

# ...And Herein Lies the Opportunity:

# THE CASE FOR ACCESS CONTROL

By Isac Tabib

**Let's face it—times are changing—**and rapidly. We now have cars that drive and park themselves; pilotless aircraft that take off, fly and even land on a moving aircraft carrier; smart-phones with countless apps that can do practically anything with little effort on our part; and so much more.

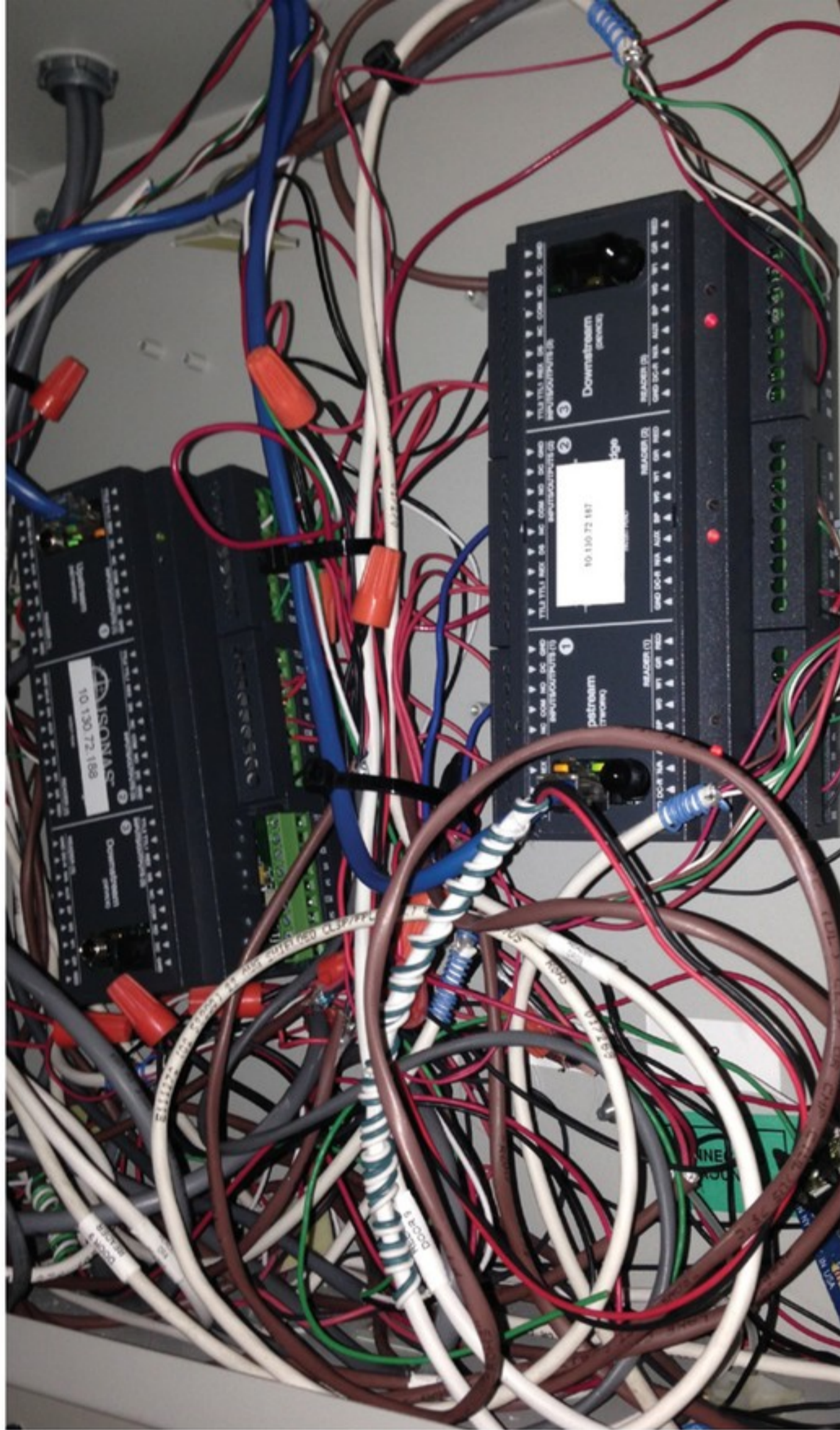
Technological advances have allowed online retailers to commoditize nearly everything, thus reducing the classic retailer's profits. Door hardware is not exempt from this revolutionary formula. For most business owners, locksmiths included, these changes have been evolving while they are focused on running their businesses in the same way they have in the past. The question becomes: is this sustainable?

Having been in the electronic security integration business for many years, I have had the fortunate opportunity to be the security integrator for many small and large projects. From designing and installing access control and CCTV systems in a small medical center with six reader doors and four cameras; to having hundreds or

even thousands of reader doors and cameras in locations such as JetBlue Terminal 5 at JFK International Airport, Westchester County Jail, the New York Times headquarters, Hearst Publishing Headquarters, and countless other locations.

For all of these projects, we contracted with many locksmith companies, since, after all, each of those clever readers and their associated software needed an electrified lock to do the job. Historically, regardless of how much time we spent on engineering and delivering an access control project, the customer's perception of its 'functionality' boiled down to a simple question: did the door unlock properly?

When thinking about that question, I first realized that, despite their good knowledge of locking hardware and life safety compliance, most locksmiths do not take advantage of the huge market opportunity they have—installing access control. Think about it: every electrified lock needs an access control system.



There are likely more than a dozen reasons why this is the case, which we will cover in different article. I will briefly focus on a few:

- The need for basic electronics knowledge.
- The need to have basic IT knowledge and skills.
- A lack of access control products that are resilient, simple to install and maintain.

You may just want to take a mental note of the opportunities and needed steps so that you can provide your customers with a complete, simple access control and CCTV system. These will improve your bottom line.

One of the most accessible opportunities for the average locksmith to capitalize on is the 'existing system' market. Electromechanical locks, by definition, fail. There are moving mechanical parts within the locks, and for various reasons—many unpredictable—they break. When they do, it is naturally the locksmith that gets called for the repair—and herein lies an opportunity. Providing solid security system design, excellent installation and ongoing service, are the antidotes to being commoditized.

## A Case Study

Recently I was called upon to work with a locksmith to fix a troubled access control system in one of the buildings of a large, multi-site customer. The customer was complaining about a plethora of issues: access doors that didn't unlock, to doors that would not lock; random 'access denied' messages; unauthorized persons "tailgating" authorized personnel to gain entry into the facility; frequent 'system is not working' complaints that were taking many resources, including multiple days and costly additional dollars, to rectify. We spent time at the facility to evaluate the conditions, come up with an action plan and provide an upgrade solution.

## Basic Electronics Knowledge: Wiring

When thinking about an upgrade of an existing system, we always try to preserve as much of the present infrastructure as possible, adding and upgrading as needed. One of the largest labor investments (and costs) is the existing wiring.

At the card access door, it is relatively simple to identify and repair wiring issues. However, at the access control system's "head end" (the "hardware controllers" of the system), wires are normally already terminated inside the system controller enclosure. These wires are typically too short to make it to a new controller destination for a system upgrade.

For this reason, very often installers use telco type "chicklets" to splice the old wires to the new controllers. Doing so only exacerbates the situation. The end result is a cabinet loaded with many intermingled wires (aka "spaghetti") that are not only difficult to identify, but worse yet, even harder to service in the future. In this building, the original installer also added a local power supply in the ceilings near each door (see below), making the system upgrade even more involved and complex as we had to find each, examine and determine what was going on.

Instead of using an inferior and unsupportable "chicklet" approach, we typically use DIN rail mounted Phoenix connectors. (You'll see the results later on.) With the use of Phoenix connectors, wires from the new controller are terminated in an orderly form on one side of the connector. At the time of the cutover from the original system to the new access control system, existing field wires are terminated on the other side of the connector. This allows for a neat and orderly installation, easily serviceable at any time (by any technician), as each of the wires are identifiable and accessible for testing, troubleshooting and repair.

Tip: I also take time to fully document the job. We memorialize device locations, wire types/runs, controller locations, assigning color-codes, IP addresses, details and the like. The more detail, the better for our future in servicing the system and keeping the customer happy.

In my case, I am AutoCAD proficient, as is my organization. Documenting the system is easy using CAD, not to mention easy to store, update and maintain. If you are not using CAD, then at a minimum, take a piece of paper and create a 'stick figure' of the building, show door locations and anything else you did, as this will make much easier for you and your technicians to service the system into the future.

### Basic IT Knowledge: The Use of Network Controllers and Software

In this case, we actually had an easy choice to make. Since the customer was a large multi-site type with an existing, high quality integrated access control (Software House Ccure-9000) and CCTV platform (American Dynamics Victor), we simply used the customer's platform hardware and controller requirements.

The benefits to the customer were many. There was no need to purchase, manage or maintain another piece of software. This saved the customer a minimum six months of time and numerous "committee" resource hours; the headache of another construction-like project that would impact much of the building; not to mention carrying a high cost.

Based on our knowledge of the system and IT infrastructure, we were able to immediately offer relief by bringing this building online with the others in the customer's networked

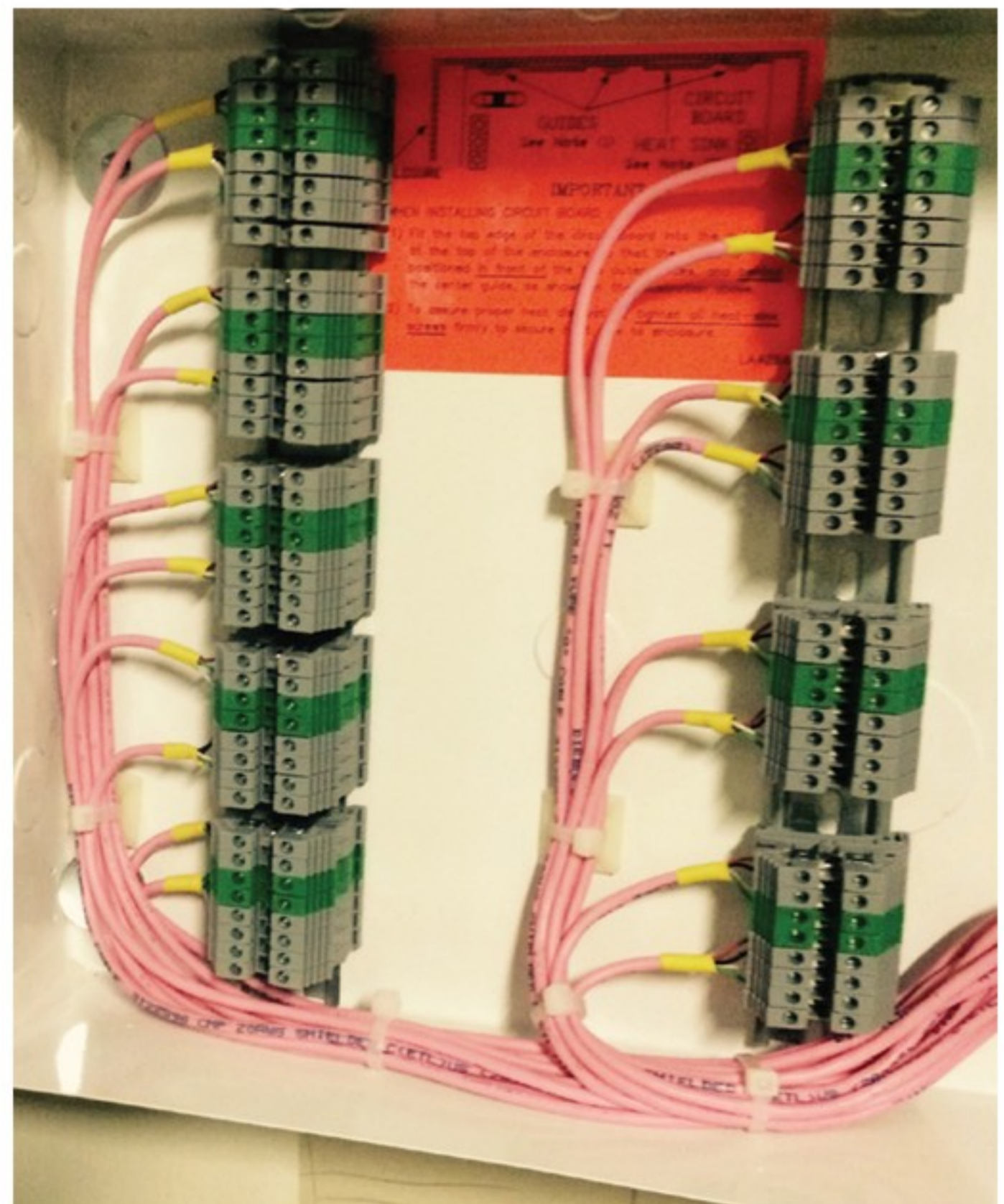
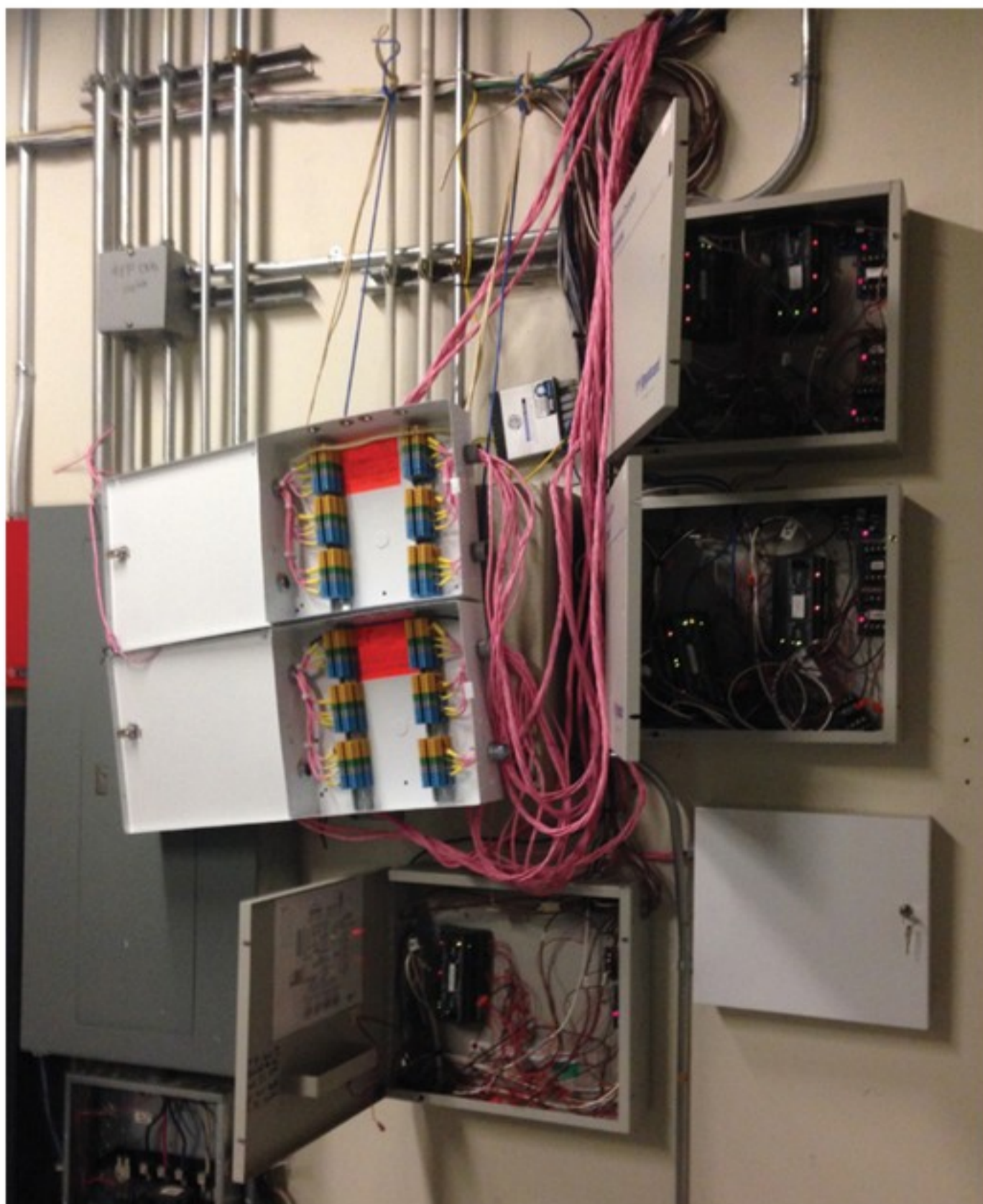
access control system. The building became a part of the customer's existing "enterprise" access control system, allowing for use of a single system-wide access card.

Employees and contractors of this facility can now travel between this and other buildings throughout the enterprise, carrying just one master proximity card containing their authorized user credentials. System administrators have control across the enterprise. The impact of cost savings and control to the customer are huge. The "user list" integrity was immediately enhanced, as system administrators were able to add/delete users and even automate credentials for new or terminated employees, from a singular centralized database.

It is worth noting here—it does not make a difference whether an access system is comprised of two doors or two hundred doors—the same rules of proper product selection, design, installation and documentation apply.

### Electrified Locks

Most locksmiths are very familiar with proper locking hardware selection and the associated life safety code requirements. Security integrators typically are not as familiar with available electrified door locking hardware and tend to use magnetic locks everywhere. Magnetic locks, or "maglocks," are easy to install and require no prior installation planning.



The conversion: work in progress on the left. New splice panels with Phoenix connectors (right) staged nearby existing equipment.



Aluminum pneumatic REX buttons

I get called to evaluate many installations and am not surprised to see maglocks installed on hollow metal or wood doors that have been prepped for an electrified mortise or cylindrical lock. I often see maglocks installed on doors that are in the path of egress, despite the fact that emergency egress hardware has already been installed prior. There are many reasons and sound opportunities for the local locksmith to both correct and profit from the use of proper electrified locking hardware for customers; not to mention save lives.

### Door Devices

As you know, correct access control door installation also requires a door contact (DC), aka Door Status Monitor (DSM). The reasons are many and include benefiting from "Door Forced Open" and "Door Help Open" alarm notifications, to "Normal/Unused" transactions, and "Door Relock" features.

The relock is an important feature. Most default timers for valid card reading in controllers are an average of eight seconds. Most people take roughly three to four seconds go through the door. That leaves a period of four seconds in which the door

remains unlocked, allowing a person to tailgate and enter the premise without presenting a valid access card.

The use of the DC/DSM is what signals to the processor (system controller) that a door remains ajar, thus causing an alarm, based on programming. Remember the complaint our customer indicated regarding unauthorized facility access; a door contact paired with a REX device is a simple way to dramatically reduce the "tailgating" problem. Please remember: when using a DC/DSM, it is mandatory to also use a Request to Exit (REX) sensor, for which many types are available.

As for the REX, especially when pertaining to maglock doors, we are all familiar with the single gang plate and green button marked "Exit." Users have to push the "Exit" button for the door or gate to unlock and allow them through. Other than the button's color and text, for life safety and code compliance, one must consider the type of switch behind the green button.

The use of a momentary SPST (Single Pole Single Throw) switch connected to the system processor 'REX input' is prohibited. At this site, we replaced all SPST switches with an all metallic, pneumatic REX device, the S106 series

## THE ULTIMATE IN CLASSROOM SECURITY



*PDQ's Exclusive  
Classroom Intruder  
Cylindrical Lock  
with LED Indicator  
Now Patented*

*Press the button from inside the classroom. Red LED will light up indicating the outside lever is locked. This eliminates the need to open the classroom door to check the security of the outside lever.*



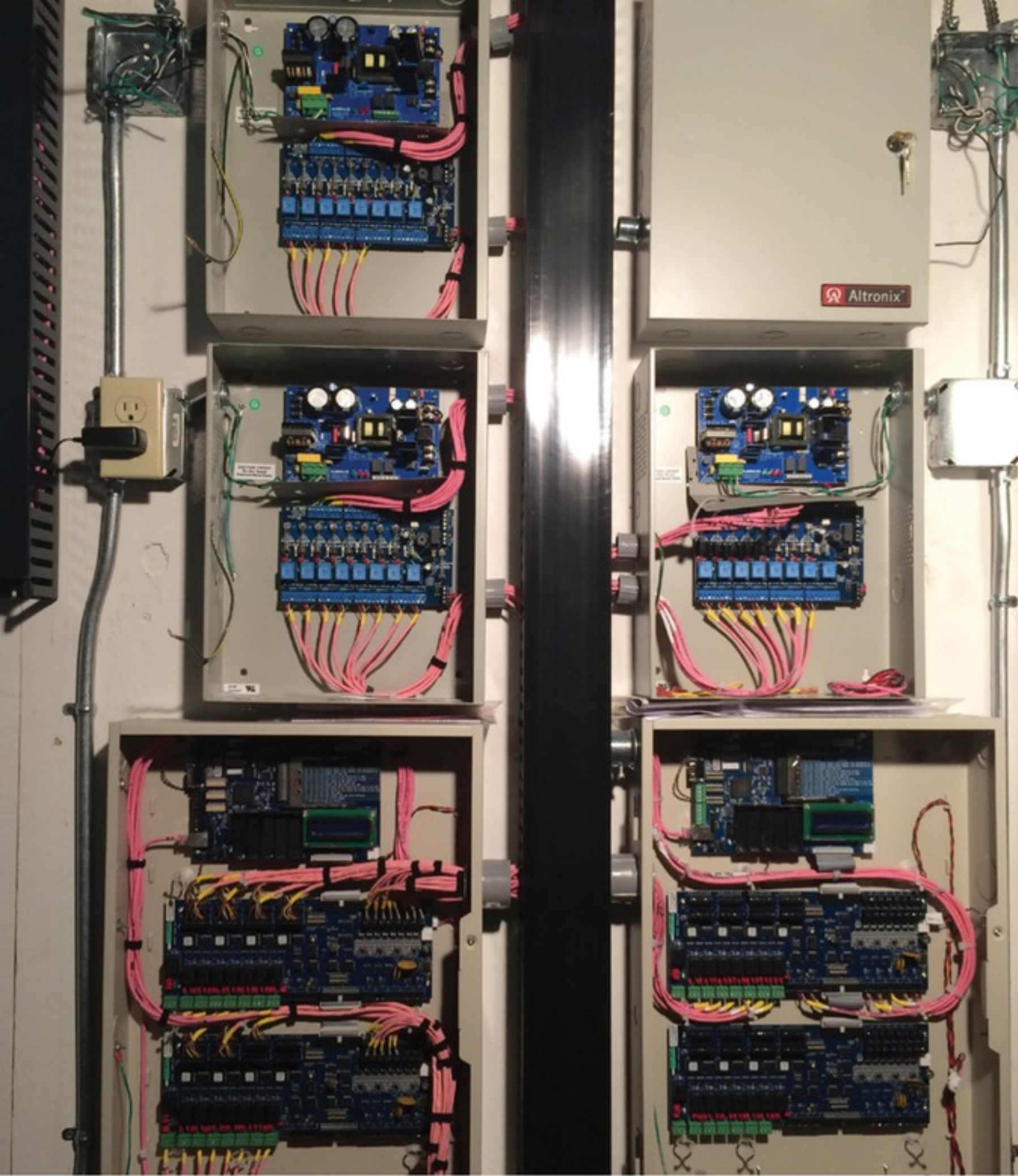
OUTSIDE LEVER  
UNLOCKED

"PRESS THE BUTTON"  
RED LIGHT INDICATES  
TO THE TEACHER THAT  
THE OUTSIDE LEVER IS  
LOCKED AND SECURE.



For more information, call us at 800-441-9692  
or visit us at [www.pdqlocks.com](http://www.pdqlocks.com)





Final conversion configuration, making it simple to service



with DPST (N/O and N/C) pneumatic time delayed switches, made by DeltrexUSA. As required, we wired the N/C set in series with the maglock power wires and the N/O contacts to the processor REX input. This assured positive fail-safe door unlocking as well as enhancing the relock feature.

### Power and Fire Alarm Interface

When dealing with a 'home run' cabling installation, it is important to use centralized, battery backed-up lock power supplies mounted next to the controllers. This is an imperative solution that offers an efficient alternative to those supplies installed at random locations in the ceiling and by the door.

Imagine the labor time required to find and service these locations, not to mention the time needed to figure out which goes to each door location. Ceiling mounted power supplies are costly, hard to maintain and typically do not include battery backup power. In this case, many doors, some of which were perimeter type, were outfitted (incorrectly) with a maglock, ceiling located power supply and no back-up batteries. A simple power failure caused card access doors to unlock, compromising the building's security.

Additionally, and from what I have seen so far, most installed "over the door" power supplies lack the required fire alarm release interface from the building fire alarm panel.

### End Results: The Final Configuration

The described case has detailed only some of the various items we had to consider to upgrade the access control system at our customer's facility. Our goals were to make it a functional and compliant system, while reducing high maintenance costs for our customer and ourselves.

Our onsite service, coupled with remote support via the network, allowed for us to react within minutes to most issues. This results in a highly functional system delivering the value the customer had envisioned, and ultimately making for a happy and well satisfied customer. For us, a happy customer is a guaranteed repeat customer, who also willingly recommends us to other opportunities. ■



**ISAC TABIB** is acting Vice President of Technology at DeltrexUSA. Isac has extensive experience in the design and construction of Integrated Security Systems and was a partner at Antar-Com Inc. Isac can be reached at [atisac@ifly51.com](mailto:atisac@ifly51.com).