The Right Fit - Choosing the Appropriate Access Control Solution for a Retrofit Application

By Gordon Holmes

With so many options on the market it is important for distributors, maintenance managers and facility managers to understand the building's characteristics and needs.

Over the past decade, there has been a considerable need for added security in schools, hospitals and commercial buildings. This heightened demand for security has led to continued growth and advancement of progressive access control systems. Due to these advancements, there is now more opportunity to retrofit existing buildings with up-to-date, advanced access control solutions. Choosing the appropriate access control solution in any building situation, especially when discussing a retrofit, can be a complex task. In addition to addressing factors such as cost, time and functionality requirements, limitations inherent to a building's design can make upgrading or installing a brand-new access control system in older buildings particularly challenging.

With so many options on the market it is important for distributors, maintenance managers and facility managers to understand the building's characteristics and needs. What are the traffic patterns in and out of the building and specific areas? What are the desired goals for the system? What are the budget constraints to create a solution that will suit the facility's needs? What kind of level of security is required?

Identifying and understanding the answers to these questions will help someone make an educated, strategic decision on what kind of access control solution works best for them. By avoiding a 'one-size-fits-all' approach to access control, decision-makers can avoid unnecessary time and costs.

Standalone Systems

Standalone systems, where certain access points are equipped with card readers but are not connected to a larger network, can provide a cost-effective access control solution. These offline solutions are especially applicable in retrofit applications where there is not enough room to install panels or monitoring equipment or in situations where it would be impossible to wire the entire building. The electronic locks also add a level of security that mechanical locks cannot provide.

There are certain situations where a building manager may need to keep a certain person out. If the access point was controlled by a mechanical lock, and that individual had a key, the locks would need to be promptly changed. However, with a standalone system, the electronic lock can be quickly programmed to not recognize that individual's card or keypad code. In additional, system administrators can download audit trails to view when certain users opened specific doors. This allows operators to monitor the activity to building entrances. Standalone readers, while fitting for facilities that contain only a few doors that need access control, are not practical in large buildings that contain numerous security points.

Standalone systems require an administrator to walk to each reader to retrieve the information and make changes to the access rights. This is not only time consuming, but it also means that standalone readers cannot be monitored in real time. The inability for real-time monitoring can be especially problematic in schools and other facilities where an immediate lockdown capability may be needed.

Networked Solutions

Implementing a networked, or online solution eliminates the need for administrators to walk to each lock to update the system or download the audit trail. Wired solutions have been around for more than 30 years. During that time, the development of wireless technology has improved to the point where wireless systems can be as effective as wired systems can but at a fraction of the cost. Both solutions can provide real-time monitoring and management, and have more efficient lockdown capabilities.

Wired solutions are more practical for new buildings as they require extensive wiring. When retrofitting a building, using wired access control can be very costly and labor intensive. In order to extend wiring to the lock, the door must be drilled with a raceway. This process is tedious, requires special skills and leaves little room for error. Special electronic hinges with thru-wires are needed to run the wire from the frame to the door and ultimately, to the lock. Another factor to take into consideration for a retrofit is the productivity of those already occupying the building. The excessive noise and dust that are by-products of modifying doors can be very disruptive in environments where people are working.

To prevent the additional cost, time and construction of having to run wire through older buildings, facility managers and other decision-makers should consider a wireless access control solution. Not only is installation significantly faster, the costs with implementing a wireless solution is far less than those associated with traditional wired solutions. This is due to the complexity of the installation, hardware and ongoing licensing. There are, however, other factors to consider when deciding on a wireless system.

One aspect that is important to consider is the type of wireless connection the device uses - Wi-Fi or a wireless mesh network. When implementing a Wi-Fi system, multiple antennas will typically be needed to support the size of the building and solution, adding to the installation costs. Wi-Fi, while extremely common, is generally less secure than using a wireless mesh network such as Zigbee. Zigbee 802.15.4 was developed for devices with long battery life in wireless applications. This technology is more secure than Wi-Fi networks, allows for fast system reconfigurations and is less expensive.

Another element to consider when comparing wireless solutions is how often the system updates. In most cases, systems will only force updates once or twice a day. This can be less than ideal for several reasons. A system might not have the appropriate rights for hours after the administrator updates the system on the computer, leaving the building open to unintended security risks. The more advanced wireless solutions on the market are designed to force an update every ten minutes. This newer technology creates a much more secure environment.

Advanced Network Solutions

Some platforms available provide much needed flexibility by allowing smart credentials to be data transmitters between access points. These data-on-card systems can both read and write update information at the lock/reader of both offline devices and head-end systems and relay it back to the server. This is known as a virtual network. This two-way communication between the card and door allows the smart credentials to act as carriers and enables the readers to each door to be updated with crucial information. Implementing this type of "virtual" network eliminates the need for having a wired or wireless lock at every opening one wishes to secure. This greatly reduces the costs of the access control system. The characteristics of how a virtual network works with the advanced smart card technology both saves time and money, and tightens security by providing actionable data in a more efficient way.

Retrofitting a virtual network into a building is a relatively inexpensive initiative. In fact, implementing a virtual network access control system can ultimately cost two to three times less than a standard wireless system. It is important for decision-makers to contact experts in the industry to understand what solution or combination of solutions is best for their situation.

There are many factors to consider when deciding to retrofit a building with an updated access control solution. It is crucial to understand the needs of the facility, as well as the pros and cons of each type of solution. A well-designed and executed access control systems can help reduce maintenance and operational costs, while still providing the highest level of security the administrator desires. There may be specific situations where it makes sense to install a combination of wireless and virtual networks to best service the security needs of a building. Applying new technologies gives distributors, installers and end users a unique chance to help facilities build a customized access control system that fits all of their specific needs.

Gordon Holmes is a product manager covering the commercial hinges, electrified product lines as well as Hager powered by Salto access control line. He can be reached at gholmes@hagerco.com.