SEVENTH FRAMEWORK PROGRAMME
THEME 7
Transport including Aeronautics

Technology follow-up plan

Project acronym: **SMART-CM**
Project full title: **SMART Container Chain Management**

Deliverable No. (use the number indicated on technical annex)		**D2.3.7**	
Workpackage No.	**WP2**	Workpackage Title	**Neutral platform and deployment of existing technologies**
Task No.	**T2.3**	Task Title	**CSD Provisioning**
Date of preparation of this version:		**22/10/11**	
Authors:		**CERTH/HIT (Joseph McKinney)**	
Status (F: final; D: draft; RD: revised draft):		**F**	
File Name:		**SMARTCM-D2.3.7-v1.doc**	
Version:		**6.0**	
Task start date and duration		**01/08/2008, 39**	

Revision History

Version No.	Date	Details
0	*08/08/11*	*First version*
1	25/08/11	First revision
2	04/09/11	Second revision
3	17/09/11	Third revision
4.0	20/09/11	Fourth revision
5.0	11/10/11	Fifth Version
6.0	22/10/11	FINAL version

List of abbreviations

3PL	Third Party Logistics Provider
CSD	Container Security Device
CEN	European Committee on Standardization
CWA	CEN Working Agreement
GCSS	Global Container Security System
GDSN	Global Data Synchronization Network
GLN	Global Location Number
GPC	Global Product Classification
GPS	Global Positioning Systems
GSM	Global System for Mobile communications
GTIN	Global Trade Item Number
HSARPA	Homeland Security Advanced Research Program Agency
IoT	Internet of Things
KRA	Kenya Revenue Authority
KUL	Katholieke Universiteit Leuven (Catholic University of Leuven)
POS	Point of Sale
RFID	Radio Frequency Identification
SCM	Supply Chain Management
SKU	Stock Keeping Unit
SICUS	Shared Intermodal Information System
US DHS	US Department of Homeland Security
WCO	World Customs Organization

Table of Contents

List of Figures

List of Tables

Executive Summary

The need for a technology such as the Container Security Device (CSD) was an acknowledgement by the global trading community that commerce and trade in an increasingly open and accessible world economy had become vulnerable to random, indiscriminate acts of violence, and that there was almost no disciplined manner of protecting global citizens from those who would perpetrate such criminal activity.

The challenge of protecting every transportation conveyance and its cargo anywhere on the globe, urban or remote, steamy jungle or frozen tundra, on land or on the sea, seemed almost insurmountable, but many entrepreneurial organizations accepted the challenge. A number of recently popular technologies seemed to be particularly useful as part of the solution:

1. wireless communications
2. global positioning systems
3. remote sensor technologies
4. the entire range of e~commerce activities conducted via the Internet
5. the Internet of Things (Internet 2.0)

Manufacturers from various existing industries started to develop devices which would be able to meet the requirements of the potential users. Early in the past decade these users were predominantly national regulatory agencies, especially Customs and Border Protection Authorities. This initial understanding and positioning of the technology seemed appropriate, especially when commercial executives ranked Global Supply Chain Security as their greatest Supply Chain operational need. But this positioning lost relevance over time as commercial stakeholders let it be known that without commercial value reflected in normal commercial financial measures—increased sales, decreased expenditures, more efficient use of assets—there would be no commercial support for incurring the costs of such a system merely for security purposes.

Another user requirement which grew as both an outgrowth of the continuing development of e~commerce and e~government, as well as the realization of the enormous amount of data that can be generated by CSDs: the realization that all governments would need to have vastly improved methods of analysing incoming data for potential security threats and various types of Customs violations. New methods of receiving, storing, securing, analysing, and transmitting these data were going to be required, and soon.

The European Union, through its FP7 Programme of collaborative research projects, funded the SMART-CM Container Management Project as a key Supply Chain Security Project. A variety of CSDs participated, including units sourced from China, Europe, and the USA, and the data management structure created an important building block for a system of international CSD Data Management.

CSD Technology is no longer “new;” it is at the stage of “rapid development not yet mature”[1]. The innovations that are occurring are a mix of truly innovative (and still corporate intellectual property) and the maturing of developments that have been sought for years.

The data management challenge remains, but the use of the System Architecture for the currently operational Global Data Management System (GDSM) or something similar will provide a “guidance” model for creating a “Global Container Security System” architecture.

“The cloud,” the most recent evolution of I/T infrastructure, facilitates the type of multi-party secured sharing of data that is required for a multi-party business process such as a Supply Chain. This development is just now emerging, so its biggest impact is still some time in the future.

There is at this time one and only one “necessary and sufficient” condition for the global adoption of CSD technologies—device and data management—which is

[1] CSD Industry Stakeholders Survey, August, 2011

> The commercial value of the data provided by CSDs and the Global In-Transit Security System must be proven repeatedly, and there must be examples in the public electronic press of the commercial financial impacts of such a system.[2]

While this is not a direct quote from any single source, it is quotable from more than 2/3 (66.7%) of the CSD Industry stakeholders who cited this as the number one factor in order for the CSD industry and CSD usage to grow rapidly. Research into the actual financial performance value that various types of commercial industries and international trade participants have delivered would be a critical contribution to the adoption of this new technology[3].

It is only with widespread adoption that the CSD System will be able to begin to deliver against its most interesting long-term economic & social benefits, including more efficient asset and materials utilization. This efficiency will be the most broadly available means of delivering sustainable resource usage to the future generations from whom we are borrowing this world.

[2] Ibid.

[3] For example, McKinney, J. and Radford, A., the CIP Report, George Mason University School of Law Center for Infrastructure Protection and Homeland Security, July, 2011, as revised by the authors October, 2011.

Allocation of Resources

Partner	Budgeted mms	Actual mms
Sequoyah	1.5MMs	1.27MMs
CERTH/HIT Subcontractor		
TOTALS	1.5MMs	1.27MMs

1. Introduction

This is the deliverable for task T2.3. CSD provisioning of Work Package 2 of the SMART-CM Project.

The purpose of this deliverable is "to document the technology trends and expected follow up plans for fulfilling the global supply chain security requirements"[4] for Container Security Device Technologies and which factors are considered important to their future adoption. The two primary technologies which are specific to this industry are:

1. Container Security Device Technology—the devices, the sensors, the communications required
2. Container Security Device data management—what types of data, security and accuracy of the data, and transmission, storage, and access to the data by Customs and other Regulatory Authorities to evaluate the risks of admitting each container into its borders.

There will be a brief review of the history of container security, the impact of the events in the USA on 11 September 2001, the current state of the technology, and the achievements foreseen by industry stakeholders for the years 2012-2017 and beyond.

The content of this deliverable has a number of different sources:

1. The results of the field trials and the data management process of the FP7 SMART-CM Project
2. A survey of CSD industry stakeholders, many of whom were participants in the CEN-- CSD Standardization Workshop, and others who were solicited individually
3. Direct interviews with various industry subject matter experts
4. Research into several specific technologies that are emerging as critical to the industry
5. The direct experience, learnings, and conclusions reached by the author as a direct participant in the industry continuously since August, 2005 until the present

[4] Call for Tenders, "Tracing Technology Trends & expected follow up plans for fulfilling global supply chain security requirements," SMART-CM Project, Work Package 4, issued by CERTH, 24 June 2011 (draft)

2. Container Security Devices—the Origins

Historically, large size freight conveyances, such as railroad wagons (cars), containers, lorries / trucks, straight-line or with trailers, and whatever others may be in use, have had difficulty ensuring the security of the freight while the freight is enroute, from location A to location B, whether this is a short distance across town or a vast distance half-way round the globe.

The first technology employed was locks and seals, of many different types. While these devices may have ensured that the doors would remain closed until the seal was removed, the issues that emerged were 1) the ease with which one could cut one seal and replace it with an identical seal after the theft, 2) inconsistent business procedures to record and report the seal information, and 3) the ease with which the conveyance walls, roof, or floor could be penetrated.

Through the 1980's and 90's there was an acceleration of the amount of international trade for many reasons, both economic and political, but the impact globally, nation by nation, was that many major ports reached their handling limits and smaller ports began to be used for freight that had never been handled there previously; consequently, many Customs Agencies and other Trade Regulatory Authorities found that their capacity to properly inspect and manage the flow of trade into their country was being severely strained.

Then suddenly, on 11 September, 2001, the ability of international, indiscriminant terrorism to reach and attack any global location added an exponentially costly challenge to all international movements of people and freight. [In this document only freight movements are addressed.]

2.1. Enabling Technologies—The Challenge

Many organizations around the globe began to work on the problem of ensuring the safety of international freight. Because of the progress that had been made in the Automatic Vehicle Identification Industry, utilizing GPS, remote sensing, and wireless communications, there was already a set of technologies which could possibly be adapted to Container Security uses. But it was also recognized that certain problems were unique, and either major changes or new technologies would be required to meet the key security challenges for container shipments:

1. Monitoring for and preventing illegitimate entry into the container through the doors
2. Monitoring and preventing penetration of the six (6) sides of the container
3. Providing power to the device without easily accessed power connections
4. Appropriate antennae, especially if covert security was desired
5. Detection of biological, chemical, and nuclear threats
6. Ability to monitor and track the entire journey of the container
    a. From point of stuffing to point of unloading
    b. Through a variety of transportation modes
    c. Through multiple types of hazardous travel conditions

Each of these challenges is also true in one way or another of motor vehicles and rail wagons / cars, and therefore the potential for an extremely large market in which every container, rail, and truck movement could be monitored led multiple organizations around the globe to explore how to serve this newly recognized need for In-Transit Supply Chain Security.

Not only did governments realize the need to ensure their own homeland security from rogue participants in the international trade process, but commercial organizations across many industries began to acknowledge that security was now their highest concern in Supply Chain operations.[5] However, these same executives ranked many other factors as more deserving of investment, with improved security valued at a mere 2% of the value potentially provided by In-Transit Visibility.[6] This conclusion was voiced over and over by almost every industry stakeholder that was interviewed.[7]

Multiple studies have demonstrated the commercial value of one type or another of container tracking and monitoring.[8],[9],[10] and a very recent market survey conducted especially for this document indicated that without demonstrable commercial value, governmental mandates will be required to accelerate the use of Container Security devices into widespread usage.[11]

[5] Smart Boxes, by AT Kearney & Co., 2005, page 2.
[6] Ibid., page 9. The greatest benefit was asset based—reduced inventory; the second greatest benefit (very slightly less) was sales related—reduced out-of-stocks; the other benefits were expense related—lead-time variance, manufacturing uptime, and labor.
[7] Interviewees listed in the Appendix
[8] Ibid.
[9] Stanford Supply Chain Study—Prof Hau et al
[10] "Understanding the Synergies between National Security and Business Value," J. McKinney & A. Radford, CIP Report, George Mason University School of Law, July, 2011. [revised October, 2011] http://cip.gmu.edu/archive/CIPHS_TheCIPReport_July2011_SupplyChain.pdf
[11] See section 6.4. "Commercial Data Utilization"; CSD Industry Stakeholders Survey, August, 2011

3. Technology Framework—Global In-Transit Container Security System

What are the components of a Real-Time In-Transit Global Container Security System (GCSS)?

While this deliverable is primarily concerned with two critical components of any of these systems—the CSDs and the methods for collecting and using the CSD data by Regulatory Authorities—an understanding of how the complete system operates is important to fully anticipate how the technologies might logically evolve. There are ten (10) key components in the GCSS:

1. Participants and Stakeholders in the Container Security System
2. Transportation Conveyances—containers, lorries and trucks, rail wagons
3. Container Security Devices (CSD)
4. A Global Position Locating System
5. Long-Range Communications Networks
6. Short-Range Communications Standards
7. CSD System Processing Centers
8. The Internet
9. Security Monitoring Center(s) or “Data Pools”
10. Communications amongst global Customs Agencies and the Security Monitoring Centers

3.1. Supply Chain Process

A simplified example Operational Supply Chain for these purposes, by step:

	Supply Chain Operator	Supply Chain Function	
1	Third Party Logistics Provider (3PL)	Coordinates the provisioning of each of the steps in the process—equipment, documentation, scheduling, etc.	
2	Shipping line (or other party)	Provides the container to be used for the shipment	
3	CSD Provider (may be the 3PL, the Shipper, or a another party)	Provides CSD to the shipper for installation in or with the container at the time of loading and sealing	
4	Shipper	Installs the CSD while loading and sealing the container	**CSD & "Neutral Platform" Functions** CSD Starts data collection and transmitting to home system; transmits to "Neutral Platform"
5	Outbound trucker (or railroad)	transports container to the terminal in originating port	CSD collecting data and transmitting…
6	Exporting Customs Agency	Clears product for export	[Inactive at present time]
7	Terminal operator	Loads container on to the ship	CSD collecting data and transmitting…
8	Ship	Transports container to destination port	CSD collecting data and transmits: often not possible at sea
9	Terminal operator	Unloads container from the ship	CSD collecting data and transmitting…
10	Importing Customs Agency	Clears product for import; may open container to inspect	Importation Customs Agency field agents request data from Neutral Platform
11	Inbound trucker (or railroad)	transports container from the terminal in destination port	CSD collecting data and transmitting…
12	Buyer or Recipient	Receives and unseals the container; returns the CSD to the CSD Provider	

Table 1: Simplified Supply Chain Stakeholders & Process

3.2.1: Conveyances (Containers and others)

The now ubiquitous "container" was invented as a reusable, standard size conveyance for the shipping of general freight, especially when shipped internationally by sea[12]. Various sizes and configurations have been created to serve particular specific needs, such as refrigerated containers, open top containers, high-rise containers, and the like. There are a series of ISO Standards (ISO Standards 668, 1161, 1496 and 3874)[13] so that standard sized and strength container can be manufactured globally, and that they can be used interchangeably on the thousands of ships designed to carry containers.

With few exceptions, containers are constructed of steel for maximum protection of the cargo from the environment—wet or dry, salt or dust, and so forth. The steel frame is also necessary so that the containers have the strength to both carry their cargo, which can be quite heavy, and to withstand the stresses of loading, stacking, and traveling via sea, road, or rail. These standard containers thus present certain physical and operational constraints on the Container Security devices and the ways that these two pieces of equipment can work together.

There are currently several projects that are working to find new materials which can be used to build containers. One example is the project underway in the USA at Maine Secure Composites LLC (MSC), awarded by the US Department of Homeland Security Advanced Research Program Agency (HSARPA) to develop a next-generation "smart" container that can detect intrusions and prevent terrorists from placing bombs in containers going into the US. Few details have been released, but what is known is that the so-called Composite Anti-Tamper Material (CATM) maritime shipping container will be 20% lighter than existing steel containers."[14] This will allow container ships to carry more revenue earning containers while riding at the same draught as today, thus raising the revenue possible from each trip that each ship.

[12] M. Bohlman, "ISO container standards are nothing but good news," ISO Bulletin, September 2001
[13] http://www.tandemloc.com/0_securing/S_ISO_Container_Info.asp
[14] World Cargo News on-line, February, 2007

3.2.2 CSD Built-In Functionality

Some specialty manufacturers are currently experimenting with building current CSD capabilities into the container as permanent equipment. This would introduce a different set of operating challenges, but would simplify the CSD handling concerns of today's nascent industry. Some carriers have begun installing CSDs in the refrigerated containers[15] and in their refrigerated truck trailers[16]. Since reefers have their own power, the CSD can use the reefer power, either directly or to recharge its battery, allowing for alerting and reporting even when the reefer itself is not powered. Dry containers only have nearby available power while they are being transported by truck, so the availability of power is a major challenge in this scenario.

As stated above, this and similar projects often utilize variations of engineered materials, such as are increasingly being used in the construction of aircraft, the newly certified Boeing 787, for example.[17] These containers will be lighter, which has the effect of increasing the number of containers that can be carried on a container ship at the same draught as today.

These materials also allow for additional changes in the construction of the container, allowing for example the incorporation of Container Security Device capabilities into the container itself, without requiring the sensors and other CSD components to be in a self-contained device which is field-installed into the container. These types of materials may also enable certain capabilities which today have been difficult to attain, especially the ability to detect a penetration of the container by drilling or cutting. However, the critical factor of cost for these materials has not begun to position these new designs into the mass availability range of the market, so these materials are not anticipated to become a measureable part of the total market for containers until sometime after the year 2020.

3.3. Devices & Sensors

The quest for producing a device which is capable of monitoring the security and the integrity of a container load of freight is a natural extension of the requirement to lock and seal a shipment for protection from both the environment and from human misdeeds. The devices themselves combine several recent technological advances—cellular phones, satellite communications, the Global Positioning System, and remote sensors. When the Galileo System is operational it will be utilized by various CSD systems.

[15] Sea Star Lines: http://www.defensefile.com/Customisation/News/Naval_Systems/Vessel_Monitoring_Marine_Telemetry/GPS_Ship_and_Cargo_Tracking_For_Refrigerated_Freight.asp ; and Horizon Lines: http://www.horizonlines.com/About-Horizon/History.aspx

[16] J.B. Hunt Transport Services: http://fleetowner.com/information_technology/news/hunt_reefer_tracking/

[17] http://www.boeing.com/commercial/787family/background.html

It is the types of data that these devices generate that will establish and solidify their actual value in the world of trade and commerce. This data is itself a completely new type of data, filling a large void in the flow of data from the operational supply chain. While some perspectives on the information which will be drawn and the new insights revealed are developing, the actual use is just at the very beginning of the beginning of its utilization for business operations and performance measurement.

Even though the commercial value of this data is still in the initial exploratory stage, and no clear industry-wide patterns of "best usage" have yet been established, it is already clear that neither commercial nor regulatory organizations will be confident in the application of this data unless the devices and the sensors can meet particular standards of performance and accuracy. The current CEN Workshop on CSDs, an outgrowth of Project SMART-CM, is one critical industry effort to reach consensus on these types of standards, and to thus set some basic industry parameters which will provide a platform from which the CSD industry can grow into widespread commercial and regulatory adoption for trade.

3.4: Global positioning systems

It is obvious to all that many of the recent advances in Location-Based services would not exist were it not for the existence of these systems. When the EU funded and developed Galileo System is operational, the CSD industry will have several choices, with the Galileo System being more directly attuned to the needs of the commercial world than the current US funded GPS system.

3.5. Long-Range Communication Networks

Both the global cellular networks and the various satellite communication networks have seen enormous advances in technologies over the past 20 years. These long-range networks are now in a relative state of maturity in terms of their communication transmission capabilities. What will continue to progress are the methods of securing these communication pathways so that users are assured that the message transmitted is actually received by only the party to whom the communication was addressed, and that it was not intercepted or somehow corrupted by any other party.

3.6. Short-Range Communication Standards

There are several points in the CSD System where short-range communications are being used: 1)communication between auxiliary equipment and the CSD, 2)communications between field agents and the device, 3)communications between CSDs for the purpose of enabling one CSD to communicate long-range through another CSD—some version of an "ad hoc mesh network".

Current short-range communications standards in place include ZigBee, Bluetooth, and the more general 802.15.4 standard which the US Department of Homeland Security (US DHS) is utilizing for its major field trial of CSDs in international trade, at present scheduled to run from May, 2012 through

April, 2014.[18] ZigBee is a specialized version of 802.15.4 currently in use by several CSD systems, and Bluetooth, the original short-range system designed for voice communications, is also used.

Short-range communications may see additional changes; for example, if the ISO 18000-7 standard is able to achieve its desired role as an active RFID communications standard, then this may see broad application as the universal method for regulatory field agents to query the CSD directly, without recourse to any long-range communications[19]. It would also serve as the container yard or truck line yard management system wherever these facilities are located.

3.7. CSD System Processing Centers

At present, each CSD in use has a particular device management system. Today each of CSD normally reports into a "home" system processing center (or "back office"), which can forward the report to various stakeholders, including "Security Monitoring Centers" such as the Project SMART-CM "Neutral Layer "[20] or the Project Integrity "SICUS" database.

However, as with any newer technology that develops with proprietary protocols and communications standards, CSD industry growth will proceed, but will not begin to approach any type of rush to acceptance until the equipment can interoperate with most other CSD systems, and most systems can accept most any type of CSD messages—a recent example of this similar process was the cellular industry, whose global expansion was rapidly accelerated by the development of the GSM protocols (Global System for Mobile Communications.)[21] The CSD Industry Stakeholders Survey revealed that a majority believe that interoperability will not become a reality until 2016 or 2017 at the earliest, with 10% of the respondents believing that this will not occur until 2021 or later.[22]

As a beginning point for the global CSD Industry, the CEN Workshop on CSDs has preliminarily agreed that the communication standards used during the SMART-CM Project, as detailed by and upgraded by the KUL Paper,[23] will be proposed as the standards for all communications between the CSD System Processing Centers and the Neutral Platform(s). The major upgrades that were suggested by the KUL Team were improvements to the security of the messages between the CSD

[18] "Secure Transit Corridors," presentation by Ken Concepcion, US DHS, 29 June, 2011, at the US DHS sponsored Cargo Security Supply Chain Industry Day, held in Crystal City, Arlington, VA, USA
[19] This is the system architecture that is being installed in Kenya: Kenya Revenue Authority, Electronic Cargo Tracking System, Phase II, Technical Requirements, 7 August, 2009
[20] Draft CEN Working Agreement document of CEN workshop of SMART-CM Project, September, 2011
[21] http://www.gsm.org/about-us/history.htm
[22] CSD Market Survey, August, 2011
[23] "Protocol Standardization: Exchange of Security Status Information Between a Container Tracking & Security Device (CSD) and the SMART-CM Middleware Platform," by Tom Goovaerts, Sam Michiels, and Wouter Joosen; DistriNet Research Group, K.U. Leuven, Leuven, Belgium; March 30, 2011

System and the Neutral Platform; nearly 75% of the Stakeholder Survey respondents agreed that Communications security will be increasingly important in the future.[24]

One open question concerns the possible issue of the CSD system processing center perhaps altering the data in the message originally transmitted from the CSD before it is sent to the Neutral Platform. Industry software expert Bernard Van Hoorde of Descartes, in the CEN Workshop of 1 June 2011, stated[25]:

1. It is in the best interests of the CSD provider to not perform in this manner
2. The application of the same types of cybersecurity applied to the communication of the CSD network to the Neutral Layer would required a tenfold increase in investment for the "Neutral Layer", thus rendering the entire system as without economic value
3. The application of the certification processes such as currently used by GS1 for the Data Pools in the GDSN network[26] may provide an economic methodology for securing the accuracy and authenticity of the CSD messages as transmitted from the home CSD system.

3.8. The Internet

Of course the Internet is developing perfectly well without the CSD Industry, but the CSD Industry is heavily dependent on the Internet for its own operational efficiency. More specifically, it is the "Internet of Things" (IoT) that will be of greatest value to CSD data flows globally, as devices report to systems which report to other systems and centralized "neutral platforms" ["data pools"]. Some define the IoT as "RFID identifiers on all physical objects," but it can be easily understood that the CSD becomes the identifier for the conveyance for the duration of the shipment, and therefore for the collection of items in the container for that same period of time.

To chose just one relevant definition of the IoT, this from software firm SAP:

> A world where physical objects [by means of some type of electronic representation] are seamlessly integrated into the information network and the physical objects can become active participants in business processes. Services are available to interact with these 'smart objects' over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.[27]

[24] CSD Industry Stakeholders Survey, August, 2011; the question specifically asked for the characteristics of CSDs at the beginning of calendar year 2016.
[25] "Minutes of Second Plenary Session of the CEN Workshop on Container Security & Tracking Devices (Smart CM)"; Brussels, 01/06/2011**;** SMART-CM Project document N 0020, page 5
[26] "What is GS1?" presentation by Anders Grangård, Director GS1 e~Com for GS1 Global, 1 June, 2011, at the Second Plenary Session of the CEN Workshop on container Security & Tracking Devices, Brussels, BE, pp 8-9.
[27] "SAP IOT Definition". SAP Research, 2011-03-18, found @ http://en.wikipedia.org/wiki/Internet_of_Things on 29/08/2011

3.9. Neutral Platform(s)

For the purposes of the CSD Industry, a "Neutral Platform" is the term which the CEN Workshop on CSD Standards is giving to the "data base" or the "data pool" or the "data fusion center" into which all required security data or supplemental information related to a particular container in transit is accumulated, and from which any certified regulatory agency can obtain specific information for its own use in assessing the risk of clearing a particular container (or other conveyance) through its borders.[28] Current examples include the "Neutral Layer" created for and used for the SMART-CM Project, and the "SICUS" database created for and used by Project Integrity, the parallel FP7 project.

3.10. Communications amongst global Neutral Platforms and global Regulatory Authorities

The need to define these communications is especially evident when the observer asks questions about national sovereignty, data security, and the like, both within and outside of the European Union. Therefore it is important that the CSD Industry, and all of its stakeholders—both regulatory and commercial—define an appropriate global system architecture which will permit data to be exchanged between these "Neutral Platforms," perhaps only on a bilateral basis to start, but it will then quickly become apparent that an efficient means of sharing on a many-to-many basis will be far more effective for all participating parties.

> Cloud-based systems are innovating the way [organizations] connect by…establishing networks that serve as global business process hubs. [Cloud-based systems] create a virtual community where all relevant business partners have visibility to the information they need to execute efficiently as part of the network.[29]

The Cloud is still such a new concept that its value has not yet been absorbed by this market. Early indications are that it will quickly start to dominate the world of collaborative business processes, of which the whole arena of international trade is a prime example. This will then lead market participants to another increasingly important factor:

> While real-time shipment status information is vital in the global supply chain, ***process visibility*** is equally important to identify and resolve systematic problems. Identification tools such as RFID and barcodes; position detection systems; and container security devices all play a role in providing [this] visibility. (emphasis added)[30]

[28] Draft CEN Working Agreement document of CEN workshop of SMART-CM Project, September, 2011
[29] "Cloudy Days Ahead for Global Logistics," Waggoner, D., Inbound Logistics, August, 2011, page 32.
[30] "Managing the Three V's of Logistics," Siplon, P, Inbound Logistics, August, 2011, page 34.

4. CSD Technology—Direction 2011 through 2016 and Beyond

4.1. Overview

The Container Security Device Industry has already passed through its early development stages, although it is still quite innovative. The devices themselves have evolved from "large and awkward" to being a bit smaller and somewhat less awkward to handle, but there are expectations that this part of CSD development still has plenty of issues to solve.

The CSD sensor functionality considered the minimum for basic security purposes, include Time, Date, Global Position, and door position indicator. There are several other types of sensors which are security condition indicators for the conveyance or for the cargo, including optic (presence of light), occasionally audio, "Hall Effect" and other sophisticated sensors detecting one type of change or another for tamper detection purposes. Carbon dioxide sensors or very infrequently infrared sensors can be used to detect the presence of humans as cargo.

There are a number of other sensors which provide security for the handlers of the conveyance or bystanders—"Homeland Security." These include nuclear substance detectors, biological threat detectors, and chemical detectors. Industry stakeholders generally agree that these specialized types of detectors will become available in affordable quantities in the 2014-2017 timeframe.[31] While much of the market considers these sensor capabilities as defense against rogue terrorist type threats, each of these might play a virtuous role much more frequently by detecting leakage from specialized shipping vessels for nuclear medical and power generation waste, by detecting leakage of many types of specialized chemical shipments (not only Chlorine), and biological substance shipments of all types.

But the security value of CSDs, whether for each nation's homeland or the cargo itself, will not be able to effect commercial adoption of the technology in the absence of regulatory directives. Therefore many CSD manufacturers have added additional environmental condition sensors into the CSDs, thus morphing the devices into Cargo Monitoring Devices (CMDs), with security as one of the essential conditions to be monitored. While improvements in the operation of these sensors will doubtlessly occur, there are now effective sensors for temperature, humidity, shocks, vibration, and simple motion. Each of these has value for certain types of shipments and not for others, and each can also serve a secondary role for security monitoring.

Since the earliest days of CSDs the industry has struggled to create the ability to detect a penetration of the conveyance that is not through the doors. Even with more than a decade of design, testing, and analysis, there is no widely available economically feasible conveyance penetration detector. The industry does think that there will be such a detector available in the 2016-17 timeframe for

[31] CSD Industry Stakeholders Survey, August, 2011

penetrations of 10 cm diameter, but that the ability to detect a penetration of 2 cm diameter will not be on the market until 2021 or later[32].

In a different form of shipment packaging—cardboard boxes—a method of penetration detection has been proven effective. These specialized boxes are constructed in three (3) layers, the outer layers being the paperboard, and the middle layer being an appropriately sized RFID tag and antenna.[33] These boxes can record any penetration or seal disturbance event, and they can also record temperature. The date and time are captured, but the GPS location cannot be determined due to the lack of a GPS capability. Whether steel shipping containers can be constructed in such a manner seems unlikely due to many factors, including the weight and the blockage of radio signals by the steel, but containers made of engineered materials have other possibilities that are being researched, and are beginning to demonstrate some limited success.

4.2. CSD Physical Characteristics

The future of the physical Container Security Devices will be similar to the technological development paths that have occurred in cell phones, personal computers, and music replay devices—smaller, lighter, with increased functionality compared to the previous version. These developments can already be seen in the product offerings of many CSD manufacturers.

Industry stakeholders forsee that the typical CSD of today will, in early 2016, be reduced in both weight and physical size, and cost less than half of today's devices[34]. These are important factors both in terms of handling the units and installing the units. The field trials of the SMART-CM Project concluded that the handling and the installation procedures must be simplified greatly, if it is presumed that the CSDs will be installed by most any person responsible for the loading of the container or the trailer[35].

It is expected that the devices will continue to operate without a reader infrastructure, use both cellular and satellite communications as the manufacturer sees fit to provide, and that the CSDs will continue to be field-installed, as they are today: this reinforces the conclusion that installation and management functions must be greatly simplified.

With regards to the weight of the CSDs, one critical factor is the weight of the batteries. There are of course other battery issues, including the handling procedures for any hazardous materials depending on the content of the battery, the ability to ship CSDs based on these factors, and then the

[32] CSD Industry Stakeholders Survey, August, 2011
[33] The Cypak Company, Sweden http://www.cypak.com/
[34] CSD Industry Stakeholders Survey, August, 2011
[35] Project Smart-CM: http://www.smart-cm.eu

need to either recharge the battery or to change out the batteries—all of these introduce some elements of risk and the need for strict adherence to procedures.

Ever since CSDs were first built there have been issues of battery size, capacity, weight, hazardous materials content, and proper shipment via air, ground, and sea; these have been either the first or second most important issue with the devices themselves.[36] There is research into battery technologies taking placed at many important research centers around the globe,[37] [38] [39] including in other portions of the FP7 Programme, both within the Energy Theme projects, as well as in other thematic areas, including the FP7 ICT Theme.[40]

There are 3 other factors related to the physical characteristics of the CSD which could become important in the CSD industry, but probably not before the beginning of the year 2016:

1. Modularity
2. Disposability
3. Conveyance embedded functionality

Were CSDs to become modular, the user would have a set of sensor modules which could be quickly and easily removed or installed in the device, so that in fact the device could have a different set of functionality for each container shipment. This does not seem likely to occur. Rather, the concept of modularity is at this time being used in the manufacturing process. In the sensor mix, the modularity is accomplished by having certain units available that can be placed in or with a shipment so that their data is supplemental to the main CSD module; it will usually be transmitted to the main CSD by some form of wireless communications; the main CSD will then transmit the information to the CSD home system.

The requirement for "disposability" has been expressed by during direct interviews with a number of potentially major users of CSDs. Their rationale is that they want to minimize the disruption to today's standard operating procedures at the time of unloading the container or the truck trailer; therefore, if the CSD can simply be tossed out with the trash, then procedures will be minimally impacted, and if at least some of the CSDs are used again, then that will be additional value beyond the budgeted expense.

The third factor, having the CSD functionality actually embedded in the conveyance itself, is currently being prototyped by various projects and manufacturers. At the present time this configuration is most often being explored with conveyances constructed from engineered materials. However, if the market demand accelerates quickly at some time in the future, there may be an opportunity for

[36] Direct interviews with key industry stakeholders.
[37] IBM Corporation, involving Lithium air batteries http://www.technologyreview.com/energy/22780/
[38] Stanford University, http://news.stanford.edu/news/2008/january9/nanowire-010908.html
[39] The specific examples cited are just two examples out of probably several thousand individual research projects being performed globally.
[40] http://ec.europa.eu/research/energy/eu/research/smartgrid/index_en.htm

conveyance manufacturers—containers, truck and lorrie trailers, and rail wagon and car manufacturers—to build current CSDs into the conveyance as permanent equipment. This would introduce a different set of operating challenges, but would simplify the CSD handling concerns of today's industry.

4.3. CSD Handling and Operating Characteristics

The major operational challenges for CSDs are:

1. Ease of Installation[41]
2. Proper Antenna positioning
3. Proper sensor coverage
4. Covert utilization
5. Power management
6. Ability to be shipped easily and safely[42]

Each of these has seen improvement since the beginnings of the industry, but challenges remain:

1. Ease of Installation—CSD users require that the installation of any CSD device cause no damage to the conveyance, and be able to be completed in a very short period of time—less than five (5) minutes, or better yet less than two (2) minutes. Ideally, this would be accomplished without requiring use of a ladder to reach the top or the container.[43] There is no industry concurrence on any solution(s) to this issue at this time.

   There is an additional issue with CSD installation and deinstallation (retrieval)—security. This was a primary concerned raised by the EADS CSD development team. According to Frank Neubauer, the Team Spokesperson, the issues surrounding proper authorization of the individuals that actually handle the devices are a major goal of their current efforts.[44]

2. Proper Antenna positioning—given the methods of transport for containers, the absolute best positioning for the antenna is either high on the doors or on the roof—but these positions normally required the use of a ladder. Satellite antennae are the most difficult, since the satellite must "see" the sky directly. Cellular network antennae are somewhat forgiving, but still cannot be completely enclosed in a metal box. GPS antennae can sometimes operate inside a dry goods container, but with decreased accuracy versus having external access to the sky. And short-range wireless antennae can normally communicate well within the container, but often require a physical means to get the signal out of the container box. The direction for antenna improvements is towards smaller and increasingly covert, but CSDs are

[41] "Minutes of Second Plenary Session of the CEN Workshop on Container Security & Tracking Devices (Smart-CM)"; Brussels, 01/06/2011**;** SMART-CM Project document N 0020, page 2
[42] Ibid., page 3.
[43] Ibid., page 2.
[44] Interview with Mr. Neubauer and other EADS/Bosch team members, 10 October, 2011.

utilizing the improvements being driven by other industries, rather than being able to drive the technological improvements in the direction required by CSDs.

3. Proper sensor coverage—the accuracy of the data recorded by a sensor of any type is directly dependent on the positioning of the sensor. For example, temperature monitoring of the cargo must necessarily be located inside the conveyance, while the antenna has requirements to be outside. The use of wirelessly communicating sensors is allowing the separation of these two requirements, but with an increased difficulty of proper installation. There are an increasing number of RFID tags with temperature sensing in use, but not yet in combination with CSDs (as best could be determined at this time).

4. Covert utilization—many CSD devices have the ability to be used covertly, and as size and weight continue to drop this will become even more prevalent. This is most easily accomplished for purely domestic shipments. For international shipments, the requirement to list the entire contents of the conveyance does create some conflicts; there is not yet a resolution.

5. Power management—this is the most critical operating challenge for the CSD industry, whether the devices will always be field installed, or if the capabilities become original equipment in containers and other conveyances. The challenge is not unique to the CSD industry, but many of the use characteristics are more difficult than the challenges of a standard cell phone. The ideal power solution for the CSD industry is to harvest power from its immediate environment. We have already mentioned reefers. There is some research into methods of harvesting energy from the movement of the rail wagon or the truck. Solar power is a possibility, but these developments are still early, and are heavily dependent on the solar industry's technological development. There are batteries in the global market which are quite suitable for use in the CSDs; the disadvantages from one to the next are weight, price, and hazardous materials. Where will the technological breakthrough occur? Quite clearly, across much of the globe solar power is readily available, and there is much research work occurring in this field; it seems that the best long term solution may be solar. In the shorter-to-medium term there may be improvements in the manufacturing of batteries, so that the amount of hazardous material can be continuously lowered.

6. Ability to be shipped easily and safely—this concern is primarily about batteries and hazardous materials, as well as some about the imposition of duties by various global Customs Authorities. Technological advances will impact the content and the configuration of the batteries being used in CSDs, but the pace of relevant changes for the CSD Industry has been extremely slow, because the size and activity in the actual market has not been able to devote large resources to solving this problem. The issue of being declared as an "Instrument of International Trade," when shipped by themselves, unattached to a cargo

conveyance, is just now, through the SMART-CM Project and other EU efforts, being raised for possible action in the WCO.

4.4. CSD Communications

4.4.1. Long-Range

Communications between the CSD and its base system while on land is today fairly easily accomplished. Each CSD has at least one means of long-range communications.

The new application of long-range communications technology will be enabling the individual container to communicate from the sea to the home system. Here there has been a steady stream of technological advances that, while often designed for other purposes, may allow much greater direct contact than today.

1. There are the satellite communications networks that exist today, including GlobalStar, Iridium, Orbcomm, Inmarsat, and others; these allow communications from ship to shore, but have no connectivity if the CSD cannot see the sky. At one time the concept of "ad hoc mesh networks," such as can be enabled by ZigBee short-range wireless communications seemed a good solution to this problem, but the lack of density of containers so equipped has meant that this concept has had very little field testing by any of the providers.

2. GSM cellular has been proven to be effective, but only when the ship is near a land mass with an appropriate cellular network; this limits it effectiveness considerably for this particular purpose

3. Several providers are now producing equipment for on-board ships which will enable GSM cellular communications through an on-board ship receiver which will process the signals into a format which can be sent over the long-standing ship to shore Inmarsat Communications network, which is in nearly constant use by the ship itself.

While the stakeholders are of the opinion that in the 2014-2017 timeframe, probably later rather than earlier, CSDs will be used on 25% of all international reefer shipments[45], it is not at all clear that the shipping lines will facilitate the ship to shore communications, or if they will simply neither facilitate nor block such messaging. Perhaps one or two lines in the industry will see this technology as a way to both increase service to the actual cargo owners through the sharing of the information about the container cargo conditions, including the security of the cargo, through the CSD reporting; this would also present the opportunity for the ship's cargo to be cleared through Customs faster than cargo whose containers were not able to report their security status through the ship voyage portion of its journey. This would then also have the serendipitous effect of allowing the cargo owner, and all of the container's other stakeholders—the forwarder, the 3PL, the shipper, the recipient, the CSD monitoring service—to supplement the ship's crew and the liner's operations staff to watch for anomalies in the condition reports, and to motivate the ship's crew to correct any anomalies

[45] CSD Industry Stakeholders Survey, August, 2011

immediately while still at sea, rather than waiting until the ship docks. This would be immediately beneficial to refrigerated shipments; for dry goods containers the value will require further study.

4.4.2. Short-Range

As with long-range communications, the CSD industry will only be utilizing short-range communication technologies created for other reasons, rather than being able to support technological advances intended for this industry alone. Until quite recently there were three primary short-range communications methods in the industry:

1. Bluetooth
2. ZigBee
3. No short-range communications

Bluetooth is a communications protocol which was created for voice; therefore it has very high requirements for speed and capacity, and is as a consequence a heavy user of power; this can be a disadvantage for CSDs.

ZigBee is a particular variation of IEEE 802.15.4 communications standard, with both supporters and non-supporters in the industry; it has not achieved substantial utilization, but is still an effective method.

By "no short-range communications" is meant that some CSD manufacturers have chosen to depend on the cellular communications capability of the CSD for all communications purposes. This simplifies the construction of the device, the coding of the firmware,[46] and lowers the cost versus what the device might otherwise cost.

There are two additional communications standards that are currently being considered—one has been implemented in the East African Community, and the second will be field tested by the US Department of Homeland Security (US DHS) in a major field trial between May, 2012 and April, 2014. In the East African Community, Kenya is implementing a container tracking system for containers entering the country through either road or sea. A CSD is placed on the conveyance upon entry into the country; it communicates by GPRS while on its journey through the country; it communicates at short-range to any Kenya Revenue Authority (KRA) agent by Active-RFID (ISO 18000-7) at particular locations, including at the borders as the vehicle is exiting the country, and the CSD is retrieved.[47]

[46] Software used by the components of the device for their own operation.
[47] http://www.kra.go.ke/notices/pdf2010/ImplementationofECTS.pdf ; http://www.kta.co.ke/index.php?option=com_content&view=article&id=142:electronic-cargo-tracking-systemects-kra&catid=48:kta

The planned US DHS trial[48] will use CSDs that do not have long-range communications capability, but which do communicate at short-range by IEEE 802.15.4 to the DHS readers, but in the least restrictive standard format rather than the ZigBee protocol version. This will restrict the field trial to only this type of communications. However, in the future beyond 2014, if the US Customs & Border Protection Agency accepts the system for nationwide roll-out, CSD providers are to be able to use cellular communications. The data provided will be of use in the Customs clearance process only with adherence to the strict communications security protocols also being verified in this trial. The US system being trialed makes no use of any data provided outside of the strict communication protocols being designated. These require that the CSD be reporting data to US CBP that the CSD manufacturer's system cannot verify or correct, since the communications security keys are not known to the CSD system provider. This system also requires that all data required by CBP be stored on the CSD itself until communicated to the CBP system at or just before approaching the US border gate.

The market is not dictating one particular communications standard for all CSDs, and there is no indication that this will change in either the short or the medium term. The market strongly disagrees with "reader dependent systems" dominating the future[49], since that would eliminate the possibility of ubiquity of coverage; but the CSD-based Revenue Authority border system that Kenya is installing and the similar system that the USA will be testing both use readers as important data collectors, and both allow for long-range cellular communications as additional communications—required in Kenya but not in the USA.

The US DHS trial is very restrictive with its proposed security procedures for data communications. Whether it is the short-range 802.15.4 or the long-range cellular communications that are used by the particular CSD, the US DHS system will control the security keys used by the CSD in its messaging, and the data thus stored for transmission to the DHS System will not be accessible by the CSD home system; the home system can store and transmit its own version of the data, but that is not what will be transmitted to the proposed US system.

4.5. CSD Data Security

The industry stakeholders believe strongly that CSD data security will be an increasingly important issue as the industry seeks to protect international trade and to facilitate regulatory authorities' ability to assess risk and to speed the clearing of non-risky shipments.[50] For Project SMART-CM, the

[48] "Secure Transit Corridors," presentation by Ken Concepcion, US DHS, 29 June, 2011, at the US DHS sponsored Cargo Security Supply Chain Industry Day, held in Crystal City, Arlington, VA, USA
[49] CSD Industry Stakeholders Survey, August, 2011
[50] Ibid.

messaging protocols and security standards have been well documented,[51] and have been proposed as the industry standard in the CEN Working Agreement (CWA) being created by the CEN Workshop on CSD Standards.[52] The proposed system in the USA, described briefly above, has one of the highest levels of communication security in any system being proposed at this time.

The US system which is planned to be field tested is, at first glance, seemingly quite proprietary and exclusive. However, the cellular communication method which has been proposed for future phases will allow most CSDs to participate in the US system. Unfortunately, since this will not be tested until 2012-14, and the test will not, at least during the earliest part, will not be testing the cellular communications process, it is not possible at this time to assess either its inclusiveness or its effectiveness.

4.6. CSD Costs

Just as has occurred with most every type of electronic technology, the prices of CSDs and their components will be dropping over time, as production capacity and efficiency increase. The industry stakeholders believe that prices will drop by half or more by the beginning of 2016.[53] This is the third most important factor which will lead to widespread adoption of CSD, number one being commercial value and number 2 being regulatory requirements.[54]

Cost is important for several reasons. Mass production will result in lower costs than the current production process, which for most CSD manufacturers is small lot production quantities, sometimes still performed by the manufacturing prototyping group, rather than a normal volume production group within the same or a different facility.

[51] "Protocol Standardization: Exchange of Security Status Information Between a Container Tracking & Security Device (CSD) and the SMART-CM Middleware Platform," by Tom Goovaerts, Sam Michiels and Wouter Joosen, DistriNet Research Group, K.U.Leuven, March 30, 2011
[52] CEN CWA 15-06-2011 or revised document number
[53] CSD Industry Stakeholders Survey, August, 2011
[54] Ibid.

5. Sensors

5.1 Types of Sensors

There many different sensors that can be included as part of the sensor package in CSDs. Sensors giving data about the Security Status of the conveyance include:

1. Door Position sensor
2. Optic sensor
3. Audio sensor
4. Device tampering sensor(s)
5. Motion sensor
6. Conveyance enclosure integrity sensor (penetration sensor)
7. “Container empty” sensor
8. Various chemical sensors
9. Various biological sensors
10. Various nuclear sensors

Of course each of these sensors can serve additional functions beyond security. There are also additional sensors which can be used by the CSD for a variety of other purposes, some environmental, some for safety, and some for detection of normally non-lethal contraband, including human cargo. These include:

1. Temperature
2. Humidity
3. Accelerometer
4. Vibration sensor
5. Weight sensor(s)
6. Power status
7. Carbon Dioxide sensor
8. Infrared sensor
9. Sensors to detect presence of various hazardous substances

Over time there will be more and more types of sensors for various purposes. There exist at least lab prototypes of all of the sensors described above, but many, especially the chemical, biological, and nuclear sensors, are not yet able to be manufactured and sold for prices which will encourage commercial adoption.

Each of these sensors should be commercially available during the next six to eight years. The one sensor which the current CSD industry stakeholders estimate will not be available until the year 2019 or later is an effective, commercially affordable sensor or sensor array capable of detecting a 2 cm diameter penetration of any of the six-sides of the container.

Approximate Commercial Availability	Type of Sensor
early 2015	Human cargo
mid-2015	Container (or trailer) empty
early 2016	Chemical threat
early 2016	Biological threat
early 2016	Nuclear weapon
mid-2016	True six-sided penetration sensing--10 cm diameter
mid-2016	Illicit drugs
2019 (earliest)	True six-sided penetration sensing--2 cm diameter

Table 2:[55] Estimated Sensor Availability

The types of functionality considered to be the minimum for basic security purposes, are Time stamp, Date stamp, Global Position, and door position indicator. These were the security requirements in the Project SMART-CM field trials. There are several other types of sensors which are security condition indicators for the conveyance or for the cargo, including optic (presence of light), occasionally audio, “Hall Effect” and other sophisticated sensors detecting one type of change or another for tamper detection purposes. Carbon dioxide sensors or infrared sensors can be used to detect the presence of human cargo.

There are a number of other sensors which provide security for the handlers of the conveyance or bystanders—“Homeland Security.” These include nuclear substance detectors, biological threat detectors, and chemical detectors. Industry stakeholders generally agree that these particular kinds of detectors will become available in affordable quantities in the 2014-2017 timeframe.[56] While much of the market considers these sensor capabilities as defense against rogue terrorist type threats, each of these may play a virtuous role much more often by detecting leakage from specialized shipping vessels for nuclear medical and power generation waste, many types of specialized chemical shipments (not only Chlorine), and biological substance shipments of all types.

[55] CSD Industry Stakeholders Survey, August, 2011
[56] Ibid.

5.2. Sensor Management

Sensor capabilities are of course basic—without the sensor for XYZ we have no data about XYZ; but the development which will greatly enhance the value of these individual sensors will be the study of the relationships amongst the various sensors—how the data is supported and the observations/conclusions strengthened by the simultaneous readings of the data from other sensors, and then the application of the combined information to produce a more complete understanding of the physical environment, the observation of which each sensor can only report on one or two actual dimensions.

This type of analysis is today most easily accomplished in the CSD "back-office" management system; in the future, given the availability of extremely powerful processors ("computer "chips") of increasingly smaller size and lower cost, more of the real-time local analysis will be able to take place nearly instantaneously in the CSD itself. Some early uses of this capability are the installation of geo-zoning data and geo-zoning business commands in some CSDs coming to market in late 2011 and more in 2012.[57]

Another sensor management capability under consideration is to enable the sensors to engage in some type of "self-regulation." One example is for accelerometers. Certain of these must be installed very precisely in the device, and the device in the conveyance, in order to accurately report in which direction did a shock occur—up/down, front/back, or side-to-side. The value of this sensor would be greatly enhanced by allowing the device or the accelerometer to determine at which angle & position the device has been installed, and therefore how to understand the observations reported by the CSD.

[57] Industry interviews, confidential.

6. Value Proposition and Data Management Techniques

6.1. Regulatory Value

Regulatory authorities anticipate deriving value from the Global CSD System through the assurance of the physical security of each container load from the initial cargo loading ("stuffing") into the container until its declaration for entry at their border. In the current global system, each country has its own filing requirements and procedures, although the European Union has made progress toward having a unified system across all member nations. However, the current system does not have requirements for or method for utilizing the type of data that CSDs provide--that of an in-transit record of any security-related alerts or events. This new data will enhance the security risk assessments that Customs Agencies must make every day, adding a new type of security data to the other information that is part of today's Customs filings. For many regulatory agencies this value is sufficient to justify the encouragement of adoption by commercial participants in international trade.

However, it important to realize that there are additional points of value which can accrue to all regulatory participants in a globally networked system of Customs filing information. For example, if commercial participants need only to submit their CSD operational data to one system, for example to the Neutral Platform built by Project SMART-CM, and all nations had access to the Neutral Platform data, the authorities would have the assurance that the data would not be changing based on which country is accessing the data. This methodology would be far different from the current process in which each filing is unique, country to country, with the possibility for simple clerical errors to introduce different information on each of the multiple filings for one single container.

But suppose another commercial stakeholder communicates with the SICUS database instead; how then does the requesting country obtain that data from a different data source besides the "normal" in a secure manner?

Fortunately, there is already exemplary model system architecture for making a system like this operate properly. This is the system architecture for the Global Data Synchronization Network (GDSN), a consumer goods / retail system administered by the global GS1 organization, which we describe below.

6.2. International regulatory cooperation

The GDSN network is currently in operation; it is in place for the global storage and global accessing of consumer goods SKU (stock keeping unit) information.

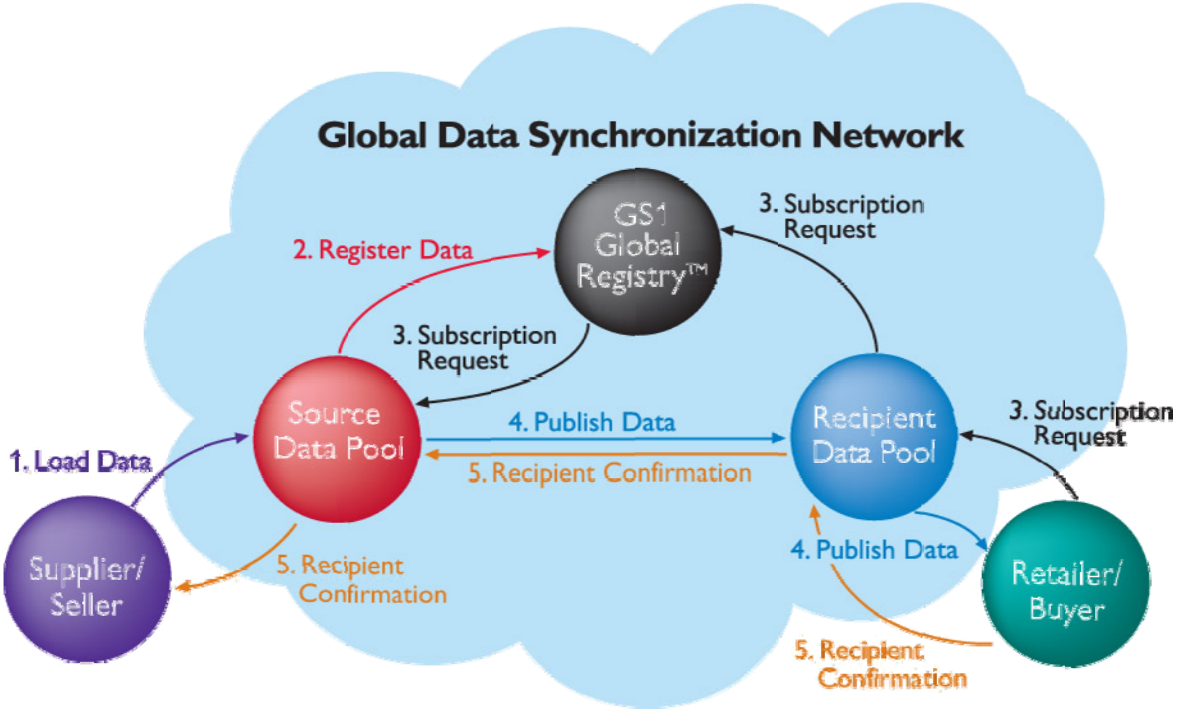

Figure 1: Conceptual Model of the Global Data Synchronization Network (GDSN)[58]

The system operates according to the following process[59]:

1. **Load Data:** The Supplier/Seller (*data source*) registers product and company information in the data pool in which it is a member.

2. **Register Data:** A small subset of this data is then sent to the GS1 Global Registry, which serves as the directory service, maintaining the information about the location of each SKU record.

3. **Subscription Request:** The Retailer/Buyer (*data recipient*), through its own data pool membership, subscribes to a seller's GLN (Global Location Number), product category (GPC—Global Product Classification), target market, or GTIN (Global Trade Item Number) to receive the corresponding product and company information. Using the GS1 Global Registry, the data pool containing the requested item and location information is identified and the subscription is forwarded to that data pool.

[58] "What is GS1?" presentation by Anders Grangård, Director GS1 e~Com for GS1 Global, 1 June, 2011, at the Second Plenary Session of the CEN Workshop on Container Security & Tracking Devices, Brussels, BE, page 6.
[59] Ibid., page 7.

4. **Publish Data:** The seller's data pool then publishes the complete item and party information to the buyer via the buyer's data pool.

5. **Recipient Confirmation:** The buyer then sends a confirmation to the seller through the buyer's data pool directly to the seller's data pool. More than simply an acknowledgement, it informs the supplier of the action taken by the retailer on the item information.

There is at the present time no equivalent "Global Neutral Platform" directory service for the Global Container Security System (GCSS), but one first step towards this type of a system architecture has already been taken between the SICUS platform and the SMART-CM Neutral Layer, in that these two "data pools" have exchanged data in both directions.[60] This is a critical step towards interoperability between Neutral Platforms, and could be one of the greatest points of value for the combined work of both project teams, given the criticality of interoperability to the establishment of an effective global system of Supply Chain Security through real-time Risk Assessment by global Regulatory Authorities.

6.3. Technology of I/T System Architecture: Impact of "the cloud"

The recent development of "the cloud" in the world of I/T systems' architectures can be an enabler of the architecture that was described above. For global regulatory authorities "the cloud" should allow the creation of much less expensive systems than were created in the past. Before this era of "data sharing." the accessibility of the data was difficult to achieve in older style "one-to-one" types system architectures, which is in most nations the current systems architecture.

The issue that will then be critical above all others will be the security of the data, the integrity and the accuracy of the data, and the accessibility to only properly credentialed users. There are various solutions in use, and doubtlessly more that will enter the market—not the concern of this discussion—rather, that solutions to this issue be reached is our concern.

There is an additional factor which must also be overcome with regard to regulatory agencies use of this data. It is an opportunity which is created by the CSD data and the system architecture cited.

Former US Secretary of Homeland Security stated the opportunity clearly in a recent public appearance in Washington, DC:

> We need to create a culture of intelligence-sharing where everyone feels empowered to hit the send button, to share -- not less: It's trying to go from the Cold War culture of need-to-know to the 21st century, a culture of disclosure, need-to-share.[61]

[60] "Minutes of Second Plenary Session of the CEN Workshop on Container Security & Tracking Devices (Smart CM)"; Brussels, 01/06/2011**;** SMART-CM Project document N 0020, page 4.

[61] CQ NEWSMAKER TRANSCRIPTS, "Former Secretary of Homeland Security Tom Ridge and Current Secretary of Homeland Security Janet Napolitano Deliver Remarks at U.S. Chamber of Commerce," Special Events, Aug. 17, 2011

6.4. Commercial Data Utilization

As cited in Chapter 2, despite the concern by commercial participants in international trade about the security of their shipments, spending resources on security systems or equipment is often viewed as only a cost, with very little commercial financial value.[62] The survey undertaken for this analysis revealed very clearly that commercial operators would invest in a CSD system first and foremost if the commercial business value is understood by shippers and other stakeholders in the trading process.[63]

To quote one prominent CSD industry provider, Dr. Christian Bogatu (Managing Director, Kirsen Global Security):

> "In 2006, we shifted all our focus on the realization of tangible monetary customer benefits, [and away from a focus on US DHS requirements for security]. This has been the superior strategy, and now we successfully realize financial value for our customers that far exceeds their CSD system costs.
>
> While the main driver of benefit comes from a reduction of up to 30% in insurance premium expense for our customers, there are multiple additional benefits—higher confidence in actual operational performance to better planning tools and even reduction of safety stock. Now, that said, we have recently seen an increased possibility of the old dream of the Green Lane – ie. the expedited customs clearance process at borders for users of smart container systems... This would give an additional boost to the industry and hence result in more efficient logistics coupled with higher security standards, from which in turn society as a whole will benefit ultimately."[64]

This finding is supported by another recent market survey, this one completed by Logistics Management magazine on behalf of Management Dynamics, Inc. in March, 2011.[65] In their listing of "Ways Shippers are Managing & Containing Costs,"[66] no less than four (4) of the top ten actions are actions which can be facilitated either completely or in part by the use of CSDs:

1. Identifying most efficient shipping routes
2. Adopting KPIs/Performance metrics for carriers
3. Improving decision-making, better planning, reporting
4. Better container and shipment tracking tools

Several academic researchers have taken a necessarily more rigorous approach towards analysing the commercial value of the CSD-provided data[67] [68]. Industry stakeholders are also starting to publish results which have been observed in client trials of CSD systems.[69]

---

[62] Smart Boxes, by AT Kearney & Co., 2005, page 2, 9.
[63] CSD Industry Stakeholders Survey, August, 2011
[64] Interview with Dr. Bogatu, 19 September, 2011.
[65] "Current Trends and the Potential for Automation in International Transportation Management," published as a white paper by Management Dynamics, Inc., 2011.
[66] Ibid, page 4.
[67] C. Bogatu, (2008), The Smart Container business case as an answer to security-related and logistical challenges, PhD Dissertation, University of Technology, Berlin) http://www.buchhandel.de/detailansicht.aspx?isbn=9783798320741
[68] T. Kelepouris, (2008), The Value of Supply Chain Tracking Information, PhD Dissertation, University of Cambridge, Department of Engineering

Data management capabilities have made substantial improvements since electronic data transmission was first made possible. The challenge from CSDs is the sheer volume of data that will be generated for every container and lorrie and rail wagon that is carrying freight; the volumetric increases in supply chain operating data will be analogous to the increase of SKU/location/date/time sales data that could be captured only with the installation of POS terminals replacing cash registers. Fortunately the advances in data storage and analysis that took place at the time that new demand side data from POS terminals was suddenly being generated can be easily adapted for the new data being generated by CSDs.

This process of examining the potential value of data provided by CSDs—both security and other environmental data, as well as the types of information that can be developed from this data and perhaps integration with other information already in existence—is currently underway around the world. Consider the context—new data previously not available due simply to the lack of the technologies which would enable this collection, recording, and transmission: consider the similar development of similarly granular data in the demand side of International Trade by means of Point-of-Sale terminals replacing old-fashioned cash registers, such as took place in the 1970's and 1980's.

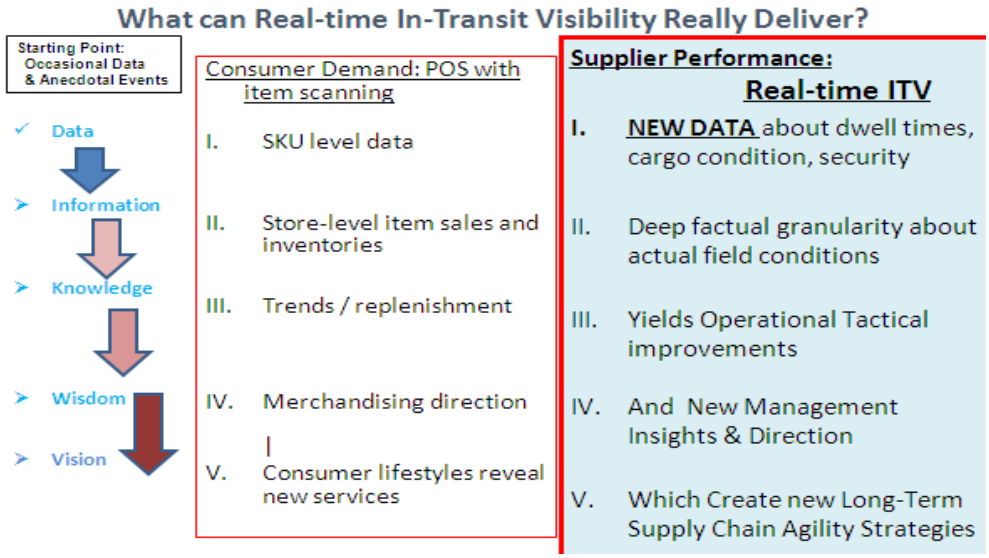

Figure 2:
Value of New Supply Chain Data—parallel comparison with New Demand Chain Data[70]

The adoption of Point-of-Sale terminals was not an overnight phenomenon in the retail industry. The organizations that tested the value of such an investment and encouraged experimentation and analysis using this new data derived huge commercial value, and the uses for this Demand side data continue to be expanded today, forty years or more after it was first provided.

[69] McKinney, J. and Radford, A., the CIP Report, George Mason University School of Law Center for Infrastructure Protection and Homeland Security, July, 2011, revised by the authors October, 2011
[70] Ibid., page 15

Container Security Devices, in their expanded commercial role as Commercial Monitoring Devices, are now for the first time providing similarly granular Supply side data to fill the one remaining major gap in Supply Chain operations data—In-Transit Visibility—enroute, between transportation nodes or milestones, with real-time alerts and regular status messages (so-called "heartbeat messages".) The analysis of this data, while not strictly speaking a technological issue, is a critical constraint / bottleneck on the "Technological Adoption Curve" for CSD technology, since failure to uncover the business value will in fact restrict or perhaps even prevent adoption. This is, in mathematical terminology, a "necessary and sufficient condition" for adoption. That is to say, if the commercial value for the use of CSDs can be established and accepted in the international commercial community, then the technology will be put into use with or without regulatory requirements. The opportunity for regulators to then tap into this data, or perhaps to request one or 2 additional data points to be collected at the same time as the commercially important environmental data, is here now.

Another factor which will be important in the commercial adoption of CSDs is the software which will manage the data. There are two versions of this question:

1. The CSD Management System—the "back office"—the system that receives the data transmitted by the CSD from "the field."
2. The Supply Chain Management (SCM) software currently in place at the commercial stakeholder's organization, and how that SCM utilizes the information provided by the CSDs.

In the CSD Management Systems in use currently, there are several levels of system capabilities:

a. Asset Management—for the conveyance, or for the CSD
b. Location reporting only
c. Location and security status only
d. Shipment environmental information
e. CSD data management and analysis

As these systems develop, they are moving from type "a" though "b," "c," and "d" until "e." Techniques differ, the speed of development differs, and so forth, but this is the evolution that is being seen.
Supply Chain Management (SCM) software includes Warehouse Management Systems (WMS), Transportation Management Systems (TMS), Trade Compliance Systems, and Supply Chain Planning Systems. For the SCM software currently in place at many of the commercial stakeholders' organizations, there are several options for utilizing this new data:

a. For "Event Management" processes
b. For normal Supply Chain Management purposes
c. For Supply Chain Partner performance measurement

There are many providers of these types of systems, serving particular industries or logistics needs, such as cold chain management and so forth. At least one of the major software system providers, SAP,[71] does explicitly have a function which is currently able to accept CSD data as part of the supply chain operations process. This is not a "necessary condition" for CSD technology adoption, but it would be a good facilitator of adoption once it is place.

When will the CSD industry achieve 25% use on:	
international refrigerated shipments (container or trailer)?	2014-15
international dry goods shipments valued at > 250,000 euros?	2016-17
international dry goods shipments valued between 250,000 and 25,000 euros?	2018-20
international dry goods shipments valued at < 25,000 euros?	2021 or later
domestic refrigerated shipments (container or trailer)?	2016-17
domestic dry goods shipments valued at > 250,000 euros?	2016-17
domestic dry goods shipments valued between 250,000 and 25,000 euros?	2018-20
domestic dry goods shipments valued at < 25,000 euros?	2021 or later

Table 3: CSD Adoption Forecast by Shipment Type and Value[72]

[71] http://help.sap.com/saphelp_em51/helpdata/en/3f/09233d32039017e10000000a114084/content.htm
[72] CSD Industry Stakeholders Survey, August, 2011

6.5. Broader Societal and Ecological Contributions of CSDs

It is only with widespread adoption that the CSD System will be able to begin to deliver against its most interesting long-term economic and social benefits, including more efficient asset and materials utilization. Whatever it is that we will call this Industry in the future, it may well become the most efficient means of delivering sustainable resource usage to the future.

According to Michael Dietmar,[73] the Director of Seafreight Product Management for DB Schenker in Essen, Germany, the use of Conveyance Monitoring Devices will be the best way to record all of the resource utilization and efficiency information that today can only at best be estimated based on gross generalizations about efficiency and so forth. As just one prominent example he cites the desire to lower carbon emissions: today these calculations are a huge exercise in application of various types of data which has normally been sourced by some means other than direct measurement, and is there really any way to verify the veracity of any of this information? This is just one example of an area in which direct collection of field generated data by remote sensors container in a CSD (or the more broadly defined "Conveyance Monitoring Device").

[73] Direct interview, 16 September, 2011

7. Conclusions

The invention of Container Security Devices was part of slowly developing global trend towards becoming increasingly accurate in accounting for corporate assets. To the tracking function multiple kinds of security sensors were added in direct response to global terrorist threats. To the security sensors various environmental sensors were added, thereby giving the CSD a multitude of potential commercial applications.

The CSD technology is still improving, and has important steps still being needed—especially in the issues of weight, ease of handling, power management, battery safety, and a number of sensors that are not yet available at appropriate broad market prices.

Nevertheless certain conclusions are appropriate:

1. CSDs can improve Supply Chain Security from threats of indiscriminate violence
2. CSDs can improve Supply Chain Security from petty criminal activity
3. CSD technology does yield provable commercial business benefits, but these results are only recently becoming publicized; therefore, many commercial organizations have not yet been able to understand or accept said value to their own satisfaction.
4. By adding data and information to the largest current gap in Supply Chain Operating data, CSDs will be providing newly revealed opportunities for cost savings and inventory savings.
5. CSD usage will increase over time as a result of a number of factors:
    a. Commercial value becoming known and provable
    b. Regulatory agency acceptance of CSD security-related data as support for proper risk-assessment and then quick clearing of shipments at borders
    c. Commercial SCM software providers accepting and using CSD data for supply chain management processes
    d. Large reductions in price

Annex

Industry Stakeholders interviewed:

1. Christian Bogatu, Managing Director, Kirsen Security Solutions
2. Ken Concepcion, US Department of Homeland Security
3. Michael Dietmar, Project Management, Sea Freight, DB Schenker
4. Andreas Döring, Strategic Projects, Bosch Sicherheitssysteme GmbH
5. Robert Draper, Managing Director, AeroStrategies SPRL
6. Eric Gill, Programme Director, SAVI Technologies
7. Rick Gabrielson, Senior Manager, Import Transportation, Target Stores
8. Stefan Holmberg, Project Manager, IKEA
9. Peter Livey, Head of Logistics, Hyundai Merchant Marine (Europe) Ltd.
10. Fabio Lo Curto, Sales Director, euro-helpline AG
11. Richard Meyers, CEO, GlobalTrak, division of System Planning Corporation
12. Rudy Muller, Sales Manager, EPSa
13. Frank Neubauer, Spokesperson, Project ContainIT, EADS Innovation Works
14. Arthur Radford, Sales Director, Agheera, division of DHL
15. Stefan Reidy, Partner & CEO, arviem AG
16. Christopher Regenhardt, Product Manager, DB Schenker
17. Tan Chin Tong, Managing Director, Envotech
18. David Taylor, US Department of Homeland Security
19. Jörn Waterstraat, Systems Engineer, Astrium Space Transportation