Asia-Pacific
Economic Cooperation

2005/STAR/017
Maritime Security Panel 2

International Convergence Trends in Cargo Security

Submitted by: GE

Third Conference on Secure Trade in the APEC Region
Incheon, Korea
25-26 February 2005

International Convergence Trends in Cargo Security

A Discussion Paper by General Electric for STAR III

Executive Summary

Advances in cargo security technology such as the Container Security Device ("CSD") now being commercialised by GE can play an important role in a "layered" system of in-transit cargo security that protects public safety while facilitating trade. In order to reap the benefits of such technological advances, governments do not need directly fund adoption of such systems, but rather must provide adequate systemic advantages such as "green lane" Customs processing to ensure that they are widely adopted by the private sector, and adopt a consistent international framework that facilitates their use in a global, integrated trading system.

Outside the APEC region, the EU and the WCO are making excellent progress towards these goals, through programs such as the development of the Authorised Economic Operator (AEO) and the Framework of Standards to Secure and Facilitate Global Trade. Importantly, such efforts recognize the significant programs already undertaken or under development by US Customs and Border Protection (CBP), such as the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative (CSI) and the 24-hour manifest Rule, and the Swedish StairSec program.

CBP's "Smart Box" program is a large-scale field trial now in operation including major US importers and trade lanes from both Europe and Asia. CBP's intention is to give importers, using "Smart Boxes", the incentive of expedited ("green lane") Customs administration.

GE's CommerceGuard™ container security solution enables the "Smart Box" via its Container Security Device (CSD), which is deployable on both legacy and new containers, affordable at a cost of less than US$10 per shipment, and which provides cargo security, enhanced theft and pilferage protection, increased supply chain visibility, and automated cargo tracking capabilities. With GE's global and licence-free reader network installed by GE at no cost in CSI ports, valuable and actionable data can be transmitted to Customs authorities worldwide.

GE recommends that the APEC Members:

- Encourage near-term development of a framework for a layered approach to In-transit maritime cargo security, including container security devices & other emerging technologies
- Update APEC Member CTAP's and Private Sector Supply Chain Security Guidelines to accommodate in-transit container security layering through these new technologies
- Support & Implement WCO Framework of Standards to Secure and Facilitate Global Trade
- Leverage progress to date
  - Support creation of meaningful Customs incentives, including 'green lane' administration for CSD & TESC containers
  - Facilitate implementation of new solutions demonstrated in programs such as StairSec & CBP Smart Box
  - Implement available solutions, but ensure future expandability
  - Support private-sector financed solutions

Introduction & Overview

Today’s international trade is heavily dependent on intercontinental movements of intermodal freight containers, with over 90% of international freight movements in such containers. Because international trade is truly the lifeblood of the global economy, the container trade lanes can be viewed by analogy as the arteries of economic health, with freight containers carrying the cargo that is the oxygen needed for national economies to survive and prosper.

Seen in this way, it is understandable that potential terrorist enemies would wish to target these arteries, either with the goal of fatally blocking them or perhaps using them to carry lethal instruments of destruction to achieve their goal of disruption of the global economic heartbeat.

General Electric Company (GE) is a large international shipper of containerised goods, a major lessor of freight containers with a worldwide leasing fleet of over 1 million TEU, and a corporate citizen with nearly 350,000 employees in over 100 countries. GE provides financing and insurance for the shipping industry. It is also a leading global technology developer and manufacturer. As such, GE is itself a very large stakeholder in the global economy and trade.

This paper will focus specifically on *in-transit security of intermodal freight containers* from point of stuffing a container to the point of unloading by the consignee. This paper will also capsulate what relevant security policy measures the United States, the European Union and the World Customs Organization are taking, all of which explicitly or implicitly include the concept of providing a “green lane” accelerated Customs clearance to encourage importers to strengthen both physical and electronic container security. GE will then introduce its CommerceGuard™ container security technology and recommend areas where this technology can be also be leveraged within the Secure Trade within the APEC Region (STAR) initiative, consistent with the objectives of these policy initiatives at an economical cost objective of less than US$ 10 per shipment.

US Initiatives

Since the terrorist attacks on September 11, 2001, the US government has taken several measures to increase border and transportation security for cargo imported to the US.

In November 2002, US Congress enacted a statute entitled the “Maritime Transportation Security Act of 2002” (MTSA) directing its Department of Homeland Security (DHS) to “…evaluate and certify secure systems of international intermodal transportation”. It also directed the department to articulate standards for container security, including standards for sealing and locking. In response to this mandate, DHS recently drafted a cargo security strategy in which one of the important elements focused on “secure stuffing procedures and container seals and sensors”, including *container security devices* (CSD’s).

Within DHS, US Customs and Border Protection (CBP) carries the direct responsibility of ensuring freight containers entering US ports do not carry dangerous cargo or terrorist contraband such as weapons of mass destruction (WMD) or their components. As a consequence, CBP has implemented several interrelated container security programs, of which the most salient are:

- Customs-Trade Partnership Against Terrorism (C-TPAT)
- Container Security Initiative (CSI)
- Automated Targeting System (ATS) built on the Automated Commercial Environment (ACE) platform
- “24-hour Manifest Rule” including Automated Manifest System (AMS)
- CBP “Smart Box”

EU Initiatives

In the wake of the terrorist attacks in Europe in 2004, it has become abundantly clear terrorists using transportation means for their attacks (e.g., the train bombing in Spain), is not only an American problem. Since then, the European Union has begun to act decisively in the area of container security. The most significant initiatives are described below.

US-EC Joint Customs Cooperation (JCC)

In November of 2004 the JCC Committee, co-chaired by US CBP Commissioner Bonner and EC Director-General Verrue, adopted the first measures to strengthen security of container transport while facilitating legitimate trade through mutually acceptable, reciprocal security standards and industry partnership programs. A joint working group was established focused in order to:

- agree on minimum standards for EC ports to participate in CSI
- identify best practices concerning security controls of international trade
- define and establish standards for the information required to identify high-risk shipments imported into both the US and EU
- establish reciprocal standards for targeting and screening high-risk shipments,
- include information exchange and the use of automated targeting systems, and
- develop minimum standards for inspection technologies and screening methodologies.

The working group, consisting of national experts, is now progressing towards realisation of the overall objective of mutual reciprocity of measures and standards and will submit its results of proposed actions and recommendations during late Spring 2005.

Authorized Economic Operator (AEO)

In parallel with the JCC the EU has started an initiative called the Authorized Economic Operator (AEO), which is similar to the US C-PTAT program. While the details of this program are still being developed, it is evident that it will build on the same principle as the C-TPAT program. It is foreseeable that incentives for European importers to adopt enhanced container security practices could be similar to CBP's plans for the US importers. Further, it is not unlikely that the Customs authorities in the EU countries will issue similar requirements to obtain "green lane" status of cargo being shipped within the EU, as in to the US, holding out the possibility of a sort of "two-way green-lane", with full reciprocity between the EU and the US.

World Customs Organization (WCO)

In November 2004, the "High Level Strategic Group" within WCO's council adopted several important resolutions as outlined in the "Framework of Standards to Secure and Facilitate Global Trade". The framework is built on two pillars:

1. Customs-to-Customs Pillar
2. Customs-to-Business Pillar

In this framework, it is clear that these emerging WCO standards are truly similar to the ones being developed by the US government, such as targeting, manifest and screening systems (ATS, AMS, ACE). In the second pillar the standard will likely draw from current innovative government-industry programs such as the US C-TPAT program and the Swedish StairSec program. Further, and as stated, the standards will include "…use of smarter, more secure containers".

More interesting is that the framework discusses "procedures that offer incentives to businesses to ensure that they see a benefit to their investment in good security systems and practices, including reduced risk-targeting assessments and inspections, and expedited processing of their goods", which would indicate some sort of a "green lane" concept.

Container Integrity – An International Problem

The integrity of containers during transit is one of the key security risks for commercial shipments not only into the United States, but also into the APEC countries and other destinations. By building upon trust relationships among people, organizations and equipment that are part the supply chain, GE's CommerceGuard™ system specifically addresses this problem to significantly enhance overall container security. By protecting against the threat of any unauthorized entry through the doors of the container, CommerceGuard™ provides an affordable and deployable solution to *verify in-transit intermodal freight container integrity* from point of container stuffing at a foreign factory to point of authorized unloading at the consignee's distribution center at the end of a trip by sea, rail or roadway.

GE brings a *secure systems approach* to container integrity rather than merely a hardware-oriented approach. The system design simultaneously guards global commerce and *enhances transport logistics management* by providing point-to-point container location data and other benefits. Extensive field tests on loaded containers moving by rail, truck, and ship demonstrated that the system met its design goal to keep false alarm rates well below 1% despite harsh container handling and in-transit racking. The cornerstone of this is the container security device (CSD) shown in figure 1.

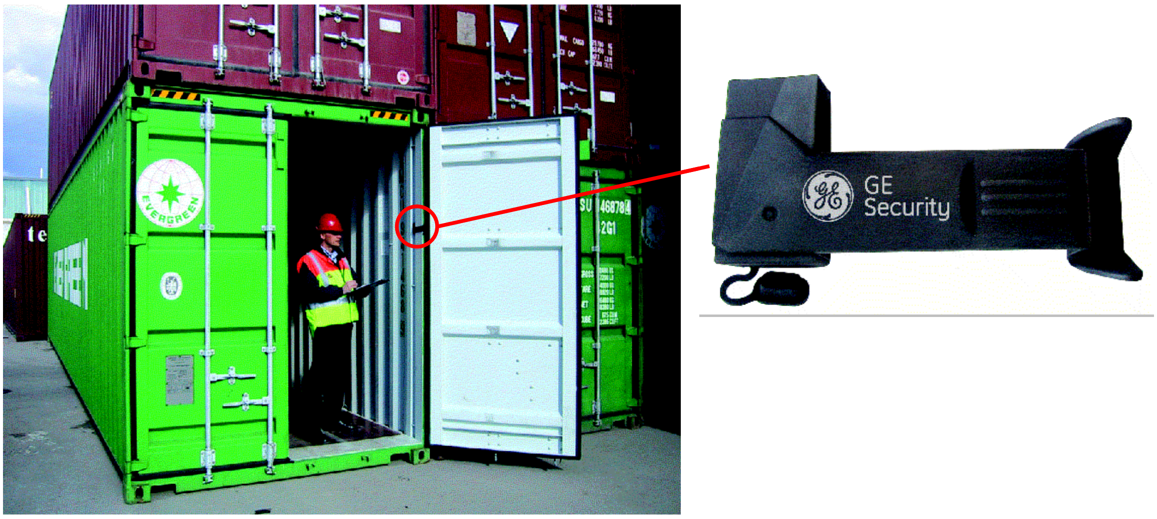


Figure 1: The GE Container Security Device (CSD) is easily retrofitted in the container doorframe

CommerceGuard™ - A European Solution Commercialised by GE

In September 2004, a General Electric subsidiary, GE Security, Inc. – www.gesecurity.com/csd - announced an exclusive technology licensing agreement with All Set Marine Security AB, a Swedish company - www.allset.se/security - see press release in Appendix 1.

The extremely innovative technology was developed in Sweden and the wireless communication platform utilised is a derivative of Bluetooth and was itself developed at Ericsson Research in Germany. The All Set technology had already been deployed in Phase I deployment of the CBP Smart Box in 2004 and by the US Department of Homeland Security for operational testing in Operation Safe Commerce at all three major US container load centres (New York, Los Angeles and Seattle).

GE felt that it could further enhance the overall performance of the All Set solution and initiated a rigorous Six Sigma design review and enhancement program jointly with All Set engineers. In October 2004 GE initiated large-scale validation of the newly redesigned CommerceGuard™ CSD in its own trade lanes in order to verify CommerceGuard in a production transportation environment. Detailed data sheets on CommerceGuard can be found in Appendix 2.

The CommerceGuard™ system features:

- A very low cost CSD that can be universally mounted on the legacy fleet of freight containers that utilizes a new Hall effect sensor to very reliably detect unauthorized door openings of both loaded and empty containers and provides a flexible expansion port for future sensors. With a 10-year operating life, this device can be mounted permanently on the frame of all ISO dry containers without tools in less than one minute. CommerceGuard™ ensures universal availability of the CSD to shippers without the necessity of recycling devices or other special handling.
- Handheld and fixed reader devices with supporting client software systems. These reader devices wirelessly communicate with CSD-equipped containers using the internationally accepted 2.44 GHz ISM (Industrial, Scientific & Medical) frequency band. Readers communicate with the GE monitoring network backbone described below using the public wireless networks (GSM or GPRS), the Internet with local area network support for WiFi, or conventional wired networks. All data communication is securely encrypted.
- A network backbone with global reach to securely monitor and report container location, to electronically arm and disarm CSDs, report security status and alarms and to provide timely notification to concerned parties of such alarms and anomalies. This GE network has been designed with state-of-the art security.

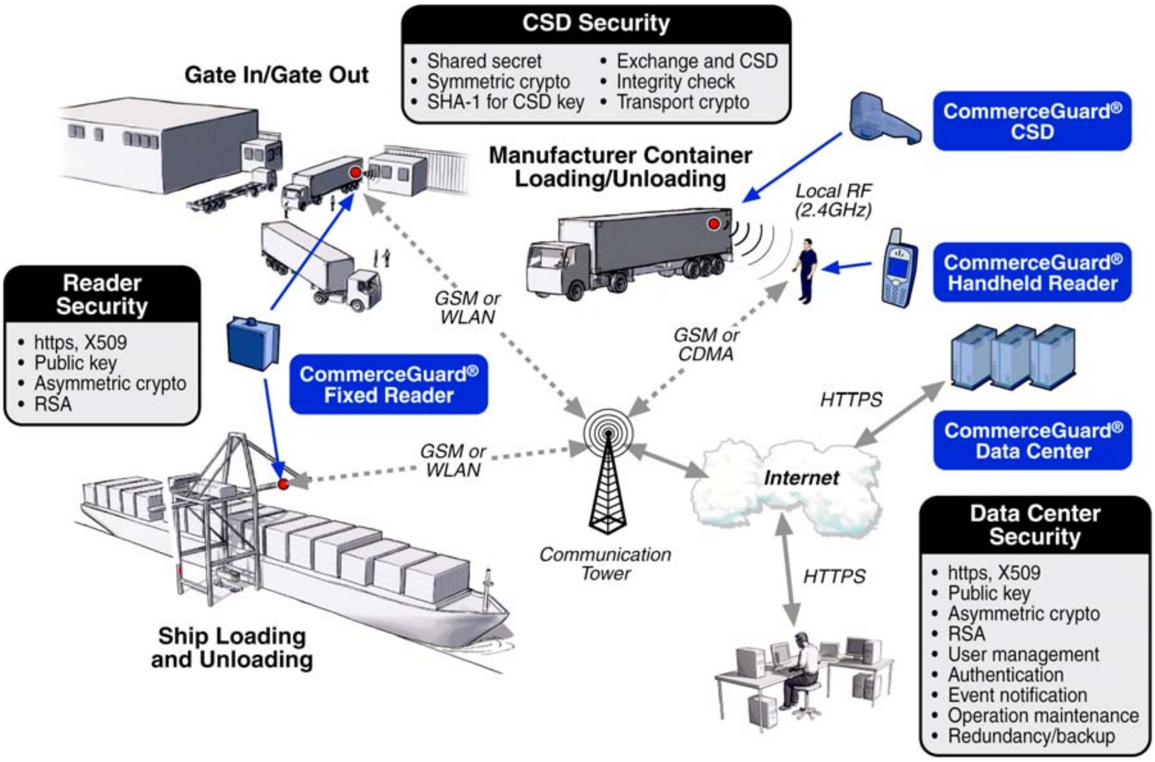


Figure 2: The CommerceGuard system architecture is build on high security standards

CBP “Smart Box” – A “Green-Lane” Pilot Program

US Customs initiated the CBP “Smart Box” program in January of 2004. The purpose of CBP “Smart Box” is to deploy and to evaluate Container Security Device technology into widely different existing trade lanes from Europe and Asia to the United States, using randomly selected legacy containers carrying a variety of cargoes, all in the “normal course of business.” As defined by CBP, the Smart Box must be fitted with:

- A high security bolt seal meeting ISO PAS 17712 in one of three CBP specified alternative locations to the door hasp mechanism and a;
- A Container Security Device that senses any unauthorized intrusions into the container via the doors after arming via an electronic encrypted arming key.

In Phase I, which ran from January to August of 2004, more than 500 moves of fully loaded containers from Europe and Asia were completed. Five large US importers that are already active members of CBP’s C-TPAT (Customs Trade Partnership Against Terrorism) program volunteered to participate in the program. Participants, including field CBP inspectors, received training on CSD mounting, arming, disarming, log file retrieval and other operations in 6 countries.

In preparation for Phase II, CBP requested that GE validate the new third generation CSD. To date GE will have completed over 1000 moves both in its own GE trade lanes and from Europe and South America. In these trade lanes, fixed readers have been installed at the point of stuffing in Europe and at the point of deconsolidation in the US.

Tamper Evident Secure Container – A Next Generation with Strong Asian Support

Between September and December in 2004, GE, Unisys, and China International Marine Containers (CIMC) jointly ran TESC as a private project, see announcement in Appendix 3. CIMC is the world’s largest manufacturer of shipping containers, and over 50 percent of all new containers worldwide are manufactured by CIMC.

The TESC concept consists of a container with an integrated CSD (iCSD), pre-installed in at the container factory and built-in in the container door structure as well as physical enhancements such as alternate mechanical sealing locations, welded hinge pins, etc. More details can be found in the TESC data sheet in Appendix 4.

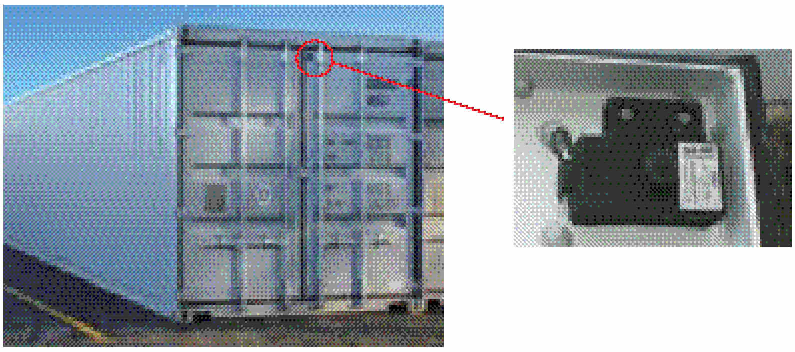


Figure 3: The TESC incorporating the integrated CSD (iCSD) in the container door.

The project involved 18 moves of newly-built TESC in a trade lane from a GE Lighting factory in Shenzhen, China, to a GE distribution centre in California. A fixed reader was installed at the in-gate in the port of Hong Kong verifying that the iCSD installed in TESC’s reported no alarms. When the containers arrived in the port of Long Beach CBP inspectors interrogated the status of the iCSD using the same Handheld Readers they used in CBP “Smart Box” Phase I. Fifteen different tests to attempt to intrude without detection into the container were also made.

Recommendations

GE believes that the above outlined international convergence trends in cargo security policies are a good match with GE's global CommerceGuard solution strategy. GE also believes that not only will there be a "green lane" for CSD equipped containers arriving into the US, but it there will be a virtual "green lane" into the EU and later an "international green lane" in to all countries that adopt the emerging WCO pillars, hopefully including APEC Members.

GE believes the key criteria when designing an effective container security solution include a CSD which:

- Has global applicability without local radio regulatory problems
- In the short term is deployable on existing containers using the retrofit CSD
- In the near term will be a permanent feature of the container itself, not an add-on accessory, so that it is always available to shippers and no recycling is required
- Adds a new layer of security to the container entirely independent of and beyond the mechanical door seal that is both very physically and electronically secure
- Is economical enough for ordinary every day commercial use on all containers, whether loaded or empty
- Easy to apply and integrate in business processes, while respecting the need for business data privacy
- Has valuable data elements that can easily be fed in to with legacy Customs administration systems
- Has non-proprietary expandability to accommodate future in-container sensors or other future technologies

GE also believes that by and large, the users of a transport system in commerce should pay for its costs. In this connection, GE has created a business model that it believes can support the economical but universal deployment and use of CSDs on containerised shipments *without government funding.*

Therefore, GE recommends that:

- In order to achieve wide deployment of container security devices without direct government expenditure, "green lane" and other incentive policies must be developed and implemented in all major trading countries in the context of a consistent global framework based on leveraging the experience already gained in the StairSec and CBP Smart Box programs.
- Every shipment in an intermodal cargo container should eventually be equipped with a CSD. While a CSD adds another layer of security, it will also increase supply chain visibility and benefit participants in the supply chain such as carriers, shippers etc. as well as guard against other shipment irregularities such as pilferage, illegal immigration, etc.
- Existing solutions should be implemented now so long as they are expandable to accommodate future technologies as they are developed and commercialised
- In order to leverage the supply chain benefits as well as to "break the cycle", a global CSD reader infrastructure should be rolled out in all major container port terminals starting with the 34 CSI ports. As part of its overall commitment in this area, General Electric is prepared to invest in and deploy a basic reader network in the CSI ports without cost to the ports.

GE respectfully requests the Third Conference on Secure Trade within the APEC Region to support these recommendations, as they will help fulfil the "twin goals" articulated at the 4th APEC Transportation Ministerial Meeting in July 2004 of enhancing intermodal security while facilitating trade.

APPENDIX 1

GE Infrastructure
Security

Contact:
Jay Pinkert
512.381.2778
jay.pinkert@ge.com

PRESS RELEASE

GE Announces Its Entrance into the Global Cargo Security Market

Intrusion Detection Technology Developed by Swedish Company Helps Protect and Facilitate Global Commerce

AUSTIN, TEXAS – Sept. 13, 2004 GE's Security business (NYSE: GE) announced today that it has begun field testing a cost-effective container security solution for use in maritime shipping. Details of the solution will be rolled out at the U.S. Maritime Security Expo in New York Sept. 14-15.

The GE solution helps detect unauthorized access to a container and monitors the container in transit for signs of intrusion, which helps manufacturers, customs officials and importers protect container integrity throughout the supply chain.

The container security device component of the overall system was developed by Sweden-based All Set Marine Security AB, and has been tested by the U.S. government and private industry. The capabilities of the device are amplified through GE's access control platform and sensor suites, and the company's expertise in wireless handheld transactional software and data management networks.

More than 90 percent of all goods moved internationally are carried in containers, and around 8 million freight containers arrive at U.S. ports each year. The GE solution will establish a global mechanism for in-transit freight container security for all classes of cargo, without impeding the movement of international trade.

"The future of global commerce depends on the ability of the shipping industry and government agencies to improve cargo security while facilitating the efficient flow of goods," said Greg Burge, President of Networked Services for GE's Security business. "As one of the world's leading shippers and container lessors, GE has a significant stake in developing and deploying a safe, reliable and cost-effective global solution."

The palm-sized container security device (CSD) easily fastens without special tools to the door jamb inside any standard maritime container. The cargo's manufacturer uses a wireless handheld device to arm the device with a unique identifier code.

The CSD automatically communicates its status to fixed wireless readers at ports, indicating when and where the container has been opened since it was initially sealed. Customs officials can also inspect the cargo at any time using a special handheld wireless device to arm and disarm the CSD. When the container is delivered, the importer verifies the access record and disarms the CSD prior to opening.

All data is stored and managed through a secure information backbone. Communication between wireless readers and container security devices is encrypted, as are all transaction records.

"GE is uniquely positioned to lead the development of a global solution because of its capabilities in high-volume manufacturing, commercial deployment, technology integration and customer support," said Burge.

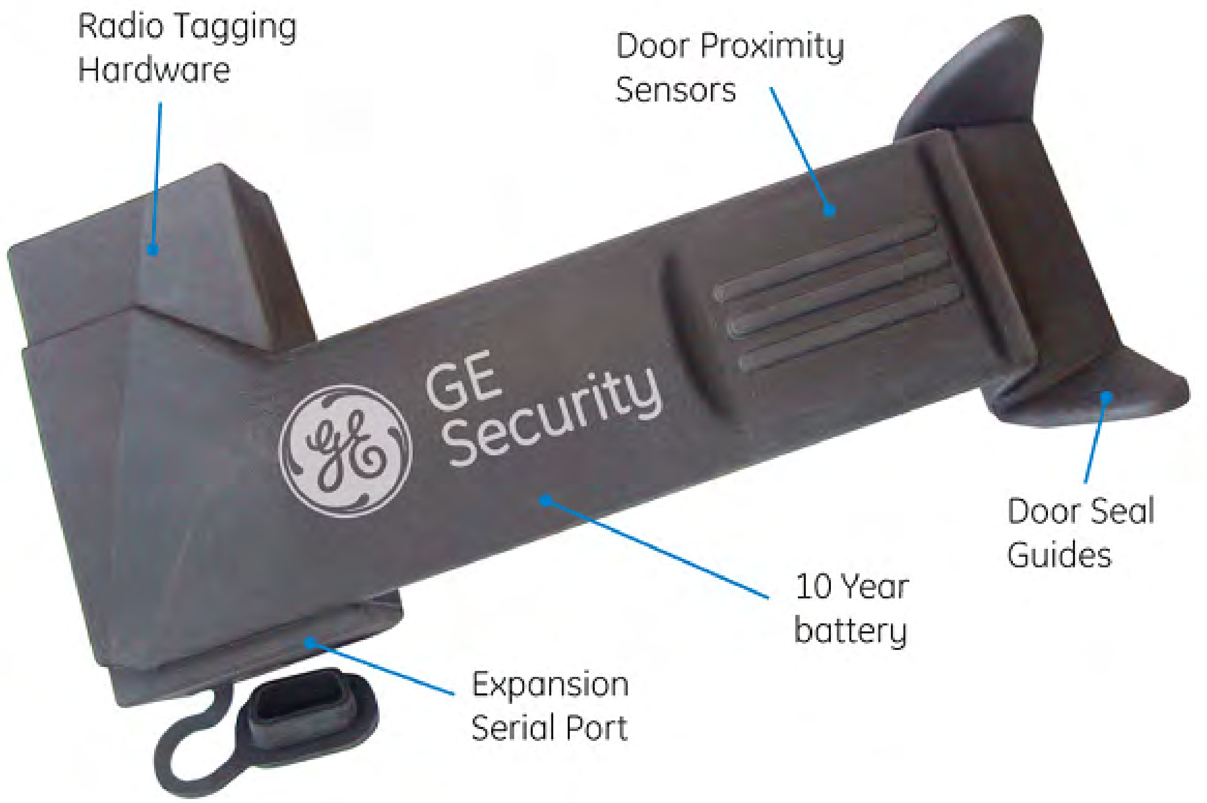
About GE Infrastructure, Security
The Security business of GE Infrastructure is a wholly owned subsidiary of the General Electric Company focused on communication and information technologies for security, safety and lifestyle enhancements. It has operations in more than 30 countries and is represented by some of the best-known brand names for intrusion and fire detection, access and building control, video surveillance, explosive and drug detection, key management, and structured wiring. For more information about GE's Security business and our product offerings, please visit www.gesecurity.com.

GE Infrastructure is a high-technology platform comprised of some of GE's fastest-growing businesses. These global businesses offer a set of infrastructure protection and productivity solutions to some of the most pressing issues that industries face: pure water, safe facilities, plant automation, and sensing applications in the operating environment. GE Infrastructure is headquartered in Wilton, CT. Learn more at www.geinfrastructure.com .

###

CommerceGuard™ Container Security Device (CSD)

APPENDIX 2

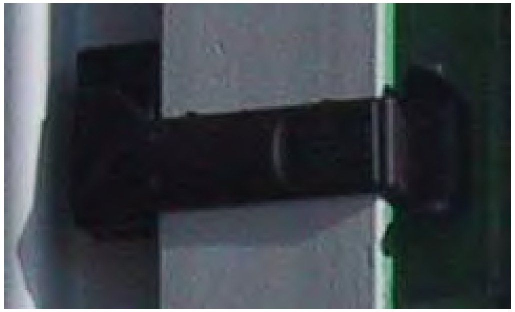


CSD Placement in Cargo Container

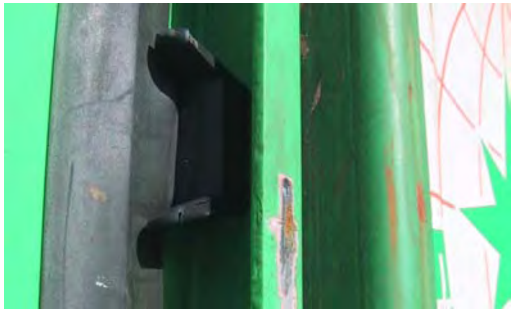
imagination at work

CSD Mounting

Opened Door



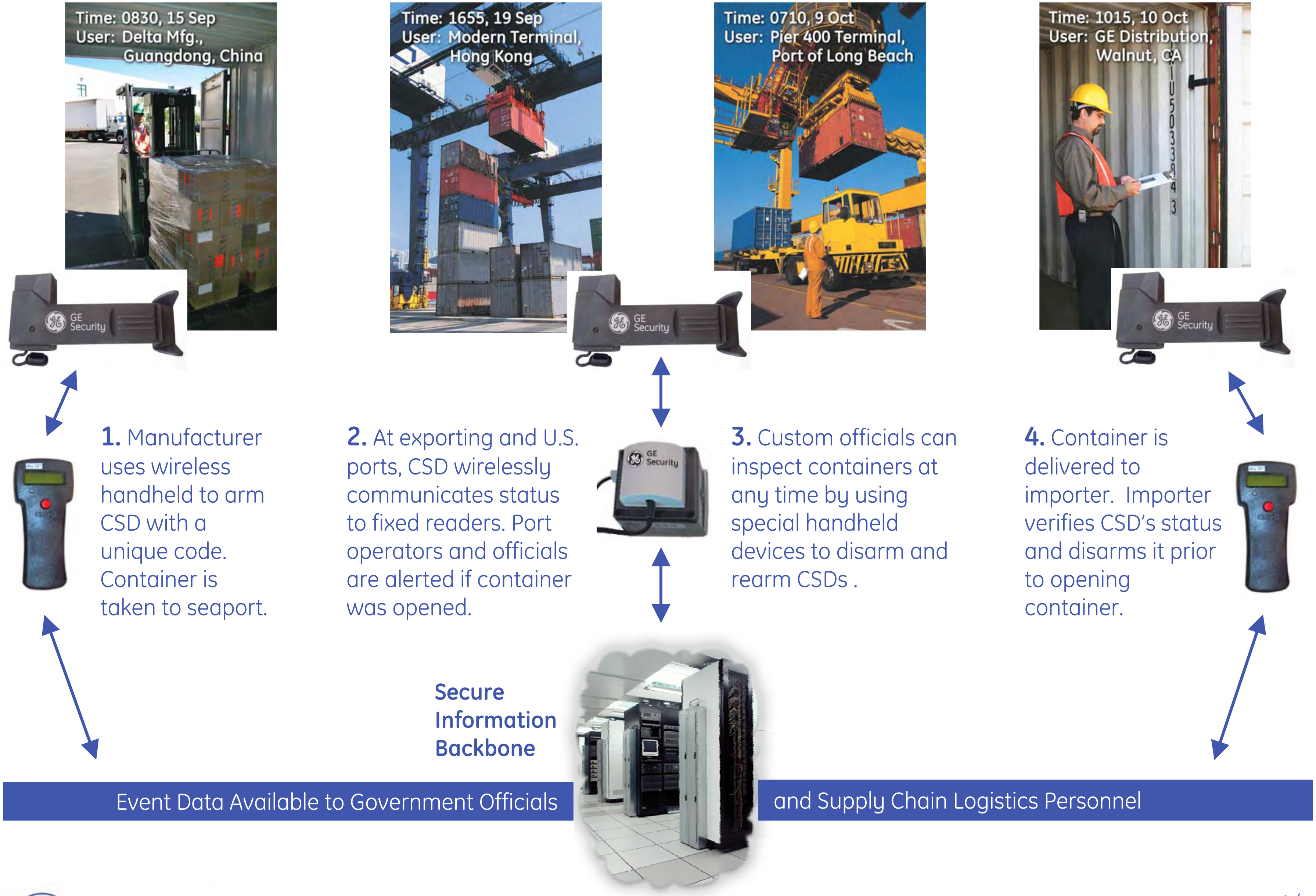
Closed Door



- Temporary Mount: Magnets
- Permanent Mount: Double Sided Tape
- CSD does not occupy useable cargo space
- Additional sensors can be added to base of CSD and also protected by container

- Container door to left of CSD antenna
- Side of container begins to right of CSD antenna
- CSD protected inside container
- Radio antenna protected in channel
- Radio range up to 100 meters

GE Commerce Guard™ Container Security System



1. Manufacturer uses wireless handheld to arm CSD with a unique code. Container is taken to seaport.

2. At exporting and U.S. ports, CSD wirelessly communicates status to fixed readers. Port operators and officials are alerted if container was opened.

3. Custom officials can inspect containers at any time by using special handheld devices to disarm and rearm CSDs .

4. Container is delivered to importer. Importer verifies CSD's status and disarms it prior to opening container.

Secure Information Backbone

Event Data Available to Government Officials and Supply Chain Logistics Personnel

APPENDIX 3

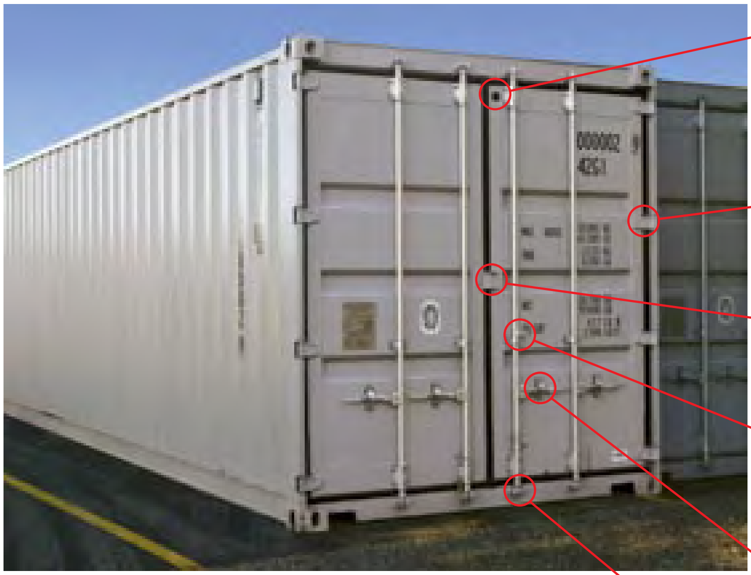
GE
Security

CommerceGuard™ TESC

The Tamper Evident Secure Container (TESC) is a new generation of freight container. It is made by the world's largest container manufacturer, China International Marine Container (CIMC), and developed in collaboration with GE. It combines GE's CommerceGuard™ technology and physical container improvements to make in-transit cargo security affordable for shippers and carriers.

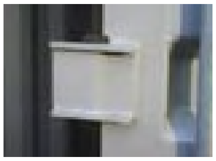
GE's integrated Container Security Device (iCSD) is permanently built into the container. It monitors container integrity by detecting door openings. If an unauthorized person compromises the container's integrity, the iCSD registers the event and stores it with a time stamp. When the iCSD comes within range of a handheld or fixed reader, for example at an in-gate, the iCSD sends out an alarm to the reader. Relevant authorities are then alerted, and the container can be halted, quarantined, and inspected.

The improved TESC container also has new tamper resistant features including reinforced door keepers, improved hinges, handle retainers and seal location assemblies. And the iCSD has an expansion port to accommodate other useful sensors inside the container.



CommerceGuard iCSD
(mounted on door interior)

Improved Hinges


Reinforced Door
Keeper

Enhanced Lock
Device

Improved Handle
Retainer and Seal
Location

Secure Cam

Tamper Evident Secure Container

U.S.A.
4001 Fairview Industrial Dr. SE
Salem, OR USA 97302
T 800.547.0252
T +1-503-581-9101
F 800.382.6119

Visit us online at
www.gesecurity.com/csd
Email: commerceguard@ge.com

imagination at work

CIMC

Licensed by GE from
ALL SET
All Set Marine Security AB

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

APPENDIX 4

imagination at work

CIMC

GE and CIMC Complete First Commercial Test of Tamper Evident Secure Container, Paving Way for Commercially Viable Cargo Security

Washington, D.C., January 12, 2005 – GE's Security business (NYSE: GE) today announced it has successfully completed the first commercial field test of the Tamper Evident Secure Container (TESC). The TESC is a new generation of freight container that integrates GE's CommerceGuard™ container security device into a standard maritime shipping container to make cargo security affordable for manufacturers and shippers and protect container integrity throughout the supply chain.

The redesigned container was developed jointly by GE and China International Marine Containers Group Ltd.(CIMC), the world's leading manufacturer of maritime shipping containers. The security device technology used in the TESC is licensed by GE from All Set Marine Security AB. Unisys Corporation (NYSE: UIS), the global IT services and technology company, was the systems integrator and observer for the test.

Unisys, with more than 12 years of container security testing and integration expertise, was responsible for the testing and analysis of the project results. Unisys tested more than 15 different security breach attempts in Mainland China, Hong Kong, and the United States. All 15 were properly detected and communicated by the TESC containers. "The test results of the TESC project are very encouraging", said Greg Baroni, president, Unisys Global Public Sector. "Embedding the container security device within the infrastructure of the container enhances both the security and financial viability of this solution. We've tested many container security technologies and the container security device is the current gold standard."

"The future of global commerce depends on the ability of the shipping industry and government agencies to improve cargo security while streamlining the flow of goods," said Greg Burge, president of Monitored Solutions for GE's security business. "With the successful completion of the TESC test, we have demonstrated a solution that meets the security demands of government and enables the ports to move goods efficiently at a cost-per-shipment that is viable for shippers is available today."

A Sensible Approach

The TESC solution is a combination of physical enhancements and an electronic integrated Container Security Device (iCSD), a technology that allows the shipper to arm the container using a unique, encrypted code after it is stuffed and sealed with a traditional bolt seal. As the container passes within range of the global wireless reader infrastructure – similar to common electronic toll collection systems – the iCSD tells logistics and customs officials where the container is located, when it arrived and if unauthorized personnel opened it en route. This information gives manufacturers, customs officials and importers the data they need to determine if a particular container was compromised at any point throughout the supply chain. Because the iCSD, which is integrated into the doorframe of the TESC solution, uses public wireless communication infrastructure and a point-to-point approach, it's significantly less expensive to operate than other technologies. "Supply chain security is critically important to our customers and the well-being of the global economy. However, until now, the cost of securing a container and building the necessary information sharing infrastructure has been cost prohibitive to exporters, which are competing in an extremely competitive global economy," said CIMC's David Wong, CTO. "The successful test of the TESC proves that security doesn't have to be expensive, especially when the features are built into the container. We believe our customers will get behind this approach."

CIMC, based in Shenzhen, China, is the world's largest manufacturer of shipping containers. In fact, 50 percent of all new freight containers are manufactured by CIMC.

GE’s CommerceGuard System also includes Container Security Devices that can be installed in less than a minute and without using tools to retrofit the world’s existing population of freight containers. Both types of devices, the CSD and the iCSD, share the same wireless reader infrastructure, making the overall system cost effective to globally deploy.

The technology was invented by All Set Marine Security AB of Sweden and is exclusively licensed to GE by All Set. The physical enhancements to the container, including improved door locking mechanisms, tamper-proof hinges and improved placement for a door seal, were designed and built into the container by CIMC. Unisys provided systems integration services and oversaw the deployment of the project.

What’s In the Box?

Each year, more than nine million freight containers arrive at U.S. ports, approximately 50 percent more than 2001 because of the proliferation of global trade and “just-in-time” manufacturing and retailing strategies. The increased threat of global terrorism has raised awareness that these containers are a vulnerable point in the supply chain.

In response, initiatives including C-TPAT, a partnership between U.S. Customs and Border Protection and the trade community, are being developed to implement security standards that better protect the entire supply chain – from foreign loading docks to American ports of entry. In exchange, companies that meet security standards set by Customs and Border Protection will get a “green lane” through U.S. ports, which translate into greater supply chain efficiency and significant cost savings for businesses.

Because the TESC gives U.S. Customs further assurance that the items in the container are limited to those packed by the approved shipper, it could potentially be used as a “layered security element,” a necessary requirement for receiving “green lane” access.

About GE Security

The Security business of GE Infrastructure is a wholly owned subsidiary of the General Electric Company focused on communication and information technologies for security, safety and lifestyle enhancements. It has operations in more than 30 countries and is represented by some of the best-known brand names for intrusion and fire detection, access and building control, video surveillance, explosive and drug detection, key management, and structured wiring. For more information about GE's Security business and our product offerings, please visit www.gesecurity.com.

About CIMC Group

China International Marine Containers Group Ltd., (CIMC) is a world leading marine container manufacturer. Its major products include full range of ISO dry cargo containers, reefers, flat racks, chassis and trailers. With its strong industrial base and domestic connection, CIMC is also involved in other industrial fields such as airport ground-support equipment, internal combustion generator and real estate development. With its head office in Shenzhen, China, CIMC employs over 28,000 people and controls over 30 subsidiaries and 20 production bases in China including Shenzhen, Fujian,Shanghai,Ningbo, Nanjin, Nantong, Dalian, Xinhui and Hong Kong, U.S.A.

About Unisys

Unisys is a worldwide information technology services and solutions company. Our people combine expertise in consulting, systems integration, outsourcing, infrastructure and server technology with precision thinking and relentless execution to help clients, in more than 100 countries, quickly and efficiently achieve competitive advantage. For more information, visit www.unisys.com.

About All Set

All Set Marine Security AB, based in Stockholm, Sweden, is a leader in development of in-transit electronic security solutions for freight containers. The CommerceGuard technology is licensed to GE from All Set.

For more information on this release, contact:

Casey Fale
Marketing Director
GE Security, Monitored Solutions Group
Tel: 503-589-8518; Fax: 503 375 9852
casey.fale@ge.com

Or

Andy Hilton
Director, Peppercom
212-931-6118
AHilton@Peppercom.com