

The facility, located at JFK Airport, is using active RFID tags and readers from Axxess International to track individuals as they move between public storage and a secured area.

By Claire Swedberg

May 13, 2010—In one of its bonded warehouses at New York's John F. Kennedy International Airport, the [U.S. Customs and Border Protection](#) (CBP) agency, part of the [U.S. Department of Homeland Security](#), is employing active RFID tags to track the movements of individuals between a public storage area and a secured area. The system enables the agency to know when and where people cross a yellow line painted on the floor to delineate those two sections, as well as whether those individuals are authorized to do so. The system was provided by [Axxess International](#). Due to interest from other organizations for a similar system, Axxess' president and CEO, Allan Griebenow, says his company is making the perimeter-crossing solution commercially available as part of its existing automated access-control and ID system, known as Dot Wireless Credential.

Bonded warehouses (also known as customs warehouses) store cargo pending the export or release of imported items that may require payment of duties or taxes. Part of the CBP's large warehouse at JFK Airport is open to the public, while access to the section for storing bonded items is restricted to certain airport personnel. The two locations are separated not by a physical barrier, however, but by a long yellow line, painted across the floor, that unauthorized personnel are not permitted to cross.

Axxess International installed RFID activators (which transmit an RF signal to awaken dormant active tags) and readers along the entire perimeter, and supplied its warehouse staff with ID badges containing Dot Wireless Credential RFID tags. This enabled CBP to track the identities of all individuals wearing the tags as they cross the perimeter, and to receive an alert if an unauthorized individual, wearing a tag with a unique ID number not listed in the authorized category, crosses the perimeter.

To detect when those not wearing a Dot Wireless badge cross the perimeter, Axxess has deployed additional hardware to sense a person's movement over that line. Griebenow declines to describe the details of the deployment, such as the type of sensors used. However, he says, the Dot Wireless Credential system with perimeter-tracking functionality can work with a variety of motion-detecting hardware, including infrared, video and pressure plates.

Typically, a detection system uses a light or infrared beam aimed in such a way as to detect any physical breach of a perimeter. Data indicating the breach is then transmitted to Axxess software via a cabled connection.

At the same time, if an individual wearing a Dot Wireless badge breaches such a perimeter, his or her badge is awoken by the activator, which transmits a 132 kHz signal encoded with an ID number. The badge's tag then sends its own unique ID number, along with that of the activator, to the RFID readers, either at 315 MHz or 433 MHz, using a proprietary air-interface protocol. AxxessView software compares the quantity of personnel who have breached the perimeter, based on the detection hardware

data, against the number of ID badges read. In the event of a mismatch—in other words, if the total number of people crossing the line is greater than the quantity of badges read—an alarm can be sounded, and a text message or e-mail can also be sent to management. In addition, if video surveillance is being used, the images taken at the location and time of the breach can be forwarded to interested parties.

Depending on building codes, Griebenow says, readers and activators could be installed on ceilings or walls. The read field could be adjusted to make it more sensitive, he adds (for example, to reduce stray reads of those near but not crossing the perimeter) by adjusting the strength of the activators' signals or the sensitivity of the readers. But typically, he notes, the read field would be four to six feet wide.

Since each activation point has its own unique ID number, the system can also detect the approximate spot at which an individual with a badge crossed the perimeter. Granularity would depend on the number of activators installed.

This latest functionality to Axxess Wireless' existing system, Griebenow explains, is part of a strategy of providing a total solution for access control that goes beyond permitting access at doorways. "We believe this is significant, because we can augment what our wireless credential offering provides," he states. "There is no product on the market that can do this kind of intrusion detection during hours of operation." Most perimeter security, he notes, is managed at night, outside of a company's regular business hours, when any movement detection would trigger an alert.

In addition, the system can be utilized to ensure assets are not taken outside of a facility's permitted sections. If, for instance, a tagged projector was carried toward a stairway or an exit, an alert could be sent, along with information regarding where that breach was occurring. If the individual with the asset was wearing a badge, the system could also link him or her with the event.