

Key Considerations in Choosing the Right Industrial Access Control Solution

A practical guide for industrial enterprises in evaluating the pros and cons of the four most prominent automation access control methodologies and solutions.

State of the Industry

Controlling access to and within the manufacturing plant and protecting information and automation systems from breaches is a business essential. Physical or logical security lapses, whether accidental or malicious, can cause significant and lasting damage, particularly when it harms personnel, the equipment or environment or impacts the quality process.

Building automation systems control a facility's climate, lighting and similar systems, and equipment automation systems control machines and processes. They are often driven by programmable automation controllers (PACs) and use a human-machine interface (HMI) for configuration, notifications and routine control. With these systems growing in number and increasingly interconnected, programmable controller and HMI access control becomes an imperative.

Everyone is a stakeholder when it comes to access management, from the facility and security managers to the personnel in operations, maintenance, engineering, inventory, purchasing, training, IT and the corporate suite. Different levels of protection, identification, and authentication are needed, depending on the HMI and application.

Leveraging the employee badge is a sound and economical approach to protecting production processes, data, and critical assets throughout the organization. Considering that nearly everyone entering a locked facility has to present a security badge of some sort to gain entry, why not apply this same concept — and smart technology — to logical security concerns inside the building?

This white paper is part of a leadership series which explores the latest advancements in smart technologies in industrial access control, including the vital methodologies and solutions that are critical in addressing today's evolving security needs.

Part 1, "New Developments in Industrial Access Control and Identification," includes discussions of new trends in access control that are changing the role that access authority plays throughout the organization. It also highlights the ways in which employee badge solutions are streamlining access control processes, improving risk management and creating significant savings for today's organizations.

Part 2, "Key Considerations in Choosing the Right Industrial Access Control Solution," provides a practical guide for evaluating the four most prominent access control methodologies in use today, including discussions of the advantages and disadvantages of each methodology. The paper concludes with an introduction to RFID access control badges and readers and their applications in today's enterprise organizations.

Part 2 of the RF Ideas Leadership Series

THIS WHITE PAPER EXPLORES:

- Advantages and limitations of the four most commonly used access control methods
- How RFID compares with magstripe and barcode badge solutions
- The unique design characteristics and capabilities of RFID badges and readers
- Data storage capabilities of RFID backend systems

Access Control Methods and Selection Considerations

The proliferation of new industrial access control technologies is making the selection of the right method challenging for enterprises searching for solutions to their unique business and security requirements. The most prevalent access control options include manually typing in passwords or pin numbers, or presenting employee badges — the most common types being magnetic stripe, barcode, and radio-frequency identification (RFID) smart cards — to a badge reader. Each approach has its advantages and limitations, though the manual method is quickly losing favor. Using a combination of methods for multi-factor authentication achieves a higher degree of security.

The determination of which methods and technologies to use must be based on the needs of the organization, and include an analysis of how the benefits outweigh the disadvantages. With various automation management platforms syncing with a directory service and databases, identifying badge-based reader solutions that are independent of those platforms will “future-proof” the investments as best as possible.

“Regarding the use of RF readers, barcodes, passwords and the like for access, it is usually a combination of the security practices of the particular company’s IT and Operations departments that determine access methodologies on a case-by-case basis, rather than a trend of companies going in one direction or another,” suggests ARC Advisory Group’s Resnick.

Manual login

Typing user ID and passwords on a keyboard or smart device remains the dominant method to access secured software. Unfortunately, this method is rife with limitations that can only be avoided with the ease, efficiency, and accuracy of badge-based access control.

Advantages:

This approach offers flexibility in the ability to change passwords from time to time.

Disadvantages:

Manual login is the most time-consuming method of access control, and it requires a fair level of dexterity and freedom of movement that is not always available in manufacturing settings. For example, it is difficult for factory workers to type while wearing heavy protective gloves, but removing the gloves may put themselves and the facility in a position of non-compliance.



Research indicates that as the number of circumstances in which individuals used passwords increased, the incidence of forgotten and mixed-up passwords also increased.

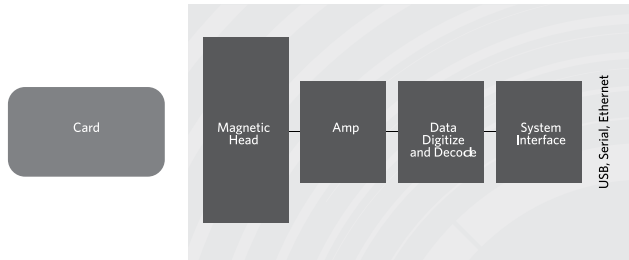
In addition, now that “secure” passwords are getting longer and far more complex, the time required for entry, the potential for error and rekeying, and the likelihood of forgetting the password and requiring help desk support is increasing. Adding to the challenge are the numerous applications and systems used by workers that each require a unique login and password. It is increasingly difficult to manage multiple, complex passwords.

Research validates these concerns. A [study](#) published in December 2012 found that as the number of circumstances in which individuals used passwords increased, the incidence of forgotten and mixed-up passwords also increased. The intricate characteristics of secure passwords also pose a problem. While such passwords are difficult to be guessed by intruders, they are in general considerably difficult to be remembered by authorized users, according to the study.

Magstripe badges

Magnetic stripe (or magstripe) badges use iron-based magnetic particles to store the employee’s unique identification number. Physically and functionally, they resemble a credit card. As the badge is pulled through a slot on the reader, an electromagnet is used to detect variations in the magnetic poles embedded onto the card’s magstripe, and those variations represent the employee unique ID.

MAGNETIC STRIPE READER



Advantages:

Magstripes were the first iteration of employee badge technology, so they are a known entity and broadly adopted. Because they are similar in function to credit cards, they are particularly common with purchase authorizations. Magstripe cards are currently evolving from swipe to contact cards, which are the next level up in access security.

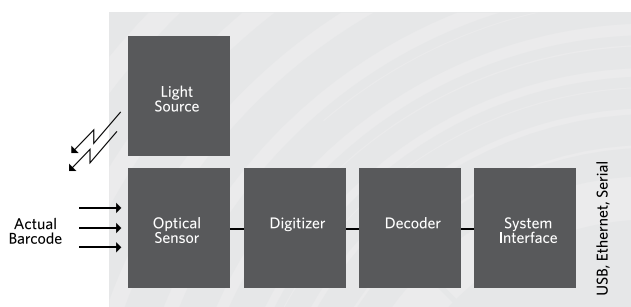
Disadvantages:

Like credit cards, a magstripe badge will usually work, but sometimes it won't. Over time, the stripes will collect contaminants, which then transfer to the magnetic heads in the magstripe reader, causing the read to fail. This tendency limits the environments where this type of badge can be used, including greasy, gritty industrial spaces. To mitigate this risk, periodic cleaning of the reader head is needed. Another concern, from a security standpoint, is that lost or stolen magstripe cards can be easily copied with a credit card copier.

Barcode badges

Barcode badges store the employee's unique ID in the variations of light and dark in the bar or QR code pattern. When the badge is presented to the barcode scanner, a photo diode measures the intensity of light reflected back from the light source. Dark stripes absorb light and white stripes reflect light, and those variations are seen by the photo detector. The decoder then converts the digital pattern to a text value that correlates to the employee ID.

BAR CODE READER



Advantages:

Barcode badge technology is well established and provides for quick and easy access to secured areas and bar coded inventory and tools. The cost to print a barcode on an employee badge is negligible. Barcode scanner apps, widely available for smart phones and other portable devices, provide a level of flexibility when inventory controls and tracking are required.

Disadvantages:

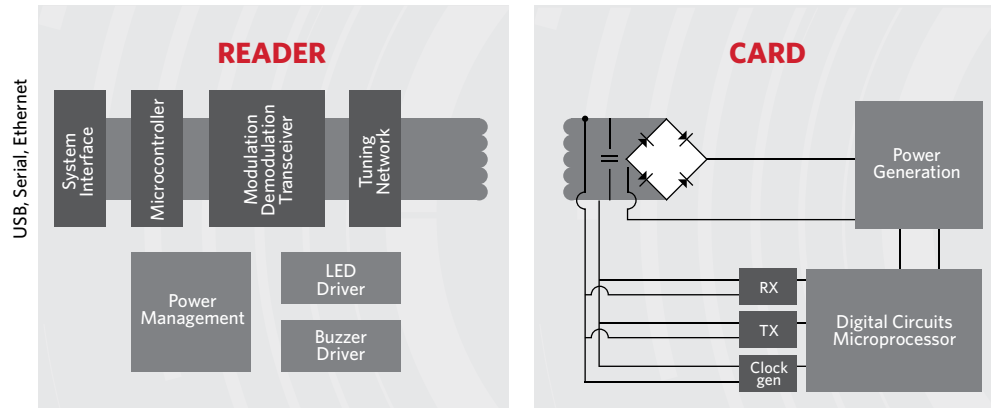
Cleanliness and image defects are typically the biggest issues with barcode badges since they cannot routinely be compensated for by the scanner. Read accuracy may be compromised by poor print contrast between the light and dark bars, whether caused by contaminants, low quality printing, or fading. The barcode must also be within the line of sight in order to be read by the scanner. Another disadvantage is the inability to make changes to the data stored on the barcode, which means that adding information to the badge, or adding additional access points or systems to the badge, requires a new bar code to be printed.

RFID badges

RFID badge-based solutions are similar to magstripe and barcode badge solutions in terms of access control, but they offer more security, and with contactless smart cards, more information. The RFID solutions have a badge that stores the unique employee ID and also an RFID USB reader device. For passive RFID systems, the reader uses electromagnetic coupling to remotely power the badge and transmit data between the reader and badge. For programmable controllers using EtherNet/IP, readers like those offered by RF IDEas have an EtherNet Industrial Protocol interface with Power-over-Ethernet for direct connections.

RFID readers are available to communicate with 125 kHz badges, 132 kHz badges, 13.56 MHz badges, UHF (860-960 MHz), or dual frequencies such as 125 kHz and 13.56 MHz in one reader. Though ultra-high-frequency RFID (for asset tracking) can function without line of sight, a greater level of comfort and security is provided by high-frequency and low-frequency badges that must be within inches of the reader for authentication. RFID technology is discussed in greater depth later in this paper.

RFID SYSTEM



Advantages:

RFID proximity and contactless badges provide tap-and-go authentication, as well as tap-in/tap-out authentication for tracking task durations, for example. Contamination is not an issue because the data is passed through the air. Passive RFID badges don't require batteries since the power for the badge is extracted from an RF field generated by the reader. Short read ranges protect against accidentally reading a nearby employee's badge and providing incorrect access rights to the intended employee. If an RFID card is lost or stolen, any data would typically be unusable due to encoding or encryption, and the security department typically deactivates the card upon notice of the missing card.

Disadvantages:

The 125 kHz RFID systems have been in use for many years without being managed by industry standards, resulting in more than 40 different types of 125 kHz RFID card types being developed and in use. While there are standards for high frequency, some variations in the 13.56 MHz badge market exist as well. Fortunately, RFID systems can be designed to account for variable card types.

Multi-factor Authentication

In highly sensitive areas, such as for automation software access and control, two-factor authentication or multi-factor authentication can be required. Joining together multiple access control technologies heightens assurance of security where dictated by security policy. For example, an access control device could be designed to require a badge, biometric scan, and password or pin in order to gain access.

How RFID Cards Work

The design characteristics and capabilities of RFID access control badges and readers are unique in many respects.

Energy Coupling

Since the RFID badge does not typically contain a battery, energy must be supplied to the badge from the reader to allow the badge to transmit the unique employee ID stored in memory. The RF energy coupled to the card is converted through a process called rectification. Once the badge has rectified the AC signal, the direct current is used to energize the badge circuits, which in turn provide an information-carrying signal that is transmitted to the reader using the electromagnetic coupling as the mechanism to transmit the unique employee ID.

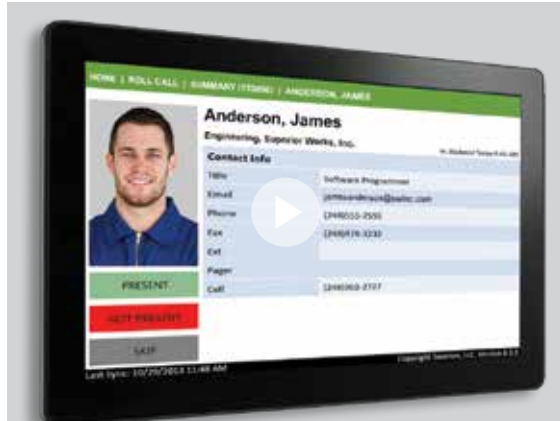
Communication

For some RFID badges, a bidirectional communication channel is created using the electromagnetic coupling mechanism between the RFID reader and the badge. The RF signal used to energize the badge is also used as the RF data carrier for the bidirectional communication channel. This communication channel allows the unique employee ID to be transferred from the badge, read by the reader, and passed onto the backend server. Data stored in the server is then used to make decisions like the validity of the unique ID and the permissions of the badge holder.

Card Types and Modulation

Card types dictate how information is stored and communicated between the reader and the card. Elements comprising a card type include the frequency, communication format, bit rates, number of bits, and manipulation of bits to get data. In addition, card manufacturers may have their own variations of card types.

Video: RF IDEas Card Readers



Watch this short video to learn more about the RF IDEas products designed for simplifying identification and access controls. Find out about the company's badge-based solutions that support nearly every door-access proximity card, contactless smart card and magnetic smart card worldwide.

[Click here to watch the video](#)

The communication method used in a RFID system is referred to as a backscatter communication system. In a backscatter system, the RFID badge sends data to the reader by repeatedly shunting the badge's coil, causing slight variations in the RF carrier amplitude that is provided by the reader. The reader detects these variations and decodes them as data from the badge.

Badges which operate at 125 kHz are not managed by an industry standard, and therefore there are many different methods of data transfer between the reader and the badge. At the highest level there are three different types of modulation used in 125 kHz systems: direct (ASK), frequency shift keying (FSK) or phase shift keying (PSK).

Badges that operate at 13.56 MHz follow RFID industry standards like ISO 14443, ISO 15693, and Felica. ISO 14443 is an industry standard that has three different types of modulation (A, B, and F) that can be used for communication between the badge and the reader.

Memory

13.56 MHz badges have been designed to allow modifications of the data stored onto the badge. This capability allows IT staff or systems integrators to add features to the badge. For example, the additional memory can be used to enhance the permissions available to the badge holder, or the additional memory can be used as a local storage device allowing tracking of the number of requests made to access a particular document or piece of manufacturing equipment. In more complicated RFID badges, often times called smart badges, the memory can be used to store financial information or encryption keys used in high-security applications.

Anti-Collision

When multiple tags are presented to a reader at the same time, communication collisions will occur. These collisions are similar to multiple individuals talking at the same time, making it difficult to determine what any one person is saying. RFID solutions that incorporate anti-collision protocols such as the Aloha, which is used to select a particular badge from a group of badges, alleviate the risk of communication collisions.

The Aloha protocol sorts through the population of RFID badges that have been powered by the RFID reader, assigning each badge a unique node address that is used to provide collision-free communication between the badges and the reader.

Back-End Systems

The data created from a transaction that uses RFID, barcode, or magstripe can be stored in a back-end server that controls access to equipment, documentation, room access, and financial transactions. The server also generates reports about when and who requested access to the equipment, documentation, room access, and financial transactions. These systems can also be used to authenticate and validate activities such as training of the badge holder to ensure they received the latest training and maintain the highest level of manufacturing compliance.

System Integration

System integrators can build solutions that require RFID readers to be available with multiple interface types, such as USB, Ethernet, RS232, and serial I/O. They may leverage keystroke application software that allows employee unique ID data to feed into the computer as if it were typed on the keyboard, making it easy to interface the RFID reader to any application that is written to accept keyboard data. RFID readers with outputs such as RS232 or serial interfaces allow the reader to leverage a serial port on the back of a personal computer.

One of the most common uses of the RFID badge and reader is single sign-on (SSO). SSO allows a systems integrator to create solutions utilizing a user login with a single ID and password to gain access to multiple systems, instead of using different usernames or passwords. RFID-enabled SSO solutions allow a single sign-on prompt for the user to present their badge to the RFID reader solution. Additional software applications will use the same badge credential for software/system access, without prompting the user to re-enter passwords for each software application. Badges that contain additional memory can also store certificates or passwords, eliminating the need for access to the back-end server for user authentication.

Other Applications

Beyond single sign-on there are many other applications of the RFID badge and reader. With print management software, employees are able to use their badge after they send a print job to allow their document to print only in their presence. The employee simply sends a print job to a multi-function printer (MFP) where it is held in queue until the user is in front of the MFP. To release their print job, the user simply presents their employee badge to the reader to release only their documents without any other interaction. The software can track usage by employee by department to control costs.

Punch card time clocks are quickly being replaced by time and attendance software solutions that utilize readers and incorporate existing employee badges. Cost-effective and precise, manual entry errors as well as "buddy punches" are eliminated. Employees use their own RFID badge and simply wave or tap it at the reader mounted on a time and attendance kiosk. Typically, time and attendance software integrates with other systems such as payroll.

The use of RFID badges with readers and various software applications opens the door to an unlimited number of solutions throughout the realm of industrial enterprises. Once the needs of the organization have been identified, ideas for access control and management applications can be developed.

Conclusion

The practical and financial benefits of extending access controls building-wide are hard to ignore, particularly when RFID-enabled smart cards and badge readers are used. The virtually unlimited application opportunities make standardizing and automating access control methods and technologies a necessity. Manufacturers in particular should incorporate this approach in their workflow and security policies to address their increasingly interconnected and mutually dependent systems.

RF IDEAS LEADERSHIP SERIES

This white paper is part of a leadership series exploring the latest advancements in smart technologies in industrial access control, including vital methodologies and solutions that are critical in addressing today's evolving security needs.

TO LEARN MORE ABOUT HOW RF IDEAS CAN HELP YOUR ORGANIZATION ENHANCE SECURITY AND OPERATIONAL EFFICIENCIES BY AUTOMATING ACCESS CONTROL, VISIT WWW.RFIDEAS.COM.

ABOUT RF IDEAS

RF IDEas, Inc., www.rfideas.com, is a leader in the employee badge and card reader space for manufacturing, healthcare, government and enterprise. Partnering with leading technology companies, RF IDEas readers enable innovative solutions for single sign-on, secure printing, attendance tracking, and other applications that require authentication. RF IDEas is a subsidiary of Roper Technologies. For more information about RF IDEas products and applications, visit the Knowledge Center at <https://www.rfideas.com/knowledge-center>.



RF IDEas, Inc. Toll Free: 866-439-4884
4020 Winnetka Avenue Voice: 847-870-1723
Rolling Meadows, IL 60008 Fax: 847-483-1129

www.RFIDEas.com

pcProx® is a registered trademark of RF IDEas Inc. Trademarks not belonging to RF IDEas are property of their respective companies.
©2016 RF IDEas, Inc. All rights reserved. Products are subject to change without notice.

WP-701