THE TECHNICAL RESOURCE FOR THE PHYSICAL & ELECTRONIC SECURITY SPECIALIST
LOCKSMITH LEDGER
International

Make the Most of Electronic Access Control

by Allan B Colombo On March 5, 2018

Mechanical locks have served society well over the course of several thousand years from before the days of Julius Caesar to the locksmiths of today. Examples of where locks continue to provide value include single-family homes and small businesses where there are only a few employees.

There are, of course, limitations associated with mechanical locks that most of us in the business of security are aware of. Probably the most notable is that of adding and deleting users where it comes to issuing unique keys. The fact is, and all of us know this, it's relatively expensive to add and remove users to a building full of mechanical locks compared to electronic access control (EAC). Here's why:

"The large government facilities that our firm works in requires EAC simply because of all the people who work there," says John Larkin, senior partner with Electronic Systems Consultants (ESC) of Greater Ohio. "EAC systems are programmable from top to bottom, which means we can automate the process of screening people at multiple doors. Compare this to a mechanical lock that inherently possesses absolutely no way to regulate the time or days when people can enter, where they can enter, or any other security-related parameter."

Probably the most compelling reason why you need to jump into the EAC market with both feet is the fact that more and more mechanical locks are either being replaced by electromagnetic locks (EML) or augmented with the addition of electric door strikes (EDS). No matter which one it is, there's almost sure to be an EAC system in control.

"There are many advantages to upgrading to an integrated [EAC] system. Some benefits that are quickly realized by a system user includes the ability to easily assign and remove access to certain doors to different individuals as well as setting schedules as to when they can access the area," says David Gonzalez, Security Solution Specialist & Product Specifier with Simplex Grinnell Inc.

According to Gonzalez, another benefit associated with EAC is the ability to run reports of various kinds. The most common is a log of who has accessed each area of a facility and when they did it. These reports can be automated and sent to the owner or manager(s) of the facility on a weekly or monthly basis, many times for compliance reasons.

Last but not least, there is a good deal of money involved in installing and servicing EAC systems. The recurring revenue that you can earn each and every month is another big incentive.

EAC Applications

There are tremendous benefits associated with EAC systems that those who work in business, government, manufacturing, retail, and other settings are sure to appreciate and it's this fact that makes EAC a slam dunk business wise. Probably one of the most notable is that of education, such as K12 school systems, colleges, universities, and sizable trade schools.

"In a university setting you may desire the access control system to be integrated with the student management system so that students are automatically granted access when they enroll in the school, and their access is removed when they [drop out or] graduate," says Gonzalez.

Integration Vs. Unification

According to Gonzalez, there are also methods whereby individual security applications can be combined with EAC such as facial recognition systems for access control, wireless locks for classrooms, and mass notification/communication systems that can be programmed to use local public address systems as well as audio/video (A/V)-based fire alarm systems as well as emails and text notifications in an emergency situation.

"When we speak of 'integration' and 'unification,' we're actually talking about computer network technology using what is commonly called IP (Internet Protocol)," says Gonzalez. "It refers to the data protocol that we use to send data back and forth over the Internet. Apparently this method of data transmission works so well that many if not most security-related manufacturers now use it as a preferred means of data transference in their systems."

The definition of ‘Internet Protocol’, according to The Free Dictionary, is “The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

Until recently, security integration has meant combining or joining dissimilar security disciplines, such as EAC with video surveillance cameras; intrusion detection; and environmental control systems, such as heating and cooling. Until recently this means purchasing individual systems and combining them with special hardware and software so they can “talk” between themselves. Now, manufacturers are working to combine two or more of these security subsystems together via the same control system, or platform.

“Integrations are easier than ever, by using existing IP cameras, and alarm systems access control panels can make actionable data, from recording failed reader attempts and notifying security, to opening exits in the event of a fire. Easily create rule based scenarios that take place without user input and lead to a harmonious sequence of events that is logged and can be used to improve site performance,”

“In the last couple of years I have witnessed a transition of Access Control companies (AC) developing their own Video Management Software (VMS) to include it as a total solution and with one particular (VMS) company called Genetec. They are the first to offer both solutions and they have called it Security Center,” says Simplex’s Gonzalez. “I have also seen pure IP-based (AC) revolutionary company like ISONAS continuing to offer great values in just the Internet Protocol (IP) vertical since they have longevity with many deployments.”

Although most locksmiths are not ready to tackle security integration, IT (Information Technology) organizations will do so for a fee. They’ll gladly contract with your firm to perform all the necessary headend work in a computer network environment. More than 90 percent of the professional security companies that work in the IP area still hire outside professionals in the IT world to work alongside their own technicians.