Opportunities in Access Control: Capitalizing on New RFID Applications

Whitepaper

Tony Diodato
Chief Technology Officer
Cypress Integration Solutions

Zachary Polikarpus
Product Engineer
Cypress Integration Solutions

Abstract

Like most businesses, those in the security industry have a need to increase revenue. For integrators, dealers, installers and manufacturers willing to think outside the box, a world of new access control opportunities is available.

Access control now encompasses more than a card reader wired to a fixed point on the wall. Complementary developments have expanded the usefulness of Radio Frequency Identification (RFID), happily at a time when costs are decreasing.

Developments such as Power over Ethernet, the new Open Supervised Device Protocol, and the advanced use of wireless technology have all emerged alongside RFID, enabling the spread of RFID beyond traditional access control applications, as illustrated here.

RFID

RFID refers to Radio Frequency Identification. According to the RFID Journal, Radio Frequency Identification has been around since at least the 1970s.[1]

An RFID tag contains a microchip with a serial number or other ID information, plus a tiny antenna.

An RFID card reader sends out radio waves. With passive tags, when those waves reach the tag's antenna, the tag absorbs enough power for the chip to modify the radio wave and reflect it back to the reader. The reader captures the chip's information and shares it with the system to which it is connected.

There's no need for the RFID tag (or transponder) to touch the reader, since the reader can capture the information when the tag is in close enough proximity. This is why RFID tags are often known as proximity cards, or prox cards.

Developments affecting RFID applications

Developments such as Power over Ethernet, the new Open Supervised Device Protocol (OSDP™) and the advanced use of wireless technology have opened the door for new, non-traditional access control applications.

Open Supervised Device Protocol (OSDP™)

OSDP is a security protocol recently adopted by the Security Industry Association (SIA) which offers standardization, as well as enhanced security and supervision. The protocol was developed in response to problems with using the de-facto Wiegand standard, as well as changes within the security industry. While work on the protocol was initially undertaken by companies such as HID Global, Mercury Security Corporation and, more recently, Codebench Inc., it was later assigned to SIA's Access Control & Identity Group.[2] OSDP products have been on the market since 2015.

OSDP benefits: Using OSDP brings interoperability, enabling access control components from different manufacturers to work together. This is especially important in future-proofing projects, making it easier to upgrade components as needed.

[1] http://www.rfidjournal.com/site/faqs - Anchor-What-363

[2] http://www.siaonline.org/blog/Lists/Posts/Post.aspx?ID=56

Along with helping different manufacturers' components work together, the protocol's Secure Channel mode uses AES encryption for beefier security. In fact, OSDP is one of the few technologies which protects a card reader from hacking, by inexpensively securing the last bit of wire between a card reader or peripheral device, and its network infrastructure.

Also, since the specification was developed with an eye toward cost-effective implementation, OSDP does not require USB, Ethernet, or expensive routers, cable, or labor. Another money-saving aspect of using OSDP is scalability: Using OSDP products means many more devices are supported than when using Wiegand.[3] Finally, OSDP is more resilient in harsh outdoor environments.

Criteria for OSDP use: Use OSDP products in any installation to reap the benefits of enhanced security and supervision, overcome the challenges of Wiegand and proprietary devices, or streamline installations (current or future) by using more readers or devices with a single connection. Since there's no downside to OSDP, the sooner OSDP products are used, the more manufacturers will be motivated to supply the market with OSDP devices and move away from proprietary technology.

> *OSDP is one of the few technologies which protects a card reader from hacking, by inexpensively securing the last bit of wire between a card reader or peripheral device, and its network infrastructure.*

[3] http://www.osdp-connect.com

Power over Ethernet (PoE)

PoE devices do not require a separate power supply, since the device receives power over an Ethernet cable. The use of PoE started around 2000, when Cisco used the technology to power IP phones.[4]

PoE benefits: Using Power over Ethernet saves time and money by using structured wire already present in commercial buildings. Along with streamlining installations by reducing wires, PoE prevents installation issues sometimes arising from the varying power supply options. PoE devices also allow unprecedented built-in supervision capabilities. In a system with multiple components, troubleshooting of power issues – including loss or drop of power – can be completed remotely instead of physically inspecting each device on site. Plus, PoE uses readily available tools, components and techniques, such as Ethernet cables. Perhaps best of all, many IT personnel are already comfortable using Power over Ethernet, a definite boon for the increasing number of projects involving IT departments.

Criteria for PoE use: Since the cost of PoE equipment is reasonable, it is useful in any projects in which the above benefits are desirable, especially in installations in which the project involves IT personnel or software developers who already embrace PoE.

PoE devices allow unprecedented built-in supervision capabilities. In a system with multiple components, troubleshooting of power issues – including loss or drop of power – can be completed remotely instead of physically inspecting each device on site.

[4] http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/white_paper_c11-670993.html

Wireless technology

Although general-purpose technologies such as Wi-Fi, Bluetooth, or cell phones have helped individuals become comfortable with wireless, this discussion refers to the dedicated wireless medium based on the IEEE's 802.15.4 wireless protocol, often used in the security industry for its reliability. People accept it takes longer for Wi-Fi, Bluetooth and cell phones to connect, and know they'll sometimes lose their connection, whereas in the security industry, wireless technology is expected to connect in milliseconds and remain connected.

This 802.15.4 wireless technology, which has been in use since early last decade, used AES encryption to secure wireless data transmission even before the same level of security was available in wired access control components.

Wireless benefits: Along with securing data, wireless has long enabled installations at the most challenging sites, such as in parking structures, and over railroad tracks and roadways. Wireless is also essential at remote sites, as well as in elevator shafts or other structures where minimal disruption is desired, such as historical sites or buildings with asbestos. Temporary installations, such as construction sites, or situations in which handheld mobile access control is needed, also require wireless technology.

An advanced use of wireless, known as Agile Access Control Technology (AACT)[5], originates with the 802.15.4 standard, at a level which transcends simply opening a "serial tunnel" to transmit data instead of transmitting over wires. AACT can wirelessly connect dozens of readers to a central point, nearly instantaneously.

AACT's speed and scalability is a major advantage over point-to-point wireless, which can be thought of as connecting two tin cans with a string. Soup-can communication is pretty impressive until you add dozens more cans and strings, with many more people trying to communicate.

Since the IEEE's 802.15.4 wireless standard is now being used to a fuller extent than before, many readers can be connected using event-driven, statistical multiplexing, which allows the supervised transfer of data without the lag from polling each reader, one at a time. The benefit is further increased by combining the wireless technology with the emerging OSDP protocol *(see below).*

Criteria for Wireless use: Because wireless technology brings a range of benefits, the main criterion for everyday use is simply whether a

[5] http://cypressintegration.com/aactmobilereader

wireless solution can be installed and maintained more cost effectively than a wired solution. Historically, wireless has been more expensive than wired installations, but is approaching the tipping point where wireless costs will equal that of wired access control technology.

Agile Access Control Technology (AACT) can wirelessly connect dozens of readers to a central point, nearly instantaneously.

Outside-the-box RFID access control applications

RFID access control applications are limited only by imagination, as seen in these examples.

1. **Non-traditional RFID use:**

RFID and OSDP in NASTAR ski race course

To automate skier enrollment for timed racing, Cypress provided a plug-and-play RFID reader solution incorporating the Open Supervised Device Protocol (OSDP).[6]

At the top of the run, skiers presented credentials to enter the race. Once a racer was enrolled in the database, the system enabled quicker enrollment for subsequent runs. OSDP-based technology linked the reader with the data host system.

The OSDP solution can leverage RFID using smart cards to collect data, whether at a secured door or on a ski race course. In this case, OSDP provided a lightweight access control-like system over a twisted-pair medium. This combination also allowed the data signal to travel farther down the mountain than with alternative technologies such as Ethernet and Wiegand.

In addition, OSDP's multi-drop capabilities meant one length of 2-conductor cable could accommodate many readers, eliminating the need to run wire all the way down the mountain for each reader. OSDP over twisted-pair was also chosen for its ability to stand up to the moisture, cold, and potential ice buildup in a ski course environment.

[6] http://www.nastar.com/articles/whats-new-with-nastar

2. Non-traditional RFID use:
RFID and AACT Mobile Wireless in Veridt's rapid deployment Mobile Physical Access Control System (MPACS)

Veridt utilized wireless Agile Access Control Technology (AACT Mobile) to secure sites in mission critical applications where conventional wired infrastructure could not be deployed, either due to critical timeline requirements or in applications in which the physical site was not conducive to traditional implementation of the PACS infrastructure.

Veridt's Mobile Physical Access Control System (MPACS) was designed to enable rapid deployment in emergencies, disaster recovery and other mission critical situations where securing of an area needed to be accomplished swiftly, with minimal effort, and with confidence in a secure outcome.

The access control hardware for the self-contained MPACS system is mounted in a rugged Pelican case on an integrated aluminum frame. Since all components are packed into the case, the system can be immediately deployed, even in harsh environments.

The system contains two module types: the control unit, and the expansion unit. The system operates as many as 16 doors in configurations of four, eight, 12 or 16 doors, as the system warrants, providing flexibility, efficiency, and cost-effective deployment. It is also prewired (more cases can be deployed; each accommodates an additional four doors).

The control unit, as shipped, is easily assembled, requiring minimal drilling. The unit's requirements include only standard AC power and Internet access, as appropriate for the deployment. No cable connections are required between the door, gate, or other perimeter location to be secured.

Communication with the central access control station (located in the Pelican case) is achieved wirelessly using 2.4 GHz point-to-point communication, while securing the door requires no existing infrastructure beyond AC power.

Using AACT Mobile technology was a significant advantage in the project versus hard-wired alternatives, which could mean waiting days to run wire, or changing over existing network infrastructure to accommodate RFID readers and panels.

3. Non-traditional RFID use:
RFID and Power over Ethernet (PoE) for data collection

In a crossover project combining security and IT, Cypress incorporated Power over Ethernet technology into RFID card readers for an international client, enabling the client to collect data from multiple devices at each of its sites.

The installation was a project of the company's IT department, rather than a security department.

The reader sent data directly to software written by IT personnel, bringing RFID into the realm of standard IT equipment, instead of forcing the client to deal with specialized circuit boards and electrical cabinets. PoE enabled the reader to act like a browser, as far as the IT department server was concerned. In addition, the IT infrastructure allowed remote monitoring of the RFID readers. Using Power over Ethernet also removed the need for a separate power supply for each reader.

This is especially noteworthy for security practitioners in an era when IT and security projects are increasingly meshing. PoE is an ideal fit for IT data collection applications using RFID readers, since there is no requirement for relatively high-current door openers.

PoE makes it profoundly simple for IT personnel to plug an RFID reader into an IT component, program it and go, allowing RFID readers to be used in applications such as collecting and sending time and attendance data directly to data management software, tracking production at work stations, allowing access to server rooms, managing inventory, or safeguarding computers by combining RFID cards with computer passwords for 2-factor authentication.

Summary

The pairing of RFID with new developments such as PoE, OSDP and wireless AACT offers a wealth of opportunities for integrators, dealers, installers and manufacturers to increase revenue.

Security practitioners can offer current clients a range of security devices, including robust wireless products using AACT, and better security using OSDP.

Along with upselling to current clients, crossover applications appealing to IT departments are more feasible than ever, thanks to PoE.

Since the data collection capabilities of RFID are enhanced by new developments, traditional access control applications can also be adapted to a range of uses outside security. Companies such as Cypress Integration Solutions and Veridt are experienced in thinking outside the box, and welcome such discussions.

Tony Diodato and **Zachary Polikarpus** together have nearly 40 years of expertise in access control protocol and format conversions, including the Security Industry Association's new OSDP protocol. Tony is the founder and CTO of Cypress Integration Solutions, manufacturer of the OSMIUM Wiegand-OSDP interface, winner of the 2015 ISC West New Product Showcase: Best in Access Control Devices & Peripherals.

Cypress Integration Solutions, Inc.
solutions@CypressIntegration.com
CypressIntegration.com

CYPRESS
INTEGRATION SOLUTIONS

Cypress Computer Systems