RFID-enabled Innovative Solutions Promote Container Security

P. S. Tsilingiris[1)], H. N. Psaraftis[2)], D. V. Lyridis[3)]

[1)] Laboratory for Maritime Transport – National Technical University of Athens, Greece, tsilipan@yahoo.com
[2)] Laboratory for Maritime Transport – National Technical University of Athens, Greece, hnpsar@deslab.ntua.gr
[3)] Laboratory for Maritime Transport – National Technical University of Athens, Greece, dsvlr@central.ntua.gr

Abstract

In this paper we address the container security problem and we investigate RFID-enabled innovative solutions to confront it. To that end, initially we set the scene of the problem by reporting existing security problems in ocean container transport and container security-originated initiatives and regulations that affect seaborne containers transportation and handling. Afterwards, we accomplish our central objective by reporting RFID-enabled solutions and how they promote container security. In brief, our research unveiled that RFID-enabled IT systems can enhance container security. Specifically, as-yet RFID applications appear to assist in container identification and location tracking, in employee and vehicle access monitoring, and in regulatory adherence.

Keywords

RFID; containerization; container security; terrorism.

1. Introduction

The millions of containers around the world are often seen as gaping holes of vulnerability for terrorist attacks. This concern has been strongly amplified by the 9/11 event. The solution to container security is not straightforward since many seaports, the primary places where inspection of containers takes place, are already congested. Thus, the policies to handle Maritime Security could have side-effects on the logistical aspects of the Ocean Container Industry (OCI).

The OCI stakeholders and the policymakers should bear in mind that modern technologies are a functional tool in their arsenal to confront the problem. For example, Automatic IDentification (Auto ID) technologies, whose utilization has significantly grown over the years, could be used for the tracking of containers. Among Auto ID technologies, there has been much controversy regarding Radio Frequency Identification (RFID) technology. RFID currently attracts the increasing interest of academics, statesmen and other stakeholders. In the microcosm of shipping, RFID was still at its infancy until five years ago. Yet, many applications have emerged during the last couple of years and the future looks promising.

RFID regards a system that transmits wirelessly the identity of an object using radio waves. RFID readers capture data on tags and transmit it to a computer system with no human intervention. A typical RFID tag has a microchip attached to a radio antenna mounted on a substrate (Fig. 1). A typical reader has one or more antennas that emit radio waves and receive signals back from the tag. Then the reader, often called an interrogator as it "interrogates" that tag, transmits the information to a computer system in digital form (Fig. 2). Readers also have antennas which are used to emit radio waves. The reader antenna energy is read by the tag antenna and is utilized to power up the microchip, which changes the electrical load on the antenna and transmits back its own signal.

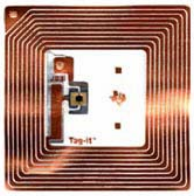

Fig. 1: An RFID Tag (www.sunshinetechnologies.com.au)

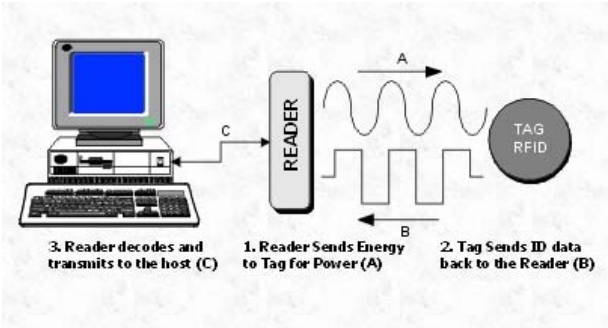

Fig. 2: How RFID works (www.rollsoft.ro)

We state right in the introduction of this paper that –to the best of our knowledge- the academic literature addressing container security via RFID-enabled innovative practices is scarce. Articles on *specific* RFID applications in the OCI abound in the World Wide Web; nonetheless, almost the entirety of those references describes specific applications and is of a rather commercial and/or journalistic nature. Some related references are the following. For the status and perspectives of RFID in the OCI the reader is referred to Tsilingiris et al (2007); however, Tsilingiris et al (2007) has an executional/operational rather than security focus. Dahlman et al (2005) propose a comprehensive code of conduct

towards container security. Optimization techniques for efficient security approaches at ports are suggested in Lewis et al (2002). An excellent related reference is that of the Stanford Study Group (2002) which describes criteria for secure systems aiming to detect nuclear material in international container shipping; however, it does not discuss at all the utilization of RFID.

The rest of this paper is organized as follows. In §2, we set the scene of the problem by reporting on relevant intermodal operations, existing security problems in ocean containers transport, and container security-originated initiatives and regulations that affect seaborne container transportation and handling. In §3, we report container applications where RFID adoption could be functional in terms of Maritime Security. The paper closes with some conclusions and directions for further research in §4.

2. The Scene Of The Problem

2.1. Container Identification, Seal Check, Damage Check and Inspection

The major objectives of container ID tracking are to perform quickly and with accuracy: (a) container identification; (b) seal check; (c) damage check. With current practices, these tasks are done by multiple players (shippers, forwarders, consignees, etc). Indeed, one stakeholder may perform each task many times (e.g., as we know at a container terminal all (a), (b), and (c) are done at the gate, at the quay, etc.). To make matters worse, the different players do not share the information of the checks and these checks are inevitably repeated.

Container identification regards the correct reading (and correct storage of this information) of the markings that associate with the container ID. The principal ID marking of the container and its explanation are depicted in Fig. 3. The container identification system specified in DIN EN ISO 6346 consists solely of the elements shown, which can only be used together: owner code, consisting of three capital letters; product group code, consisting of one of the capital letters U, J or Z; a six-digit registration number; and a check digit. Typically, container ID check is done visually by employees and, rarely, via video check done again by an employee. In any case, human intervention takes place.

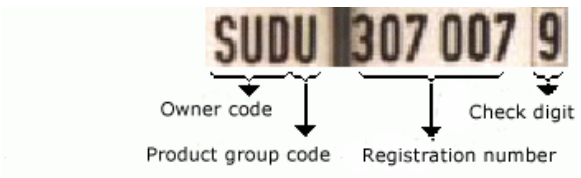

Fig. 3: Explanation of container ID markings (Source: www.containerhandbuch.de)

Container identification check should not be confused with seal check. The use of container seals aims to "stamp" the correct loading of container and ensure its non-malicious contents. Thus, if someone tampers illegitimately the container, the seal will unveil this. After applying the seal so that the internal locking mechanism comes into play, the operator must ensure that pulling hard on the head locks the seal. This will confirm that the seal is locked and secure at the time of closure. Tampering is not only suggested by a completely broken seal but also by other events. At destination, before breaking the seal, the operator must check if the seal itself has indentations or scratches, which would suggest tampering with the integrity of the seal. The head of the seal should be checked - if it opens easily, this again would suggest tampering. Naturally, the identity (usually with numbers) of the seal should also be checked. It is implied that the check of a mechanical seal is necessarily done by a human. A container mechanical seal with a bolt is depicted in Fig. 4.

Fig. 4: Container seal (www.tenacent.co.za)

However, it is possible that a seal is broken and replaced in a way so that tampering is not identified in the next check. To solve this, a specific workforce in ISO TC 104 discussed various approaches to an electronic seal. Some basic principles have been agreed on meanwhile: The standard electronic seal will be an attachment device fixed to (or integrated into) the mechanical seal that secures the door of the container. A photograph of an electronic container seal is depicted in Fig. 5.

Fig. 5: Container e-seal. (www.ops.fhwa.dot.gov)

As regards damage check, it is observed that most of the damages occur on the top of the containers because the spreaders of the straddle carriers exert forces on the containers. A complete damage check must regard all six sides (top, bottom and four sidelong sides) of the container. This is usually done visually by employees and rarely via video check from an employee. For example, when a container is unloaded from the sea it is checked from the bottom and sidelong. Moreover, when a straddle carrier moves it to the stack, its driver checks for damage on container top.

Contrary to the container ID, seal, and damage check,

inspection does not take place in all containers. In the example of a certain EU port we investigated, ca. 2% of all the ocean incoming containers are checked for security purposes. Truck incoming containers are usually not checked. This check is not homogeneous in the sense that the majority of certain sets of "suspect" containers may be inspected while other non-suspect sets may not be opened at all. This is performed via a decision-support inspection system, which produces a probability inspection function. Variables of the function are cargo data like origin, destination, etc. In essence, this program resolves the containers that will be checked. The inspection takes place only after the container has been stacked, the operator has adduced declarative documents to the customs, and the container has been stored in the port information system as a stored container. If the decision support system suggests the inspection of the container, the customs broker/clearer communicates with the customs the inspection command. Promptly, the container is "blocked" and the container operator is informed via an XML message. Then, the container is moved to the area where the inspection takes place. When the inspection finishes, a new seal is put to the cleared container, the customs "unblock" the container, and the container is again stacked. Thus, the unblocked container can be retrieved by a trucker.

US and EU port operators currently inspect 2-5% of the more than 6 million containers that enter the US per annum. However, since the US fears that containers will be a modus for terrorist attacks, they want to increase the number of inspected containers. This could create chaotic delays as the infrastructure is certainly not ready to handle this.

2.2 Existing Security Problems in OCI

Currently, the OCI experiences both operational/executional and security problems. The former problems are epitomized in the policy statement of the International Chamber of Commerce on maritime transport: "Freight transportation infrastructure into and from ports and to the regions they serve is increasingly incapable of adequately handling current cargo volumes." (ICC, 2005) The latter problems are exemplified in a memo issued by the USA House Subcommittee on Coast Guard and Maritime Transportation: "Despite the importance of seaport security, perhaps no other mode of transportation is currently more vulnerable to future attacks that our Nation's Marine Transportation System." (HSCGMT, 2004) In this paper, we will restrict our description to security problems only.

We clarify that the security symptoms we diagnosed regard security and not safety. The difference between security and safety should be clear-cut: although both safety and security initiatives aim to avoid events with negative consequences, security differentiates from safety in the sense that it regards incidents that are incurred by *intention* (e.g., terrorism, theft).

Specifically, we think that seaborne containers could be the modus for the following illegal actions:

- Smuggling of nuclear weapons, radiological dispersal devices, or conventional weapons
- Nuclear and radioactive materials smuggling
- Drugs smuggling
- Smuggling of persons and stowaways
- Contaminate containers with nuclear, radioactive, chemical or biological agents
- Container boxes theft (piracy)
- Containers contents theft (pilferage)

The following two problems pertain also to safety:

- Damage to containers containing hazardous materials - explosion or leakage of hazardous materials
- Damage to conventional containerized cargo caused by ordinary container transportation and handling operations and/or inspection

2.3 Initiatives and Regulations that Affect Container Transportation and Handling

To enhance maritime security, a significant body of initiatives has emerged in the last years. These initiatives have forwarded many new –or not so new- concepts in ports of embarkation, transshipment and disembarkation as well as in-transit. Among other concepts, it is proposed that ports infrastructure should be such so that the storing and other container handling areas are secure. RFID is introduced in some of these initiatives in order to create smart containers. (However, RFID utilization is not mandatory, but could assist in regulatory compliance.) Moreover, these initiatives envisage the electronic container seal (e-seal) that tracks –normal or illegal- openings and closings of the containers and informs automatically the authorities.

A non-exhaustive list of these regulations and initiatives is as follows.

Introduced by the International Maritime Organization (IMO):

- International Ship and Port Facility Security Code
- International Convention for Safe Containers
- International Container Security Organisation
- Ship security alert system

Originated by the EU:

- Regulation on Enhancing Supply Chain Security
- Directive on Enhancing Port Security (EC 2005/65)
- Regulation on Enhancing Ship and Port Facility Security (EC 725/2004)
- Green Paper on a European Program for Critical Infrastructure Protection (EC, 2005)

The USA alone has originated a plethora of regulations and initiatives:

- 24-Hour Advanced Manifest Rule
- 96-Hour Advance Notice of Arrival
- America's Waterway Watch

- Automatic Identification System
- Bioterrorism Act
- Cargo Handling Cooperative Program
- Container Security Initiative
- Customs-Trade Partnership against Terrorism
- Intelligence Fusion Centers
- Maritime Safety and Security Teams
- Maritime Transportation Security Act
- National Targeting Center
- Non-Intrusive Inspection Technology
- Operation Drydock
- Operation Port Shield
- Operation Safe Commerce
- Port security act of 2006
- Port Security Assessment Program
- Radiation, Chemical, and Biological Screening
- Seal Verification Program
- Security Boardings
- Security Committees Port Security Grants
- Smart and Secure Tradelanes
- Smart Box Initiative
- Transportation Workers Identity Card
- Trusted Shipper Program

Finally, some national (e.g., the Bund-Laender-Arbeitkreis Maritime Security in Germany) as well as bilateral agreements (e.g., between the EU and the US) exist.

Indeed, the regulatory complexity increases if we factor the guidelines in safety and environmental protection that affect directly or indirectly the ports:

- The Bathing Water Directive
- The Dangerous Substances Directive
- The Environmental Impact Assessment Directive
- The Environmental Liability Directive
- The Habitats Directive
- The Health and Safety in the Workplace Directive
- The Shellfish Directive
- The Strategic Environmental Assessment Directive
- The Urban Waste Water Treatment Directive
- The Waste Reception Facilities Directive
- The Water Framework Directive
- The Wild Birds Directive

The above cornucopia of regulations and initiatives, especially in the US, leads to the natural question whether the OCI is becoming overregulated. This concern is amplified by the fact that not all of the above are of the same nature; some are initiatives, others are regulations, others rules, acts, conventions, codes, etc. Surprisingly, there are both overlapping regulations and certain vulnerable gaps. Probably, an archetypal gap is the "global" definition of what exactly a port is; actually, this term and its characteristics (e.g., what are the exact boundaries of a port?) is different between countries and even between ports of the same country.

For 100% security cannot be guaranteed, it is functional to investigate the permissible failure rate of the regulations and of the business practices they imply. Harmonization between measures taken and their potential side-effects should be pursued. Another "hot" topic is the financing of container security (see, Rotterdam Maritime Group, 2005). Moreover, we judge that "risk assessment" techniques could prove vital in subsequent regulatory analysis.

It is clear that regulations should sidestep additional bureaucracy. Furthermore, regulations should not result in exceedingly costly operations and should not affect productivity. To attain the above, innovative IT technologies, like RFID, could be of value.

3. RFID-enabled solutions enhance seaborne containers security

Our description of RFID-enabled solutions promoting container security is based upon the review of dozens of real projects. For individual descriptions of some selected projects the reader is referred to the appendix of this paper and to Tsilingiris et al (2007). Here, we briefly present the generic findings of our study.

Some initial remarks are the following: (for a more detailed discussion of the following, see Tsilingiris et al, 2007)

- Commercial projects dominate over academic ones.
- The EU lags far behind the USA as regards RFID utilization to promote maritime security.
- The central motivation for RFID use in OCI is mainly security and not operational excellence.
- RFID does not only revolutionize technology employed, but also serves for business processes re-engineering.
- Intermodal port-rail RFID-enabled applications are scarce.

Generally, the RFID applications can be categorized as follows:

Container Identification. In practice, many a time intermodal containers have multiple identification numbers. Moreover, even if the container ID number is unique, the personnel often store inaccurately this information. With the RFID technology, the ID of the container can be stored on the RFID tag according to the ISO standards automatically leaving no room for wrong ID recordings. Moreover, the container ID cannot be forged. On the implementation side, readers placed on cranes, vehicles and other equipment enable the automatic recording of each container ID as it is offloaded and transported within the terminal.

Staff identification. RFID identification cards, be they proximity RFID cards or contactless smart cards, can be an antidote to employee identification cards forgery. These cards can store information like holder data (name, photograph) and data related to the job function. In unmanned areas, the RFID tag could be used as an entry card. Moreover, in unmanned areas the check could be done via Closed Circuit Television. In manned areas, the benefit is equally important. In this case, forgery is rendered difficult, if not impossible. Other personnel may be relieved of burden as the RFID badge can contain clearances or permissions. One could think the workers may oppose to using RFID tags; in this case, using the RFID badges as stored value cards, enabling the employees to make certain purchases, could catalyze employee acceptance. Thus, RFID can support, if not ensure, that authorized staff only can enter the secure areas.

Vehicle access, control, and tracking. Exact location and time tracking of equipment should be a part of fleet and yard management. RFID tags can be adduced to equipment like straddle carriers, tractors, chasses, etc, in order to locate the equipment used. For example, to implement this solution at a container terminal yard, RFID tags can be attached (or buried) at certain places of a container yard. The tags can be read by RFID readers placed on vehicles, thus, signaling the location of equipment. The information can be communicated to the offices via wireless LAN, which is already commonplace in modern container terminals. Moreover, RFID could be used for equipment access. For example, synergies could be developed with RFID employee badges to check that the right driver is driving the right vehicle. RFID tags applied to personnel badges and vehicles can secure the correct usage of equipment (e.g., RFID tags could lock/unlock the equipment). Furthermore, readers placed at access points of intermodal nodes can validate entry and exit to/from a port.

Activity monitoring. Apart from locating and tracking personnel and equipment, RFID can promote the monitoring of activities in a real-time fashion.

Sensors. RFID could develop excellent synergies with sensors. Active tags can have sensors, GPS, satellite systems, and other extras. The sensors could measure certain attributes of interest and the RFID technology could store these values. Each time the RFID container tag enters the field of an RFID reader, the values of these attributes will automatically be transmitted to the IT system of the respective stakeholder(s). In turn, based on atypical values of any of these attributes, the IT system could right away identify "suspect" containers and, indeed, rank the "potential hazard" of these containers according to the deviation of their attributes' values from the acceptable ones. The sensors used in parallel with the RFID technology can measure the following:

a. *Humidity*. Atypical humidity values could imply leakage of a liquid inside the container or leakage to container damage. We also note that the breathing of a person changes the humidity of its ambient place.
b. *Light*. By measuring the temperature it can be determined if the container has been opened or from end to end damaged. Light generating events, like fire or electronic devices (e.g., a timer) could be detected. Lights could even imply the presence of a person inside the container.
c. *Temperature*. By measuring the temperature it can be determined if the container has been opened or from-end-to-end damaged and if a chemical reaction or other exothermic process is taking place inside the container. Even the presence of a person could be identified.
d. *Air pressure.* Heat could result in a rise in air pressure. Moreover, if the container is air-tight, we could determine if a container is damaged or a door is opened.
e. *Vibration.* By measuring vibrations we could identify intense mechanical movements inside the container.
f. *Sound.* Determine if a person speaks inside the container or a mechanical/electronic device is working inside it.
g. *Chemical agents.* Chemical sensors could identify explosives, toxins and even nuclear or radioactive materials.
h. *Position.* GPS systems could track the position of the container en-route.
i. *Motion.* Determine if a person or something else is moving inside the container.

Other sensors could measure acceleration, air exchange, etc.

We note that applying these sensors to each container is unrealistic due to cost considerations. A limited number of sensors could be adduced to certain containers. The number and type of the sensors used is dependent on the usage the container is designed to have and on the value of cargo transferred. For example, high-tech US military containers in practice have many sensors. In any case, sensors complement RFID usage and are not required. RFID technology even without the use of sensors offers -as we saw above- many benefits.

Data Collection. RFID can be the modus to automatically collect container transport information. Current risk analysis does not factor container route details at a global level, like the loading/unloading ports and transshipment hubs. Data mining techniques could be used to spot suspicious movements. Thus, atypical container itineraries or uncharacteristic collective behavior of groups of containers, which could not be targeted before, are likely to be timely noticed.

Regulatory adherence. The above functionalities can help to comply with the rapidly increasing number of regulations. For example, the use of RFID in employee identification can assist in meeting the objectives of "Transportation Workers Identity Card". Moreover, RFID enabled e-seals can promote the objectives of the "Container Security Initiative" and "Safe and Secure Tradelines". Data collection could assist "Contraffic", a

system developed by the European Commission's Joint Research Centre in collaboration with the anti-fraud office of the EC, which automatically collects container transport information. Our opinion is that RFID can assist in meeting the objectives of the various container security initiatives and guidelines.

As we can infer from the above, real RFID applications succeed in enhancing different aspects of container security from container identification to regulatory compliance. In order to enable the reader understand how this technology mitigates risks, selected operations along a multi-modal route with and without RFID are outlined in Table 1 (list is by no means exhaustive).

Table 1: Selected operations with and without RFID

Route leg	Without RFID	With RFID
Ship approaches port of discharge	No check or information exchange regarding the status of containers	Readers placed at strategic port points automatically collect information before unloading begins
Container is unloaded at the quay	Cont ID, seal, and damage check are all performed manually	Automatic check leaving no room for wrong storage of information or forgery
Within Port	Limited	Monitoring of employees, equipment, activities, and containers
Port gates	Cont ID, seal, and damage check are all done manually	Automatic check leaving no room for wrong storage of information or forgery
En-route	Limited	Readers placed at strategic points along the route check the status of containers

An indicative outline of an RFID operational system at a port can be seen in Fig. 6. Specifically, Fig. 6 regards the principal components of a specific RFID seaport system, as this has been proposed at the Technical Annex of the CHINOS project (for more on CHINOS, see the appendix or www.chinos-rfid.eu). This system has two main components: the *Automatic Container Identification Unit* and the *Damage Documentation System*. One or more *Communication Controllers* integrate these main components into the ports' and related stakeholders' IT systems. Moreover, the system can be tested with a *Chain Event Manager*.

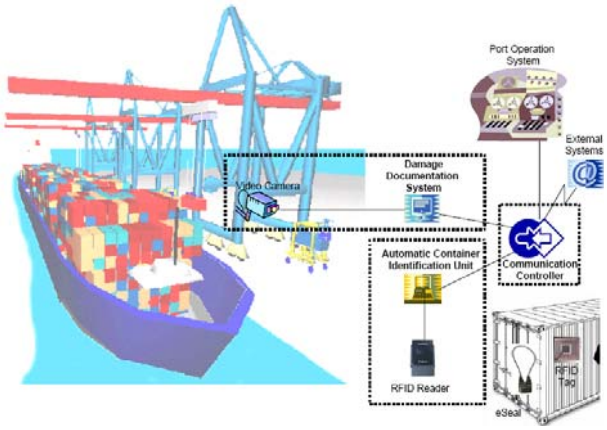

Fig. 6: RFID functional system at a port: principal CHINOS components (CHINOS, 2006)

As regards costs, Table 2 sheds some light on related expenditures. As it can be inferred, the cost of RFID equipment should not be a major issue in OCI applications insofar as the ratio of the cost of RFID equipment per container to the value of containers and their contents is rather low.

Table 2: Costs of components of RFID applications

Component	Actual cost	Cost depends on
Passive tags	20-40 cents (up to several USD for more sophisticated solutions).	• Frequency • Memory size • Antenna design • Packaging around the transponder
Active tags	10-50 USD	• Battery size • Chip memory
UHF readers	500-3,000 USD	• Dumb vs. intelligent readers • Single-frequency vs. multi-frequency readers
Middleware	Depends on application	Depends on application

The reader is referred to Tsilingiris et al (2007) for the perspectives of RFID in the OCI and, specifically, drivers for its adoption, paths for its future exploitation, and open challenges.

4. Conclusions

RFID-enabled applications in the OCI appear to partly confront the issue that originated them, namely, container security. The success of the first attempts and trials along with the rosy trends of RFID beyond the maritime industry fuel our cautious optimism regarding the adoption of RFID in the OCI. Our understanding is

that although the industry was very skeptical of RFID in the beginning, they were encouraged by the fact that the trials proved to reduce cost and time and to increase security levels. It appears that the major ocean carriers and the big ports will be the leaders of RFID adoption with smaller players being the followers. In general, the feedback from the industry is positive.

Since the academic literature on RFID in the OCI is scarce and the problem is "hot", research in the topic could be rewarding. For example, one could conduct a cost-benefit analysis of RFID vs. satellite systems for container applications. Another interesting topic of research is the generic system architecture designed to confront maritime security and, specifically, terrorism.

6. Acknowledgements

Part of the work on this paper has been supported by the EU research project CHINOS: Container Handling in Intermodal Nodes – Optimal and Secure! (Proposal/Contract Number: FP6/2005-031418).

References

Bacheldor, B (2006). "Georgia Cargo Terminals becoming RFID-enabled," The RFID Journal, http://www.rfidjournal.com/article/articleview/2493/ (accessed 21-7-2007).

Bizjournal (2006). "Mitsui subsidiary to offer RFID services at a port," Jacksonville Business Journal, http://www.bizjournals.com/jacksonville/stories/2006/01/09/daily28.html?from_rss=1 (accessed 4-3-2007)

Chen, T (2005). "RFID and sensor-based container content visibility and seaport security monitoring system," Proceedings of the International Society for Optical Engineering (SPIE).

Chin, L-P and Wu C-L (2004). "The Role of Electronic Container Seal (E-Seal) with RFID Technology in the Container Security Initiatives," Proceedings of International Conference on MEMS, NANO and Smart Systems.

CHINOS (2006). "Annex I – Description of Work".

Collins, J (2005a). "Korean seaport tests RFID tracking," The RFID Journal, http://www.rfidjournal.com/article/articleview/1438/1/12/ (accessed 21-2-2007).

Collins, J (2005b). "GE uses RFID to secure cargo," The RFID Journal, http://www.rfidjournal.com/article/articleview/1317/1/1/ (accessed 28-2-2007).

Dahlman et al (2005). "Container security: a proposal for a comprehensive code of conduct," Defense & Technology Papers Series, National Defense University Center for Technology and National Security Policy.

EC (2005). "Green paper on a European programme for critical infrastructure protection," Commission of the European Communities.

EC (2005/65). "Directive 2005/65 of the European Parliament on enhancing port security," Official Journal of the European Union.

EC (725/2004). "Regulation 725/2004 of the European Parliament on enhancing ship and port facility security," Official Journal of the European Union.

Friess, P (2006). "European Perspective on RFID," RFID Academic Convocation, Boston (USA), January 23-24, 2006

Hulme, G V (2005). "RFID helps to track cargo containers," Information Week, http://informationweek.com/story/showArticle.jhtml?articleID=160501261 (accessed 21-1-2007).

HSCGMT (2004). "Hearing on Implementation of the Maritime Security Act," Memo, House Subcommittee of Coast Guard and Maritime Transportation.

ICC (2005). "Policy statement of the ICC Committee on Maritime Transport," International Chamber of Commerce, Paris.

IndustryWeek (2006). "Savi networks extends RFID to largest container port in UK," IndustryWeek, http://www.industryweek.com/ReadArticle.aspx?ArticleID=12746 (accessed 4-3-2007).

Lewis, BM, Erera, AL, and White, CC (2002). "Optimization approaches for efficient container security operations at transshipment ports," Technical report, The Logistics Institute – Georgia Tech and National University of Singapore.

Mueller, R (2007). "Developing a Security Event Management System for intermodal transport," abstract submitted to the International Symposium on Maritime Safety, Security and Environmental Protection to be held on 20-21/9/2007 in Athens, Greece.

Mullen, D (2005). "The application of RFID Technology in a Port," Port Technology International.

Muprhy-Hoye, M, Lee, HL, and Rice, JB (2005). "A real-world look at RFID," Supply Chain Management Review.

Park, D-J, Choi, Y-B, and Nam, K-C (2006). "RFID-Based RTLS for Improvement of Operation System in Container Terminals," Asia-Pacific Conference on Communications.

RFIDJ (2003). "Port turns to RFID for security," The RFID Journal, http://www.rfidjournal.com/article/view/367/1/1/ (accessed 21-7-2007).

Robert, M (2005). "RFID container seals deliver security, value," The RFID Journal, http://www.rfidjournal.com/article/articleview/1965/ (accessed 21-2-2007).

Rotterdam Maritime Group (2005). "Study on Maritime Security Financing," Final Report.

Sheffi, Y (2004). "RFID and the innovation cycle," The international journal of logistics management, 15(1).

Stanford Study Group (2002). "Detecting Nuclear Material in International Container Shipping: criteria for Secure Systems," Center for International Security and Cooperation, Stanford University.

Swedberg, C (2006a). "RFID adds to security at Virginia Port Authority," The RFID Journal, http://www.rfidjournal.com/article/articleview/2748/ (accessed 21-7-2007).

Swedberg, C (2006b). "Colombian Shipper to use RFID," The RFID Journal,

http://www.rfidjournal.com/article/articleview/2335/ (accessed 21-7-2007).
Swedberg, C (2006c). "APM terminals readies its RFID system," The RFID Journal, http://www.rfidjournal.com/article/articleview/2323/ (accessed 21-1-2007).
Tsilingiris, PS, Psaraftis, HN, and Lyridis, DV (2007). "RFID technology in ocean technology transport," 2007 Annual Conference of the International Association of Maritime Economists, Athens, Greece.
Violino, B (2006). "APL Reaps Double Benefits from Real-Time Visibility," The RFID Journal, http://www.rfidjournal.com/article/articleview/2375/1/352/ (accessed 19-11-2006).
Wessel, R (2006). "Bremen researchers developing intelligent containers," The RFID Journal, http://www.rfidjournal.com/article/articleview/2774/1/1/ (accessed 21-1-2007).

Appendix: Résumé of selected RFID-enabled solutions in the OCI

RFID is a research topic, which has been addressed by the EU. To start with, the EU has an "RFID inter-service working group". The group, whose members belong to all 12 Directorates-General of the EU, has the objectives to: coordinate EU activities; collaborate with national authorities and standardization bodies; and enhance international collaboration. Regarding the last, there is active engagement in international exchanges (for example, EU-US Information Society Dialogue, EU-China Information Society Dialogue, OECD/ICCP RFID Forum in Paris, etc).

The interest of the EU in RFID projects is reflected on the number and the respective funding of projects under its umbrella. Project budget of RFID-related projects can be seen in Fig. 7. Fig. 8 depicts the specific areas of RFID projects.

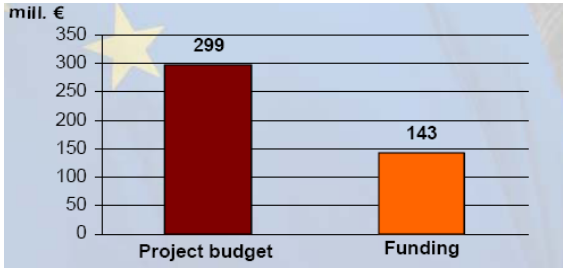

Fig. 7: EU-funded RFID-related projects. Total for Framework Programs 4-6, 1995-2005. (Source: Friess, 2006).

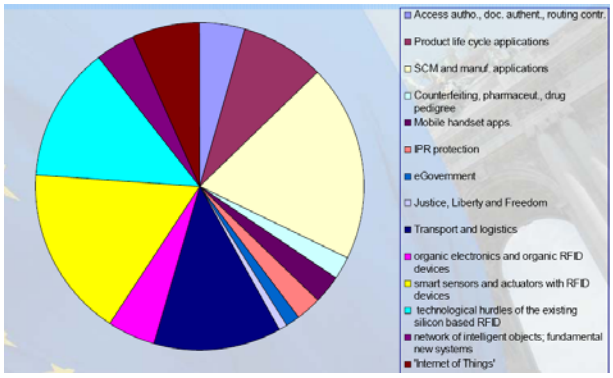

Fig. 8: Research areas of RFID projects. (Source: Friess, 2006)

As regards EU projects, research via Cordis and Extr@web showed that there is only one EU project regarding the use of RFID in the OCI, CHINOS: "Container Handling in Intermodal Nodes – Optimal and Secure!" CHINOS, whose anticipated duration is 3 years and had a kick-off date October 2006, aspires to examine how to employ RFID technology to enhance container handling practices both from a commercial and a legal/security aspect. CHINOS is coordinated by the Institute of Shipping Economics and Logistics (ISL) of Bremen. There are also a few other EU projects with which synergies can be developed. One of these projects is ConTraffic, a system developed by the European Commission's Joint Research Centre in collaboration with the anti-fraud office of the EC, which automatically collects container transport information.

We now present short summaries of the most important and relevant references on RFID use in the OCI.

Mullen (2005) presents the direct benefits of RFID on ports: accurate and complete data collection and better utilization of employees' time. The paper also identifies the five major areas of potential RFID applications in a water ports mindset: access control, container security, container identification and location, activity tracking and regulatory compliance. Robert (2005) mainly explains the motivation for the creation of Savi Networks, a joint venture between Hutchison Port Holdings, a global terminal operator, and Savi Technology, an RFID technology provider. RFIDJ (2003) describes the Port of Houston's use of RFID as part of the Smart and Secure Tradelanes initiative (SST). The Smart and Secure Tradelanes initiative was established by the container shipping industry to ensure the security of cargo containers. Swedberg (2006a) describes the RFID system of the Virginia Port Authority (VPA) to improve the security and efficiency of the processes surrounding its cargo container shipments.

Swedberg (2006b) describes the system of Colombian shipper Emprevi, which mainly dispatches pharmaceuticals, to use RFID to track containers shipment within Colombia. Bacheldor (2006) describes the system of the Port of Savannah, Georgia, to enable shipments' tracking. Collins (2005a) discusses the case of the Port of Busan, South Korea's largest port, which utilizes RFID to track containers, thus, securing and speeding its business processes. Violino (2006) presents the use of an RFID-enabled real-time locating system by APL Ltd., a

subsidiary of Neptune Orient Lines (NOL), at its Los Angeles facility. Swedberg (2006c) discusses the case of APM Terminals in Long Beach, CA, that has successfully tested an RFID system at its port terminal. Wessel (2006) describe the LogDynamics research cluster, a University of Bremen's interdisciplinary center, which has created a working model of an intelligent container handling system.

Hulme (2005) describes an RFID-enabled cargo-container tracking system with an emphasis on accurate container identification. IndustryWeek (2006) discusses the application of SaviTrak software and RFID readers to the container terminal of the Port of Felixstowe, UK. Bizjournal (2006) discusses the RFID applications at the ports of Jacksonville, Los Angeles, and Oakland, California, offered by Japanese carrier Mitsui and Savinetworks. Collins (2005b) discusses some progress of General Electric (GE) on the new generation of containers; the great innovation of the GE method is that seals are affixed on the internal side of the containers to enhance security.

One of the few relevant academic papers also reviewed is that of Muller (2007), who presents the state of Bremen's founding of the centre for Global Monitoring of Environment and Security (GMES). In addition, Park et al (2006) describe an RFID-enabled Real-Time Location System (RTLS) whose objective is to decrease ship turnaround time at ports. Chen (2005) devised an original RFID and sensor-based container content visibility and seaport security monitoring system. Chin and Wu (2004) confer on the potential use of RFID-enabled e-seals rather than describing an original application. Murphy-Hoye et al (2005) report their real-world look on RFID and propose the use of "decision-rule" algorithms to promptly spot and respond to deviations.