



http://www.csoonline.com/article/473165/CBP_and_Smart_Containers_What_Does_It_Know_

[Industry View](#)

CBP and Smart Containers: What Does It Know?

Dr. Jim Giermanski, chairman of Powers Global Holdings, gives us a break down of both RFID and Satellite Communications, two container security device technologies.

By Dr. Jim Giermanski

December 30, 2008 — [CSO](#) —

In January 2009, Customs and Border Protection (CBP) will conduct a pilot program to test a type of container security device (CSD) used to make [containers smart](#). The test will take place with containers crossing the border into the United States from Mexico. That sounds like a good thing. A deeper look will suggest something else.

It is truly incredible that [container security](#) as the U.S. government sees it, that is, as the [Department of Homeland Security \(DHS\)](#) and the [Department of Defense \(DOD\)](#) see it, seems to be focused on [Radio Frequency Identification \(RFID\)](#), probably the worst technology for that use. It also seems that, in spite of all the money available to these two giant agencies, and the research entities used by them or could be used by them, they seem to have little appreciation for the value of not just smart container usage, but also CSD technology. I hope in this short treatment of two CSD technologies, that the reader will see the stark differences between RFID and Satellite Communications technology. I will take the essential and specific elements of each and make a comparison.

RFID

RFID is a radio frequency based technology. As such, it is regulated by the [Federal Communications Commission](#) (FCC). The FCC has decided that for container security, certain frequencies must, not should, but must be used. These frequencies are published. Anyone who desires to transmit or receive these signals can do so by purchasing an off-the-shelf transmitter and receiver. Without getting into the difference between active and passive RFID, the essential issue is that its use requires the transmission and reception of a radio frequency (RF) signal. The FCC also specifies the strength or amplitude of that signal, and the duration of that signal. All of this information is publicly available.

1. RFID Benefits

In general, RFID has been in use for a long time. Its hardware and its application in certain environments are hallmarks of efficiency and effectiveness in the control of handling and warehousing products, specifically in conditions and settings where antennas and transponders, and environmental conditions are controllable. Bar-coding, pallet control, and item-control such as that used by retailers in attaching RFID tags to garments, electronic equipment boxes, and other selected products are a few examples. In these settings, the RF frequencies are the same and are used in the same way a very good profitable application of RFID.

2. RFID Weaknesses

While its benefits in controlled environments are obvious, its weaknesses in container security within a global supply chain are just as obvious. The very nature of a global supply chain brings lack of control, the antithetical condition of effective and efficient usage. Its application to international transportation across the U.S. land border with Canada and Mexico was tested by the government in the mid 1990s with the involvement the U.S. Department of Transportation (USDOT) and U.S. Customs (now Customs and Border Protection, an agency of the Department of Homeland Security). The test was called the North American Trade Automation Prototype (NATAP) and it took place at six of our U.S. land ports. As a participant in the NATAP test along the southern border, this writer can state unequivocally that the test failed, both because of institutional and RFID-technology reasons.

a) Infrastructure Access, Maintenance, and Costs

With containers, there is a fundamental requirement: antennas at fixed locations. There is a need for physical infrastructure and equipment on the ground, either fixed, or handheld. Handheld transceivers bring in the human element with the resulting higher costs, damage, maintenance, or loss. Regardless, they are needed so when changes in the container status are, they can be transmitted by RF signals when, and only when, the container is interrogated by a transceiver physically positioned or used in the case of handhelds. somewhere along the global supply chain. The fixed transceiver, through an antenna, sends the triggering frequency, which carries a request for a return transmission of any change of status of the container since the last time it passed an antenna and transceiver. The message could be that the container was breached somewhere in-route.

Since the transmission of these data is by radio frequency, the successful transmission is subject to not only the use of government-approved frequencies or waves, but also the absence of distortion like noise or same-frequency emissions from competing antennas whose direction (footprint) unintentionally or intentionally obstructs or interferes with the intended RFID transmissions of the intended transponder. Thus, so far there are some very clear weaknesses: first, the need to own or lease property to place an antenna; second the absence of interfering RF signals which cannot be guaranteed; and third the historical nature of what information is transmitted, a very critical weakness. For instance, the last place one wants to learn that the container was surreptitiously accessed and an explosive device placed in it destined for the United States is at the foreign port of departure or at the U.S. port of arrival since these ports are where most of the transmissions take place. Finally, all these multiple antennas and transponders at fixed sites must first be permitted to be installed and then must be maintained and functional.

b) Frequencies and Protocols

There are no global standards for frequencies or protocols. Protocols are basically the instructions on how the messages are transmitted over a certain frequency or carrier of the message. Imagine the lack of standardized instructions for a container and its transponder on a global voyage, i.e. China to South Africa to Europe and then to the U.S. Different regions will have different standards. There are national standards like ANSI ([American National Standards Institute](#)), international standards like ISO (International Organization for Standardization), and industrial standards like EPC (EPCglobal, Inc. which alone is in about 100 countries).

For instance, RFID frequencies on which the data ride in the United States will not work in another part of the world. The foreign transceiver cannot trigger the data transmission because the U.S. may use a different frequency or protocol. Therefore, RFID for container security is applicable only to those areas of the world which have agreed on the same frequency. This weakness is in addition to the corresponding need for a land-based infrastructure of antennas and readers. Unlike RFID tags used in products and pallets that are read in controlled distribution systems, active RFID devices in containers that move around the world through uncontrolled environments, require the construction of antennas at global chokepoints where containers are interrogated. Who determines the number and location of these points?

Constructing a controlled distribution path globally is really impossible. Typically, chokepoints are locations where readers could be positioned that cannot be avoided by the carrier of the container. They include the spot where a truck is loaded or unloaded, on a crane that transfers containers, a weigh station, the port of loading, or at the port of discharge. Only for these obvious chokepoints at origin and destination, is a land-based system a reasonable option. In areas along the route of the container's movement, a land-based system is virtually impossible to establish.

c) The IED Connection

Recently, concerns about RFID usage as a vulnerability at seaports and land ports have surfaced, suggesting that the use of RFID can constitute an Improvised Explosive Device

(IED). In fact, it is true that RFID emissions can serve as the trigger-mechanism for detonating an explosive device within the container. Because an explosive device can be easily wired to detonate with the proper RFID frequency signal at any of our nation's seaports and land ports, all out nation's ports that employ the approved RFID frequency for shipping containers become more vulnerable to terrorist attack.

To verify this vulnerability, in November 2007 a Southern city's police department's bomb squad, and three business firms connected to RFID usage demonstrated how RFID can be employed for that purpose. The demonstration was 100% successful, and it showed empirically the vulnerability of RFID transmissions as approved for use with containers passing through our international ports-of-entry. Present at that demonstration were representatives of the Department of Defense. In DOD's own words, the U.S. Army representatives examined the device and wiring and confirm that a commercial RFID interrogator was use to 'wake up' a commercial RFID tag. When the RFID tag responded on the 433 MHz frequency, the relay closed and the blasting cap set off the explosive

Months later DHS responded to the demo:

DHS recognizes and benefits from the use of RFID technology to ensure the smooth and secure movement of both people and cargo into the United States. It is accurate that RFID systems are in use at U.S. ports of entry (air, sea and land) and have been adopted by a number of private-sector companies for supply chain management, asset and shipment tracking and inventory purposes. While RFID system used in maritime ports rely upon a variety of transmission frequencies for port and terminals operations, there is currently no one common RFID frequency in use throughout the global supply chain.

While it is technically feasible that the detection of RFID emissions could be used to trigger an explosive device within a container, DHS does not agree with the report's assessment that ports that employ RFID technology become more vulnerable to terrorist attack.

DHS admits in writing that using the FCC-approved frequency for shipping containers as a trigger mechanism for detonating an explosive device is technically feasible (capable of being carried out). In summary, the weaknesses of RFID use in container security are linked to significant problems:

1. The acquisition of or access to real property;
2. The cost of installing fixed antennas and transceivers;
3. The maintenance of these fixed sites;
4. The absence of a common global frequency;
5. The existence of diverse RF protocols;
6. The age of data transmitted (distance between choke points); and
7. Its use as and IED.

Satellite and Tracking Communications

In general, there are two broad categories of satellite systems. The first and most widely known is geostationary or high-orbit satellites in equatorial orbit that appear to be stationary. Geostationary or geosynchronous satellites are approximately 36,000

kilometers or 23,320 miles above the Earth and rotate along with the earth. The second category is a low-earth-orbit (LEO) system which consists of satellites approximately 800 kilometers or 496 miles above the earth; these do not rotate with the earth. Both LEO and geosynchronous systems offer tracking and communications throughout a supply chain.

1. Satellite Benefits

Smart containers and their CSDs using satellite tracking and communications can provide a virtual chain of custody from foreign origin to U.S. destination. The container can send information and data in real time or close to real time 24 hours per day, 7 days a week. Messages from to and from the container can be simultaneously sent to multiple links in that chain, importer, exporter, carrier, or government agency. Unauthorized access into the container can be detected and reported as it happens. Diversions of the container can be detected, to include the container's reporting of its own hijacking. Identification of the person supervising its stuffing, verifying contents and arming the container's satellite security system at origin will be recorded. The identity of the person authorized to open the container at destination will also be recorded and included in all the electronic records of the container's movement. Satellite equipped containers not only can utilize these sensors and transmit immediately what was detected, but also send signals to make changes like temperature adjustments in the container as the need arises. Satellite applications even allow for remote unlocking of the doors.

Perhaps the best way to summarize its benefits is in relationship to the weaknesses of RFID smart containers. First, there is no need to acquire infrastructure for antennas or transceivers. Second, there is no need to install that infrastructure and equipment at these points around the world. Third, since there are no land-locked, global chokepoints, there is no need for their maintenance. Fourth, there is no concern for a common global frequency for transmissions. A single satellite provider can accommodate all transmissions in the licensed areas worldwide. Fifth, there is no need to have common global protocols. Sixth, all transmissions are in real time or close to real time and are not historical and delayed as with RFID. In other words, one knows about an unauthorized access to the container at the time it happens and before it arrives at the port of departure. Seventh, and probably most significant, it does not serve as a potential IED since it is not equivalent to random RF emissions. Instead, it is a programmed transmission within an established system for which there is a method of defeating its use as an IED transmission.

2. Satellite Weaknesses

There are very few, if any weaknesses especially compared to RFID. Perhaps one most commonly pointed out is that to transmit globally, one needs a license from the countries over which the satellite transmits. This has not been shown to be a significant weakness. For instance Iridium can just about transmit in over every international trade lane. Another weakness is its inability to transmit from dead spots like below deck in the vessel. The fact is, it can if the carrier cooperates and joins with the shipper in providing the technology to do so. It is a matter of cost, not capability.

The Mystery

There cannot be any serious comparison between RFID container applications and container Satellite tracking and communications applications. In every way satellite is superior. Yet government agencies like DHS and DOD continue to use and/or approve RFID for container control in a global supply chain, knowing that it can even serve as an IED. They do so at a time when the other trading nations of the world are developing satellite systems for container security. Just recently China began movement to test container satellite security systems, and it is rumored that China may even ban RFID for container security at its ports. The [EU](#) has instituted a special program called the Seventh Framework Program, a major component of which is to test and evaluate satellite container security systems.

Yet, in January 2009, CBP on behalf of the OFO-INDUSTRY PARTNERSHIP will conduct their field test of only a single source provider (GE) of radio frequency CSDs with shipping containers crossing the U.S. Mexican border. It does this while knowing the failure of RFID usage in the North American Trade Prototype tests done in the mid 1990s. It has excluded other technology and is testing a sole-source RFID system only, even though a firm employing a container satellite system has offered to participate in the pilot at only the cost of some travel and the cost of the container satellite units needed for and utilized in the field test. The satellite security firm would provide volunteer C-TPAT certified Mexican shippers and carriers without cost to the pilot or CBP. Yet, there has been no response by CBP to the offering of a head-to-head comparison of RFID and Satellite, this in the face of Mexico's own interests in seeing a satellite container security system, and at the official request in writing of a member of the U.S. House of Representatives to modify the pilot by accommodating the request of the satellite security system firm.

Does CBP really not want to know what other systems can do? Is its choice of a single-source product political? If not political, did CBP not know of the differences between RFID and Satellite? Does not CBP know of the movements in the EU, and China in recognizing the obvious superiority of satellite monitoring and control? Certainly, CBP knows of GMs Onstar capabilities with automobiles. Or can it not relate the concept of Onstar and container security? It is a mystery to many in and out of Congress why CBP does what it does, or fails to do what it should in the area of container security. It is clearly behind the rest of the trading world in this regard. There is certainly a challenge for the new Administration to improve CBPs level of awareness in this area.