RFID is not the one

James Giermanski from Belmont Abbey College argues that RFID is not the silver bullet for container security

James Giermanski is the Chair of the Department of International Business for Belmont Abbey College and Chairman of Powers International Inc.

It seems that RFID – the short term used to refer to radio frequency identification – has become the current 'buzz word' among some of the largest retailers and importers in the United States.

Wal-Mart and **Target** are just two of the giants discussed in the literature. Recently, an **A. T. Kearney** report entitled *Smart Boxes* lauded the potential and actual use of RFID for certain supply chain applications.

However, the application of RFID to container security and port security is less laudable, less effective, more costly, and certainly questionable as a primary means of international transportation security for containers. RFID applications, whether active or passive, have very clear weaknesses and impediments to usage in a world-wide context. The impediments are these: the absence of agreement on RFID world-wide standards; its land-based character; and the rights to acquisition, cost, and control of required RFID infrastructure.

Protocols and standards

RFID applications require the carriage and transmission of data through a wireless system. Data can be loaded into a device called a transponder, and can then be transmitted via radio waves when the transponder is triggered by a corresponding device called a transceiver or reader. The transponder is a slave RFID unit that reacts to a triggering radio frequency message from the master transceiver. The transceiver, through its antenna, sends the triggering frequency, which produces a return transmission of the data pre-loaded into the transponder like manifest or shipping data or information acquired by the RFID device like the opening of the container door. Since the transmission of these data is by electromagnetic waves, the successful transmission is subject to the use of the proper frequencies or waves and 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.

In order for the transponder and reader to talk to each other, they need to speak in the same way. In other words, they must follow a protocol or a set of instructions. While no analogy is perfect, assume it is something like one person speaking Spanish and the other English and at different speeds, with different volumes, and both talking at the same time. In our analogy, protocols tell each person (in the real world, the container and the reader) when to start and stop, what language to use, how fast to talk etc. Unless the instructions are clear to each, communication may not take place. There are no global protocols or standards, however. Imagine the lack of standardised instructions for a container and its transponder on a global voyage: different regions will have different standards.

There are national standards like those from the **American National Standards Institute (ANSI)**, international standards from the **International Organization for Standardization (ISO)**, and industrial standards like the Electronic Product Code (EPC) from **EPCglobal Inc.** ISO has 12 standards related to RFID. In other words, until there is some universal or global protocol or set of instructions, RFID usage on shipping container security is unlikely.

Frequencies, too, have different bands, like low, intermediate, and high. Each band is more appropriate for unique usage. For instance, low-frequency RFID is used for short to medium distances, low speed, and simple applications such as access controls. Intermediate frequency bands can also be used for access control also but offer a little faster read speed. High-frequency RFID is used for fast read speeds and if the specific standard allows high wattage output, longer range can be obtained.

The major problem is the frequency approved for use by different

governments. Like protocols, RFID-approved frequencies differ globally. Thus, RFID 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 US may use a different frequency. For example, the **United States Federal Communications Commission (FCC)** issued a final rule effective on 23 June 2004 that only 433 MHz RFID systems can be used for commercial shipping containers. Likewise, other countries in other RFID frequency regions have approved different frequencies for different uses. Therefore, RFID for container security is applicable only to those areas of the world which have agreed on the same frequency for the same usage, precluding a standardised global use of RFID for shipping containers.

Land-based character

In addition to the frequency problem exemplified by a lack of world-wide standardisation, an equally troublesome area for RFID usage in container security is the overland movement of containers and the corresponding creation of a land-based infrastructure of antennas and readers. Unlike RFID tags used in products and pallets which are read in controlled distribution systems, active RFID devices in containers which move around the world through uncontrolled environments require the construction of antennas at chokepoints (those points along the journey of the container which cannot be circumvented by the carrier). Constructing a controlled distribution path globally is really impossible. The A.T. Kearney report defines chokepoint location this way: 'Chokepoints where readers might be positioned 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.

RFID generally requires line-of-sight transmissions. In the case of container security, each RFID transponder connected to a container would have to 'see' the transceiver that triggers the transmission of data from the container. The approved 433 MHz frequency requires line of sight. How close the reader is to the container is also a troublesome issue. Geography and topography are consequently a potential issue in constructing antenna systems close enough to the container but far enough away to see the antenna of the transponder connected to the container.

Cost of RFID infrastructure

Although the land-locked constraint can probably be overcome by proper use of topography and construction techniques, there is another problem related to a land-based system of security, particularly container security. The issue for RFID technology on containers is that the user will probably not own the land on which readers (transceivers) would have to be installed as fixed sites, nor have rights to install its antenna system along the routes the container and chassis travel. This is a problem for commercial motor carriers using public roads. Railroads, in contrast, are much better candidates for RFID usage because they have 'rights of way' and own their own track infrastructure. However, there is some concern about whether 433 MHz (the low end of the high frequency band) is good enough for reading rail-carried containers and railcars at the speed they pass a fixed transceiver or antenna. Another good candidate for RFID container security usage is the US **Department of Defense (DOD)**. Like the railroad, the DOD can often, although not always, control its chokepoints in a manner superior to that of a commercial motor carrier.

To construct fixed-position readers one needs access rights to the land or the equipment on which one installs the reader. Take, for example, a seaport. Who owns the port? Is it the property of the city in which it is located? Is it managed by a port authority? Who owns the gantry cranes on which a user of RFID technology wants to place the transceiver? The same scenario is applicable to US land ports-of-entry. In the case of Laredo, Texas, on the US-Mexican border, the city owns the bridges. Therefore the city would have to give or lease the right to erect an antenna or fixed-position reader on its bridge for a single shipper or carrier. Since private or government property will be on each end of the bridges between Mexico and the US, will the governments or landowners provide proprietary usage to individual shippers or carriers?

Finally, how does one control the footprint problems at busy ports with multiple transceivers, transponder-fixed containers, and antenna footprints? As mentioned previously, the protocol or instructions for the container and transceiver to communicate have to be clear. Who talks first and what bandwidth is used are critical. The combination of finding the corresponding talkers (transceivers outside and transponders inside containers), instructions on which talks first, the speed of talking, and the volume of data transmitted make for increased distortion and interference, especially at congested ports and land-based chokepoints. In the mid 1990s, the North American Trade Automation Prototype (NATAP) tests, of which I was a part, were conducted at a few selected land ports-of-entry along the Mexican and Canadian borders using RFID. These tests encountered these exact problems.

At major modern seaports like Rotterdam, everything is moved by RFID applications. There are no drivers in the tractors that pull the containers. There are multiple gantry cranes seemingly working on their own in coordination with moving trucks and chassis. Superimpose on this RFID-layered sea port RFID frequency and protocol differences between the US and the Netherlands, for example, and one will

see immediately that RFID applications to container security would be quite difficult, if not impossible.

Associated with the access and cost of RFID infrastructure is the cost of container modification. An inexpensive passive RFID tag can be hung on the outside of the doors and respond to a transceiver as to whether the doors have been opened in the normal manner. A more expensive active RFID device can also be hung on the outside of the doors and send a signal on its own at a chokepoint indicating whether the doors have been opened (assuming the doors can be read at the chokepoint). However, an active RFID device placed inside the container that can sense access to the container through means other than the doors is an expensive proposition compared to the inexpensive passive tag. Not only does the active device, itself, cost more, but also the container has to be structurally modified to accommodate the internal RFID transponder and its antenna. Since the RFID frequency approved for containers does not emit through steel, the RFID device internal to the container must have access through the steel to the outside in order to function – a required modification to the container. Permanently modifying a container for only RFID may be unacceptable to the owners.

Conclusion

RFID alone is certainly not the 'silver bullet'. It is not an ideal method, nor even necessarily the least expensive method, for delivering container security. So far, the literature on this subject has focused not on a solution to the problem of security, but on a communication device which is one part of the solution. The security solution requires a complete system of end-to-end coverage, a solution from origin to destination, one without the disparate protocols and frequencies, and the problems of access to and cost of land-base infrastructure.

The future of container security is a satellite solution which by its nature avoids the limitations and infrastructure costs of RFID configurations. The global movement of containers requires a global solution, not encumbered by the constraints inherent in current RFID applications and lack of standards. The apparent rush to RFID applications for container security in a global market is premature and limited as a land-based system.

Contact:
James Giermanski
Belmont Abbey College
Tel: +1 704 825 4741.
Email: powersintnlinc@bellsouth.net