

July/August

ACCESS CONTROL 2017

TRENDS & TECHNOLOGY

Supplement to
*Locksmith Ledger
International, Security
Dealer & Integrator,
Security Technology
Executive*

www.LocksmithLedger.com
www.SecurityInfoWatch.com



INTERNET
OF THINGS

IoT Expands EAC Possibilities

- Connectivity is the Key and IoT is the Link
- Wireless Power Transfer for Access Control Applications
- 10 Triggers for Transition
- Making the Grade with Wireless EAC

DID YOU KNOW?

We stock the full line of Schlage security products, from durable mechanical locks to comprehensive electronic access control solutions like the AD Series.

Our technical sales experts have prior field experience and are factory-trained to spec your job as efficiently as possible.

We stock all seven AD Series reader modules, in all four lever designs and eight available finishes.



Now You Know.

EXTENSIVE INVENTORY | INNOVATION | TECHNICAL EXPERTISE | IMMEDIATE SHIPPING

LCN. **SCHLAGE** VON DUPRIN.

seclock.com | 800-847-5625

Request information: www.SecurityInfoWatch.com/10215009

SECURITY
LOCK DISTRIBUTORS

INFORMED. IN STOCK. IN DEPTH.

THE DEADBOLT SPLIT LATCH SOLUTION

THE UNCONVENTIONAL SOLUTION FOR DEADBOLT ACCESS

4100DBDL

THE ONLY ELECTRIC STRIKE WITH **TWO LOCKING MECHANISMS**

THAT FUNCTION SEPARATELY.

4 Faceplates included.

LATCHBOLT MONITORING AVAILABLE. With two (2) sensors to monitor the top and bottom latch.



Originally designed for dorm room deadbolt **privacy**, while allowing for an **emergency** override of the deadbolt.

Other uses include:

- ▶ Institutional bathrooms where an emergency override is necessary.
- ▶ 2 person credentialing.
- ▶ To allow privacy and an override in doctors sleeping rooms, lactation rooms, and labs.



PATENT PENDING

TRINE
ACCESS TECHNOLOGY.

Request information: www.SecurityInfoWatch.com/10215438


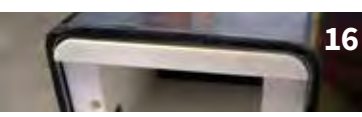


SEND US YOUR IDEA'S FOR THIS UNIQUE STRIKE @
TRINEONLINE.COM/DBDL

ACCESS CONTROL

July/August 2017

TRENDS & TECHNOLOGY

Features

-  **6 Access Control's Grand Convergence**
– Steve Lasky
-  **8 Connectivity is the Key and IoT is the Link**
– Steve Lasky
-  **16 Wireless Power Transfer for Access Control Applications**
– Cameron Sharpe, CPP
-  **22 10 Triggers for Transition**
– Brandon Arcement
-  **30 Case Study: Making the Grade with Wireless EAC**

Departments

- 28 Product Showcase**
- 4 Ad Index**

Advertiser's Index

Company Name	Page #	Request more info at
Alarm Lock Systems, Inc.	S-5	www.securityinfowatch.com/10212743
CCL Security Products	S-25	www.securityinfowatch.com/10213160
Command Access	S-20	www.securityinfowatch.com/12140374
Continental Access	S-19	www.securityinfowatch.com/10213301
D&D Technologies	S-23	www.securityinfowatch.com/10929523
DKS DoorKing Systems	S-13	www.securityinfowatch.com/10213482
dormakaba	S-29	www.securityinfowatch.com/12304402
Dortronics Systems, Inc.	S-27	www.securityinfowatch.com/10213494
DSX Access Control Systems	S-31	www.securityinfowatch.com/10214208
JLM Wholesale	S-27	www.securityinfowatch.com/10214128
SDC-Security Door Controls	S-32	www.securityinfowatch.com/10214991
Seneca Data	S-28	www.securityinfowatch.com/12348632
Securtron Magnalock Corp.	S-7	www.securityinfowatch.com/10214963
Security Lock Distributors	S-2	www.securityinfowatch.com/10215009
Top Notch	S-21	www.securityinfowatch.com/12129499
Trine Access	S-3	www.securityinfowatch.com/10215438
Yale Commercial	S-15	www.securityinfowatch.com/10215674

Visit SouthComm Security Media on the Web at www.SecurityInfoWatch.com

ACCESS CONTROL TRENDS & TECHNOLOGY 2017



SOUTHCOMM BUSINESS MEDIA at 125 S. Wile Rd., Suite 300, Arlington Heights, IL 60005. Phone: 847-454-2700, Fax: (847) 454-2759 • (847) 454-2700 and is a supplement to *Locksmith Ledger*, *Security Dealer & Integrator* and *Security Technology Executive* magazines.

PUBLISHER

Group Publisher Nancy Levenson-Brokamp
nbrokamp@southcomm.com

EDITORIAL

Editorial Director Steve Lasky
Editor, *Security Dealer & Integrator* Paul Rothman
Editor, *Locksmith Ledger* Gale Johnson
Editor, *SecurityInfoWatch.com* Joel Griffin

ART & PRODUCTION

Art Director Bruce Zedler
Production Manager Jane Pothlanski
Audience development manager Terri Pettit

SALES CONTACTS

East Coast Sales, SD&I, STE, SIW.com
..... Janice Welch
jwelch@southcomm.com

West Coast Sales, SD&I, STE, SIW.com
..... Bobbie Ferraro
bferraro@southcomm.com

Midwest Sales, SD&I, STE, SIW.com,
Locksmith Ledger, LocksmithLedger.com
..... Brian Lowy
brlowy@southcomm.com

Display/Classified Sales, SD&I, STE, SIW.com,
Locksmith Ledger, LocksmithLedger.com
..... Kristy Dziukala
kdziukala@southcomm.com

List Rental Elizabeth Jackson
ejackson@meritdirect.com

SUBSCRIPTIONS CUSTOMER SERVICE

Toll-Free (877) 382-9187; Local (847) 559-7598
Email: Circ.SecDealer@omeda.com

REPRINTS

To purchase article reprints please contact
Brett Petillo at Wright's Media:
877-652-5295 ext. 118 or bpetillo@wrightsmedia.com

SOUTHCOMM BUSINESS MEDIA

CEO Chris Ferrell
CFO Ed Tearman
COO Blair Johnson
EVP Public Safety & Security Scott Bieda
VP Events, Public Safety & Security Ed Nichols
VP Production Operations Curt Pordes
VP Technology Eric Kammerzelt







No, this isn't a lock, It's a... network

- > **Wireless ID Reader**
- > **Wireless Access Keypad**
- > **Wireless Networked Access Controller**

Networkx Wi Fi Access System:
Installs in place of a lock,
on any door, in under an hour.
(Free Security Management Software, too.)

Networkx. It's just easier to install, afford, network, manage & use. Simple. WiFi. No wires to run from gateways to locks. Runs right on customer's network or Ethernet. Proven performance, and providing many years of battery life, it's very low maintenance. Free Windows-based software, or enterprise platform integration options, with leading brands** too.



 EASY INSTALL Replaces any door lock, on any door type, neatly, quickly	 MORE AFFORDABLE Lowest labor & equipment costs without sacrificing top electronic access features	 EASY NETWORK No wires to run to doors. Uses customers' existing network or Ethernet & multi-lock gateways & optional repeaters	 CENTRALLY MANAGED Auto-Schedule program updates, queries, or free access by time, by door & more	 USERS Supports thousands of PIN, ID or iLock App users. Easily added/removed local or remotely	 GLOBAL LOCKDOWN or unlock in seconds from the server or any lock
---	--	---	---	---	---

Ask for **Alarm Lock Networkx** at your distributor
or call us **1.800.ALA.LOCK** or www.alarmlock.com

Trilogy, Networkx, ArchiTech & iLock and ** Continental CardAccess or CA4K™ CardAccess are trademarks of Alarm Lock, a division of Napco. **Lenel Open Alliance Program Partners is a trademark of United Technologies Corporation.



Access Control's Grand Convergence

The access control industry is in the midst of a grand convergence. The emergence and now dominance of IP-centric video surveillance technology has overtaken the world of analog and that migration is swiftly infiltrating today's access control systems.

The attractive nature of network-based technology that has become a foundation of video systems is also the hook for IP access control solutions. The ability to customize an IP-based access control system with an integrated approach using several complementary vendors, while maintaining the flexibility to expand and scale a system to fit a customer's needs provides both security and a sound ROI argument.

Yet, as IP-centric access control options grow, the potential for even more dynamic solutions are evolving as IoT capabilities expand. It is this convergence of traditional access control with networked IoT devices that is the future of security so says most of the industry's technology experts.

"The advent of IP has definitely been a boon to ACS, leading to new innovation in terms of IP-connected door controllers and modules. It may not have driven the growth of IoT in terms of consumer devices, but has definitely had an impact on ACS and the strategy of ACS vendors," says Jimmy Palatsoukas, Director of Product Marketing at Genetec.

Stuart Tucker, Vice President, Enterprise Solutions at AMAG Technology, adds that "by opening the communications between systems and devices using common easy to implement protocols, barriers have been removed. Once these barriers are out of the way, new technology can easily be integrated into IP-based solutions yielding new use cases."

Peter Boriskin, VP of Commercial Product Management at ASSA ABLOY Americas stresses that the IP migration has allowed access control vendors to accelerate that deployment.

"Legacy systems that aren't networkable require a dedicated hardwired connection to a central system or data gathering point, and there is only intelligence at the headend. With distributed intelligence, you can take advantage of device-to-device communication. This was really a precursor to IoT," continues Boriskin. "These intelligent devices run their own IP, support intelligent controllers and a database of logic. With these systems where devices are already on the network, users are taking advantage of the available information."

Michael Coniff, Global Product Marketing Manager at Honeywell points out that building environments are

rapidly changing. He says that as property managers look to attract people to their facilities, there will continue to be a massive growth of technology use within buildings.

"This consumer-driven growth of IP is essentially going to make our buildings smarter and provide structured wiring that's easier for people to take advantage of within a network. We're seeing a rapid growth of interconnected buildings that are more advanced, as well as the growth of cutting-edge devices that are providing a plethora of information that managers can tap into," says Coniff. "There is a general movement toward the adoption of technology from property managers, company owners, and building owners. These individuals are taking advantage of what they currently have, as well as replacing outdated devices with new, smarter solutions."

Robert Martens, a futurist and Vice President of Strategy and Partnerships at Allegion stresses that the componentry necessary to deliver a robust connected user experience is less expensive, more capable and more easily supported than ever before.

"Sensor technology is relatively inexpensive and allows for the collection of great amounts of data. The pipes needed to transport that data are less expensive than ever and more dependable than ever. The tools that transform that messy data into cleaner, more usable information are more available, less expensive and faster than they have ever been. This all adds up to a strong cost/benefit equation that will help to drive the usage of IoT-enabled devices," he says.

Jason Ouellette, Senior Product Line Director for Access Control at Tyco Security Products concludes that the rapid advancement of IP has enabled electronic access control solutions to become a part of the devices and data that can feed wider IoT solutions. "I wouldn't say that access control has really paved the way for growth in IoT, but rather the industry is getting on the highway to IoT-based solutions, ensuring its relevance and compliance to overall IT industry and trends."

So goes the theme of this supplement. I encourage you to flip to page 8 and read the complete technology trends roundtable we hosted for these vendors. It is both enlightening and entertaining.



Steve Lasky is the Editorial Director of South-Comm Security Media, which includes print publications Security Technology Executive, Security Dealer & Integrator, Locksmith Ledger Int'l and the world's top security web portal SecurityInfoWatch.com. He is a 30-year veteran of the security industry and a 26-year member of ASIS.



Solar Power Supplies



Power Transfers



PoE Injectors & Extractors



Power Distribution Boards



Inductive Coupling Power Transfer



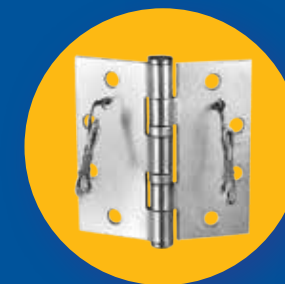
Linear Power Supplies



Switching Power Supplies



Plug in Power Supplies



Electric Hinges

TAP INTO THE **POWER** OF SECURITRON

SECURITRON
ASSA ABLOY

SECURITRON.COM | 1.800.MAGLOCK

ASSA ABLOY, the global leader in door opening solutions



Securitron is your one-stop source for all power management components.

Securitron products integrate better and work seamlessly together. Your system is easier to set up, easier to customize and more reliable to operate. What's more, Securitron offers the best warranty and the finest tech support in the industry.

Contact Securitron.

We are your single source for excellence in access control.

Request information: www.SecurityInfoWatch.com/10214963

Connectivity is the Key and IoT is the Link



Image Courtesy of BigStock.com

Access control customers are using myriad devices to controls their doors

by Steve Lasky

Connectivity is the name of the game when it comes to satisfying the almost insatiable thirst customers have for their static and mobile devices. Now, a growing number of access control vendors are incorporating the power of connected devices into their technology development. Editorial director Steve Lasky recently sat down with several top industry access control vendor to discuss their specific roadmaps related IoT and the future trends users can expect throughout the industry in general. Joining us on this roundtable is:

- Jimmy Palatsoukas, Director of Product Marketing at Genetec Inc.
- Stuart Tucker, Vice President, Enterprise Solutions at AMAG Technology
- Matt Barnette, President at Mercury Security
- Peter Boriskin, VP of Commercial Product Management at ASSA ABLOY Americas
- Robert C. Martens, Futurist and Vice President of Strategy & Partnerships at Allegion
- Michael Coniff, Global Product Marketing Manager at Honeywell
- Jason Ouellette, Senior Product Line Director for Access Control at Tyco Security Products

Steve Lasky: What role will IoT play in conventional electronic access control in the near future and beyond?

Jimmy Palatsoukas: Our customers are naturally looking for greater connectivity between devices. IoT is a catalyst for vendors to continue to integrate new sensors and also find ways to better present the information so it is easily digestible by users. From an access control system (ACS) perspective, IoT will be the driving force for new devices that connect to an ACS system. That includes devices that help extend physical security coverage outside of a building and towards the perimeter. Examples include automatic license plate recognition cameras, radar systems, and so on.

Stuart Tucker: IoT is already playing an ever-expanding role in electronic access control. Many large companies are embracing mobile and other devices in their current plans. We see many instances of mobile credentials, mobile identity and access management, situational awareness and even augmented reality in place or testing now. Additionally, new "IP-enabled Things" such as drones, robots, beacons, and others are finding their way into projects to extend the notions of what a Physical Security system can do.

Matt Barnette: There is a lot of buzz around the IoT and physical access control and time will tell to what degree the two technologies intersect and leverage each other. One influence the IoT will have on the industry today

is that it will push hardware manufacturers to develop and build their hardware to easily integrate, communicate and secure IoT devices.

For example, Mercury is ahead of the curve by starting to add the MQTT protocol to our panels. MQTT is a protocol for how devices communicate with each other in a more connected environment — specifically for the Internet of Things. We are helping to make it possible to create such a connected environment by enabling our panels to communicate with each other as well as with third-party systems. Our first iteration of this is through the integration of our panels into an elevator destination dispatch system that offers tenants and visitors personalized elevator service while improving the flow of building traffic.



IoT will be an integral part of enabling systems to share data more easily and in a more standardized format.

— Matt Barnette,
President at Mercury Security

Instead of pressing traditional up or down buttons, passengers enter their destination floors using keypads or interactive touch screens before entering an elevator. This is one of the many use cases in a more connected and smart building in an IoT environment.

Peter Boriskin: On the residential side, IoT is being driven by the connected home and our solutions play an important role in that ecosystem. For example, IoT allows homeowners to manage access to their home remotely using their smartphone. With our Yale Look Digital Door Viewer, you can actually have a video chat with someone who arrives at your door and sends a mobile key directly to their phone to let them in the house.

More so than ever before, the growth of technology in the home is now driving adoption in business. This is especially true with IoT. For the institutional market, the ability to provide intelligence and sensing to centralized systems for complex reporting is critical. For the IIoT (Industrial Internet of Things), we now have the capability to leverage what is being done in small business environments and bring that into the commercial and institutional space. An example of this would be quick service restaurants leveraging access control to see when locations are opened and closed as a way to monitor employees without being onsite. We are bringing intelligence and decision making out to the edge instead of it being done exclusively at a centralized management system. The

ability to de-centralize systems allows us to make intelligent decisions faster and provide greater functionality.

Michael Coniff: The way devices themselves are becoming more intelligent through IoT is going to play a big role in the shift of conventional electronic access control in the near future and beyond. As an alternative to general end devices, we now see devices learning and optimizing on their own. And beyond the devices themselves, the data and information they collect are going to be utilized more and more — especially within security systems.

For instance, a traditional access control system has a panel connected to a reader, and that often is connected to a video or alarm system. But now, end users are now looking for a singular system that can take advantage of any available information within a building. These devices, once deployed to meet safety codes and perform simple security and energy functions, are evolving into smarter, sleeker and more aesthetically pleasing systems. The information and data now captured extends beyond simple surveillance and focuses on improving the overall user experience of the entire system, whether in emergency situations or everyday operations.

Rob Martens: The IoT stands to play a large role in conventional access control in the near future and beyond. The costs involved with sensor and connectivity technology continue to trend down, while functionality and

capability trend up. This is a great recipe for manufacturers, solution providers, and integrators to focus on new, enhanced use cases and productivity gains for their customers and end users.

Jason Ouellette: I see this as providing a justification and acceleration for the shift towards cloud-based access control. IoT and cloud technology will allow the conventional providers to start to leverage the larger sensor aggregated data to provide improved security solutions and services.

Lasky: One of the main benefits of IoT is the aspect of connectivity. How does systems connectivity improve basic door access control and how does it improve managing large multi-door EAC systems?

Palatsoukas: Several areas are greatly improved. The speed of communications of IP has led to real-time connectivity with ACS, from both a monitoring and command & control perspective. With real-time connectivity, threat level management and the instantaneous lockdown of an area or building is now possible with door controllers. Central management of multiple remote and independent sites, such as issuing credentials centrally or configuring systems remotely, is that much easier with greater connectivity. IP has also led to being able to manage or monitoring your ACS from mobile apps and receive push notifications in real-time.

Tucker: By adding functionality via new types of devices, you expand the notion of what is physical security, for example, when you can merge basic access control with things like GPS positioning, Bluetooth beacons, and video analytics you can do things that were not possible just a few years ago. This is true from an administration side as well as from a user perspective. Imagine you can correlate a person's position at all times with beacons and provide manned

or automated responses through IP-based intercoms or even drones. This is a game changer in critical situations where you can minimize risk and still have full capability to communicate, see, and even react.

Barnette: IoT will be an integral part of enabling systems to share data more easily and in a more standardized format. It might also enable data to be shared in multiple ways, such as with OEM partners who have deep integration with our products through API for control and command and work within their systems. The role of the IoT may also make it possible for Mercury to open secondary and tertiary paths of communication to such things as preventative maintenance programs for integrators who have cloud-based maintenance applications. In this scenario, the IoT potentially gives integrators direct communication to Mercury controllers, providing data on how the device is performing. This is one of the many examples of how the IoT can impact the industry from the perspective of the panel hardware.

Boriskin: This level of connectivity dramatically reduces infrastructure costs, and takes advantage of the network to expand the system at a much lower cost. Without networked devices, you would have to run separate cable and power supplies for access control with all of the processing done at a central location. Facilities would incur additional infrastructure costs simply to bring the devices online and would still not have an avenue for device-to-device communication.

Coniff: Today, our lives are centered on a smartphone. We don't need to be sitting in front of a computer in order to feel connected. It's this mobile-first mentality that has everyone demanding immediate and instantaneous access to everything — both at home and at work.

For example, a building owner with a traditional access control system has to run specific software on one or two computers within the facility in order to access secure data on a server. But now, building owners want to access their control systems on a mobile device. They want to add

a new card user by taking a picture with their phone and creating a mobile badge. They want to be able to send credentials for an expected visitor, have them already know where to go and be approved to access the building before they arrive. Building owners want to be capable of working wherever, and whenever, without being tied to a computer. You also see changes in connectivity with small to medium business owners who manage a handful of locations that require quick access

access without a physical interaction. Historically, we have seen electronic access control limited to the perimeter doors of a facility. With the introduction of enterprise class interior door hardware, electronics are now being brought to those doors at a fraction of the cost that they once were. The ability to override manual actions and to monitor openings throughout the entire facility drives a whole new level of use case, security and productivity at a rational cost.



We believe that physical security systems will continue to move towards a unified platform.

— Jimmy Palatsoukas,
Director of Product Marketing at Genetec Inc.

via a mobile device. For example, they can unlock the building to let a worker in on the weekend, then lock back up remotely once they have left. In addition, when combined with a camera focused on that door, the user can quickly verify that it is the correct user and that the user has entered the building. This ease of being able to quickly access any facility, no matter where they are all from a mobile phone isn't just a luxury — it's a necessity in today's always-connected world.

Martens: Systems connectivity can vastly improve door access control when implemented properly. First and foremost, the ability to identify the "real-time state" of any given opening without actively having to be present is of great value. No touring capabilities can greatly enhance a facility executive's productivity — allowing team members to audit the state of their equipment remotely or to manage

Ouellette: From a big data perspective, IoT allows for better-converged visibility across physical and logical access to more practically detect stolen or lost credentials or cyber-attacks.

Lasky: What array of connected devices do you see building out a future electronic access control system and how will that system be managed?

Palatsoukas: We believe that physical security systems will continue to move towards a unified platform. This platform will manage not only ACS devices but also cameras and encoders, communications (intercom) devices, intrusion panels. Newer integrations will include connectivity and management of elevator dispatch and perimeter detection devices. Our Security Center platform is leading the way.

Tucker: Smartphones, ID Sensors (Beacons), Drones, and Robots. The key is to come up with a solution that allows simple configuration of workflows that incorporate all of these things to solve current issues that are difficult, dangerous, or extremely routine. For example, in an active shooter or fire evacuation, drones or robots with embedded cameras could go to the critical areas and stream live video back, enabling security to make intelligent decisions based on what is happening right now, even if traditional cameras are not in operation in a specific location.

Barnette: Access control systems will join advanced smart building applications through cloud-based monitoring applications that deliver robust analytics capabilities used to proactively pinpoint and troubleshoot potential system failures. These applications will also monitor secure connections between PACS peripherals and trigger firmware updates to address potential cyber threats. IoT functionality will be embedded in PACS panels as app extensions to enable connections to the cloud-based services; these IoT connections will deliver preempted alerts, real-time diagnostic information to the cloud to ensure protection against emerging vulnerabilities and streamlined system operations.

Boriskin: It's many of the same things we are connecting to today such as intrusion, video, fire, emergency notification and access control. The difference is not the what, but the how. Today, to tie into all these systems you have to do an integration that is unique to each system, and as the system evolves it likely has to be



Peter Boriskin,
VP of Commercial
Product Management
at ASSA ABLOY
Americas.

likely has to be



The IoT stands to play a large role in conventional access control in the near future and beyond.

— Robert C. Martens, Futurist and Vice President of Strategy & Partnerships at Allegion.

redone each time.

With IoT, there is the potential for devices to communicate and provide meaningful data to one another. In the future, it's possible there will be a standardized approach to add and change systems with devices that become part of an eco-system.

There will also be a variety of openings that need to be managed, including high traffic openings such as transportation hubs and higher education environments. The benefit will be a more de-centralized approach to access control, which will make the system more resilient. If there is an emergency such as a power outage, it will only take out a specific area and not necessarily an entire building.

Coniff: We are going to see a focus on mobile interfaces that provide instantaneous connections. With that, the devices that will have the ability to interact with these advanced security systems are almost unlimited. Manufacturers are taking advantage of what they currently have, such as access, video, intrusion and smart energy devices, while simultaneously leveraging the data and information from these individual devices, in order to bring everything together into an interconnected, cloud-based, mobile-first environment. As the industry shifts to devices, with buildings becoming smarter and interconnectivity becoming easier, we're going to look at things beyond

security. We're transitioning from the traditional capabilities of a security company and moving into all the ways we can make someone's life easier, safer, and even more productive using the equipment and software we provide.

Martens: Many of the usual suspects will be in play- electronic locks, smart panic bars, smart closers, readers, motion sensors, and cameras. That said; the vast majority of these devices will be IP-based, with an emphasis on connectivity and the flexibility to be upgraded and maintained over time. Use cases based on increasing ROI will drive certain categories to new heights of interest and emphasis. Touring physical devices will become less and less frequent, and these devices will share their status with administrators when they require attention. A wide array of low cost, high functioning sensors will be embedded in devices that are not typically thought of as being "smart" today.

Ouellette: I think open standards will come to bear under the pressures of scalability, sustainability and the sheer economics of the connectivity of devices. Many manufacturers will be looking at how to provide software-based solutions and services on the value of the number of supported devices and the solutions they can provide based on the data.

ALERT: By 2020, Copper Phone Lines Will No Longer Be Supported.

No Worries! Retrofit *any* of your existing DKS Entry Systems with a Cellular signal.



DKS has taken the hassle out of converting existing Telephone Entry Systems! No longer will you be at the mercy of unsustainable phone lines or rising rates – nor the cost of running cable. It's the total package: voice communication and programming* over a 4G LTE cellular connection. Finally, a sustainable wireless solution for connecting managers and users to Telephone Entry Access Control Systems.

* Voice & Data (programming) with DKS 1830 and Access Plus series, Voice only with DKS Standard series.

	Cellular
Sustainable	✓
Voice & Data	✓
Voice Only	✓
Programmable	✓
No Wires	✓
1830 Series	✓
Access Plus Series	✓
Standard Series	✓

DOORKING For more information:
doorking.com/retrofit
800-673-3299 info@doorking.com

Parking Control Access Control Telephone Entry Gate Operators
Member: AFA, DASMA, NAA, IDA, NOMMA, NPA, SIA, SSA, CANASA

Lasky: Much discussion has taken place related to how the IoT presents a new set of security challenges for video. But as more IP-centric access control solutions begin to appear, what special issue do they face?

Tucker: I don't really see IoT as a challenge but as an opportunity. You now have thousands of IP-based mobile devices in an enterprise that



Stuart Tucker, Vice President, Enterprise Solutions at AMAG Technology.

can now be leveraged, whether for video, physical security, situational awareness or mobile administration. The real challenge is in managing the large numbers of devices. However, with well-designed integrations and proper

planning, deploying IoT devices in bunches should not become a burden for IT or security teams.

Boriskin: As the network becomes more populated, there are more identities to manage than ever before. The challenge becomes creating a federated identity for so many different devices, whether it is a laptop, server, or part of the physical security system. We are now at the point where it is necessary to manage the identities of devices in the same way we manage identities of individuals. This shift from a person-centric approach to a device-centric approach requires a comprehensive review of the policies in place for how devices are used, accessed, managed and to whom they are available.

Barnette: There are many concerns when it comes to the IoT and electronic access control. Connecting, more devices and systems, plus sharing more data opens new potential security threats, and work still needs to be done to better understand the potential associated risks.

A major consideration to prepare for the IoT is a comprehensive cybersecurity strategy that begins at the hardware level to establish a solid foundation of protection against potential threats. For example, our approach includes secure design lifecycle practices; proactive testing of our products through third parties; and industry-standard data encryption methods for end-to-end secure communications. Beyond ensuring a multi-layered approach to cybersecurity at the hardware level, Mercury recommends that access control software manufacturers also carefully review their code and control all possible connection points supported by their software, given that vulnerabilities are discovered in commercial software platforms on a regular basis. It is also recommended that hardware and software manufacturers work with professional labs to conduct vulnerability analysis on a regular basis.

Coniff: In many respects, the access control system is often considered the gatekeeper to a facility. People often ask how to make access to system configuration easier for the end user. While this may provide more convenient access for building and security staff, it also makes it easier for others to gain access through non-conventional means. It's a constant balance – designing products that are easy to use and modify for approved users, while also protecting against external threats. The ultimate goal is to make it easier for security managers and operators to efficiently, effectively and securely manage their facility using smart devices, while also protecting against unauthorized access.

Martens: Connectivity at the device can provide tremendous benefits, but it also can expose the user to heightened risks when applied and or maintained improperly. The secure storage and transmission of information are table stakes in the burgeoning world of the Internet of Things. Whether it is a lock or a video camera, certain basic elements must be observed by manufacturers, service providers, integrators and end users. One of those key elements is the ability of these devices to securely receive

updates. This allows the firmware or software elements of the smart device to maintain its level of security, functionality, and robustness through updates from the manufacturer or service provider. Another key element would be to never leverage pre-set administrative settings or passwords. Just following these two simple suggestions will greatly enhance your level of security and ability to respond to an incident. Another element to consider is how you maintain your network itself. Does a member of your organization manage your firewall? If so, how comfortable are you that they are at the same level of understanding and skill as someone at AWS, Google, Microsoft, etc.? Malware and ransomware can be fought at many levels, so companies need to decide where their core competencies exist and where they don't.



Jason Ouellette is the product line director for the access control brands of Tyco Security Products. (Photo courtesy Tyco Security Products)

The manufacturers will need to provide the means for getting software and firmware updates for operating systems as well as devices that minimize truck rolls and lengthy deployments while providing notifications of any corrective actions for identified cyber-security issues that allow a customer to provide a highly secure and reliable solution. Manufacturers of the access control solutions will need to be engaged with vulnerability scans and open source code scans during product lifecycle development to minimize risks to IP centric solutions and provide higher degrees of assurance that the products they manufacture are cyber ready, responsive and secure. ◀

Ouellette:

Access control devices will need to be made Wide Area Network (WAN) friendly and address the problems presented by having to open ports for firewalls which create cyber vulnerabilities. The manufacturers will need to provide the means for getting

The next big thing in access control



nexTouch™

Introducing nexTouch™, the next generation of keypad access control from Yale®. nexTouch combines effortless installation and innovative technology for a truly scalable solution:

- ▶ Use as a stand-alone keypad lock to **manage access with PIN codes**
- ▶ Utilize **Data-on-Card technology** as part of the Yale Multi-Family Solution
- ▶ Easily expand **ZigBee or Z-Wave** capable alarm or automation systems for use in small businesses
- ▶ **ANSI/BHMA Grade 1** certification ensures strength and reliability

When you need the perfect balance of security, convenience and flexibility, Yale Works for YouSM.

Learn how you can take the next step in security

www.yalelocks.com/nexTouch



Wireless Power Transfer

for Access Control Applications

Is this a disruptive technology?

by Cameron Sharpe, CPP

Bryan Nicholas CML, of San Diego-based Door Systems Inc. needed to power the electric strike on a removable mullion. Years of real-world experience convinced the integrator that wires would be vulnerable. An inexperienced maintenance staff was likely to tear up the wiring harness assembly when taking the mullion down. So what to do? Bryan had previously worked with Securitron's Inductive Coupling Power Transfer for EAC applications and knew this would be a good solution.

Integrators need to power electric strikes on removable mullion, but feared standard wiring would be vulnerable.

How Wireless Power Transfer Works

Essentially, wireless power uses an alternating current to transmit energy across an open space. Alternating current energizes a wire coil, creating a magnetic field. This field then produces an alternating current in the receiving coil. ^[i](End references will lead you to a plethora of technical papers, beyond the scope of this article.)

Close Coupled systems, like the Securitron device, produce rather efficient current transfer at limited range. This technology is now working well in numerous access control applications. The Inductive Coupling Power Transfer device (PowerJump[®]) produces six watts of continuous power. Higher current options are discussed below.

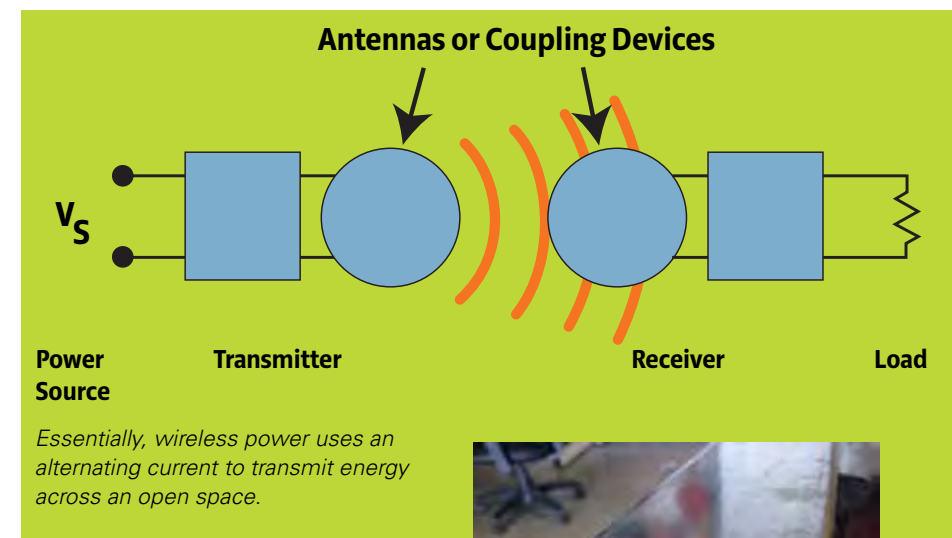
Resonant Circuits can also increase the range considerably, as does an increase in input frequency. In an unrelated development, the Wireless Power Consortium has developed the (*Resonant Circuit*) Qi standard (pronounced "chee") which has been adopted for cell phone and notepad charging over distances up to 1.6 inches.

In addition to access control, a number of other applications are being developed, including electric vehicle charging, industrial power, and many others. Auckland, New Zealand company, Power by Proxi, currently has ICPT products delivering from 12 to 150 watts in commercial use. ^[ii](Ibid).

History

During the 1800s, work by Ampere, Faraday, Maxwell, and Hertz developed electromagnetic theory and led to the discovery of radio waves. ^[iii]

Serbian-American inventor and engineer Nikola Tesla went on to demonstrate wireless energy transmission



with *resonant* transformers known as Tesla Coils. ^[iv]A long-range demonstration project was actually attempted in 1901 using *Resonant Inductive Coupling*. RFID tag experiments began in the 1970s and in the 2000s professors Hui and Tang developed resonant chargers for small electronics.

"Today, wireless power is used for everything from industrial motors to charging smartphones and tablets." ^[v]Other applications are beginning to emerge, with considerable interest in Electronic Access Control (EAC), industrial processes, and transportation.

Access Control Market Needs

Although door loop cords and electric hinges were well developed, applying power to electrified locks and exit devices still offers challenges. Core drilling issues, the need for specialized tools, esthetics, preserving fire ratings, and fragile connectors have led several to explore Inductive Coupling Power Transfer as an option for swinging or sliding doors. Until now, physical size restraints, installation quality, and the need for EAC data transfer have inhibited the application of wireless power transfer in the EAC industry.

Providing power to removable mullions has been a particularly vexing problem. Some early attempts at wirelessly powering these movable parts were sidetracked when installation consistency proved challenging.



Extensive laboratory work verified the validity of the ICPT concept, and beta field test ensued. Technical staff at San Diego integrator Door Systems, Inc., worked out frame mounting details for removable mullions with the creative use of a 3-D printer.

Former HES electric strike manufacturer Lee Hanchett had been watching the growth of wireless power, more properly called *Inductive Coupling Power Transfer*. Existing magnetic coil, potting, and electrical engineering expertise convinced Hanchett and Securitron management that this technology was well within their field of expertise.

The engineering team began to explore wireless power options for access control applications. They found it could get very complicated. A case in point: Wikipedia cites 133 references under the title "*Wireless Power Transfer*." (See endnotes below). Quite a number of technical articles like the one from the University of Alexandria

by Hassan and Elzawawi on *Wireless Power Transfer through Inductive Coupling* appear to be rapidly advancing the knowledge base. ^[vi]

By 2014, Securitron introduced the PowerJump ICPT product. Integrator Bryan Nicholas was confident that this was a good solution for his removable mullion problem. Multiple installations have proved this to be a solid solution.

PowerJump Design Criteria

Commercial products up to 150 watts are available from Power by Proxi in New Zealand. Cost and size currently preclude their concealed use in swinging or sliding door applications. On the other hand, recent developments in energy efficiency have dramatically reduced the current required to unlock most door hardware.

Although higher frequency transmission can increase current, the added cost did not justify more than six watts of power (500 mA @ 12VDC or 250 mA @ 24 VDC). Where more power has been needed, two PowerJump coils have been installed in close proximity with no power degradation. Capacitors can be applied to increase start-up current when required. Efficiency tends to run in the upper 90 percent range with no heat build-up in intermittent use.

Several additional design issues were considered. The first was durability. Design endurance is for 2,000,000 cycles. Structurally sound potting is designed to withstand +/- 150 psi, and is ANSI/SDI-BHMA Windstorm Listed. The product is FCC Part 15

Since an ICPT device can be mounted anywhere on the door, power can be routed from any position on the frame, directly to the lock with no other door prep.



compliant. One critical issue for the access control industry is what happens when the door sags. The PowerJump product is designed to deliver full power across gaps of up to 3/16". Normal vertical alignment sagging can be accommodated with no significant power loss. ^[viii]

Extensive laboratory work verified the validity of the ICPT concept, and beta field test ensued. Technical staff at San Diego integrator Door Systems, Inc., worked out frame mounting details for removable mullions with the creative use of a 3-D printer. During numerous removable mullion installations, the integrator worked with Securitron to produce a pre-packaged removable mullion kit that allows easy installation in the mullion and header assembly. A number of other real-world beta field tests also helped Securitron refine the system into a rather bulletproof product.

The result is a well-documented and simple installation process. Clear

instructions, good templates, and an included install kit with screws, shims, and tabs ensure a solid fit. Maintenance staff can now remove the mullion and re-install without even knowing a power connection existed.

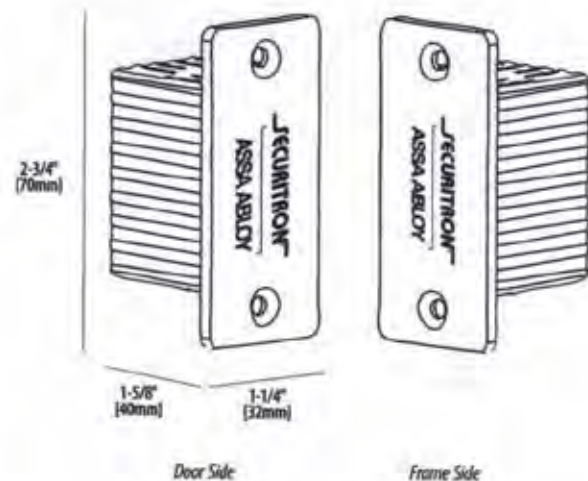
Since power is switched upstream at the power supply, there is no current flow (or heat) across the air gap until activation. Capacitors can be used to energize larger devices, with no visible time lag. Although continuous duty power transfer is certified and practical, surface heat near a lock can be disconcerting to users.

Additional Applications

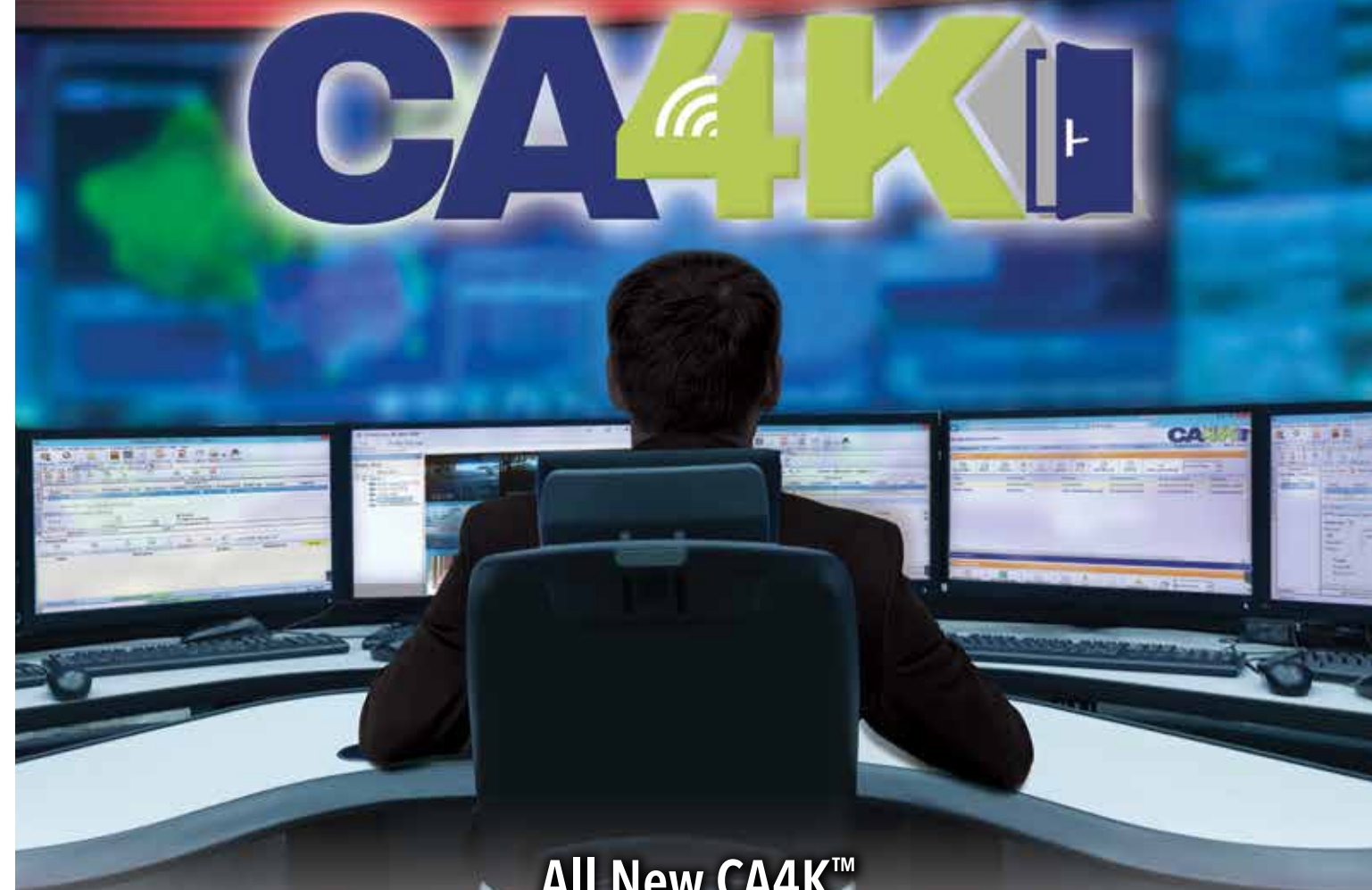
One pleasant surprise came when installers advised that the ICPT provided an exceptionally easy means to provide power to aluminum channel storefront doors. Since the channel is hollow, it was a simple task to drop a wire from the ICPT power source on the header to an electrified lock or exit device.

Since an ICPT device can be mounted anywhere on the door, power can be routed from any position on the frame, directly to the lock with no other door prep. In some cases, the PowerJump has been embedded in continuous hinges. Other developments are in the works to further enhance the utility of the technology.

Corrosive and explosive environments appear to be promising applications since the inductive coupling device is potted. And then there's the problem of battery life in hotel guest-room locks. Every guest has had at least one (or several) dead-battery lock-outs. Of course, the maintenance staff



In 2014, Securitron introduced the PowerJump ICPT product and integrators found that this was a good solution for his removable mullion problem.



All New CA4K™

Continental's Enterprise Security & Access Control Management Platform

- Easy** – New CA4K was designed top to bottom to be Super Easy to Install, Program & Use
- Flexible, Versatile & Scalable** – Grows & keeps pace with any application, from a few doors and users to many many thousands, without the need to replace software or hardware
- Simultaneous Multi-Credential Support** – Ideal for retrofits and fully compliant for TWIC/CAC/FIPS 201 credentials. Mobile credentials, too
- Wireless Access Options** – Wireless Real-time Networked Access Locks (PIN code &/or built-in smart card readers) & Gateways; New Wireless &/or POE Controllers
- Integrates Well with Others** – Seamlessly integrates with alarm systems & expanding list of video, DVR/NVR and other partners
- Fastest, Fully-Distributed Processing** – Door-opens in a fraction of a second & fastest full downloads in minutes
- Labor-Savings** – Dramatically decrease installation time and costs for easiest deployment and little/no downtime
- Open System API for easy new or future integration**
- Managed Services** – Turnkey dealer program for new RMR-producing, cloud-based access & managed services for integrators
- Comprehensive Web Client** – Secure total control from anywhere
- Lowest TCO - Lowest Total Cost of Operation** – Proven low maintenance; upgradable hardware with longest warranty; longest battery life on wireless devices; no annual license fees

Continental Access

www.continentalaccess.com or 1-800-645-9445

Continental Access, CA4K, uniVerse POE & iLock are trademarks of Continental division of Napco. Other marks property of their respective cos.

is always busy replacing dead and dying batteries. Some see ICPT technology as a viable solution for this problem.

Since electrified locksets that communicate with host controllers generally use wires to communicate, the electrified hinge has remained the conventional installation standard. Bluetooth and other RF technologies are sure to stimulate a reassessment of this process. The Power by Proxi company already has a number of applications with wireless power and data.

So far, Securitron is the only player we've been able to locate in the North American access control market, although a Korean startup demonstrated a working model at the 2017 ISC West show in Las Vegas. It is probably a lot easier for other OEMs to use this existing PowerJump product than spending precious R&D resources on reinventing the wheel.

Is Inductive Coupling Power Transfer a Disruptive Technology?

It probably is. The technology did lay dormant for nearly 100-years, but it appears to be picking up speed. ICPT is probably not yet the integrator's silver bullet, but it already charges your cell phone, is charging electric cars, powering locks and electric strikes, industrial applications, and will likely become as ubiquitous as the smartphone. ◀

About the Author: Cameron Sharpe, CPP worked in marketing for Caterpillar and Honeywell before serving 25-years with Best Lock Corporation in New Jersey and Arizona. "It is always a pleasure to watch a real professional like Nicholas, who knows what he's doing, and takes pride his work."

Attributions

^[i] Wireless Power & How it Works: A brief history. <https://powerbyproxi.com/wireless-power>

^[ii] Ibid

^[iii] Wireless Power Transfer – Wikipedia. https://en.wikipedia.org/wiki/Wireless_power_transfer#History

^[iv] "Wireless Power Transfer through Inductive Coupling." <http://www.inase.org/library/2015/zakynthos/bypaper/CIRCUITS/CIRCUITS-18.pdf>

^[v] Wireless Power & How it Works: A brief history. <https://powerbyproxi.com/wireless-power>

^[vi] "Wireless Power Transfer through Inductive Coupling." <http://www.inase.org/library/2015/zakynthos/bypaper/CIRCUITS/CIRCUITS-18.pdf>

^[vii] Securitron ICPT PowerJump®. <http://www.securitron.com/en/site/securitron/products/power-transfers/icpt-inductive-coupling-power-transfer/>

SUMMER'S HEATING UP WITH NEW EASY TO INSTALL KITS!

CALL US FOR MORE INFORMATION, A DEMONSTRATION OR WATCH ONE OF OUR INSTALL VIDEOS AT WWW.COMMANDACCESS.COM



Command Access latch pullback/retraction kits are quiet, smooth and durable. Add one of our industry leading power supplies and power transfers to create a superior electrified opening that exceeds the performance of original factory products – for a fraction of the price.

PD15-UL-M-KIT



- Works with Jackson 1285/1295, Kawneer 1686/1786 & PD16
- Push to Start (PTS) Technology
- Custom ball screw integration for increased torque
- UL Listed

VLP-UL-M-KIT



- Works on Von Duprin 33/35 & 98/99 series devices
- Push to Start (PTS) Technology
- Fast, Quiet, Smooth
- UL Listed

FLP-UL-M-KIT



- Works on Falcon 24/25 series devices
- Easy to Install "Drop in" Kit
- Push to Set (PTS) Technology
- UL Listed

ARLP-UL-M-KIT



- Works on Adams Rite 8200, 8400, 8600, 8800 series devices
- Easy to Install "Drop in" Kit
- Push to Set (PTS) Technology
- UL Listed

* ALL KITS COME WITH 3 YEAR NO HASSLE WARRANTY *

WWW.COMMANDACCESS.COM | CUSTOMER SERVICE (U.S) 1-888-622-2377 | CUSTOMER SERVICE (CA) 1-855-823-3002

Request information: www.SecurityInfoWatch.com/12140374



800.233.4210
sales@topnotchinc.com
www.topnotchinc.com

Pennsylvania • Missouri • Nevada • Massachusetts



Connect and control more doors a whole lot easier than ever before

Introducing the Schlage® LE wireless lock for mortise door applications. LE wireless locks are ideal for interior openings requiring increased security in applications such as commercial, mixed-use and multi-family settings, where improving efficiency and reducing costs are an increasing concern. LE provides flexibility for mortise entries as the newest member of the ENGAGETM technology family of products.

Allegion offers an array of products and solutions for a multitude of applications.



Schlage is the property of Allegion plc. All other brand names, product names or trademarks are the property of their respective owners.

C11530 © 2017 Allegion

Request information: www.SecurityInfoWatch.com/12129499

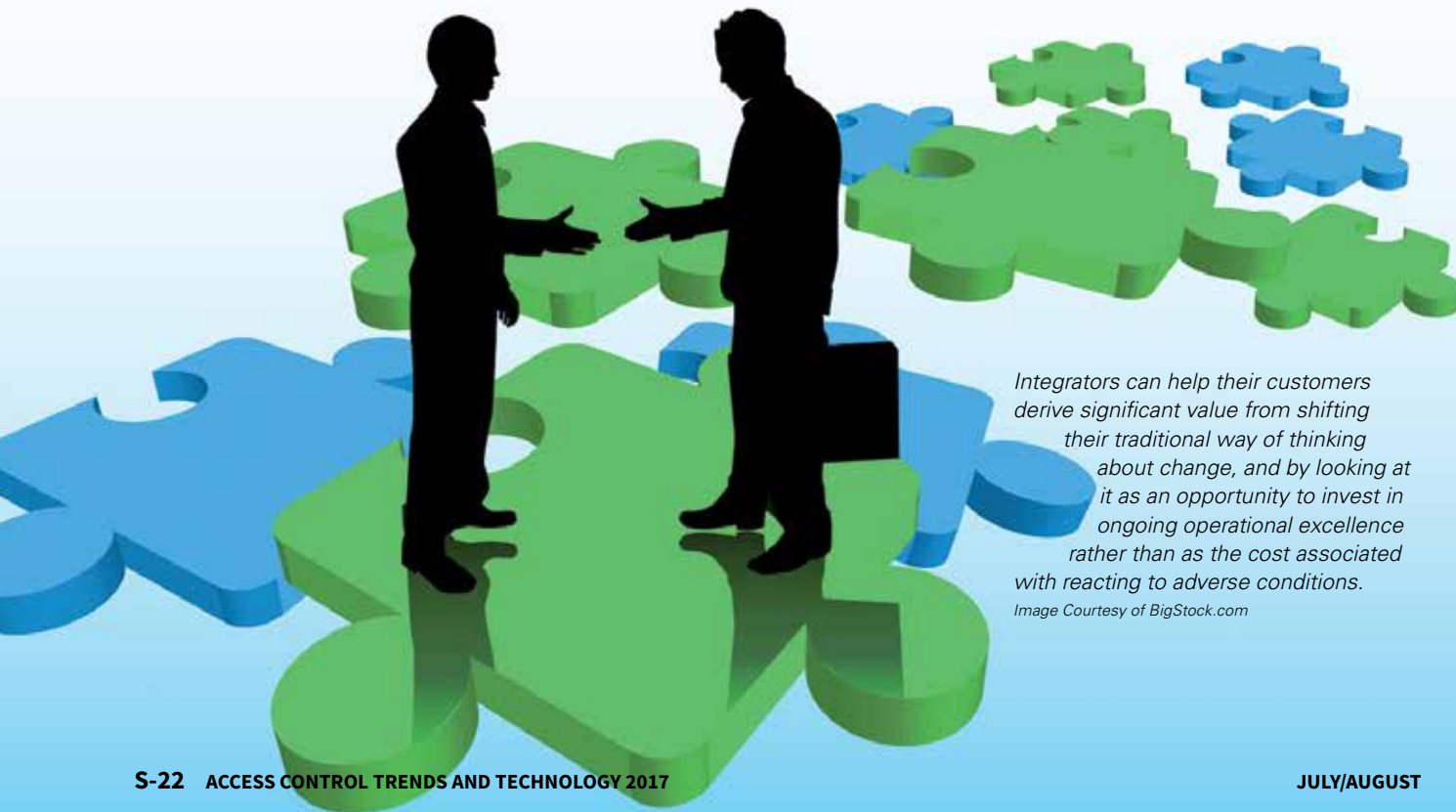
10 Triggers for Transition

Integrators help customers embrace change to upgrade their access control technology

by Brandon Arcement

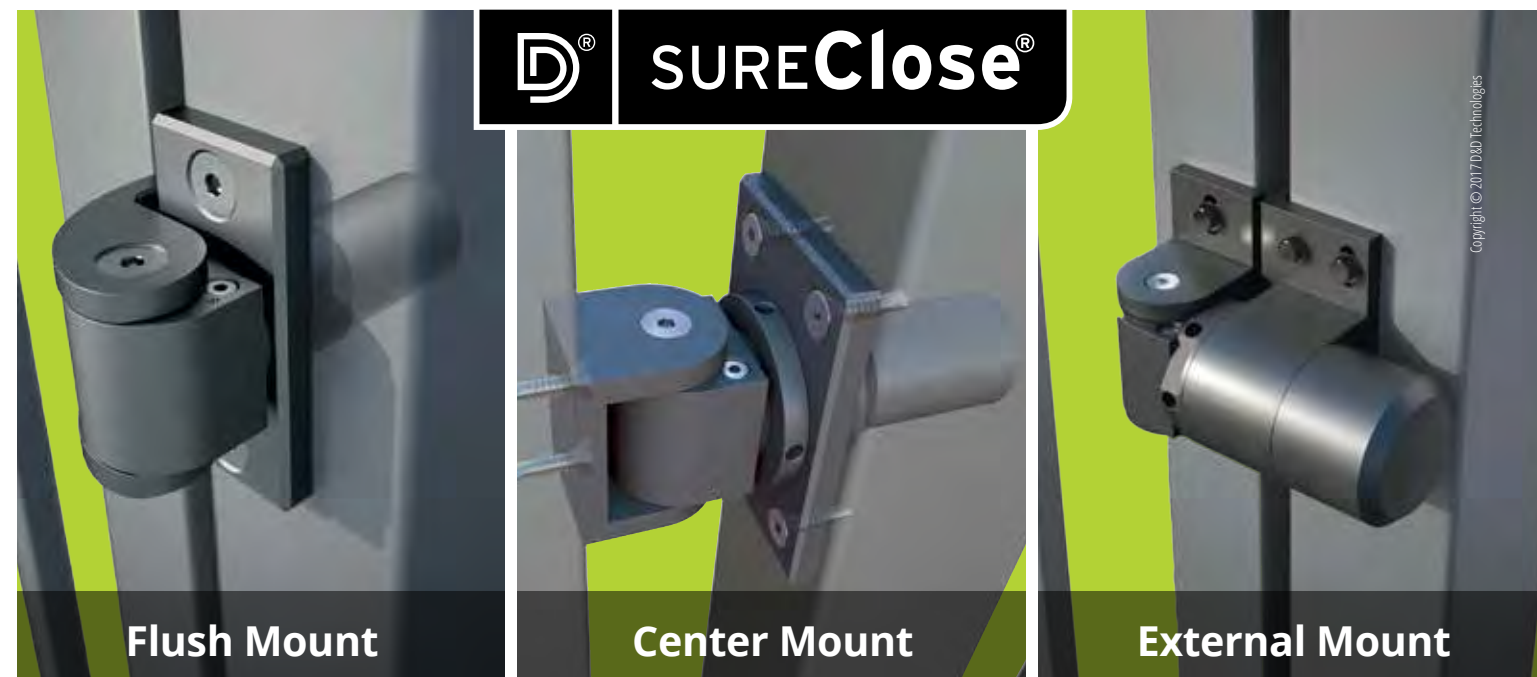
A key area where organizations need help from security integrators is in the assessment of their current access control solutions and whether and when to make the transition to new technology. Organizations often delay transitions over budget concerns or because of worries that the process will

adversely impact productivity and workflow. But these delays can be dangerous, and integrators offer important perspective and guidance about escalating security threats that place increasing pressure on obsolete access control infrastructure. Based on their extensive experience serving customers across a variety of applications and circumstances,



Integrators can help their customers derive significant value from shifting their traditional way of thinking about change, and by looking at it as an opportunity to invest in ongoing operational excellence rather than as the cost associated with reacting to adverse conditions.
Image Courtesy of BigStock.com

Hydraulic Gate Hinge-Closer, in One Small Powerful Package

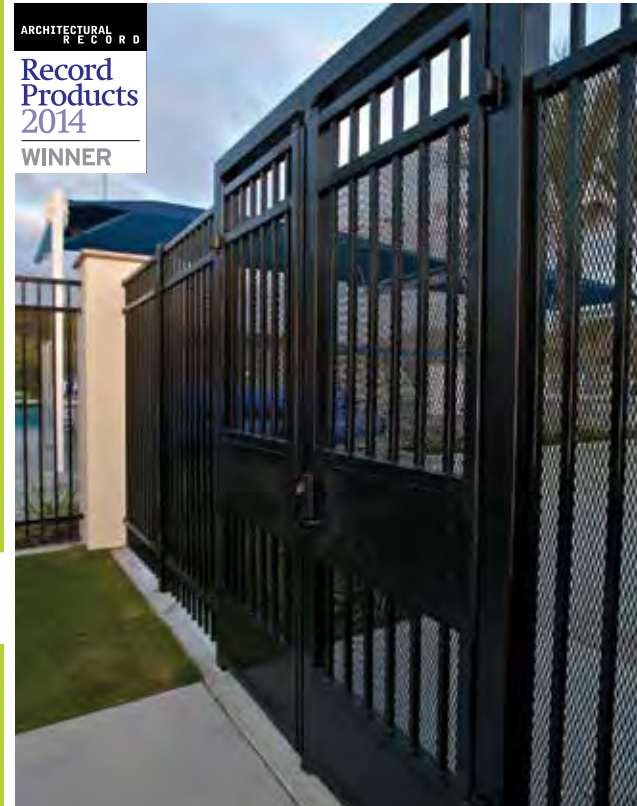


The choice is yours... Internally or Externally Mounted

- Aluminum screw-on or steel weld-on
- Dual Bearing Glide System™ for superior performance
- High strength anodized aluminum body – 1,500 lbs gate load capacity
- Tested to 500,000 cycles
- Adjustable - vertical, horizontal, closing speed & final snap force
- ADA compliant
- Highly tamper resistant
- Maintenance free – no messy grease

Self-closes gates up to 260 lbs

Ideal for residential and commercial gates



Organizations often delay transitions over budget concerns or because of worries that the process will adversely impact productivity and workflow.

they know it is far more effective to be proactive rather than reactive when making decisions about upgrading to new and improved technology.

There are also many positive reasons that integrators can share with their customers about why they should embrace change. These include enhancing investment value, improving user convenience, and paving a more flexible path to future capabilities. The ability for organizations to embrace these more positive aspects of change requires an access control platform that can meet today's requirements with the highest levels of security, convenience, and interoperability while enabling organizations to adopt future capabilities without disrupting the ongoing business operations.

These are the advantages of the latest technologies. Integrators can educate their customers about how these technologies enable organizations to presume and prepare for ongoing change, not only to combat continuously evolving security threats but also to anticipate and address new and emerging operational requirements. Today's systems also enable decision-makers to preserve investments in their current infrastructure as they transition to new technologies and capabilities. The following are 10 common triggers that integrators can share with their customers as they plan for the transition to new and improve access control capabilities:

1

There is growing demand for combining many different access control applications on a single card – and adding new ones in the future: Today's contactless smart cards can be used for many different purposes beyond opening doors, from time and attendance to secure print management and cashless vending. Administration of these functions is centralized into one efficient and cost-effective system. Organizations also can seamlessly add logical access control for network log-on to create a fully interoperable, multi-layered security solution across company networks, systems and facilities.

2

Employees increasingly want a mobile option: Today's access control systems also enable organizations to upgrade their systems to the convenience, flexibility, and security of carrying mobile IDs on smartphones and other devices. Mobility transforms the user experience for a more convenient, trusted and secure digital world, dramatically elevating how users regard security by enabling them to confidently connect to and use more applications, on the go, than ever before, with a single, trusted ID that can be carried on a smart device.

3

There is a change to security requirements: An organization may be required to increase its security because there has been new legislation or regulatory requirements. Or, the organization may win a new client or acquire building tenants that necessitate an increase in security. Any of these triggers presents an opportunity to upgrade security at other locations, as well, as part of a larger upgrade to new standardized, centralized systems.

4

Company undergoes a merger or acquisition: At some point after an M&A event, an organization will need to issue new credentials. This presents the opportunity to merge what previously were disparate administrative and other systems, technologies, and processes. The investment in new technology is often comparable to the cost of integrating separate legacy systems, so this is the perfect time to migrate to a new, more secure, sophisticated and capable system.

5

The headaches of managing multiple cards and systems exceed threshold of frustration: In the same way that an M&A event can trigger the need for access control system consolidation, so can a long period of rapid growth or the use of



Smart | Profitable | Exclusive

Padlock Markets:

Oil & Gas | Manufacturing | Municipalities | Education | Government

Our products are higher quality, better value & offer much better margins!

4-Dial Resettable Brass Body with Brass Internal Parts

- 10,000 possible combinations which can be easily changed and set
- 2" (51mm) wide solid brass case for superior security and weatherability
- All brass internal locking mechanism
- Automatic "0000" stop
- 1", 2-1/4" and 4" shackle available
- Best Used For: Job boxes & gang boxes, Utility meters, substations & cable boxes, Tool chests, boxes and cribs, Lockers



K410D Series Rotary Dial Combination

- Anti-shim feature resists the most common shimming methods
- Aluminum body for greater security and durability
- Hardened steel shackle
- Most cost-effective locking solution
- Other Colors available special order
- All Padlocks have a 1 year warranty from time of shipment
- Requires a padlock hasp of at least 5/16"



936/937 Series Round Body Hardened Steel

- Keyed 936/937 in the popular American® AM3 Keyway
- Molybdenum alloy shackle is standard
- 2-1/2" (64mm) wide round solid steel body
- Chrome rustproofing provides longer life
- 1-1/8" (28.57mm) or 2" (51mm) tall, 7/16" (11mm) molybdenum alloy shackle for superior cut resistance
- Dual ball bearing locking mechanism resists pulling & prying
- High security, rekeyable 5-pin cylinder with spool pins virtually impossible to pick
- All padlocks come Non Key Retaining
- Key retaining set screw included with each lock
- Product of Taiwan; designed in Wheeling, Illinois
- Best Used In: Industrial, Storefront & Business Gates, Manufacturing Environments, Utility Meters, Substations & Cable Boxes, Marine Recreation



900 Series Aluminum Safety Lockout

- Solid Anodized Aluminum Lock Body
- Quality Chrome Plated Hardened Steel Shackle
- Patented Quick-Change Shackle Design
- Double Ball Bearing Locking Mechanism
- 4 shackle sizes; spare shackles ordered separately
- Nine Colors and engraving available
- All KA and KD come Non Key Retaining
- Features American® Keyway 6 pin cylinder
- Product of Taiwan; designed in Wheeling, IL
- Best Used For: Maritime, Agriculture, Oil & Gas, Construction, Food Service
- Specifications:
 - 1-1/2" Aluminum Body; 1/4" Diam Shackle
 - 1-3/4" Aluminum Body; 5/16" Diam Shackle
 - 2" Aluminum Body; 3/8" Diam Shackle



Est. 1882 in America

Telephone: 800.733.8588 | Fax: 847.537.1881 | www.CCLSecurity.com | info@CCLSecurity.com

Request information: www.SecurityInfoWatch.com/10213160



Organizations may need to implement the highest levels of security including strong authentication at the door.

decentralized administration systems across multiple physical locations. Standardizing and centralizing management of secure identity ensures consistency, higher security and a more efficient use of resources.

6

There is a facility consolidation, additions or relocation: Any move or addition will generally trigger the need to issue credentials for the new location. Mass rebadging is much simpler to coordinate and manage using a single, centralized system, making it an ideal time to simultaneously re-examine access control across the entire organization.

7

Company rebrands and triggers a re-issuance process: Any time there is a re-branding, companies generally purchase new ID cards for current employees and enough cards to onboard new employees down the road. Forward-thinking decision-makers use this as an opportunity to simultaneously invest in new access control technology with the flexibility and advanced capabilities to carry them well into the future.

8

Risk management needs improvement: Organizations often face new, more stringent insurance requirements, or need to reduce their liabilities and associated risk management costs. This can be done by dramatically improving security through a move from an outdated system to one that supports current standards.

9

There is the need to adopt strong authentication throughout the organization: Organizations may need to implement the highest levels of security including strong authentication at the door.

This requires transitioning to an access control system that supports PIV, PIV-I and CIV cards, along with an easy path to compliance with government requirements, where needed.

10

There is a breach or other major security event: Ideally, organizations should upgrade before there is a problem, especially when the current system uses legacy technology that is easily breached. But the reality is that sometimes it takes an unexpected event or security breach to move an organization to make the investment in a new access control system.

When making the jump to a new access control system, it's also important for organizations to evaluate the companion secure issuance system that will be used to produce the ID cards. Large organizations issue a staggering amount of ID cards every year. Sometimes this issuance is done by a service bureau but, more often; this process is done on site by the organization itself, relying on a desktop printer that personalizes blank or pre-printed card stock with visual cardholder information.

Organizations generally choose from two major technology categories for printing and encoding cards: high definition printing (HDP®) retransfer technology, and direct-to-card (DTC) technology. Ideally, a solution should also support both centralized and distributed issuance models, by combining the high-volume reliability and advanced credentialing features of larger centralized printers with the lower cost and smaller footprint of a distributed printing model.

There are other important secure issuance considerations for integrators to share with their customers, particularly in the areas of energy consumption, overall waste, and cost efficiency. The latest secure issuance systems are significantly more sustainable than in the past. Two key developments include "wasteless" lamination, and reducing carbon footprints as defined through the GreenCircle® certification program.

With wasteless lamination, the lamination patches that are applied to cards for increased durability are attached to one another in a continuous stream of material on a single roll. This eliminates the need for an underlying carrier. As each patch is detached from its supply roll and adhered to a card, the lamination cycle is complete. Once the supply roll has been depleted, all that's left is a single empty core.

This process significantly reduces both the cost of the consumables and the waste product. Wasteless lamination has proven to be very cost-effective, reducing lamination consumables costs as much as 50 percent while maintaining the highest levels of security and durability.

GreenCircle certification recognizes the energy savings that are achievable through advancements in card lamination technologies that have reduced the significant energy required to heat up and maintain optimal operating temperature. These technologies can conserve significant amounts of energy while also saving time.

Integrators can help their customers derive significant value from shifting their traditional way of thinking about change, and by looking at it as an opportunity to invest in ongoing operational excellence rather than as the cost associated with reacting to adverse conditions. By showing customers how to take advantage of these 10 common triggers for transition and implement a more sustainable approach to secure issuance, they will deliver two important benefits. First, their customers will be able to easily and inexpensively expand and upgrade their systems to meet changing needs, take advantage of new technologies and capabilities, and produce ID cards in a more environmentally responsible manner. Second, as they evolve beyond current abilities, they will be well-positioned to adapt to and combat continuously changing threats, with the confidence that they can preserve investments in their existing infrastructure. ◀

About the Author: Brandon Arce-ment is the Director of Product Marketing with HID Global.



JLM IS NO ORDINARY WHOLESALER

WE OFFER AN EXTENSIVE STOCK OF PRODUCTS AND SERVICES TO MATCH

JLM Wholesale is stocked with thousands of products from over 80 manufacturers including the biggest name brands. We carry the latest access control systems, closers, exit devices, and much more! JLM can provide you with not only the best products, but services to match.

Let our expert sales and technical associates assist you TODAY!



WE HAVE WHAT YOU NEED THE INDUSTRY'S MOST TRUSTED SECURITY DOOR HARDWARE WHOLESALER

MI: (800) 522-2940
NC: (800) 768-6050

TX: (877) 347-5117
WWW.JLMWHOLESALE.COM



Request information: www.SecurityInfoWatch.com/10214128

1107 Series Maglocks



*Lack,
These new slim mag
locks look as great
as they operate.
— Ed*

Dortronics Systems' new 1107 Series Maglocks offer smart features in a slim configuration – at a competitive price. **1107xD Slim Line Magnetic Locks** are only 1-1/4" deep and deliver fail-safe operation, releasing instantly upon command or loss of power. **1107xEDR Delayed Egress Actuating Locks** operate with the 7101-P Delayed Egress Panel, and employ an actuator which senses door movement. 1107 Series Maglocks are NFPA Life Safety and BOCA compliant, tested to UL294 & feature limited lifetime warranties, and are proudly made in the USA.

DORTRONICS SYSTEMS, INC.
1668 Sag Harbor Tpke., Sag Harbor, NY 11963 (800) 906-0137 (631) 725-8148 Fax www.dortronics.com



Request information: www.SecurityInfoWatch.com/10213494

Access Control TRENDS AND TECHNOLOGY 2017 S-27

Seneca

Seneca i-Series NVR systems featuring the Intel® Xeon® Processor



Intel Inside®. Powerful Productivity Outside.

Intel, the Intel logo, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation in the U.S. and/or other countries.

www.SecurityInfoWatch.com/12348632

Showcase



Door Entry System

Paxton Access has launched the Net2 Entry Touch panel, which features a 7-inch color touchscreen and personalization options, making it suitable for more sites. Ideal for a range of applications, including commercial buildings, leisure facilities and hotels, the product's stylish design has been awarded two prestigious design awards. It is available in three variations: flush-mount, surface-mount, and rain hood. It has an IK7 impact protection rating with an easy to read anti-glare screen for optimal daytime viewing.

Request more info: www.SecurityInfoWatch.com/12331321



Alarm Lock Trilogy® T2 Series

Amityville, NY – Alarm Lock, a division of NAPCO Security Technologies, has expanded its Trilogy® T2 Series, to include Mortise, LocDown & Exit Trim Standalone Keyless Access models.

Request more info: www.SecurityInfoWatch.com/12303922



Request more info: www.SecurityInfoWatch.com/12321090

AMAG Technology's Symmetry Security Appliance

Torrance, CA, March 27, 2017 - Access control leader AMAG Technology, announces the release of a new security appliance designed specifically for smaller businesses that need security management. Introducing the Symmetry Security Appliance, a powerful all in one security device that delivers access control and video management together.



SDC UniFLEX™ 45 Series Strikes

SDC's UniFLEX™ 45 series commercial duty electric strikes utilize the same strike body with a choice of four application faceplates for compatibility with all cylindrical locks and most centerline latch entry locks with up to 3/4" latch throw. Features include 12/24V AC/DC operation, field reversible failsafe/failsecure, low profile with only 1-1/8" depth, mounting tabs and wire connectors cast housing and keeper.

Request more info: www.SecurityInfoWatch.com/12329097



Intelligent Access Controller

Sielox LLC has unveiled a new Lock Toggle feature as part of its 1700 Intelligent Controller, which fully integrates with Schlage AD, NDE, and LE wireless locks. The Lock Toggle enables users to lock and unlock doors without a second credential to override pre-set schedules.

For more information about Sielox, visit www.Sielox.com, email info@Sielox.com or call toll free 800-424-2126.

Request more info: www.SecurityInfoWatch.com/12318752

Smart access begins with end-to-end solutions.



E-Plex Wireless and Stand-alone Access



Keyscan Networked Access Systems



RCI Electronic Access Controls

Trust dormakaba for solutions that provide the perfect blend of form, flexibility and function. Our comprehensive line of networked access systems, electronic access controls, wireless and stand-alone access solutions are designed for multihousing, healthcare, financial, retail, transportation and commercial applications with a single goal in mind—making access in life smart and secure.

DORMA and KABA are now dormakaba

Visit dormakaba.us



Request information: www.SecurityInfoWatch.com/12304402

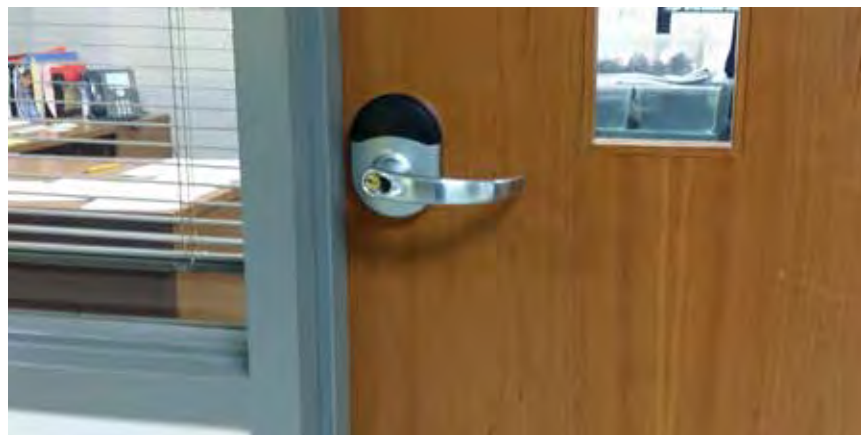
Making the Grade with Wireless EAC

Sielox delivers layered access control solution to New Jersey school district

School safety today requires a broad-based effort to address the many security issues that can hamper a safe learning environment. These initiatives often include technology and human-based solutions and both play an essential role in preventing and controlling security vulnerabilities throughout the school. The on-going development of access control and lockdown technology by leading manufacturers such as Sielox also plays an important role in helping schools achieve their goals as New Jersey's Upper Township School District learned.

The Upper Township School District is a comprehensive community public school district, serving students in pre-school through eighth grade from Upper Township, in Cape May County, New Jersey, United States. Located in Petersburg, New Jersey, the UTSD wanted to strengthen classroom and building security by upgrading the locks on classroom and perimeter doors. Their options at the time included an interior classroom mechanical lockset; a wireless lockset that was not online; and an online communication wireless lockset.

The online wireless lockset was selected for UTSD because it allowed the school to be locked down immediately and remotely. The problem, however, was that the cost of deploying wireless locks for the more than 130 doors throughout the three buildings was significantly



Wireless locks solved New Jersey's Upper Township School District's access control and lockdown issues.

more than UTSD had budgeted.

During the course of UTSD's search for a more affordable solution, new wireless lock technology became available and at a cost that was approximately 50 percent less. The savings allowed UTSD to move forward with the project that now had the capability for a layered approach to school security. This included installing Sielox's Pinnacle access control system for control of interior and perimeter doors and the 1700 intelligent controller integrated with the new Schlage NDE wireless locks.

"We were looking for the best solution to handle a lockdown situation at the three schools in our district," said Vincent Palmieri, Superintendent, Upper Township Schools. "Given the fact that we also wanted the ability to lock the perimeter and interior doors of each school, Sielox had the complete solution for our needs."

Another element of the layered solution implemented at UTSD was Sielox's Class (Crisis Lockdown Alert Status System) emergency notification and lockdown solution. CLASS

provides real-time classroom status, updates and notifications to administrators and first responders using graphical maps, email and text messaging to assist in making split-second decisions in the event of an incident or developing situation.

The system was designed and built by CM3 Building Solutions, a security channel partner with Sielox. Along with the capability to secure classroom doors remotely, the system designed by CM3 provided additional benefits to the school. Card readers installed on both sides of certain perimeter doors automatically records entry and exit activity via the Pinnacle access control system, eliminating the need for staff to sign in when they come in and leave the building. Perimeter doors that didn't require access control are supervised and monitored via the Sielox Pinnacle software and a local sounder/strobe at the physical door location. This allows for notification of a door propped or a door forced open condition and assists the district in keeping a secure building perimeter. ◀

CREATING THE FUTURE OF SECURITY... TODAY



The Security Professionals' first choice for today's security infrastructure, from one room to multi-location complexes around the world. Our reputation is based on a time-honored tradition of rock-solid quality, premium reliability and the integrity of DSX and our network of factory-trained, authorized dealers and support.

When you are staking your reputation on a solution – choose the most powerful and intelligent access control systems in the world, choose the total security relationship with DSX.



- No "Per Seat" Licensing In System Pricing
- LAN/WAN Compatible
- Smart Card and Biometric Integration
- Unlimited Access Levels Per Cardholder
- Integrated Photo ID Badging
- Backup SQL Server

DSX Access Systems, Inc.



www.dsxinc.com

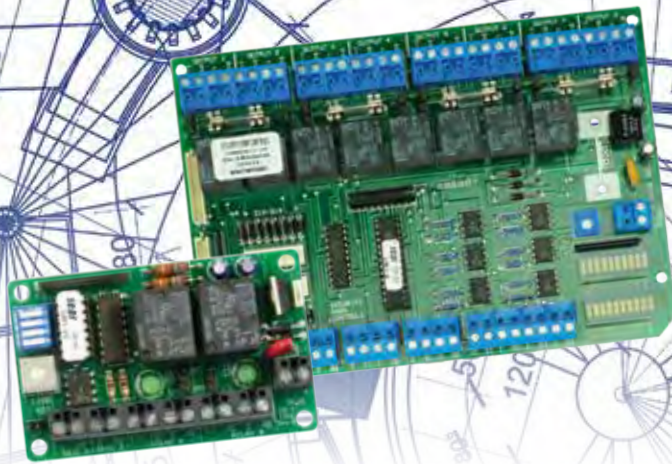
10731 Rockwall Road | Dallas, TX USA 75238-1219
888.419.8353 | 214.553.6140 | sales@dsxinc.com

- Backwards Compatible Architecture
- Alarm Text Message/E-Mail Notification
- Hot Swap Redundant Communication Server
- High Level Elevator Control Interface
- Integrated Wireless Locksets

Quality. Reliability. Integrity. The Security Professionals' First Choice.

Request information: www.SecurityInfoWatch.com/10214208

DOOR CONTROL MADE EASY



Whether you need to control one door or many doors, there's an affordable, field programmable **SDC UR Series Hardware Controller** to create your perfect door opening system to reduce costly programming and wiring time. The award-winning UR Series is the same simple, reliable, flexible solution to door control trusted in thousands of installations since 1998.

- Use the same controller for multiple applications
- Selectable relay modes permit installer configuration per application requirements
- Microprocessor based system logic reduces need for standalone relays
- Centralized wiring for locks, access controls, monitoring contacts and peripheral equipment provide easy troubleshooting and enable uniformity for multiple installation applications

For details and specifications: SDCsecurity.com/power-controllers.htm

Request information: www.SecurityInfoWatch.com/10214991



the lock behind the system

SDCSecurity.com • 800.413.8783 • service@sdcsecurity.com

