

RFID v. Satellite in Smart Container Cargo Security

Why RFID systems for global supply chain and cargo security fall short when compared to satellite technology

Jim Giermanski
SecurityInfoWatch.com

Although most retailers use RFID, it seems that because retailers like Wal-Mart, Target, Home Depot use it, it must be good for the supply chain too. And because firms like Maersk, GE, Siemens, IBM, SAVI and others have already adopted it for global supply chain use, it must be good. And, of course, since nobody of that stature has gone to satellite communications that does more than simple GPS tracking, satellite communications must not be good for global supply chain communications. Well, here is the reality: RFID is not good for global supply chain usage and satellite is good. In fact, RFID usage is actually dangerous for applications in U.S. seaports. It's time to compare. I've chosen six areas of comparison: technical application, infrastructure needs, timeliness of reporting, features available, costs, and risks.

Technical applications

RFID is critically impaired for global usage, first because there is no worldwide agreement on frequencies. The RFID frequency on which data are carried is not the same RFID frequency in Germany that is approved for use in the U.S., nor approved by China for use there. Since frequencies vary, so do the equipment requirements, making it virtually impossible to use everywhere in the world. That presents an obvious problem, since global supply chains allow containers to go everywhere in the world.

Additionally, protocols differ. Protocols are like someone speaking French and the other English at different speeds, stopping and starting at different times. In other words, there are no global RFID communicating rules.

Satellite has no such limitations. A satellite system using either low earth orbit (LEO) constellations or a high-altitude geosynchronous satellite transmits data differently, but the vendors' systems will work anywhere in the world that they have coverage. Therefore, satellite applications are not critically impaired by regional differences and are useful for global container security.

Infrastructure

RFID, since it is radio frequency, needs antennas in every location where one wants to read or talk to the RFID unit of the container. Antennas for RFID readers must be placed on property owned by the RFID user, leased by it, or provided to it. Acquisition, then, is both a legal and operational issue, especially when RFID signals have only limited distance and direction. Readers with antennas also require maintenance and control. Furthermore, other users of RFID can select locations for their units which interfere or distort another RFID user's signals - a footprint problem. It also seems that fixed antennas may not be practical given legal access rights and costs. Therefore, handheld transceivers must replace the fixed antennas, creating another problem of equipment needs, the need for increased personnel to interrogate each container, and the high costs of handheld units. Satellite has virtually none of these problems.

Timeliness & Features

Automated RFID systems can only make use of chokepoints or physical areas through which the container must pass, such

as at the gate of a port, or on the crane in charge of unloading a ship. Similar to the transceivers used at department store doors that alert if the RFID tag is not removed for the product just purchased, no alert is given until one passes through the chokepoint. In other words, RFID is land-based and historical in nature. The container reports what happened to it before it reached the chokepoint only at the time it passes through the chokepoint where there is an antenna and transceiver to interrogate it. Of course, if the container were breached and goods stolen or an explosive device inserted prior to the chokepoint, it would be too late to actively respond to the breach, assuming the RFID unit was integrated with a container alarm system which could detect breaches into the container in addition to container door access. The benefit of a satellite system is that it can communicate in real time or nearly real time depending on the satellite system used.

RFID can utilize different sensors for different purposes. It can be electronically linked to sensors such as light, vibration, and temperature, in addition to access, humidity and more. The problem, again, is that it lacks the capacity to report what it detects until it reaches a choke point where it's data can be read. Satellite-equipped containers can likewise utilize these sensors, but the benefit is that satellite systems can be programmed to transmit immediately what was detected, and also to send signals to make changes like temperature adjustments in the container as the need arises. Satellite applications even also allow for remote unlocking of the doors because of the variety of data that can be sent. Finally, satellite offers redundancies in notifying the user of problems encountered during the international movement of the container. An RFID user only knows something when and if the container reaches the point where RFID readers are installed.

Costs

Both RFID and satellite require hardware, and RFID and satellite require the installation of an antenna into the container. However, the use of RFID means costs of infrastructure acquisition, antennas for fixed sites, handheld transceivers, the people to use them, and maintenance. Certainly, there are notable expenses of installing any type of signal creating, sending and receiving device in a container in a manner which allows its electronics to be protected in the not-so-gentle world of global shipping. Those expenses and design challenges apply to both RFID and satellite container communicators, but once installed in the container, satellite costs are limited to the cost of message traffic since the rest of the technology is provided by established vendors in this market like Orbcomm, Iridium and others. Satellite message traffic typically involves short burst of data, and that traffic can be designed to occur only when needed, making satellite a less expensive proposition, especially when compared to the infrastructure, maintenance, handheld readers, and corresponding personnel costs needed for a large-scale cargo security RFID deployments.

Risks

In this writer's opinion, RFID connected to container interrogation should not even be allowed in U.S. ports. It actually could serve as the means to detonate an explosive device. Because of its radio frequency characteristics and the legal requirement to use a frequency established and mandated by government regulations, anyone who knows the frequency can design a dirty bomb to explode when the container is interrogated in the U.S. seaport, making an RFID security system in effect, the detonation trigger.

While there is risk of this in any communication system, satellite signals are not as susceptible to this type of usage. With satellite, the antenna in the container is tuned to the correct frequency range and constantly picks up signals from the satellite. The modem understands the message protocol and intelligently answers. The information is then transferred between the container unit or modem and the satellite. Due to the constant communication between modem and satellite, one has to be a lot smarter to use the signal. One has to understand the message protocol, be able to decipher it and then use it to trig-

ger a device. The mere presence of a signal is not enough.

Satellite signals are unique to each container, ciphering and deciphering are required, and the satellite modem would have to be designed to accomplish this type of triggering, requiring the manufacturer of the unit to design it to trigger a specific device in a specific container.

With RFID, it is, however, possible to listen for the correct frequency signal and trigger a device based on the presence of such a signal. Such a signal will, for instance, be automatically present in a port when interrogating a container using RFID.

Conclusion

In summary, it's my opinion that RFID is inadequate in almost every way for the needs of global container security. Then, why do industry giants seem to be committed to it? Its use is certainly understandable for retail, warehouse controls, and in any situation where one can control infrastructure and location, but when we approach global supply chain security, the technology falls short. The GEs, Maersks, and IBMs of the world may have simply jumped prematurely on the RFID bandwagon and many of those companies now want the U.S. government to support their RFID investment that they have made. But the more one knows about global supply chain security, the more one has to accept the inevitable: The future of global container security is not RFID; it is satellite.

About the author: Dr. Jim Giermanski is now Professor of International Business and Director of Centre for Global Commerce at Belmont Abbey College. He often serves as a consultant on international transportation and transportation security, border logistics, and trade matters involving Mexico. He has frequently given invited testimony on NAFTA, transportation, and other international business issues before the U.S. Senate and House, the Texas Senate and House, EPA, and the U.S. International Trade Commission. Dr. Giermanski is chairman of the board of Powers International, Inc., which provides supply-chain security solutions, consulting, and training. He currently provides transportation security lectures on C-TPAT, and other Customs and Border Protection (CBP) programs.