maximize the flow of legitimate trade by modernizing supply chain infrastructure and processes to meet future market opportunities; developing new mechanisms to facilitate low risk cargo; simplifying our trade compliance processes; and refining incentives to encourage enhanced stakeholder collaboration.

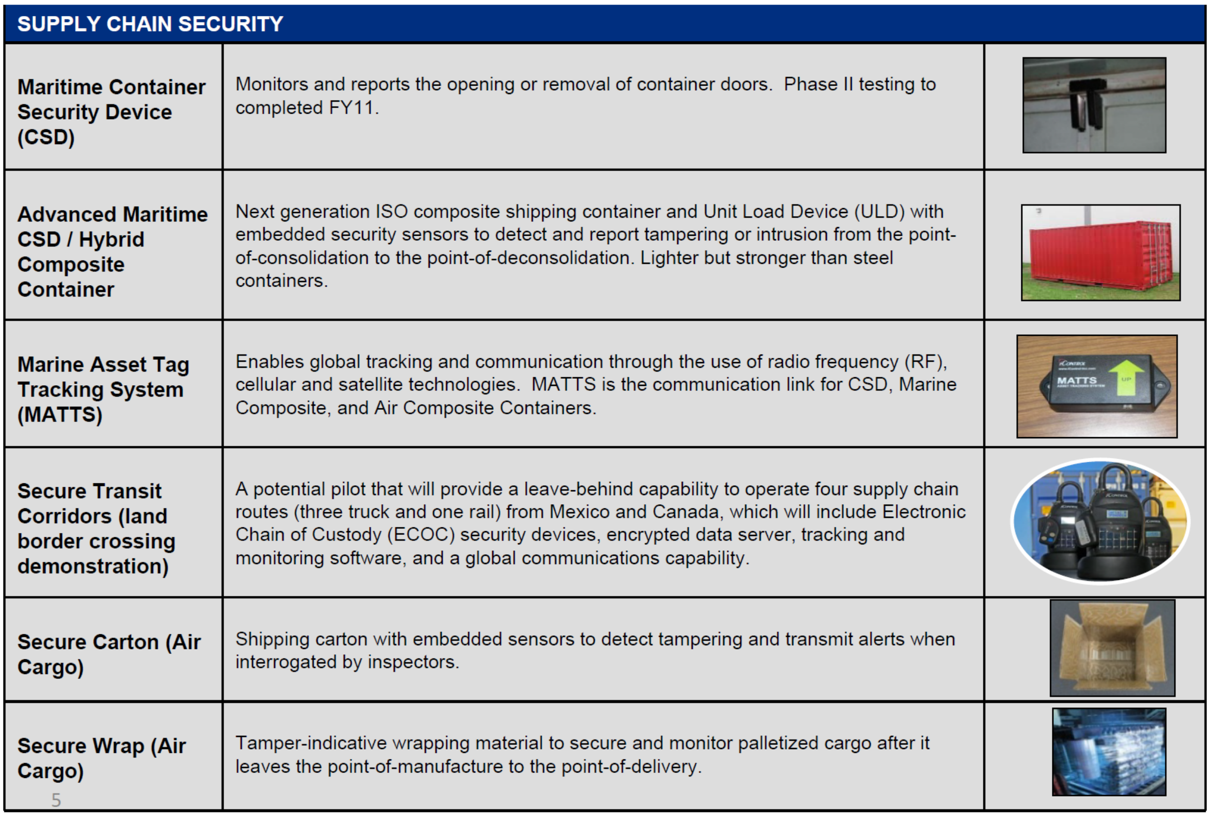
**Goal 2: Foster a Resilient Supply Chain**

- Mitigate systemic vulnerability to a supply chain disruption prior to a potential event by using risk management principles to identify and protect key assets, infrastructure, and support systems; and promoting the implementation of sustainable operational processes and appropriate redundancy for those assets.
- Promote trade resumption policies and practices that will provide for a coordinated restoration of the movement of goods following a potential disruption by developing and implementing national and global guidelines, standards, policies, and programs.

In connection with the workshop this US strategy has an important dimension of international cooperation, which especially needs the following to be successful (7):

- research of new technologies, their implementation and assessment of their usability,
- tailored solutions in cooperation with manufacturers and government institutions,
- review of current and upcoming procedures and standards.

The next part of the presentation dealt with six concrete DHS SCS-related projects (such concrete attitude was not shown by any of the EU SCS-related project representatives):



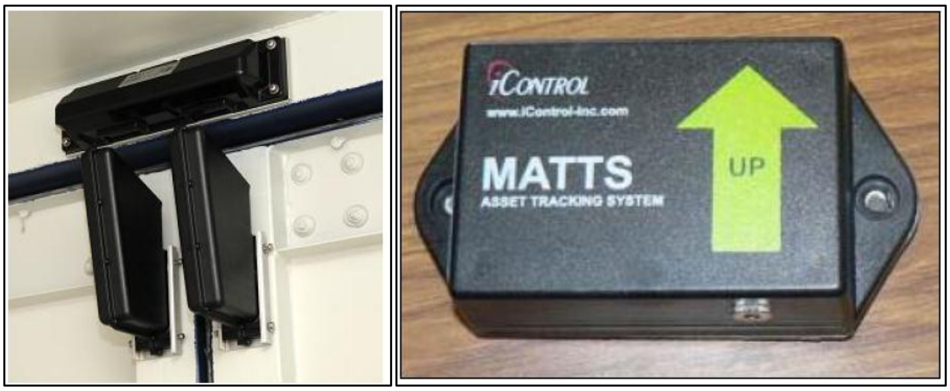
| SUPPLY CHAIN SECURITY | | |
|---|---|---|
| **Maritime Container Security Device (CSD)** | Monitors and reports the opening or removal of container doors. Phase II testing to completed FY11. | |
| **Advanced Maritime CSD / Hybrid Composite Container** | Next generation ISO composite shipping container and Unit Load Device (ULD) with embedded security sensors to detect and report tampering or intrusion from the point-of-consolidation to the point-of-deconsolidation. Lighter but stronger than steel containers. | |
| **Marine Asset Tag Tracking System (MATTS)** | Enables global tracking and communication through the use of radio frequency (RF), cellular and satellite technologies. MATTS is the communication link for CSD, Marine Composite, and Air Composite Containers. | |
| **Secure Transit Corridors (land border crossing demonstration)** | A potential pilot that will provide a leave-behind capability to operate four supply chain routes (three truck and one rail) from Mexico and Canada, which will include Electronic Chain of Custody (ECOC) security devices, encrypted data server, tracking and monitoring software, and a global communications capability. | |
| **Secure Carton (Air Cargo)** | Shipping carton with embedded sensors to detect tampering and transmit alerts when interrogated by inspectors. | |
| **Secure Wrap (Air Cargo)** | Tamper-indicative wrapping material to secure and monitor palletized cargo after it leaves the point-of-manufacture to the point-of-delivery. | |

5

Source: (7)

Fig. 10 – DHS SCS - related projects

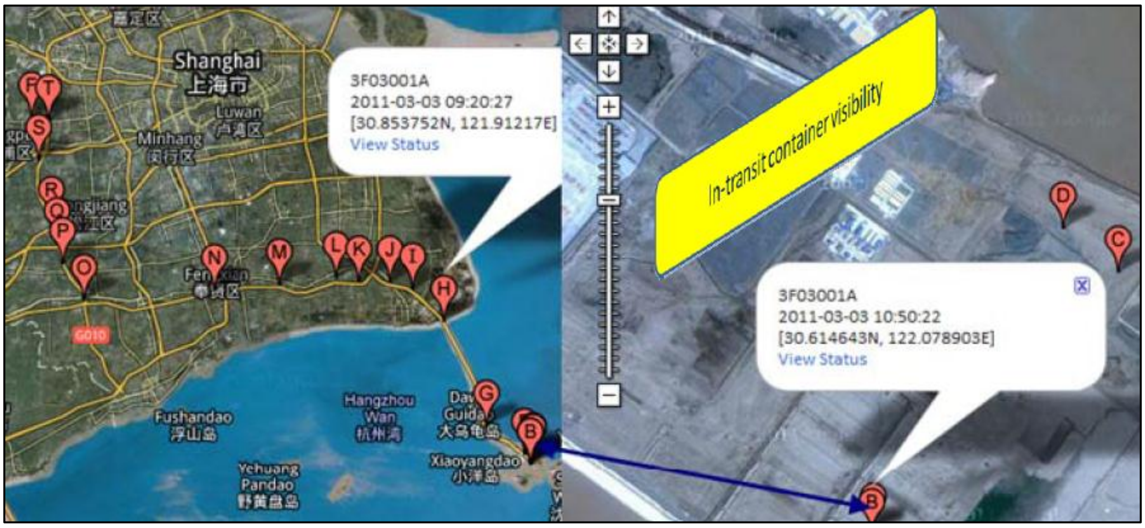
Three of these projects, Container Security Device (CSD), Marine Asset Tag Tracking System (MATTS) and Hybrid/Composite Container were introduced in detail. CSD is currently able to detect opening or removal of container doors and transmit information through secured channel using MATTS to e.g. DHS or to the container owner.



Source: (7)

Fig. 11 – CSD and MATTS devices in detail

Set of these devices was already successfully tested on the Shanghai, China – Savannah, GA, USA route. The tracing & tracking outputs can be seen in Fig. 12.



3F03001A
2011-03-03 09:20:27
[30.853752N, 121.91217E]
View Status

3F03001A
2011-03-03 10:50:22
[30.614643N, 122.078903E]
View Status

Source: (7)

Fig. 12 – Tracing & tracking test on Shanghai – Savannah route

Further tests are expected in cooperation with U.S. Department of State a U.S. Customs and Border Protection. Current research focuses on the following areas (7):

- detection of intrusion through any of container's six sides,
- detection of container door removal and human inside,
- standard interface protocol for future sensor integration (explosives, radiation, nuclear, chemical, biological, etc.),
- sensor monitoring & notification through event logging and alarming,
- reliable and secure communications.

Both CSD and MATTS devices have already been tested together with composite containers. Unlike its steel counterpart, composite container is not subject to random or intentional penetration deformation defects that could damage the detectors placed inside. Composite container is also15% lighter than the steel one, however, it is (for now) more expensive.

In the end of his presentation, Mr Taylor urged international research and start of common US-EU research projects or at least signing of mutual agreements on exchange of information in the field of SCS research. He proposed to include manufacturers and customs in the research in order to find tailored solutions for everyone to keep up with the new technologies and lower costs of SCS measures, which is connected to introduction of global standards.

## 3.2 Links to EU SCS-related projects

To meet conditions for scope of this paper, we are not describing EU SCS-related projects. We are just including links to current or recently concluded EU SCS-related FP7 projects that were presented on the workshop:

- INTEGRITY (Intermodal Global Door-to-door Container Supply Chain Visibility) www.integrity-supplychain.eu

- SMART-CM (SMART Container Chain Management)
  www.smart-cm.eu
- CASSANDRA (Common Assessment and Analysis of Risk in Global Supply Chains)
  www.cassandra-project.eu
- CONTAIN (Container Security Advanced Information Networking)
  www.containproject.eu
- E-FREIGHT (European e-Freight capabilities for Co-modal transport)
  www.efreightproject.eu
- CONTRAFFIC (Container Traffic Monitoring System)
  contraffic.jrc.ec.europa.eu

We do not want to say that all EU projects but INTEGRITY are inherently valueless. We do not have background nor willingness to say that. What we would like to express is merely a wish that European projects embrace more practical way of thinking as is probably the case of (probably not all) US projects. We think that such attitude could boost usability of the project outputs (in some cases it could even help to generate some outputs) and increase willingness to involve in international cooperation that is vital for solving SCS-related issues since these issues have, due to the global nature of supply chains, truly global impact.

## CONCLUSION

In this paper we summarized the most important current Supply Chain Security related technologies that we extracted from more than one-hundred page long Supply Chain Security Guide released in 2009 by The World Bank. The decision whether or not to include the technology in our summary was made on the basis of our first-hand account of proceedings of the workshop “Towards an R&D Demonstration Programme on Logistic and Supply Chain Security” from January 2012 and US “National Strategy for Global Supply Chain Security” published also in January 2012. In the last chapter we introduced the main points of one of the workshop presentations on Supply Chain Security agenda made by the US Department of Homeland Security representative to show example of how useful and refreshing (we do not say flawless) the practical approach to the matter could be in contrast with some rather impractical EU projects dealing with Supply Chain Security research.

The research was supported by Research Plan “Development of Methods for Optimization in Transport System Operations” – MSM 6840770043.

## REFERENCES

(1) DONNER, M., KRUK, C. *Supply Chain Security Guide* [online]. Washington: Transport Division Energy, Transport and Water Department. The World Bank, 2009 [viewed May 28, 2012]. Available as PDF:
<http://siteresources.worldbank.org/INTTRANSPORT/Resources/336291-

1239112757744/5997693-1252703593834/6433604-1256564181444/guide_full_version.pdf>.

(2) *DHS | Science & Technology Directorate Borders & Maritime Security Division* [online]. Last modified on Apr 3, 2012 [viewed May 28, 2012]. Available at: <http://www.dhs.gov/xabout/structure/gc_1224536495175.shtm>.

(3) Seventh Framework Programme (FP7) [online]. Last modified on May 25, 2012 [viewed May 28, 2012]. Available at: <http://cordis.europa.eu/fp7/home_en.html>.

(4) Towards an R&D Demonstration Programme on Logistic and Supply Chain Security [online]. Last modified on Feb 7, 2012 [viewed May 28, 2012]. Available at: <http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=5659&lang=en>.

(5) *INTEGRITY. Intermodal Global Door-to-door Container Supply Chain Visibility* [online]. Last modified 2011 [viewed May 28, 2012]. Available at: <http://www.integrity-supplychain.eu/>.

(6) *National Strategy for Global Supply Chain Security* [online]. Washington: The White House, Jan 23, 2012 [viewed May 28, 2012]. Available as PDF: <http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf>.

(7) TAYLOR, D. *DHS Science & Technology Directorate Presentation to: European Commission Workshop on: "Toward an R&D Demonstration Program for Logistic and Supply Chain Security".* [presentation]. Brussels: DG Enterprise and Industry, Workshop "Toward an R&D Demonstration Program for Logistic and Supply Chain Security", January 31, 2012. Available as PDF: <http://ec.europa.eu/enterprise/newsroom/cf/_getdocument.cfm?doc_id=7215>.