

**MIGRATING
COMFORTABLY
FROM
DEADBOLT
LOCKS
TO
MORE SECURE
ELECTRONIC
ACCESS
CONTROL**

By Scott Lindley



A combination proximity card/keyboard reader provides high security to the entrance of this Hawaii gated community.

There is no doubt about it—

mechanical locks will continue to be part of a security solution for many years. Nonetheless, more and more customers are wanting—and needing—electronic access control (EAC). Door providers will need to get into EAC in the future to be competitive and successful versus the myriad of EAC providers in the market. Some might say that door professionals are being dragged, kicking and screaming, into the EAC market. If you are leery of EAC, don't be. It's just different, that's all.

Groups who have taken the leap have found the secret to being successful with EAC are those who have operated in their comfort zones. They started out by creating elementary EAC systems and, as they have done more and more EAC projects, the systems have become more sophisticated. In other words, if your first opportunity is to do a 128-door, three building campus needing a wireless system, find an access control integrator, "sell" them the deal, and watch and learn. But, if your first EAC is going to be four standalone doors, why not just go for it on your own?

What Type of Customer Needs EAC?

Why would a customer need controlled access on a specific opening in the first place? There are a score of reasons, from protecting HIPPA files at a doctor's office, to securing valuable inventory on a factory floor, to providing an extra level of assurance to public housing tenants. Perhaps there is a safety issue, such as providing ingress/egress to and from the electrical room. Are there theft issues in the warehouse or vandalism problems at the front door to the store? Oftentimes, there are local codes that

must be met, such as those from the National Fire Protection Association.

Remember, access control is simply controlling who can go where and when. But, that alone raises questions. How many people will be using the system? Do they all come at once? What kind of doors are there? Regular? Powered? Sliding? Glass? Will there be varying times when your customer wants different people entering? Do some areas call for increased levels of security, compared to others? Would it make sense to provide audits of who has been where and when?

Let's remember the basics for answers to questions like these. To control people, the user first needs to be identified. Even with a key, you are saying the bearer is authorized to enter the door with the matching lock.

Instead of keys and their management costs, you might consider numerical codes that work with electronic keypad locks. Codes, commonly referred to as PINs—personal ID number—are easily added and deleted from these locks, eliminating the high costs associated with re-keying. Selling and installing these systems is really not that different than selling and installing their purely mechanical cousins. However, for greater security, you may wish to propose that access be limited to something the user holds that is difficult to duplicate, such as proximity cards and fobs. A quick presentation to the reader and the cardholder successfully gains access.

Now that you have determined how to identify "who," you need to control "who." You might provide momentary access to individuals or keep doors unlocked at some times and locked at other times for all. Perhaps you want a pass-through mode for the bosses,

There are even card readers that will withstand bullets.

allowing them to come and go as pleased. For temporary personnel, you may want to set up a one-time use.

Simply stated, different people need access at different times to different locations. Perhaps regular employees can be admitted between 7 a.m. and 6 p.m. but nighttime maintenance workers gain access only between 8 p.m. and 6 a.m. However, managers can come and go as they please through all doors except on Sundays and holidays. Don't lose site of the need for exit devices or panic bars. Egress control is equally important as access control. Whatever you select, be sure your system provides an override period and is code compliant.

Regarding Software

It is most likely that your access control system will be governed by management software. The features and benefits of the particular software are equally as important as the hardware.

The first thing to check is if the software is secure. You want to assure that unauthorized operators cannot get their fingers on the keyboard to alter it. At the very least, it must be password protected. It must also be flexible enough to manage the various user groups within your customer's organization. As such, it must be user-friendly and easy to learn because several people must use it. And, in today's world, what type of operating system does the software require,



(continued on page 18)

ACCESS CONTROL

SOPHISTICATED SECURITY SOLUTIONS



Access control systems can be deployed in almost any type of facility and

with a varying range of system and product benefits. Depending on what is expected and needed from the system, **traditional access control locking solutions can be a significant investment.**

The **HS4 platform** is a robust and dynamic solution that can provide tailored benefits to nearly every type of installation at a fraction of the upfront and ongoing costs.

For more information, please visit hageraccesscontrol.com.

 **HAGER**
COMPANIES
powered by **SALTO**

www.hagerco.com





Reading up to 200 feet, long-range readers are popular for authorized cars to get into facilities without having to stop.

such as Windows or iOS? Perhaps the solution is cloud based.

Lastly, your software must provide a management hierarchy, allowing others besides the main security administrator to manage certain elements, such as Human Resources adding or eliminating an employee's access.

Offline, Online, Hardwired and Wireless

There's the question of an online system versus offline or standalone systems. Do you have the budget or does the facility's construction allow for online, hardwired systems? Original construction is when such investments are at their lowest. If not, software managed offline locking systems provide most of the benefits of an online system at a fraction of the material and install cost.

You might want a mixed system, one where perimeters are managed by online systems and internal openings are managed by offline systems. If the door has high frequency use, you will need to review high quality magnetic locking systems that can handle constant locking and unlocking.

Getting Down to the Specifics

Here are other considerations:

- ▶ Are other access control systems already installed? Will these systems work with the proximity cards you are planning for this project?
- ▶ It is rare that a system without UL listing of the components would be allowed.
- ▶ Are the components backed by a lifetime warranty?
- ▶ What's the supplier's track record on delivery and customer service?
- ▶ Electronic hardware must meet ANSI/BHMA Grade 1 requirements.
- ▶ Will any of the hardware be installed out-of-doors or in vandal prone environments? Can the hardware selected handle the install environment?
- ▶ Products must adhere to FCC regulations where applicable.
- ▶ Knowing the number of users is imperative. Flow is critical. (You will find that out if the boss waits too long to enter the building.

- ▶ In many cases, you will want to audit or monitor events that occur at the controlled openings. Can your system provide information on who was there and when?
- ▶ Are additional add-on components easily obtainable? Leading providers often measure their lead times in hours.
- ▶ If standalone battery-powered products are to be used, what are the number of cycles you expect at each opening? Will frequent battery changing be required?
- ▶ If you select a networked access control system, can users still get out in an emergency when there is no power?

Going through all these questions will alert you whether or not you are comfortable in taking on this specific project. Can you make a profit on it or are you going to get all tied up in a technology that you don't quite yet understand? Successful organizations learning EAC have started out with simple systems and then tried to incrementally increase technological sophistication with successive jobs. Within a relatively short amount of time, they are ready to take on the systems that include networking, smart cards and the other many facets of EAC. ■



SCOTT LINDLEY is a 25+ year veteran of the contactless card access control provider industry. He has been president of Farpointe Data since 2003.