



## Container Security: Is it working?

By Jim Giermanski, Chairman, Powers Global Holdings, Inc.

Currently, the U.S. uses four categories of security technology in the global supply chain. We asked our security expert to define each category, examine where they are in the evolutionary process, and then assess which type of technology is most effective. Here's what he has to say.

**S**ince September 11, 2001, and the creation of the Department of Homeland Security (DHS), there have been four distinct phases of security involving containers moving in the global supply chain: the maritime phase, the port-to-port phase, the origin-to-destination phase, and the electronic chain-of-custody phase.

Each of these phases has seen recent advancement in the security technology employed to keep up with more sophisticated demand and government

requirements; and, of course, each type of technology does something very distinct from the other. Essentially, the United States uses four categories of security technology to help carry out the phases defined above. Each category represents a “crawl before you walk” process; each maturing into different security hardware and processes over time. In general, the order is as follows:

1. doors-only security with mechanical barrier seals and electronic door seals (e-seals) that utilize Radio Frequency Identification (RFID);
2. doors-plus security that utilizes door seals combined with satellite for tracking;
3. scanning security; and
4. chain-of-custody satellite and satellite-cellular combinations that detect and report internal container integrity with active supply chain management.

Each of these technologies also makes use of distinct electronic processes that are manufactured into the hardware. While each has its own benefits, the best of all the benefits to the user are those that will actually produce the in-container satellite and satellite/cellular combinations. Over the next few pages we’ll clearly define each of the four categories of container security, examine where they are in evolutionary process, and then assess which type of technology is the most effective.

### Door seal technologies

The first assumption by Customs organizations, and unfortunately an assumption that’s still lingering in U.S. Customs and Border Protection (CBP), is the idea that protecting container access is limited to doors-only technology.

There are two general types of door seals: mechanical or barrier seals (or doors-only) and electronic seals. Door seals have international standards against which they’re measured; in fact, a high security door seal standard was determined by voting on publicly available specifications (PAS). The International Standards Organization’s (ISO) 17712/PAS Standard is the high-security bolt and cable H-seals standard – it even has standards for the facilities that examine and certify high security seal compliance to ISO/PAS 17712.

The ISO 17712 Standard was published in 2003. However, ISO standards are not binding on nations and are not necessarily the only guide for sealing a container. According to Ray Fernandez, vice president of door seal manufacturer Sealock Security Systems Inc., CBP has mandated as of October 15, 2008, that as a minimum security requirement all containers destined for the U.S. be secured with a so-called “H” designation high security bolt seal that is ISO/PAS 17712 compliant and has been tested and examined by a certified lab.

However, according to Fernandez, there’s an issue revolving around the credentials of some certifying labs that performed these tests. He believes that, in fact, all seals, whether compliant or not, are being used. So no one really knows if the seals meet the standards. CBP is simply not verifying the compliance of these to ISO standards and to CBP’s standards of best practices.

A basic door seal becomes a “doors-plus” seal when it does more than just function as a physical barrier. Door seals can also be electronic, in that the barrier

seal contains an active RFID system or electronic feature that communicates the Container's ID number, contents, and integrity with respect to whether the seal was tampered with. These seals can also offer GPS and/or cellular tracking.

GPS is a satellite-based navigation system made up of a network of 24 satellites placed into low-Earth orbit by the U.S. Department of Defense. GPS satellites circle the Earth twice a day in a very precise orbit and transmit signal information. A GPS receiver must be locked on to the signal of at least three satellites to calculate a 2D position (latitude and longitude) and track movement. With four or more satellites in view, the receiver can determine the user's 3D position (latitude, longitude, and altitude).

These almost-smart containers are able to provide the tracking function now required by the Implementing Recommendations of the 9/11 Commission Act of 2007. However, tracking is not two-way communications; therefore, it falls short of my definition of what constitutes a "smart" container.

### Scanning technologies

Because a terrorist may use a cargo container to smuggle a nuclear weapon, radiological material, drugs, contraband, or humans into a country, and since millions of containers cannot be opened for a physical inspection, scanning has been determined by some governments – particularly the U.S. government – as a form of cargo inspection. Scanning is a federal requirement. Both the SAFE Port Act of 2006 and the Implementing Recommendations of the 9/11 Commission Act of 2007 mandate the scanning of containers. Therefore, it is done at all U.S. seaports and land ports-of-entry, and in some foreign ports.

The first assumption by Customs organizations, and unfortunately an assumption that's still lingering in U.S. CBP, is the idea that protecting container access is limited to doors-only technology.

There are basically two categories of scanning: Non-Intrusive Inspection (NII) for all types of cargo, including unshielded radiation; and special radiation portal scanning machines as part of the Security Freight Initiative (SFI) specifically for shielded, highly enriched uranium (HEU) detection. Non-intrusive imaging equipment comes in many sizes: large-scale X-ray and gamma-imaging systems, as well as a variety of portable and handheld technologies that include radiation detection technology.

The VACIS imaging system is an example of NII. VACIS is deployed at U.S. seaports as well as land ports-of-entry and allows CBP to detect and interdict contraband (such as narcotics, weapons, and currency) hidden within the transport container and/or its cargo. The mobile gamma ray imaging system employs a gamma ray source that permits officers to quickly "see" inside

tankers, commercial trucks, cargo containers, and other conveyances without having to physically open the conveyance and/or container. NII machines can scan vehicles up to 125 feet in length in one pass. One version of the system is mounted on a truck chassis and is operated by a three-man crew. It operates by slowly driving past a parked vehicle with a boom extended over the target vehicle.

SFI is a scanning project composed of radiation portal monitors specifically to detect radiation through NII imaging systems. SFI is active at only three ports at full capacity: Puerto Cortes, Honduras; Port Qasim, Pakistan; and Southampton, U.K. It was also active in a limited capacity at Busan, Korea; Singapore; Port of Salalah, Oman; and Hong Kong.

Manufacturer	Siemens/ GE/ Samsung/ Mitsubishi	SAVI	Brooks GlobalTrak	Impeva Labs	IBM	European Datacomm	ZOKA/ Rainer Koch
Product name	Commerce Guard	SensorTags	GlobalTrak	Global Sentinel	TREC	EDC76	CSB
<b>UNIT SPECIFICATIONS</b>							
Basiscommunication technology	RFID 2.4 Ghz	RFID 433Mhz	Satelite (ORBCOMM)	Satelite (IRIDIUM)	Satelite (IRIDIUM)	Satelite (IRIDIUM SBD)	SMSvia GSM
GPS	-	-	Yes12 Channel	Yes12 Channel	Yes12 Channel	Yes12 Channel	Yes16 Channel
Land infrastructure need	Yes	Yes	No	No	No	No	No
Othercommunication protocols	-	-	CellIWLAN	CellIWLAN	-	-	-
Range	30m near reader	30m near reader	Depending on Orbcomm network	100% coverage	100% coverage	100% coverage	Dependi ng on cell network
Battery	-	3.6 V	12 V	12 V	12 V	12 V	12 VSolar cell
Battery uptime	6 years	4 years depending on 2 collections /day	2 to 3 months depending on message frequency	2 to 3 months depending on message frequency	-	3 months depending onmessage frequency	-
Battery life Rechargeable	6 years No	4 years Replaceabl e	2 years Yes	3 years Yes	- Yes	3 years Yes	- Yes
Tamper sensors	Door proximity sensor	Door sensorLigh t sensor	Optional (ex: Sensor node)	Light sensorDoor sensor	-	Ligth sensor	Magnetic bridge
Enviromental	-	Temperatu	External	Temperatu	-	Under	-

sensors		rehumidit yshock	sensor node	rehumidity shock		development	
Operating temperature	-40C+70C	-40C+70C	-20C+60C	-20C+60C	-20C+60C	-20C+60C	- 20C+60C
Storage temperature	-50C+85C	-40C+85C	IP67	IP67	IP67	IP65	IP66
Mounting	Flexible(Door)	Flexible(Door)	Fixed(Door)	Flexible(Door)	Flexible(Door)	Flexible(Door)	Flexible(Rooftop)
Mounting time	30 seconds	30 seconds	5 minutes	Within 5 minutes	Within 5minutes	Less then 30 seconds	Within 5 minutes
Form factor	ISO	ISO	All	All	All	All	All
Estimated unit price	\$1,000*	\$100*	\$1,000	\$3,000	\$3,500	\$1,000	-

**Remark**

Commercial not available

\* Exclusive the infrastructure cost + maintenance **Source:** Kiok Hyung, customs overseas senior researcher, the Korea Customs Service

However, SFI still cannot detect HEU. Congress is expecting that the new portal machines called Advanced Spectroscopic Portals (ASP), or crane-mounted machines, will be developed and commercialized to detect this form of dangerous radiation. However, in April 2007, the Government Accountability Office (GAO) stated very clearly that the Domestic Nuclear Detection Office (DNDO), which was established and responsible for ASP development, has not even collected all the testing data on its basic polyvinyltoluene (PVT) portal detectors and is not close to any developed ASP portal detector. Experts do not expect a commercial version of the ASP anytime soon, nor is it likely that there will be one by 2012 as required by Congress. Because of the lack of this technology, Congress allowed for an extension of compliance until such time that these radiation portal detection machines become available.

The basic problem for existing NII equipment is that gamma rays and neutrons emitted from shielded HEU are detectable at only short distances and only when there is adequate time to count a sufficient number of detected particles. Five issues are relevant in the successful detection of shielded HEU: the mass of the HEU core; the degree of shielding; the size of the radiation detector; the distance to the source; and the time necessary to integrate photon counts. Therefore, the closer a detector is to the source of emission and the longer it “sniffs,” the greater the probability of detecting HEU. This isn’t possible with current portal, pass-through NII equipment.

To date, scanning is costly, inefficient, and really not doable without seriously interrupting the flow of international trade. Even CBP insiders admit that their security dogs often “alert” inspectors to areas of the conveyance which are then moved to the scanner – where the ultimate discovery and recovery is credited to the scanning function and not the dogs.

### How smart is your container?

As there are different levels of door seals, there are different levels of “smart.” The basic smart container is simply one that uses a global positing

system (GPS) for tracking and for satellite communication between the container and the user. The addition of communication capacity—the user and container being able to talk to each other—makes the container smart.

The user can program how often it should broadcast its position as well as how to respond to the user's query to the container. Satellite tracking can be done by low-Earth orbit satellites, like Iridium or Orbcomm, or geostationary satellites like Inmarsat D+. At the present time it seems that Iridium, Orbcomm, Europe's Galileo, and China's Compass are likely to provide most of the smart container tracking.

An even smarter container combines satellite or satellite/cellular to provide total supply chain control. These high-IQ containers employ a chain-of-custody technology that identifies the following: the contents at "stuffing" (loading); who supervised the stuffing of the container; who is accountable for the accuracy of the contents at origin; the time the container was sealed and who sealed it; when it left 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—all in electronic format.

This container can even report its own hijacking. So far, there are only two licensees for this global technology: GlobalTrak and European Datacomm (EDC), which has sub-licensees in Asia. The chain-of-custody process coupled with smart container hardware technology is now being evaluated by the Seventh Framework Program (FP7) that was created by the European Union Commission to research and design a premier supply chain management system.

The issue of technology involving containers moving through the global supply chain has also been studied by South Korean Customs. Kiok Hyung, customs overseas senior researcher for the Korea Customs Service, has created a list of those major firms currently in the smart container business. Because they make the supply chain visible, efficient, fast, and profitable, smart containers represent the future of global container movement.

### What works? What doesn't?

What works depends on the user's level of need and the financial consequences produced by the technology. If a smart container moves the shipper through Customs faster and that improved speed and visibility turns a larger profit for the shipper, then a smart container it must be for that company.

However, if the user only locks the doors with a seal because Customs requires it, that can be perceived as effective security as well. Let's quickly revisit the four distinct levels of technology and attempt to assess their level of effectiveness.

**1. Doors-only:** In this writer's view, doors-only is not the best way to go. I have bypassed seals in a number of ways without disturbing the seal or the hinges. If you want to get in, you can.

E-seals can be even less effective than barriers seals. First, RFID is not applicable globally. There are too many divergent frequencies, protocols, and infrastructure problems. What's worse, RFID for container security as it's mandated in the United States serves as an improvised explosive device (IED), making it a vulnerability, not a security technology. Even CBP acknowledges its limited use. CBP's director of cargo control, Greg Olsavsky, recently stated that "RFID is only an interim solution and that ultimately CBP will use container security devices."

**2. Doors-plus:** There is no difference between doors-plus and doors-only with respect to access; but the GPS function serves the tracing requirement specified in the Implementing Recommendations of the 9/11 Commission Act of 2007.

**3. Scanning:** At this stage, if not for CBP canines, scanning wouldn't do much either. It disrupts our trade flows and our trading partners simply don't like it. Sometimes it works, but most of the times it doesn't. It certainly does not work for detecting shielded enriched uranium, and even if it worked in our Container Security Initiative (CSI) ports – there are 58 of them – the scanned container could be subsequently accessed if it went through a transshipment port.

**4. Chain-of-custody smart containers:** What does work – and is just beginning to be used – is in-container satellite and satellite/cellular systems that have unique detection and environmental sensors. As stated above, these employ the chain-of-custody process and can communicate in real-time (or close to real-time) with the user and/or to government authorities.

Additionally its system's control center personnel and servers can provide third-party verification as well as evidentiary, legal defense, and legal prosecution value should container conditions or route change during its international movement from origin to destination.

This system's value is not only the security it provides, but also in the increase to the user's bottom line.

*Jim Giermanski is chairman of Powers Global Holdings Inc. and a frequent contributor to Logistics Management and Supply Chain Management Review.*