Smart containers: their use, their payback

The world is trying to ensure that global container traffic is controlled and secure; reducing the vulnerability containers could pose for nations and their ports. Governments and non-government organizations are constantly debating and demanding certain protocols be adopted to achieve this security, for instance the demand by the United States (US) for scanning.

Unfortunately, these organizations do little to demonstrate that they understand the business needs of the private sector and that securing the supply chain actually provides business benefits to the private sector, specifically it makes money for those who secure the supply chain. There really doesn't have to be opposing sides to this issue. It is time for both industry and government to understand the value of smart containers: protect the homeland and make a profit!

Smart containers today

First, how do we define smart containers? Second, what do they detect? Third, how smart is smart? Fourth, how does it know when to begin and end working? Fifth, what are the benefits? Sixth, who pays, and finally, does their usage meet the requirements of Customs security programmes?

- **How do we define smart containers?**

Smart containers are smart because they can carry on a conversation. The user or their international control center ("platforms") can communicate with them, depending on the programming, sensors, and technology used, in real-time or close to real-time. We define smart containers by what they do, more specifically what they are programmed to do. Their sophistication ranges from simple reporting of location only to a chain-of-custody system from origin to destination. Some containers are simply more intelligent than others because of how they are equipped and programmed.

- What can be detected and reported besides location?

Each type provides a different benefit for varying users. If you are a pharmaceutical company like Pfizer, Inc., you may need to have additional information such as the container's internal environment like temperature, and for high-value cargo like Viagra, security against theft. In general, while different shippers, carriers, and consignees have different needs, the basic features of smart containers include location (historical and real-time reporting); detection and reporting of unauthorized access or breach through any portion of the container; internal environment like temperature, excessive vibrations, the presence of substances like WMD, human cargo and illegal drugs; and logistics data.

- How smart is smart?

Tracking and tracing functions, a trait of a mentally-challenged smart container, merely monitor location by RFID fixed antennas or by satellite or

To assist Member administrations in the process of purchasing and deploying scanning/imaging equipment, the WCO Secretariat has produced guidelines with the assistance of the Scientific

Sub-Committee, which describes in detail the key aspects to be examined, issues to be settled in advance and the different stages and procedures to be followed. They are available on the Members pages of the WCO web site, but their scope is limited to x-ray and gamma-ray imaging type equipment and does not cover nuclear and other radioactive material detection equipment including radiation portal monitors which may be considered as optional extras when purchasing container scanners.

The International Atomic Energy Agency (IAEA) has produced suitable technical guidance for nuclear and other radioactive material detection equipment (see WCO News No. 59 – June 2009, pages 46-47).

More information
www.wcoomd.org


© Madagascar Customs

cellular, depending on the level of communication latency the user is willing to accept. The very smart containers can tell you the following electronically: the contents of the container; who supervised loading the cargo and who is accountable for the accuracy of the contents at origin; the time the container was sealed; when it left its origin; its route; its internal environment; its progress; whether it deviated from its course; its arrival at port of embarkation; when it was loaded aboard the vessel; whether it was breached; when it arrived at the destination port; and who opened it and verified the cargo.

Shielded, weapons grade, uranium not detectable by non-intrusive portal scanners, can be detected by smart containers appropriately equipped with sensors that can detect and report its presence. [Davabhaktuni Srikrishna, A. Narasimha Chari, and Thomas Tisch, "Nuclear Detection: Portals, fixed detectors, and NEST teams won't work for shielded HEU on a national scale, so what next?", 16 May 2005, p.1]

Companies out there can provide smart containers now. For example, the features of Onstar that monitors General Motors vehicles in the US are available for containers from other companies. There are also multiple satellite service providers like Iridium, Orbcomm, Inmarsat, Europe's Galileo, and Compass – the Chinese entry into satellite communication – that can provide position detection at relatively low costs.

- **When does smart start and stop?**

Everything depends on the security programme and software utilized. At present the smartest container has a sophisticated, comprehensive chain-of-custody system that begins at the stuffing (loading) of the container at origin and maintains, monitors, and reports its integrity to the end of the global supply chain path at destination. Its process includes the human element in the supply chain and the electronics of the system. No system is 100% effective and one cannot depend on technology alone. However, technology often overshadows the role of humans in security systems. Container systems have to include the identification of the party responsible and personally accountable for final inspection of the cargo prior to its sealing and dispatch and subsequent international movement to destination. Someone must necessarily take responsibility for confirming the cargo on the bill of lading or booking sheet, for activating the smart container system, and for locking the doors. This responsible party must be vetted with respect to integrity and competence.

Equally, there must be a counterpart at destination. Both parties are electronically connected by a unique identifier to the smart container to complete the system. This can be done with an electronic activation key or equivalent that is loaded at origin with the bill of lading and booking information, or information needed by Customs authorities, and other data such as the identity of the supervising and arming agent at origin and the final agent deactivating the system at destination. This secure electronic key protocol is then used to insert the data from the company's logistics system into the device affixed in the container and is carried to destination. Therefore at activation, the accountable party becomes an integral element in the smart container security system. Once the container is activated by using an electronic key protocol inserted in the electronic memory of the container, the device can be read at almost any time during the voyage through satellite communication.

When a smart container is opened at destination by an equally accountable person and cargo is missing, and there were no breaches detected, recorded and reported, the accountable person at origin can face either disciplinary, or worse, criminal action by appropriate authorities. Worldwide control centres offer the capacity to serve as a third-party electronic record of the transaction recorded automatically in its servers. The smartest container offers an electronic receipt of delivery, accomplished by the opening of the container by a person at destination approved and authorized to open the container, which is provided by another specialized electronic key protocol usable only with and by an authorized individual at the point of destination.

European Datacomm (EDC) and GlobalTrak in the US can today provide these smart containers.

- **What's it worth and who pays?**

While we all pay one way or the other, the private sector really pays for all of this. In fact, in March 2006 US Customs and Border Protection (CBP) boasted about how the US zone of security is being pushed back to the point of origin which "…allows for better risk assessment and targeting, freeing CBP to allocate inspectional resources to more questionable shipments." The conclusion seems obvious: let other nations and private enterprises spend their money to push back the US border and free up CBP for something else. The problem is that pushing back the border of the US is not the duty of the private sector or other nations.

Realising the cost to the private sector, CBP commissioned the University of Virginia to determine the cost/benefit outcome to taking security measures. Published in a 2007 cost/benefit survey report, CBP indicated several benefits for simply participating in its Customs Trade Partnership Against Terrorism (C-TPAT) programme. [Abdoulaye Diop, Ph.D., David Hartman, Ph.D., Customs-Trade Partnership Against Terrorism Cost/Benefit Survey Report of Results, Weldon Cooper Center for Public Service, University of Virginia, August 2007, p. 47]

Unfortunately, it seems that the return on investment (ROI) is not known to, appreciated by, or significant enough to the user, to employ smart containers. Or the user is simply focusing on the costs involved in using smart container technology, not weighing the bottom-line benefits of a visible supply chain. All agree that at a minimum there will be expedited treatment, at least, by US Customs authorities for the use of smart containers as defined in the US SAFE Port Act. The benefits of expedited shipments, alone, vary from US$ 600 to US$ 700 per container per move (Bearing Point Study, 2003); and

US $ 1150 per move (AT Kearney Report, 2005). Therefore, if a smart container costs you an additional US$ 100 from origin to destination, and you save US$ 1000 on the expedited treatment, what was the cost? Costs are associated with the loss or delay of cargo; diversions; increased insurance premiums; supply chain disruptions; increased labour to reship or replace the cargo; business downtime; loss of seasonal promotions; or the costs of the sale. Benefits include minimizing financial risks, reduced inventory carrying costs, protection against counterfeiting; reduced or eliminated diversion costs, reduced out of stock, and reduced insurance costs.

A Stanford University recent study revealed that the quantifiable benefits of security controls and technology included: improved product safety; improved supply chain visibility; improved product handling; more efficient Customs clearance; speed; and higher customer satisfaction. [Barchi Peleg-Gillae, Gauri Bhat, and Lesley Sept, Innovators in Supply Chain Security The Manufacturing Institute, Stanford University, July 2006, p. 4]

Other sources, including the US Congressional Budget Office in March 2006, offer different, but compelling, benefits to using smart container technology. In a 2006 A.T. Kearney survey report, respondents stated that "…they need real-time data for accurate visibility into their supply chains"*. Since accurate data does not exist within the current logistics industry, smart boxes can provide that missing data deemed important to shippers. The report further revealed that the US Department of Defense is now utilizing smart containers even though they are not the smartest containers. These smart boxes "…reduced overall losses (military supplies) to less than 8%"**. There is a favorable bottom line to using smart boxes based on speed alone. [*Smart Boxes, A.T. Kearney, 28 July 2006, p. 1] [**Smart Boxes, A.T. Kearney, p. 2]

- **Are Smart Containers Compliant?**

Only the smartest (chain-of-custody) containers meet all or most of the following: the World Customs Organization (WCO) revised Kyoto Convention of 1999 which focused on simplifying Customs procedures and called for greater use of information technology and more e-commerce; the UN Economic Commission for Europe's Recommendation 33 of 2004 which called for a Single Window through which "…trade-related information and/or documents need only be submitted once at a single entry point to fulfill all import, export, and transit-related regulatory requirements."; the WCO revised Kyoto Convention ICT Guidelines of 2004 which called for the electronic exchange of information at export and import, a chain of "electronic" data and a single global schema linked electronically; and the WCO Framework of Standards to Secure and Facilitate Global Trade of 2005 which called for security from stuffing to destination, control at stuffing, intermediate handling, loading, off loading, terminal, and destination; and use of electronic communications.

Finally, smart containers meet the requirements of the US C-TPAT, New Zealand's Secure Export Partnership (SEP), Jordan's Golden List Programme (GLP), Canada's Partners in Protection (PIP), and the European Union Authorized Economic Operator (AEO) programme that countries around the world are adopting in one form or another. All of these governmental programmes call for security at stuffing, tracking and monitoring, electronic records, and the use of advance electronic data and more. And now in the US because of a change in its Federal Rules of Civil Procedure, electronic data generated from or linked to smart container usage can now be used in litigated civil proceedings as evidence for the prosecution or defence. In addition, smart containers meet, in part, and complement the electrotechnical International Standard 28000 of 2007 (Specification for Security Management Systems for the Supply Chain).

Conclusion

Smart containers know when they are breached or entered, when their internal environment changes, where they are, how to talk, when to start and stop talking, what to say, and when to begin and end being smart. They exist now, are getting more sophisticated, and offer to the world, knowledge of where any given product is, and its condition. It is even smart enough to generate revenue for the user while offering protection to all of us. What is missing is government's support for them. Their increased use will ultimately depend on government incentives and benefits in spite of possibly being smarter than the governments that need them.

More information

Dr. James R. Giermanski
powersintnlinc@bellsouth.net

Dr. James R. Giermanski (Jim) is the Chairman of Powers Global Holdings, Inc. and President of Powers International, LLC, an international transportation security company. He was a Regents Professor at Texas A&M International University (TAMIU) and is a member of the graduate faculty at the University of North Carolina in Charlotte (UNC Charlotte).

Besides having served as Director of Transportation and Logistics Studies at TAMIU's Center for the Study of Western Hemispheric Trade, Jim is a reviewer for the US National Research Council's Transportation Research Board. He has authored over 130 articles, books, and monographs, and has been published extensively on transportation and trade issues in addition to having written the International Insight column in Logistics Management for five years.

As a former FBI special agent, OSI special agent and a Colonel in the Office of Special Investigations where he handled counterintelligence matters, he currently provides transportation security lectures on C-TPAT, and other Customs and Border Protection (CBP) programmes. Jim holds a Masters degree from UNC Charlotte, a Masters degree from Florida International University, and a Doctorate from the University of Miami.