Another Friend, Another Door, Another Foe

Compiled by Bill Zalud, Editor

Andy Rooney of 60 Minutes fame knows his security. "The closing of a door can bring blessed privacy and comfort -- the opening, terror," he once grumbled.

Except for garage door openers and lights, the most employed security devices

Tailgating is a problem. Technology has an answer.

control doors and entrances. There is single door equipment. Stand-alone electronic door controls. Some are wired or wirelessly networked. And for inside and outdoor entrances, there's a variety of gear.

Single-door, stand-alone access control devices are actually far less complicated than the elaborate industry parlance describing them. Non-computerized and key or membrane pad-based, they provide protection when a lock and key is not enough but more heavy-duty security measures are not mandated.

STAND-ALONES

On another level, door systems are computerized, but still battery-powered and not networked. Nevertheless, they are "intelligent" systems. Programmable via a PC

Door control equipment can handle a diversity of installations including glass doors.

or PDA or through the door device itself, these stand-alones can be scheduled to lock, unlock and relock at times of day. They also can be cued to accept or reject electronic credentials, such as magnetic stripe cards and proximity cards, for example.

The mechanical stand-alone offers a convenient way to control access between public and private areas. There are no keys or cards to manage, no computers to program, no batteries to replace and combinations can be changed in seconds without removing the lock. The major disadvantage is the fact that there's no audit trail allowing a review of who's come in and out of a protected space. For that you need a software program.

Typically an online system would allow for more users than a stand-alone. While online systems are programmed with an internal database population, they also allow you to expand that database from without.

For network-based access control systems, there are some basics.

Number of users -- The number of users determines which control panel will be capable of supporting the requirements. It is important to consider all of the users – not just those who work in the building every day, but also those employees who may need regular access. Every access control system should be designed for future use. It is standard to plan for a minimum of 20 percent expansion for the future.

Entry portals (doors) – A thorough inspection of the existing doors is essential to access control design. Identifying the number of doors that will require electronic lock hardware is important in determining the control panel and power supply requirements. The type and quality of the doors will determine the type of lock hardware needed.

INGRESS AND EGRESS

Type of ingress – The building owner must determine how personnel will gain

In a Bind

Security departments know the call: "I presented my card but the door won't unlock." Well, often the user has pulled on the door, binding the electric strike and preventing it from releasing.

Pre-load is defined as the force that is applied to an electromechanical locking device that may bind or restrict its ability to release or unlock. Electric motors or solenoids are the most common technologies used to retract a latch bolt in a lockset or to release a keeper in an electric strike. It is difficult for these devices to overcome even small amounts of pressure that may inhibit the movement of the latchbolt or keeper. Pre-load could be caused by door and frame misalignment, heavy sound seal or weather-stripping, or it can be caused by someone pulling on the door before the electric strike is energized.

However, there are electric strikes and other electromechanical locking devices available to compensate for pre-load conditions. This is achieved by incorporating the use of cams and/or clutching mechanisms within the locking device to create enough leverage to overcome the load. These features may add cost to the initial installation, but could later reduce maintenance cost and service calls.

Electric latch retraction means the door control is fail secure.

A smaller package for the door access control device can fit more types of doors.

access to the building. There are several types of entry readers available today, including proximity, magnetic stripe, biometric, and keypads.

Stand-alone or networked access control – this decision will determine the capabilities of the system. Smaller applications or remote facilities may use stand-alone systems. If the building has more than 100 users or multiple doors, a networked access control system may be the best solution.

According to Mitchell Kane of Schlage Electronic Security, "The one to 32 door market makes up a majority of the total market. Most do not have on-site IT or security personnel. The firm's Web-based offering, bright blue, is embedded on the board. "Just hook up to the control panel. You don't need a dedicated PC."

Said R. Steven Booth, operations manager and /route supervisor at Waste Management, "Our staff and scale office is off the foyer at the front of our building. We wanted to restrict customers entering through the front from coming into that office. Even though we had 'Employees Only' signage up, customers would just wander through. Although we needed to secure that office, we wanted more than just a lock. We started looking for an access control system that could show accountability, provided expansion capabilities and was still economical."

The occupancy and size of the building. NFPA 101, the Life Safety Code, specifies requirements for means of egress based on the occupancy classification of the building. Some buildings are permitted to have electronic access control, while other building-occupancy classifications have certain limitations. The size of the building will determine the amount of wire needed.

WHAT ABOUT BADGING?

Badging permits security to individually identify those with permission to access areas with a special badge. Maintaining the database of users is an important part of the system.

Electric strikes – Both fail-safe and fail-secure strikes are available. The most commonly used is the fail-secure strike, because in most cases it is desirable to maintain the doors in a locked position upon loss of power. Some applications may require the use of fail-safe strikes by code or legal reasons. Fire-rated doors require special fire-rated strikes.

Magnetic locks are generally available in small, medium and large categories, based on pounds of resistance. The holding force used should be appropriate for the type and quality of the door. NFPA 101, the Life Safety Code, must be followed for egress requirements. There's also a need for smaller but strong door exit delay system. For instance, Securitron has one that is only 12 and one half inches long that boasts 1,200 pound holding.

Means of egress -- Getting into the facility is important, but getting out in an emergency can be a matter of life and death. The egress portion of most access control systems must be intuitive so that no special training is required to exit. NFPA 101 requires two means of egress. A request to exit motion detector and an exit push button or touch sense bar are commonly used to meet this requirement. Most access control systems are designed to allow free egress, meaning no code or credential is required to exit. Some systems may have controlled access on certain doors, or delayed egress.

Almost all exit device manufacturers offer the option of electric latch retraction on their touchbar-style exit devices, according to Tom Rubenoff, in the hardware business for almost three decades and a HubPages writer. "Different manufactures may call it by other names such as 'latch pull-back' or 'remote dogging.' Some people refer a device with electric latch retraction as an 'electrified exit device,' but that could also refer to electric unlocking of outside trim, a different animal altogether. Electric latch retraction is accomplished by using a powerful solenoid or electric motor to actually retract the latch or latches of an exit device."

LATCH RETRACTION

One example comes from Security Door Controls. The new SDC electric latch retraction exit device has a low current draw

Eight Things to Avoid

When talking about door installations, whether wireless or traditional hard-wired, Dave Barnard of RS2 has his list of things to avoid.

1. Avoid powering the door strike from the same power supply as the access control panel. It is more likely to burn out the power supply (or cause the panel to reset) if you do so.
2. Avoid putting magnetic locks, sheer locks, power bolts or any other "positive locking" device on a door without making sure that all Life Safety Codes are met.
3. Avoid using "Fail Safe" door hardware on building perimeter doors unless compelled to by Life Safety Codes. If you must do so, be sure to provide adequate battery or generator back-up for a worst case power outage.
4. Avoid using open face electric strikes on perimeter doors directly exposed to inclement weather.
5. Avoid mixing "power limited" and "non-power limited" wiring or systems.
6. Avoid "current loops" by grounding the shields from your shielded cable in only one location.
7. Avoid creating an "antenna" with your shielded cable by keeping the shield continuous throughout the entire RS485 (or other) circuit and "grounding" it in only one location.
8. Avoid powering electrified door hardware that has not been tested and certified to be Power over Ethernet (PoE) Compliant with PoE access control devices.

and its operation includes momentary or maintained fail secure electric latch retraction with rim mount, vertical rod and mortise panic or fire exit devices.

There's a major push with wireless and PoE (power-over-Ethernet) locks. According to RS2's Gary Staley, "These wireless locks provide centrally managed access control to locations that were previously difficult or cost-prohibitive to incorporate using hard-wired technology. A typical hard-wired access controlled opening takes an average of eight hours to install and bring to operational status. Wireless locks take about an hour to install by a single technician."

For more sophisticated card access control systems protecting doors, there also is a concern over tailgating.

Advances have been made in door hardware, access control systems, and reader technologies to authenticate who can enter an area. The bad news is its only step one and it is not enough to keep unwanted people out. A second and crucial step is detecting unauthorized people who enter once the door is opened. This is called tailgate detection.

There are many obstacles to overcome to catch tailgaters or piggybacking. In some cases, a person sneaks into a facility or sensitive area by walking in unobserved behind a person or through a secure door that someone has just exited. The everyday, often innocuous form is when someone kindly holds the door for a tailgater, not feeling they're a part of the security process or bold enough to ask to see a badge. The third type of tailgating occurs when the authorized person is in collusion with the unwanted visitor.

TAILGATING

This last problem was the case at Anytime Fitness.

Anytime Fitness is a fast-growing health club chain with over 800 locations open 24 hours a day and often not staffed. The business model required an access control system to allow members into the clubs at all hours. Frequently, relatives or friends of members would sneak in with a member which presents numerous problems. "The safety and security of our members and staff is our number one priority," said Mark Daly of Anytime. The company chose to install Smarter Security Systems' Fastlane Door Detective to help it with this tailgating problem. The technology is deployed at hundreds of club locations and now alarms violations and marks surveillance video to help club owners easily track unauthorized entries. "Often the tailgaters know a person they're following in and the club can give the person a call and many times turn them into new members," said Daly.

Exterior doors, such as those at Anytime Fitness, are certainly candidates for anti-tailgate systems. Doors inside a facility also make sense to protect. In many cases, security officers are at doors through which visitors regularly enter. While officers can watch for tailgaters, they are expensive and impractical for many doorway locations with either, too many doors, too few entrants, or too many entrants to identify without queuing issues. Sensitive areas with a critical need for tailgate protection include data centers, cash rooms, parts storage areas, command and control centers, R&D labs, and executive suites. Some companies have enhanced security at these doors by installing smart card or even biometric readers to increase the certainty that they know for whom they are unlocking the door.

THE MISSING LINK

But these technologies, while strong in their own right, are blind to who else comes in once the door is unlocked. The truth is that this vital "missing link" is not addressed unless you install tailgate detection systems on those critical doors.

So we've established that once a door is open the access control system is blind to any passage in either direction.

When exploring ways to prevent tailgating, obviously the accuracy of the tailgate detection itself is paramount. Less obvious and often overlooked are the operational aspects that allow the system to work smoothly beyond the tailgate aspect alone. Unless the technology is extremely intelligent, you'll likely be plagued with false alarms that "cry wolf" all day and therefore get ignored and defeat the purpose. It pays to invest in systems with intelligent algorithms that can discriminate between people and common inanimate objects like briefcases on wheels. These smarter systems also give you better speed, allowing streams of authorized people to present credentials and proceed quickly without even closing the door.

You want to be sure to choose a technology that recognizes the direction people are passing through the door to stop someone from entering the secure area while the door is still ajar from somebody who just left it. You may want to install video cameras to record the people involved in violations, both the authorized person who let them in and the tailgater, so you can remind them of security procedures. A final consideration is what measures to take to physically stop the intruder once the unauthorized entry is alarmed. Perhaps guards respond, adjacent doors are automatically locked, or some temporary barrier blocks the way, as with an optical turnstile.

"The tailgating problem is probably the biggest weakness in your [building entry] security system," stated Michael Silva, CPP, of Silva Consultants. "It is far more likely that someone who wants access to your facility will simply tailgate into the building rather than use one of the more exotic methods companies often work to prevent."

If tailgating is a risk you had not considered, know that you have an ever-present hole in your entrance security system, and in these troubling economic times, that risk is even greater. If you want to completely control access to secure areas, you must ensure authorized entry not just when the door is closed, but when it's open too, and stop the tailgater.

LOOKING AT INTEGRATION

Integration is also a door control advance.

For instance, MATE-Intelligent Video has integrated with Hirsch's Velocity security management system. Its Behavior Watch turns nearly any camera -- IP or analog -- into an intelligent sensor able to detect intrusion, suspicious objects (e.g., backpack), removed objects (e.g., a painting), and undesirable behavior (e.g., loitering). The server-based approach sends real-time alarms and alerts to Velocity, which performs the appropriate actions. SECURITY

What about the Entrance?

There are times when the look of security is as important as the need for security. It this case,

Entrances can use turnstiles that can work with other access control systems. Photo from Automatic Systems

look for new-age turnstiles. Here aesthetics and detection come together. Today, some models include retractable glass in which security can also include intelligence.