Published in DHI Doors Security + Safety, March 2019

Understanding Applications for Today's Access Control Solutions

by Ginny Powell

Electronic access control systems offer an effective way to control and manage access for facilities large and small. From retail and office space to education, government, healthcare and multifamily complexes, today's systems are versatile enough to not only meet current needs, but also have the ability to expand in the future – giving you and your clients the peace of mind of knowing they are making a sound investment.

Electronic access control technology delivers value beyond security and safety by also providing valuable business intelligence – allowing you to monitor who is entering and leaving your facilities, time and duration of visits, traffic flow and more.

TYPES OF ACCESS CONTROL TECHNOLOGY

Recognizing that a one-size-fits-all answer doesn't work with today's designs, access control technology is a diverse solution to secure any new or existing facility. Here's an overview of three types of electronic access control solutions.

Stand-Alone Access Control

With stand-alone access control technology, all the decisions are made at the lock, by the lock. A stand-alone lock needs to be told what access to be given, so if a company wants to add – or delete – a user, they must physically go to the lock to reprogram it using a handheld device.

Stand-alone access control works best where there aren't many users and just a few locks, such as a doctor's office, a pharmacy or in retail – anywhere you want to give access to only a few individuals. The stand-alone locking system works best with a maximum of 50 users.

This access option takes the place of a traditional keyed lock. With this option, however, "If someone misplaces their access card, the lock is easily reprogrammed and the person gets a new card," explains Gordon Holmes, Product Manager at Hager Companies.

Wireless Real-Time Networks (WRNs)

Real-time networks provide system administrators with real-time functionality, such as immediate updates of blocked or deleted users, door position status and lockdown capabilities. As soon as a person presents a credential to a lock, that information is being recorded at the server, and conversely the server can control the lock remotely and deliver other updates as well.

These systems can be hardwired, but many facilities are opting for wireless platforms because they provide the same control found in traditionally wired systems but without the higher product and installation investment. Depending on the technology and system infrastructure, these locks can be in communication with the server every four to eight seconds.

Virtual Network

A popular combination of a stand-alone system and real-time networks is a "virtual network," and it takes a completely different approach to access control. Traditionally, access control systems have required that each networked lock have a direct method of communication for it to be in constant communication with other doors and the server.

With virtual networks, the openings work in the same manner as real-time networks, but the locks are stand-alone battery powered giving facilities the flexibility to pick-and-choose which openings have electronic access control. This system also provides the flexibility for an end user to build out their security over time.

"These readers are in communication with the system's server and work just like most other readers," notes James Stokes, Director of Access Control Business Development for Hager. "The only difference is that the lock doesn't communicate with the server in real time. Instead, data is transferred from offline locks to online locks and readers through the user's credential."

The virtual network has another feature that makes it attractive – two-way communication. The lock and the credential communicate and exchange specific data, such as user access rights, battery status and an updated blacklist of deleted and added users as well as lost cards. At access points – usually high-traffic openings – user credentials are re-evaluated every day and given an updated blacklist to spread throughout the facility. This process also allows for audit trail data to be extracted -- the users and the credentials ***are*** the network.

CARD UPDATING AT THE DOOR

There is also technology available to enhance the virtual network: a stand-alone, battery-operated lock that becomes an updating point. Not only is this an additional level of security, it also makes it much easier for systems administrators to organize the infrastructure of their building – without wires. This dramatically reduces the cost of adding or modifying traditional update points since any door with a battery operating locking mechanism can now be a point for updating user credentials.

The updating technology can be fitted to practically any opening or lock type," notes Stokes, "so there are few restrictions to identifying which door you want as an update point."

SELECTING ELECTRONIC ACCESS CONTROLS

Determining the right access control solution for your project comes down to how the building needs to operate based on desired security levels and user habits. A school has different requirements and will need to operate differently than a hospital, commercial office space, assisted-living facility or multi-family housing project. And in every case, specific building and fire codes must be met.

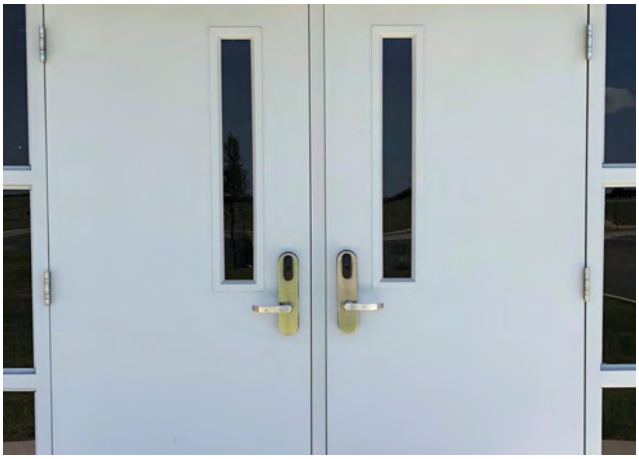
Holmes further explains, "For example, a church will probably select a stand-alone access control because you have only a few entry points and many people going in an out throughout the week. On the other hand, multifamily projects will most likely need a virtual network. Having said that, today's projects are pretty complex, so we are seeing more and more of them incorporating a mix of stand-alone, real-time and virtual networks. It really depends on how the building and openings are expected to be used."

Additionally, many different types of locks work with each system, including mortise locks, cylindrical locks, deadbolts, interconnected locks, padlocks, cam locks, locker locks and glass door locks. This allows for enhanced security no matter the design.

Consider these applications where selecting the right access control system contributes to the success of the project.

- **School Districts**. Each school district has lockdown capability requirements, but how lockdown is accomplished varies. When an incident occurs, some school districts want all doors to become secured, while others want the ability to define which wings or areas to lock down.

  For example, in Spring 2018, the Abilene Wylie Independent School District (near Abilene, Texas) underwent the construction of a new performing arts center, and it was during the construction process that the school district elected to have electronic access control installed. Like most school districts across the country, they were concerned with safety and wanted to increase security in the new building. A challenge with this project was determining what openings were best suited for electronic access control. They chose to first add virtual network control on nearly every interior door that locked and then later decided to add card readers to the exterior doors.



- **Newly Constructed Facilities**. During the design of a new building, traffic flow will be outlined, but after construction of the project is complete, it can be discovered that one or more openings may operate differently than intended. This is particularly true for commercial office buildings where the front door and parking garage were the intended access points, but after completion, it's discovered that a third door closer to the metro is being used.

  While accessing the building through this third door isn't the issue, per se, the problem is that any employees using that third access point weren't getting their credentials updated. With the ability to update credentials at a battery-operated wireless locking point, the system administrator can see the traffic flow differential between what was planned and what is occurring and can easily make a change in the software. Once done, the third opening acts as a credential update point as well.

- **ADA Projects.** Many building codes include provisions for ADA Low Energy Operators. These operators require a knowing act for the operator to open the door, such as pushing a plate so that the door automatically swings open. When a virtual network is installed, instead of pushing the button, the user can present their credential to the reader to initiate the operator. This meets the knowing act requirement, but it also registers the event and passes a new key to the user's credential, downloads the blacklist (to be passed to offline locks) and captures previous events registered on the user's credentials.

- **Renovations.** In retrofit applications, running power and cables to existing openings can be cost-prohibitive. Therefore, it usually makes sense to go with a battery-powered access control device. In these cases, the battery operator lock would enable its reader to become an update point.

- **Mixed-Use.** The growth of mixed-use buildings provides a greater challenge – not simply with security but also with being code compliant. The right access control solution is found when all parties (owner, architect, hardware supplier and installer) work together to identify what type of access control device makes sense for each of the openings, which is best accomplished before the spec is written. They "walk around the project on paper" to ensure the right hardware is selected to meet the owner's needs and comply with code.

Electronic access control devices and systems have advanced greatly these last five years allowing architects and general contractors to provide a variety of levels of security to fit the project. Whether it's an office complex, multifamily high-rise, school district or multi-use building, there is an access control application that will fit your client's specific needs.