

Major problems applying wireless security devices in supply chains

Marcus Engler, Institute of Shipping Economics and Logistics, engler@isl.org

Abstract

Different technologies developed recently may help to secure international intermodal supply chains at a technical level. The devices to be used are Electronic Seals, Smart Devices or Smart Containers (commonly named wireless security devices throughout this document). The installation of new devices will probably not be the only change at the transport business to enhance today's security needs

Reading devices for RFID-based technology have to be acquired, installed and activated by well trained specialists. Some kind of data forwarding and data management system has to be operated day and night to keep track and verify information contained. And finally existing procedures will have to be adapted or even revised. When introducing wireless security devices the existing supply chain has to be taken into account. But each of these has its own characteristics which have to be taken into account.

At each supply chain the very same security device should be used from the first place of supply to the final destination. Numerous legitimate checks during the transport are involved. The device mounted at the origin is not to be removed for any reason. The device used should be handled as easy as today used High Security Bolt Seals.

These rather simple requests may generate subsequent technical, operational, legal and procedural problems.

Some of these problems are to be discussed in this paper based mainly on electronic seals.

Superior Systems using Smart Devices and Containers are momentarily under development but without any international standardization. These Systems are part of the discussion in this paper as well.

Keywords

Supply Chain Security; Container Security; RFID; eSeal; Smart Containers

1. Introduction

Today the discussion about securing complete international containerized Transport Chains against theft

and terrorism is widespread and diverse.

One of the solutions discussed is using one pre-registered RFID-Seal which is almost equal to today's High Security Bolt Seal.

This eSeal is able to monitor and report its own status and identification number via radio communication as described by ISO/TC104 SC4^[1]. Numerous companies and organizations worldwide are concerned with manufacturing (and applying) eSeals^[2] and Smart Units^[3] creating as many solutions as organizations are involved. Few companies combine their effort^[4] while others rather keep their developments and results in private offering (joint) services.^[5] This is not unexpected since many results of the research done is directly concerned with the processes of companies offering transportation.^[6]

Own experiences have shown that a close look at processes from the point of an innocent bystander may unveil more leaks of security than a company admits. Sometimes these leaks are known to the company management and some kind of risk management can be developed to realize counter-measures to terrorism.^[23]

Usually actions are taken after some bad incident happened^[7], this may be too late next time, maybe some further disastrous event is already planned. Taking actions after some incident happened can be observed at the attacks from 9/11 or the intended attacks with bombs made of liquids recently: At 9/11 the terrorists may have used knives and box cutters to hijack airplanes. These weapons were not suspected by officials and customs for that kind of use.^[8] At another potential attack liquids appearing harmlessly should have been used as explosives inside an airplane.^[9] After these incidents cutter knives and liquids and gels exceeding 100ml per container were prohibited to bring on board an airplane.^[24] This is checked today very carefully.

With a few more serious concerns and thoughts about such themes and having potential criminals and terrorists in mind might have led to some appropriate regulations beforehand. To moan about these and many other past events would not help pushing thoughts about security regulations. These should be invented before such disastrous events where many innocent individuals are heavily endangered or would be killed. We must concentrate on upcoming tasks

and themes in order to be able to avoid corresponding future scenarios.^[13]

The international supply chain has up to now not been subject for a terrorists attack to cause the deaths of many people or to create immense chaos. Opinions mentioned in private say this would never be the case since there were none so far and for 9/11 cutter knives and chemicals used for the UK-Scenario legally bought at local stores. Even the terrorists entered the US lawfully and passed experienced immigration officers (just one potential terrorist was refused).^[8]

On the other hand this example shows clearly that the thoughts of terrorists to obtain their wicked targets are always unpredictable and attacks are always well planned, prepared, accomplished and even funded. There must be some tense global organisation behind it.^[10] These thoughts lead us to the fact that all existing supply chains have to be made more secure to avoid such unpredictable events.^[11] Securing could be done using additional technical devices^{[2],[6]} and standardised processes.^[12] But apart from technical and operational problems discussed later on there is one thing to be stated here: A great concern is the enhancing of security regulations until the transport of goods between countries just stops. This is not the intention of the authorities of major im- or exporting countries which partly rely on the free movements of goods.^[14]

Such and many more different topics and concerns have to be taken into account when trying to have a reasonable security system invented at local, regional, national, trans-national and global intermodal supply chains. A global system may contain more than one single type of security device. The system has to be well balanced between needs of users, requirements of authorities, reasonable cost for customers and practicable regulations for each participant at the global transport chain.

With the application of mentioned automatic devices further security equipment might be invented.

These systems may range from Self-Controlled Damage Recording^[15] up to tags for containers (according to ISO10374^[17]) and each means of transportation.^[16] Automated Damage Recording uses advanced photographic and data storage devices. Such systems offer a long-term reliable proof of the state of the hull of each container at a defined place and time. Such a system can be used together with an eSeal-System to bring together the number of the seal and the container number. A further invention might be the Container Tag which sends all data which is painted on the hull of the container via radio. Trucks, Trailers and Railway waggons can be tagged similar to gain a complete set of data when a container enters a terminal. Data of these systems can be checked against each other for security reasons.

The eSeal System

One of the feasible (and today the most standardized) systems is the application of electronic seals (eSeals).

These devices are able to report their own status and unique serial number wirelessly and without direct (eye) contact to another device (called antenna) within the specific communication range^{[1],[18]}.

Thus eSeals are capable to help securing each international intermodal supply chain at a rather low technical level.

The installation of additional devices at various places and means of transportation for sending and receiving information of the rolling stock will probably not be the only change at the transport business to enhance the transport chain security:

(1) Long-term existing and well-rehearsed processes and procedures of many companies might have to be adapted and refined in order to use the new technology with a benefit.

(2) Devices apart from the eSeals and antennas have to be acquired and installed by professionals. These installations are power and data communication lines as well as computers to process data.

(3) Software programs to integrate 'new' data into existing systems and maybe one or more kinds of data management system giving registered operators and authorities access to the data obtained have to be operated. Such integrations have to be well conceived.^[25]

The Application of electronic Seals^[19]

Generally the use of electronic seals is no secret and can be operated similar to the High-Security-Bolt-Seals used today: At the place of loading each container should be sealed by an examined, registered and reliable person immediately after loading with no break between loading and sealing. The eSeal is then to be initialized if necessary and announced to the data management-system. This is to be done immediately in order to create an authentic data record to ensure full integrity. Then the container is sent from the place of loading to its destination. During this voyage many authorized checks can be performed in order to ensure full integrity of the eSeal. The data obtained from the eSeal is to be checked against the initially stored record of the data management system in time. Furthermore each query of a system to check the stored eSeal data is to be recorded as well. This is to be done in order to keep track of all activities along the transport chain. Checks should be performed at least at each change of liability thus supporting today's container handling processes. Additional checks can be done after transports breaks when no change of liability occurs. But this claim needs appropriate places where checks can be performed which have to be build and operated. Just before the container is being opened legally by a stripping company or the receiver of the goods a message should be sent to the data management which indicates the end of the journey. This final action would help to signal a clear ending of the physical transporting process to the data management. Maybe this message could be used to free the container from being used. Otherwise a new voyage for this special container cannot be initialized.

The complete data recorded of a single voyage for a single container could be used later to retrace the whole voyage. The data recorded should contain complete eSeal data^[1], the place and the time a check was performed and who conducted it. Maybe some further information about totally automated systems could be attached.

Smart Units and Smart Containers

A system as just described might not fulfill the needs of all companies using the transport business.

When transporting goods of high value, goods which are easily to sell on a black market or via the internet, art treasures or certain types of dangerous goods (ex. nuclear fuels) more information might be of interest.

An eSeal is able to report a container was tampered between the last and the actual inspection. With proper eSeal data sets recorded checking-sites and times can be obtained. The exact transportation route including breaks is known to the driver only.

The information available might not be enough to recover lost goods or for sending out warnings where unsecure places are located to avoid future attacks.

This concern led to the development of smart devices and smart containers.

Both systems have their main features^[20] in common with a few differences^[21] and options for further development.^[22]

Mainly three different business models are discussed and partly realised today.:

(1) The first business model is characterised by the ownership of smart devices: monitoring devices are owned by the company which is willing to let goods being transported with surveillance.^[5]

These companies buy the devices to be attached and hire the service to control incoming messages.

The owner of the device has to make sure the equipment is at the right time at the loading place in sound condition (ex. batteries are loaded) and loading personnel is instructed how to install and activate the devices firmly.

The service provider has to be instructed about the do's and don't's of each (batch of) container transport.

If a security event occurs the service provider alerts the appropriate authorities in charge and/or private security companies according to the type of security alert.

(2) The second business model contains the feature the devices are owned by the company which offers transport capacity.

The challenges which formerly the customer had to face are now transferred to a company which probably has already contacts to terminals and packing centers to have well trained people at the right place at hand. The problem having the equipment at the right place is still there but a large company probably owns more devices which makes repositioning easier.

Transports may be offered with grading of security features: either without any security attributes at all (ex. when transporting used car tyres), just using global tracking and tracing in time or utilising the most advanced monitoring devices (ex. forwarding the stages of maturity of bananas) in order to be able to redirect routes transport according to the content if needed. Maybe companies specialise on certain types of transports.

(3) The last business model to use Smart Units is to equip each container worldwide with a system resulting in having smart containers for each transport. Existing containers are to be upgraded by appropriated devices. Containers build in the future devices have to be integrated. This approach would transfer asset cost to the owners of containers^[26] – which may deny globally since prices for new containers would rise by a significant amount^[27].

The advantage of a build-in system is clear – there is always a device at hand which could be used everywhere. There is no special appointment to be made, transports are not delayed by missing or inoperable security devices, personnel is trained everywhere in the world, spare parts are at hand globally.

But the disadvantages are clear as well: apart from additional asset cost just a few transports conducted do need such advanced monitoring. This depends on the value of the transported goods. If the monitoring is not mandatory by global law customers are not willing to pay extra service when surveillance is not needed.

Another threat are these parts in the world where containers stay long-term and bind asset cost for the owners and lessors. Sometimes empty redelivery or repositioning shows a container contains rubbish, is heavily damaged or is just unusable. This may also lead to missing security devices of high technology which have to be replaced in order to maintain the security chain.

2. Major issues from various points of view

2.1 'Realtime' Checks

During the voyage of a standard container equipped with an electronic Seal, checks for integrity at least at each change of liability should be made to proof full integrity of the seal at these handling areas.^[19] The usual container check at terminals today is a quick and standardised procedure^[28] which takes usually about a minute.

The advantage of this rather traditional process is the human being on the site: all information is at hand, the decision – taking over a container or not – is made within seconds. The checker may take other factors into account which are hardly to seize technically. These may be a possibly sudden uptightness of the driver or an unknown smell out of the container.

When introducing a complete security check using electronical devices no extra time should be con-

sumed between stopping and starting the truck in order to keep the existing constant flow of containers through the gate. Furthermore the management of the checking company expects to save time in order to have more trucks inspected at the same time than before inventing electronic devices. This is a technical challenge to the whole checking system. The database which contains the data to be checked against might be somewhere in the world and answering millions of enquiries each second.^[29]

This leads to the invention of distributed databases^[31] containing data of different transports^[32]. The amount of data to be stored and checked against as well as the number of enquiries is smaller. Additionally the distance between the physical checking site and the site where data is stored is smaller. This could make the whole invention of eSeals more feasible and reliable.

2.2 Complete Pre-Planning and Announcing

In order to secure the supply chain each transport could be planned thoroughly and reported with all data needed to each checking station in advance. This makes the inspection of data at the same site as the security check with stipulated reporting on checks performed. This procedure has an advantage: Security Data is transmitted in advance. This speeds up the check enormously and minimizes delays. Another advantage might be that containers which are not allowed on a certain terminal may not enter it. This could be due to a mistake (data was not forwarded in time) or some security alert. But a large restriction on this scenario is the inflexible transportation route where changes are not allowed.

2.3 Legal Inspections by Authorities

Legal checks from authorities in charge^[33] are to be integrated into the system – meaning changing the eSeal with no obstacles at downstream security checks.

When talking about having one and the same seal from origin to destination^[19] in order to have a togetherness of an eSeal and a container for a certain voyage, intrusive checks of the cargo are excluded. This is not the own notion of authorities in charge when asking for their opinion. They always intend to be legally entitled to check each container they choose internal physically^[33].

When using centralized data collection as described before the whole affair is far more complicated. Equipping surveillance authorities with a few bolt seals and some printed documents to sign is feasible and done today.

But changing this equipment to eSeals and some kind of Handheld Computers to initialize new datasets sounds impossible since each car needs such equipment. Cost for purchase and maintenance as well as training courses have to be taken into account.

On the other hand, inspection of each container by authorities before doors are closed is also unthink-

able. X-raying each container inside terminals is not feasible with today's equipment^[34].

2.4 Data Spoofing

Network data security according to Spoofing^[35] is another challenge of the system: Does data received in fact originate from the original device or is some other device just pretending to be the original one? When using many identical wireless devices globally the interfaces have to be published. The contents have to be made known to manufacturers which are to create the devices. This may be another security leak when thousands of people are involved in such research, development and construction activities. This enables potential criminals to obtain the information needed.

Another possibility is just to buy or steal these data sending and receiving devices and read them out in order to create a new device which pretends to be the original one.

2.5 Tampering of Data Readers

Security Checks should be done everywhere with handheld computers or fixed installations. At this stage another security problem might arise: If there are fixed installations how to make sure these objects are not tampered or removed or made inoperable by force?

Making these devices inoperable can easily be done with crashing a car into the installations superstructure, stealing the devices, using blockers of frequencies^[36] or just cutting down power or data lines.

Most times the company tampered will not stop operating – the risk of being abandoned by shipping lines is always present. In most cases the fall-back-solution (meaning today's processes) could be used. This means eSeals are checked manually by reading and noting down the information.

This idea of using old-fashioned processes at a supermodern container terminal is shocking and opens many possibilities for criminals to do their craft. This could result in hiding weapons, drugs, contraband or even persons inside a container after breaking the eSeal. Then doors are closed and a replacement seal is mounted. This has exactly the same number printed on or engraved as the original eSeal. Through checking the number of the seal visually and comparing with data delivered the seal is confirmed and the container seems to be in sound condition.

2.6 Differences in prices and incomes in different countries

When thinking of a global system of securing and monitoring devices known differences at incomes in countries and continents have to be thought of.

At a western country the cost for a handheld computer or a device for fixed installations is just a part of the monthly income of a worker at a terminal. At the Third World the cost for devices may be 10 times of the monthly wage of a worker. The threat such a de-

vice is suddenly being 'lost' and can later be found at the possession of criminals or terrorists seems to be larger at countries with low wages.

On the other hand countries having very low cost of labour facing high-volume investments for high-technology automatic devices sounds being absurd.^[37] Humans are more easy to handle by supervisors and inventing new processes and expensive state-of-the-art technology is always a reason to reject. When taking into account 75% of all container handling is performed in China^[38] where no terrorist attack is reported rejections are anticipated^[39]. Convincing decision makers that the new system is needed and used worldwide is not a dream job.

2.7 Automatic Data Forwarding

When talking to surface hauliers about these systems the possibility of enhanced surveillance creates resistance.^[40] These companies have mostly the notion of being monitored, not just the cargo. In addition trade unions might object even if laws do prohibit specifically combining such data^[41]. And it is to clarify which law is to be used at cross-border transports.

Even the question 'Who should receive an alert?' has to be settled before inventing automated systems. Each participant of a transport has the notion he is to be informed first^[42]. The owner of data is to be clarified in advance otherwise a security alert might be sent automatically from a Postpanmax Container Vessel heading the USA without the captains knowledge.

2.8 Cost is paid finally by end-customer

The actual cost for installing and operating a system to monitor and save voyage data at each plant and (multiple) centralized data management systems is unpredictable momentarily. If companies are forced to do so (either by law or requirements from their customers) then the installation is absolute necessary.

This probably will rise the prices of companies involved for their direct customers and users of the facilities^[45] and finally cost are transferred to the end-customers of goods which will stop complaining after a while^[46].

Transport companies probably fear the cut of employment as seen at the invention of the German Road Toll^{[43][44]}. At the ISPS-system and the German Road Toll the cost were constantly passed on the next customer and the end user pays the cost.

2.9 Impacts on Insurances

Another question when talking to hauliers about these systems is often at hand. Who has the real benefits? This implies mostly how much money is saved when using (or allowing to use) these advanced technologies.

One idea is the reduction of transport insurance fees which sounds feasible since potential criminals and terrorists always fear aggravating circumstances to keep their business to their own. These new electronic

systems might help to fight criminalism at least through narrowing down the place and the time where and when an incident happened. This information helps authorities in charge.

2.10 Spot-Checks against continuous monitoring

The system for container security using eSeals as described above (The eSeal System, Page 2) is able to check the integrity of the containers using the system at certain spots only. On the track between these spots no additional security is applied^[47].

A superior system would enable continuous monitoring with Smart Units and a sophisticated evaluation software. Such systems are available, companies offer either a complete service or just devices and a monitoring service.^{[3][5]} But this surveillance system is still at high cost, not widely being used and there are no standards neither from worldwide operating standardisation organizations nor from the companies themselves^[48] in sight. This lack of standards makes the different systems inoperable^[19] which has to be avoided by the eSeal system.

The approach of using different competing systems globally does not operate according to the needs of transport offers. These companies acquire transports from many customers which may use different types and brands of supply chain security maybe with different preferences. These companies which offer transport capacity are not able or willing to have to observe ten or twenty different monitors to follow each transport monitored by a different system.^[19]

This leads to the perception that all of the different monitoring systems will have to be made interoperable with each other or to have one system which is able to receive all information needed for the transports observed and display with one monitor. Small, regional operating enterprises are not able to start such a demand but global operating companies should get into the discussion about these systems. Maybe the Industry-driven initiatives could help.^[49]

3. Conclusions

An easy way to invent a global container security system is the usage of eSeals. A similar system using mechanical bolt seals is already used today. This would have the least changes at the operating level.

Changes would be integrating readers for eSeals into the transport chain and adopting handling processes at each terminal. The standard seals used today are to be replaced by the newly invented eSeals. Communication lines, an appropriate global data management and response on enquiries is to be established. If this type of securing global supply chains is the system to be used further challenges have to be conquered.

Existing superior security systems also still suffer from queasy and/or unsolved problems and fewer standards.

Some countries would like to implement these wireless security devices rather today than tomorrow and

complain about the international standardisation organisations for marking time than publishing norms.

But the technical standardisation of frequencies, ranges and communication protocols is just one part which is to be harmonized. The other part is the answer to many unsolved questions of which a few are stated above.

A global common understanding of supply chain security is needed. But even a unified Europe is unable to keep up their own ideas regarding transport security^[50] creating complications than getting each nation into one boat^[51].

The current situation might bear a threat: One country takes matters into own hands and enacts a regulation to use wireless security devices at each imported, exported and transshipped container. Then each other country has to comply with these regulation or the trade between these two countries is abandoned. With this step forward a virtual standard is set and might be used globally.

A further barrier to invent these systems is the uncertainty regarding cost and return on investment. Each company will not suffer from the invention of further systems but with the prospect of rising revenues each CEO would start using wireless security systems rather today than tomorrow.

Thus the current situation of companies, governments and organizations – wait and see – helps terrorists to step ahead, while the supply chain is still endangered.

References

Important Note:

All brands named (designated or not) inside this document are the property of their respective owners.

All lists are not exhaustive.

Not all implementations for electronic devices named use the ISO-Specifications.

^[1]ISO (2003) “Freight Containers - Radio-frequency communication protocol for electronic seal”: ISO TC104 SC4: 104sc4wg2n0143_18185r9.pdf
http://209.85.129.104/search?q=cache:xb_F9W-RDVcJ:www.autoid.org/metatraffic2/track.asp%3Fmt r%3D/1_2003%2520Documents/Sep/104sc4wg2n0143_18185r9.doc+ISO/IEC+18185+tamper+flag&hl=de &ct=clnk&cd=1&gl=de

^[2]Examples of companies developing eSeals and offering solutions:
Hi-G-Tek, USA, Member of OSC (Operation Safe

Commerce by US Government)

<http://www.higtek.com/>

SAVI Technologies, US DoD Supplier

<http://www.savi.com/>

^[3]Examples of companies developing Smart Devices.

Bulldog Technologies Inc. USA

<http://www.bulldog-tech.com/>

IBM: Tamper Resistant Embedded Controller

[http://www-](http://www-03.ibm.com/industries/travel/doc/content/solution/1761688106.html)

[03.ibm.com/industries/travel/doc/content/solution/1761688106.html](http://www-03.ibm.com/industries/travel/doc/content/solution/1761688106.html)

^[4]Examples of companies combining efforts

CommerceGuard AB, jointly owned by GE Security, Mitsubishi Corporation, Samsung Corporation, and Siemens Building Technologies

<http://www.commerceguard.com/pages/about.php>

^[5] Examples of companies offering solutions of wireless security devices: The Container Security Box (CSB®) offered by

Rainer Koch Kommunikations GmbH, Germany

<http://www.koch-kommunikation.de/csb>

Robert Bosch GmbH, Germany

http://www.bosch.de/start/media/news_0506_2_Date nblatt_CSB_de.pdf

ZOCA Container Security BV, The Netherlands

<http://www.zoca.nl/product.html>

^[6] Examples of companies using solutions of wireless security devices:

Claire Swedberg (2005) “Mitsui Completes Successful E-Seal Trial” RFID Journal LLC.
<http://www.rfidjournal.com/article/articleview/1846/1/>

News from IBM (2005) Maersk cooperates with IBM
<http://www.ibm.com/news/de/de/2005/10/041.html>

Michael Korn (2006) “Containern weltweit auf der Spur“

http://rfid-imblick.de/index.php?option=com_content&task=view &id=432&Itemid=141 (german)

Powers International, Inc. USA (2006) “Trial of a Revolutionary Container Security System with Satellite Monitoring”

<http://www.powersintlinc.com/BremenPressReleaseNov13-2006.pdf>

^[7] Examples of actions taken after incidents happened or plots were discovered:

answerd.com (2003) “Homeland Security, United States Department of” DHS established after 9/11

<http://www.answers.com/topic/homeland-security>

tsa.gov (2007) “3-1-1 Gains International Acceptance” New global regulations on liquids and gels after the liquid explosive bomb plot in the UK August 2006.

http://www.tsa.gov/press/happenings/311_intl_acceptance.shtm

[8] National Commission on Terrorist Attacks Upon the United States (2004) “We have some Planes”: Box-cutter knives may have been used to hijack airplanes, immigration officers refused just on terrorist (from about 20) to enter the United States.

http://www.9-11commission.gov/report/911Report_Ch1.htm

Wikipedia, the free encyclopedia “Airport security repercussions due to the September 11, 2001 attacks”

http://en.wikipedia.org/wiki/Airport_security_repercussions_due_to_the_September_11%2C_2001_attacks

[9] Wikipedia, the free encyclopedia “2006 transatlantic aircraft plot”: Plot for liquids appearing harmlessly used for bombing airplane

http://en.wikipedia.org/wiki/2006_transatlantic_aircraft_plot

[10] Roth, Greenburg, Wille “National Commission on Terrorist Attacks Upon the United States” Organisational structures behind terrorists of 9/11

http://www.9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf

[11] Andrew Grant (2007) “Transformational Diplomacy to Protect the Maritime Supply Chain”

<http://www.state.gov/t/isn/rls/rm/79524.htm>

[12] Examples for adding security through standardised processes/procedures

International Maritime Organisation (2002) “IMO adopts comprehensive maritime security measures”

http://www.imo.org/Newsroom/mainframe.asp?topic_id=583&doc_id=2689#xi2

US Customs and Border Protection (2006) “C-TPAT Security Guidelines for U.S. Marine or Port Terminal Operators”

http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/security_guideline/guideline_port.xml

[13] US Department of Defense (1996) “Dealing With Terrorism Before, Not After an Attack”

<http://www.defenselink.mil/news/newsarticle.aspx?id=40688>

[14] Concerns against additional security regulations disrupting or stopping the free flow of goods

urocommerce (2006) “Enhancing supply chain security: European business associations suggest reconsidering the proposal”

<http://www.eurocommerce.be/content.aspx?PageId=40703>

The US Whitehouse (2005) “The National Strategy for Maritime Security”

www.whitehouse.gov/homeland/4844-nsms.pdf

[15] Virage/ Autonomy, Inc., USA (2007) “Container Surveillance and Management (CSM)” Automated Damage Recording, OCR etc.

<http://www.virage.com/content/securityandsurveillance/products/csm/index.en.html>

[16] Container and equipment (ex. wagon, trailer) Tag Manufacturers

Intermec Technologies Cooperation, USA (2007) “915 MHz Container Tag”

http://www.intermec.com/products/rfid1_915container/index.aspx

Identec Solutions, Inc., USA “Transportation and Logistics”

<http://www.identecsolutions.com/transportationlogistics.html>

[17] ISO (1991) “ISO 10374 (1991): Freight Containers, Automatic Identification”

<http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=18435&ICS1=55&ICS2=180&ICS3=10>

[18] Wikipedia, the free encyclopedia “Radio-frequency identification”: RFID Communication Range

http://en.wikipedia.org/wiki/Radio-frequency_identification

[19] OHB technologies, HEC, ISL: (2006) “COSI: Bremen pilot project on container security” A Field Test using wireless Security Devices

<http://www.isl.org/news/meldung/04032602/index.shtml.en>

[20] Main Features of Smart Devices and Smart Containers: position sensing via GPS, data communication via GPRS or satellite link, sensors to monitor the containers integrity (not mandatory), regular reports on position via communication link, immediate report when device/container is tampered.

[21] Differences between Smart Devices and Smart Containers: the smart devices may be attached to existing standard containers or may be sent with project cargo whereas a smart container already contains

the whole security system inside which is firmly installed

[22] The main challenge for Smart Devices and Smart Containers is the energy supply. The lowest continuous operation time today is at least 30 days and ranges up to 8 years (according to published specifications, depending on operational mode).

In the authors opinion the average lifecycle of active devices attached to a container should be at least 30 months since inspections by skilled employees in order of the owner are mandatory each 30 month according to

International Maritime Organisation (1972) "International Convention for Safe Containers (CSC)" (http://www.imo.org/Conventions/contents.asp?doc_id=673&topic_id=257).

[23] ECMT (European Conference of Ministers of Transport) and OECD (Organisation for Economic Co-Operation and Development) (2005) "Container Security Across Modes", ISBN: 92-821-0331-5

[24] Canadian Air Transport Security Authority (2007) "Restrictions on Liquids, Gels and Aerosols": Restriction on transporting liquids, gels and aerosols with more than 100ml on baggage worldwide

http://www.catsa-acsta.gc.ca/english/travel_voyage/faq-liq.shtml

[25] SAP "Process Integration"

<https://www.sdn.sap.com/irj/servlet/prt/portal/prtroot/docs/library/uuid/6a90d6aa-0b01-0010-8a83-cf0e6c70dce>

[26] Jonathan Collins (2005) "IBM, Maersk Developing Cargo Tracker" Different Business Models used for introducing Wireless Security Devices:

<http://www.rfidjournal.com/article/articleview/1884/1/1/>

[27] Companies normally do not publish prices for Containers freely, but taking the price for a new 40Foot Container of 2000 USD into account and the price for a firm installed security device of 1000 USD raises the original price by 50%. Additional cost for the lessor for repair and maintenance and the surveillance system maybe as a service is out of the question.

[28] The usual container check at terminals today is a quick and standardised procedure. Own observations at various terminals have shown the following:

The complete Container Check which allows a container to enter a terminal consists most times of the following procedures:

(1) a visual inspection of damages of the hull of the

container,

(2) noting down pre-defined codes of the damages observed along with the position of damage,

(3) a verification of the container number to ensure data contained at the transport papers or at in-house data management systems do correspond to the container itself and

(4) an inspection of the integrity of the seal(s) along with the correctness of the seal identification number(s).

A complete inspection of this kind performed by well trained employees at good sight needs about a minute. His time is taken from stopping the truck and trailer at the right position, performing all checks necessary, maybe noting additional data with some kind of handheld computer or on paper and finally giving permission to the truck driver to leave the checking site, sometimes with new or additional information what to do next.

[29] When taking the existing 22 Millions of Containers with 4 voyages each year and 6 handlings each voyage (changes of liability) into account, 528 million checks per year are required – with a strong rising tendency^[30]. Taking these numbers into account, each second of a year more than 17 enquiries (using a single data management system) have to be answered. This sounds feasible, but having just 30 seconds from sending data to receive an answer, maybe half-way around the globe twice is rather a tight restriction. The internet is quite fast and reliable but having these requirements in mind it might be not capable. Another challenge is the amount of data to be stored which rather delays enquiries than speeding them up.

[30] Heideloff, C.; Stockmann, D (2007) "ISL market analysis 2006" Page 3.: Container transportation has risen strongly

[http://www.dmkn.de/1779/seeverkehr.nsf/B1DDE85B96014468C12572360034A97D/\\$File/2006_shipowners_operators.pdf](http://www.dmkn.de/1779/seeverkehr.nsf/B1DDE85B96014468C12572360034A97D/$File/2006_shipowners_operators.pdf)

[31] Mahipal Padigela (2006) "Article on Distributed database Systems"

<http://www.mahipalreddy.com/dbdesign/dbarticle1.htm>

[32] Heiko Müller (2007) "Containersicherheit und Security Devices": Invention of Distributed Databases at Security Systems using the Internet as Communication System

http://www.isl.org/news/meldung/07050701/pdf/6-Heiko_Müller_HEC_Workshop_Promit_24_04_2007.pdf

[33] Authorities in Charge for Container and/or Transport Safety and Security differ in each country. Mostly the following authorities are involved: police,

customs, port authorities, specialized forces.

Own talks recently have shown these authorities always keep the right to inspect Containers internally.

Today this physical check is made easy since the containers use standardised seals. The authorities in charge stop the truck, break the original seal, open the doors, check the contents, close the doors (when the content is legal) and attach a new seal. The driver receives a document which approves that the original seal was replaced by a new one for a security check.

At the next stop the driver hands in this document along with the freight papers. This procedure confirms the replacement and the officer who takes the order is able to change the seal number at his order data to forward the data to the next person, company or organization which needs it.

[34] Hitachi "Cargo Container X-ray Inspection Systems"

http://www.hitachi.com/ICSFiles/afieldfile/2004/06/18/r2004_02_106.pdf

Ammendment: Taking a minimum of 12 containers per hour into account and anticipating the 12 containers are equally divided by 20 and 40 Foot Containers, about 20 TEU can be inspected per hour making about 500 TEU per day resulting in 180000 TEU per year.

The Ports of Hamburg/Germany did handle about 8 Million TEU in 2005 is reported by ISL. In order to x-ray each container results in about 45 facilities – all operating 24 hours a day and each day throughout the year. In addition, personnel to operate these facilities is needed.

[35] Wikipedia, the free encyclopedia "Spoofing attack"

http://en.wikipedia.org/wiki/Spoofing_attack

These ideas can be adapted: The container is sealed with the original eSeal. This is initialized as usual creating a reliable data record on the data management to be checked against. Then the data exchange between the eSeal and the receiver is done multiple times and the data sent from the eSeal is recorded with another device. After this preparation the eSeal is dismounted and the fake device is mounted. Each time the container at legal checking sites one of the pre-recorded datasets is sent by the fake device. This can be overcome by sending the actual date and time of the data exchange between eSeal and the data reader equipping the eSeal with an internal clock. This additional data exchange may check immediately the time and provide a sound or tampered seal. The disadvantage is the internal clock of the eSeal itself, it consumes energy from some kind of battery and reducing the operation of the active RFID-Device. But this additional security could be faked as well.

[36] Netline Communications Technologies (NCT) Ltd. (2005) "Counter Terrorism Electronic Warfare Jamming and Detection Systems": Blocking wireless communication (cellular and satellite phones, VHF/UHF, GPS etc. can easily be done:

<http://www.netline.co.il/Netline/>

[37] An own experience showed the cost to operate a washing machine in India was more expensive than hiring a laundress.

[38] SASI Group (University of Sheffield) and Mark Newman (University of Michigan) "Container Ports"

<http://www.worldmapper.org/display.php?selected=38>

[39] It is not intended to compromise authorities of countries and managers of companies involved. On the contrary the anticipation to object installing new technology or inventing regulations is justifiable: having vast additional cost for devices which are mainly controlled from outside and which are really needed somewhere else is subject to refuse. Even when the same task could be done with conventional methods easily.

Maybe this can result in a kind of trench warfare (every side sticks to his own mind without having results) or the more probable result is let somebody else do the start, if it works I will do it likewise, but later on.

[40] Talks with road and rail hauliers have shown resistance against inventing such systems:

The actual road haulier and the driver in particular might be much more subject for control operations than today.

Each break, each small (private) detour or even combining transports, using different means of transportation than promised (or anticipated by the shipper) can be observed when using the most sophisticated systems available today. It is not intended by many companies to 'publish' their own business conduct this way. Hauliers have contracts containing addresses and times where and when to collect and deliver cargo. How the cargo is transported from one place to another is seen as private business of the haulier as soon as the safety of a transport is not endangered.

[41] Wikipedia, the free encyclopedia "Data Privacy"

http://en.wikipedia.org/wiki/Data_privacy

Some countries have a protection of data privacy which prohibits putting different data sources together in order to evaluate further information. But the view on these data protection is different. There are countries which place the national security above individual privacy.

[42] Who is to be informed by an automated system that a container is tampered, first of all? Who is not to be informed? Each participant is the most important party by own notion at this issue (received by own talks):

- (1) The shipper sends the goods. If there is something wrong with the goods he has to know it first.
- (2) The haulier physically moves the container. If there is something wrong with the container he has to know it first.
- (3) The consignee receives the goods after opening the container. If there is something wrong with the container he has to know it first.
- (4) A terminal or storage has the container at his custody. If there is something wrong with the container he has to know it first.
- (5) Authorities in charge do always have an interest of being informed first in order to prevent further damage.-

This list is easily expandable.

Large companies rather keep such security alerts in private in order to avoid bad publicity. The larger a company is, the more money is spent enhance the own reputation. Even this matter influences the question of the party to be informed first.

[43] DW-World (2004) "German Road Toll Prepares for Launch"

<http://www.dw-world.de/dw/article/0,1564,1414832,00.html>

[44] Abendblatt (2003) "Lkw-Maut bringt 100 000 Jobs in Gefahr": Report about threats at the invention of the German Road Toll System: (in German)

<http://www.abendblatt.de/daten/2003/08/28/201586.html>

[45] Earbital "ISPS charge at the port where is applicable and the implementation date": Extra ISPS-Charge at ports after inventing the code:

<http://www.arabital.com/ISPS.pdf>

[46] Many companies of the transport business objected and argued a road toll in Germany^[43] will cut employment through rising cost for transportation in general. After some time of operating the toll system charges are paid, the system is running properly, there are just a few fare dodgers and it seems nobody still complains about this new invented 'tax'.

The companies of the transport business have risen the prices for conducting transportation or bringing the toll direct to the account and got used to the system.

The share for the end-customer for an extra security charge ranges from just cents of one piece of bulk production transported in a large container up to the

total additional cost for the invention of security charged per container at each port affected by the transport. If a single security device is attached to each unit, the amount of data transmitted and stored and hence cost will rise enormously. In the end fewer end-customers will buy products which had long voyages from manufacturing to the end-customer.

But maintaining or lowering the actual cost for secure transportation means to keep the whole system as it is at the moment or rather stop the already invented security laws and regulations and additional customs checks. These more or less recently invented laws and regulations range from using a mechanical bolt seal at container doors which is developed and approved by international organizations and customs up to the exchange, the advanced exchange of data to check against blacklists and inconsistencies of the record set up to the exchange of customs officers to shift checks into the exporting country and using green lines for approved companies.

[47] The complete system using eSeals, fixed installations and antennas, handheld computers, some data management system and firmly working communication lines between all plants could observe the whole transport at certain spots only.

This implies at places where installations are applied and connected to the data management system each container is marked as in sound condition or tampered.

A truck driver normally has to be instructed or even forced to approach these mostly private plants if they are available and let checks conducted. Otherwise otherwise the eSeal-system is completely inoperable. When a company instructs the driver to perform checks at a long journey ex. 2000 km, the instructing company will have to pay for the checks and the time needed to perform the checks. Additional cost may be generated by having a detour to approach checking facilities and waiting cost if the plant is busy. Additionally a dense system of checking sites is needed.

If there is a mandatory system forced by law orders to have a security check performed are easily to arrange and settled (ex. after each larger break and after each 1000 km) but if this regulation is optional or for a certain clients (ex. just German truck drivers only) the best system is not being used.

[48] Today companies are at the market which use the continuous transport security control by selling devices and offering monitoring as a service. Each company or consortium uses a different system, thus having separated, interoperable systems. The common aim seems not to establish a global virtual standard.

There are companies which work for years with large organisations ex. SAVY from US equips US-Military containers transporting all types of goods (from high-tech weapons to simple hand creme) to US-military camps all over the world. Companies with a background like this use the knowledge gained by the

service established. These companies enhance the equipment and develop further applications for other customers more easily than start-up companies. But this does not help establishing one global standard.

[49] Transported Asset Protection Association “Welcome”: An Industry-driven Initiative to fight cross-border theft of high-value goods
<http://www.tapaemea.com/>

[50] Commission of the European Communities (2006) “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on enhancing supply chain security”
http://ec.europa.eu/dgs/energy_transport/security/intermodal/doc/2006_02_27_impact_assessment_sec251_en.pdf

[51] Demands for changes or the withdrawal of the Supply Chain Security Regulation by the EC
Amcham EU (2006) “Position Paper on the proposal for a regulation on enhancing supply chain security”
http://www.eucommittee.be/Pops/2006/proposalforregulationonenhancingsupplychainsecurity_020506.pdf

Group 4 Securicor plc (2006) “EU REGULATION ON ENHANCING SUPPLY CHAIN SECURITY Position Paper by Group 4 Securicor”
http://www.g4s.com/supply_chain_position_paper.pdf