rf IDEAS

WHITE PAPER

Access Control Enters the Realm of Industrial Automation

Smart technologies for evolving authentication needs

State of the Industry

Controlling access to and within the manufacturing plant and protecting information and automation systems from breaches is a business essential. A physical or logical security lapse, 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 credential 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 card of some sort to gain entry, why not apply this same concept—and smart technology—to logical security concerns inside the building?

Purpose of This White Paper

This white paper explores the latest advancements in smart technologies for industrial access control, including methodologies and solutions that are critical in addressing today's evolving access control needs. We will discuss two major topics:

1. New developments in industrial control and identification: Trends in access control that are changing the role of access authority throughout the organization, including how employee credential solutions are streamlining access control processes, improving risk management and creating significant savings for today's organizations.

- The effect of information and operations technology convergence on manufacturing and processing industries
- How new automated systems are creating smart factories
- Potential savings from smart card deployments
- Applications of card-based reader solutions throughout the enterprise

2. Key considerations in choosing the right industrial access control solution. A practical guide for evaluating the four most prominent access control methodologies in use today, including an introduction to RFID access control cards and readers and their applications in today's enterprises.

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

1. New Developments in Industrial Control and Identification

Implications and opportunities of evolving authentication needs and smart technologies

Employee ID cards (hereafter referred to simply as "cards") are commonly used credential to gain access to a facility, just as usernames and passwords are used to access software applications. With the cloud and big data accelerating the convergence of information technology (IT) and operations technology (OT), more refined security and risk management opportunities are available.

"We believe the growing IT/OT convergence is having a significant effect in the manufacturing and processing industries," says Craig Resnick, vice president of consulting at ARC Advisory Group. The two functions have begun working together over the past 5 to 10 years, and although companies today are at all different levels of convergence, Resnick believes the direction towards greater convergence is clear.

"When the IT/OT convergence is done, many times a company will utilize IT's security access and practices and try to apply that to control systems access, whether that's passwords or multilevel passwords, all the way up to iris scans depending on the level of security desired," explains Resnick.

Manufacturing is on the brink of a massive change as new connected, automated systems are now making their way onto the factory floor, serving as the foundation for creating smart factories, according to a report from research firm MarketsandMarkets published in September 2015. The Industrial Control and Factory Automation Market is expected to reach US$202.42 billion by 2020 at a CAGR of 6.73% from 2015 to 2020, the report says.

New card-based readers coupled with partner applications are standardizing and streamlining manufacturing access control processes. The same employee credential used to enter a building can now also be used to authenticate access to equipment, factory lines, gated robotic rooms, documents and software, and to

regulate activity on control systems, networks and equipment. Virtually any movement within the facility and any activity throughout the day could potentially be tracked and managed with the right card reader, apps and an employee credential.

Card-based authentication is not only faster, but it eliminates the errors associated with manual password entry, thus improving accuracy and ease of use. For instance, in situations where a supervisor periodically helps an operator, a card-based access solution would prevent the operator from reusing the supervisor's username and password, avoiding intentional misuse or errors. The ability to leverage existing employee ID cards or key fobs with readers provides a desirable and cost-effective solution.

There are a variety of card readers available depending on the credential type used by an organization. There are magnetic stripe cards, barcode cards, proximity cards (125 kHz) or the increasingly popular RF-enabled contactless smart cards (13.56 MHz). On the manufacturing floor, contactless smart cards are used more frequently because of the amount of information these card types contain.

> Everyone is a stakeholder when it comes to access management.

For organizations that may have acquired another business and find themselves with both proximity and contactless smart cards, there are dual-frequency USB readers that can be easily configured to read more than one card type. This ability to leverage the existing credential investment and avoid retraining, while gaining process efficiencies through access control standardization, enables substantial cost savings that directly benefit the bottom line.

Based on a study of enterprises published in 2004, Datamonitor found that by deploying an integrated smart card security solution for both data (logical) and physical access, an enterprise may annually save more than $2 million for every 2,000 employees covered by such a combined identity and access management system. In today's dollars, that equates to roughly $2.5 million. Cost savings are attributed to factors such as:

- Reduced time spent on sign-on procedures
- Consolidation of employee access privileges onto a single, multi-functional smart card
- Improved quality control with access permissions
- Reduced numbers of password-related queries made to IT departments
- Better management of PKI certificates
- Greater automation of card provisioning

But the cost benefits extend well beyond access efficiency. After a large paint manufacturer installed a card reader on its mixers to ensure that only authorized, trained employees could unlock and operate the equipment, the number of bad batches fell from 12 per week to less than one per week, saving the company nearly $2.5 million annually.

> Requiring employees to use their credentials throughout the workday improves work management and accounting of people and projects.

The proven value of this technology is driving increasing investments. "The American [North and South America] market for electronic access control readers was worth about $237 million in 2015 and is projected to grow to $252 million in 2016," says Blake Kozak, principal analyst for the Security & Building Technologies group at IHS Technology. IHS defines readers to include magnetic stripe, smart card readers, proximity readers, biometric readers and multi-technology readers.

Applications Are Varied and Growing

Growing interconnectedness and the ability to standardize access control are revealing opportunities for risk management that were not previously viable. Both physical and logical access controls are an essential part of a complete security policy. And increasingly, access controls are becoming an important element of quality control policies. As the following examples indicate, security procedures and applications can be found throughout the plant to control access, manage access levels by user role, and track employee actions. Authentication solutions that read employee ID cards enable practically unlimited possibilities.

> RFID card-based solutions offer enhanced security, and with contactless smart cards, more information.

Information Technology

- Information systems and networks are vulnerable to hacking, malicious software, and lost or stolen devices. At the most basic level, IT needs to ensure that computer logins are the first step to protecting information. However, passwords can be forgotten, which consumes employee and help desk time. Switching from passwords to card-based authentication eliminates the manual keystrokes and associated problems. Leveraging two-factor authentication, such as a password and card, further increases the level of security.

Operations

- Putting a card reader on PAC-based machine control software can prevent remote software updates and require the physical presence of the personnel authorized to make software changes. The use of an employee ID card as an authentication device prior to allowing software updates may reduce the likelihood of a malicious computer event like the Stuxnet worm that hijacked nuclear power plant motor control in Iran.
- Readers programmed to communicate with PAC or HMI operator interface software ensure that only authorized users can log in to the computer and use the software. This limits who can run the production line, how it works, and who can make changes, for example, to parts, ingredients or product colors.
- Requiring card authentication at a production line allows tracking of who is on the line and when, so that quality issues or other problems can be traced back to the individual, and retraining or other corrective actions can occur.
- Card readers used for access control purposes can be used for start-up control of forklifts or other material handling equipment, ensuring that only trained or certified employees can start them. It is important for OSHA safety purposes to ensure forklift operator identification, access control and monitoring, as this information is very helpful should an accident occur.

Maintenance

- When hazardous equipment such as a large press is due for maintenance, requiring card authentication before allowing safety features to be disabled can ensure that only properly credentialed employees are exposed to this risk.
- For specialized equipment, access control applications tied to employee training records can be used to ensure the maintenance technician's certification has not expired; otherwise the machine will not turn on.

Item Dispensing

- Industrial vending machines with card readers can control who accesses the machines, track which items are dispensed, and account for the costs. This provides the ability to monitor consumption trends, ensuring the appropriate quantities are reordered at the right time to keep carrying costs low. It also provides a means to troubleshoot excessive withdrawals and reduce costs due to loss prevention, for instance if safety gloves are inadequate for a task and replaced often or an employee is taking gloves home.

- Tool access controls can be established so that an employee only has access to those tools specified for a job, helping to avoid defects or delays caused by incorrect tools. With the proper application, a card-based reader solution can dispense the right tools to the appropriate person for their specific task. The application could also be designed to associate the items to a project or work order, and validate whether the expected types of items are taken.

Training

- Taking training class attendance is easier and more accurate when employees use their cards to sign in and out, rather than using a sign-in sheet. Poor handwriting and forgetting to sign in reduce the efficacy of attendance tracking. Leveraging the employee card helps ensure training completion, which increases productivity and reduces defects. It also facilitates OSHA training requirements by automating the tracking and validation of class attendance, training dates and other pertinent information.
- When processes or equipment change, card authentication can be used to ensure employees have completed the necessary training. For example, when the card is presented to the computer software, a message can pop up informing the employee of the need to complete training on the new process.

Compliance

- In regulated industries such as food processing or nuclear power, compliance and compliance reporting are essential. Access control and tracking applications can validate whether employees have the authentication to perform their assigned duties, whether it's reading a file, running a program or operating a machine. They can also help to capture the necessary regulatory records.
- Using cards for chain-of-custody documentation requirements ensures that only authorized personnel can obtain and print physical or electronic evidence.
- In industries like food processing and pharmaceuticals, federal inspectors have audit rights to check who is handling various activities on a production line. The addition of a presence detection device with a card-based solution will give the auditors confidence that an operator's HMI is not accessible in the event it is left unattended. When the operator steps away, the presence detection device's sensors will close the screen until the operator returns and waves his or her card.

Purchasing

- Securing purchasing files protects against credit card and identity theft. Requiring card access to the computer software ensures that only authorized personnel can access and manipulate personal or financial information.

Corporate

- Requiring employees to use their work card throughout the work day improves work management and accounting of people and projects. Using a backend data management system and a card, the actual time and expenses spent on a task can be easily tracked and billed, and resource assignments can be more effective due to improved personnel and skills visibility.
- Secure printing is needed to ensure that document privacy issues are avoided. Card authentication at the printer prevents print jobs from printing until the requestor is in the presence of the printer. In addition, printing costs are reduced because employees are compelled to become more selective in what they print, and print functions can be limited to specified work functions.
- Card-based cashless cafeteria applications link the employee's record to a financial account, allowing them to move much faster through the sale.
- Mergers and acquisitions combine companies with different security practices and technologies. Using a card reader that reads virtually any card type avoids the expense of replacing cards, simplifies the transition, and improves efficiency for better operational workflow.

New solutions leveraging employee cards, readers and application software offer combined identity and access management capabilities for a wide range of applications in today's industrial enterprises. From providing enhanced security on the production line to authenticating training completion, these solutions play an important role in improving risk management and driving operational efficiencies. Their proven value is creating significant growth in the market for electronic access control readers.

2. Key Considerations in Choosing the Right Industrial Access Control Solution

Pros and cons of the four most prominent automation access control methods

Access Control Methods and Selection Considerations

The proliferation of new industrial access control technologies is making it challenging for enterprises to choose the right methods and solutions for their unique business and security requirements. The most prevalent access control options include manually typing passwords or PINs, or presenting employee cards to a card reader—the most common types being magnetic stripe, barcode and radio-frequency identification (RFID) smart cards. 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 choice of methods and technologies must be based on analysis of the organization's needs against the proposed solution's benefits and disadvantages. With various automation management platforms syncing with a directory service and databases, identifying card-based reader solutions that are independent of those platforms helps to "future-proof" the investment.

"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 Craig Resnick.

Manual Login

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

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

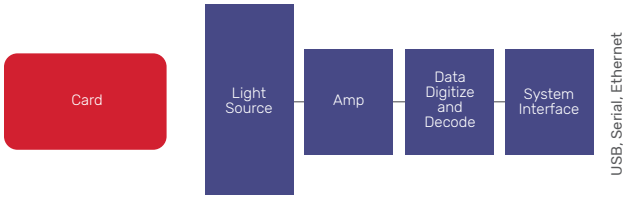
Disadvantages:
Manual login is the most time-consuming method of access control, and it requires a fair level of dexterity and freedom of movement that is not always available in manufacturing settings. For example, it is difficult for factory workers to type while wearing heavy protective gloves, but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

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 for intruders to guess, they are also considerably difficult for authorized users to remember, according to the study.

Magstripe Cards

Magnetic stripe (or magstripe) cards use iron-based magnetic particles to store the employee's unique identification number. Physically and functionally, they resemble a credit card. As the card 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.

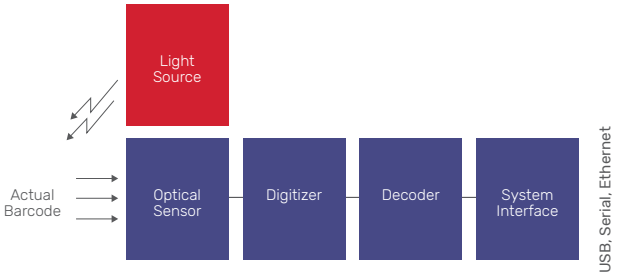


Advantages:
Magstripes were the first iteration of employee card technology, so they are a known entity and broadly adopted. Because they are similar in function to credit cards, they are particularly common with purchase authorizations. Magstripe cards are currently evolving from swipe to contact cards,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

Disadvantages:
Like credit cards, a magstripe card 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 use of this card type in many environments, 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 Cards

Barcode cards store the employee's unique ID in the variations of light and dark in a bar or QR code pattern. When the card 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.



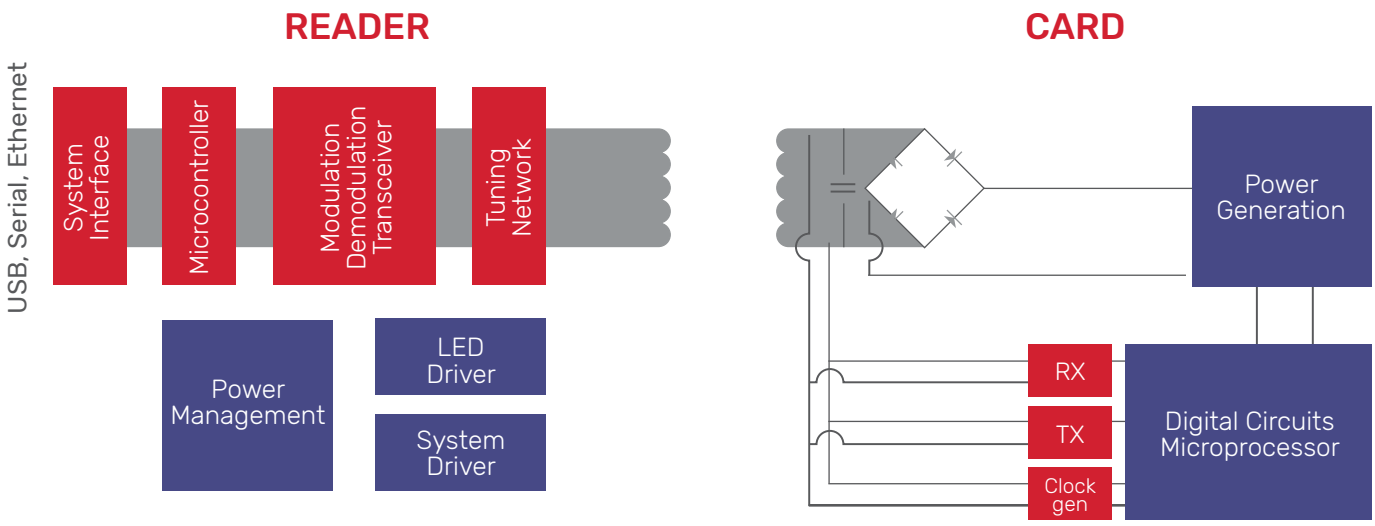
Advantages:
Barcode card technology is well established and provides for quick and easy access to secured areas and bar coded inventory and tools. The cost to print a barcode on an employee card is negligible. Barcode scanner apps, widely available for smart phones and other portable devices, provide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

Disadvantages:
Cleanliness and image defects are typically the biggest issues with barcode cards since the scanner cannot reliably compensate for them. 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 scanner's line of sight. Another disadvantage is the inability to change the data stored on the barcode, which means that adding information to the card, or adding additional access points or systems to the card, requires printing a new bar code.

RFID Cards

RFID card-based solutions are similar to magstripe and barcode card solutions in terms of access control, but they offer more security and, with contactless smart cards, more information. RFID solutions comprise a card that stores the unique employee ID and an RFID USB reader device. For passive RFID systems, the reader uses electromagnetic coupling to remotely power the card and transmit data between the reader and card. 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 cards, 132 kHz cards, 13.56 MHz cards, UHF (860- 960 MHz), or dual frequencies such as 125 kHz and 13.56 MHz in one reader. Ultra-high-frequency RFID can function without line of sight and is typically used for asset tracking. However, for most industrial applications, a greater level of comfort and security is provided by high- and low-frequency cards that must be within inches of the reader for authentication. RFID technology is discussed in greater depth later in this paper.



Advantages:
RFID proximity and contactless cards 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 cards don't require batteries since the power for the card is extracted from an RF field generated by the reader. Short read ranges protect against accidentally reading a nearby employee's card and providing incorrect access rights.

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 that it is missing.

Disadvantages:
The 125 kHz RFID systems have been in use for many years without being managed by industry standards, resulting in the development and deployment of more than 40 different 125 kHz RFID card types. While there are standards for high frequency, some variations in the 13.56 MHz card 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 automation software access and control, multi-factor authentication can be required. A security policy that combines two or more access control technologies heightens assurance of security. For example, an access control device could be designed to require a card, biometric scan and password or PIN in order to gain access.

How RFID Cards Work

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

Energy Coupling

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

Communication

For some RFID cards, a bidirectional communication channel is created using the electromagnetic coupling mechanism between the RFID reader and the card. The RF signal used to energize the card 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 card, read by the reader, and passed to 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 card 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.

Watch a short video to learn more about the rf IDEAS products designed for simplifying identification and access controls to improve industrial automation operations.

Visit www.rfIDEAS.com/Knowledge-Center to view the video "Improving Industrial Automation Operations."

The communication method used in an RFID system is referred to as a backscatter communication system. In a backscatter system, the RFID card sends data to the reader by repeatedly shunting the card'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 card. Cards that 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 card. 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).

Cards 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 card and the reader.

Memory

13.56 MHz cards have been designed to allow modifications of the data stored on the card. This capability allows IT staff or systems integrators to add features to the card. For example, the additional memory can be used to enhance the permissions available to the card holder, or it can be used as a local storage device to track the number of requests made to access a particular document or piece of manufacturing equipment. In more complicated RFID cards, often called smart cards, 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 Aloha, which is used to select a particular card from a group of cards, alleviate the risk of communication collisions. The Aloha protocol sorts through the population of RFID cards that have been powered by the RFID reader, assigning each card a unique node address that is used to provide collision-free communication between the cards and the reader.

Back-End Systems

The data created from a transaction that uses RFID, barcode or magstripe can be stored in a backend server that controls access to equipment, documents, room doors and financial transactions. The server also generates reports about when and who requested access. These systems can also be used to authenticate and validate activities—for example, to ensure card holders have received the latest training—to maintain the highest levels of manufacturing compliance.

System Integration

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

Single Sign-On

One of the most common uses of the RFID card and reader is single sign-on (SSO). SSO allows a systems integrator to create solutions that allow a user to access multiple systems with a single ID and password instead of requiring different usernames or passwords. Users are presented with a single sign-on prompt to present their card to the RFID reader solution, and additional software applications use the same credential no need to re-enter passwords for each. Cards that contain additional memory can also store certificates or passwords, eliminating the need for access to the backend server for user authentication.

Other Applications

With print management software, employees send a print job to a multi-function printer, where it is held in queue until the user presents their card at a reader on the printer. This ensures that sensitive documents are only printed in the authorized user's presence. The software can track usage by employee and by department to provide and audit trail and control costs.

Punch card time clocks are quickly being replaced by time and attendance software solutions that utilize readers and existing employee cards. Cost-effective and precise, these solutions eliminate manual entry errors as well as "buddy punches." Employees use their own RFID card 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 Benefits Are Compelling

These are just a few examples of how RFID cards and readers can be used with a variety of software applications, opening the door to an unlimited range of solutions throughout the industrial enterprise. The key is to identify the needs of the organization, then develop ideas for access control and management applications to meet those needs.

The practical and financial benefits of extending access controls building-wide are impossible to ignore, particularly when implementing RFID-enabled smart cards and card readers. With virtually unlimited application opportunities, standardizing and automating access control methods and technologies becomes a practical necessity. In particular, manufacturers should incorporate this approach into their workflow and security policies to address their increasingly interconnected and mutually dependent systems.

Let's Talk

rf IDEAS is the proven leader for RFID-based reader solutions, providing the most advanced technologies, the most knowledgeable expertise for manufacturing industries, and the most responsive service and support. Let's talk about your unique authentication requirements and opportunities.

Visit rf IDEAS.com today, or contact your rf IDEAS representative at sales@rfIDEAS.com

About rf IDEAS

rf IDEAS, Inc. is a leader in logical access solutions for healthcare, manufacturing, government and enterprise. Backed by the company's strong partnerships with leading identity access management providers, rf IDEAS readers enable innovative solutions for single sign-on, secure printing, attendance tracking and other applications that require authentication. rf IDEAS readers support nearly all credentials worldwide including the growing set of mobile credentials. For more information, visit www.rfIDEAS.com.

4020 Winnetka Avenue, Rolling Meadows, IL 60008 // Toll Free: (866) 439-4884 //
Voice: (847) 870-1723 // Fax: (847) 483-1129 // Email: sales@rfIDEAS.com // rfIDEAS.com