

Why should you move from mechanical to electronic access control?

The benefits of electronic security

By April Dalton-Noblitt, Allegion
October, 2012

You may already recognize that mechanical locks and keys alone are not enough to keep a perimeter secure. But not every door has to be a controlled entrance, nor is it always necessary to have 100 percent, 24-hour monitored control. The good news is that a reliable and secure electronic access control (EAC) system does not have to be complicated to be effective.

Moving from a mechanical security system to an electronic one offers a host of benefits, including a higher level of security, less risk of illegally duplicated credentials, a simpler and less expensive method of replacing lost or damaged credentials, and the ease of programming locks instead of rekeying them. There are two basic types of electronic access control systems: offline and networked.

What is “offline” EAC?

Offline systems are those that are not connected by a network. You may also hear these referred to as “stand-alone” systems. These include mechanical key programs, but an offline system is most often thought of as including electronic locks that are programmed by either using the lock’s keypad or with a personal handheld device to download data from a software program. In an offline system the locks do not communicate with each other, but otherwise they work the same way as most other electronic locks, providing authentication of a PIN or card-style credential to permit access and providing audit trails.

What is “networked” EAC?

Networked access control systems are becoming more common in today’s business environment. These are systems in which the access devices are connected to a network either wirelessly or by being hardwired to the system. Networked systems can be as simple as a network of electronic locks or may be a very sophisticated, integrated system that incorporates access control, video cameras and digital video recording, alarm monitoring and badging.

Why should you move from mechanical to electronic access control?

Here are some guidelines to follow when considering the move from a mechanical to electronic access control system:

- Mechanical access control represents the fundamental mechanical locking system that restricts free access or egress through an opening. It includes keyed locks and other mechanical products that provide dependable, affordable security. With these basic devices, security is focused mainly on protection from threats, such as theft or vandalism and on providing a physical barrier to intruders. Mechanical locking solutions are appropriate applications for areas that do not require audit trails or monitoring.
- Offline or stand-alone EAC devices can be programmed individually to allow access to users based on any requirements you may have, such as days of the week, time of day, etc., and require a credential to allow access. Usually, these locks are battery-powered and are programmed using the lock's keypad or a handheld device that downloads to the lock the settings you have determined. You can choose from a variety of credential types, including PIN, magnetic stripe, proximity card and smart cards. Offline locks also provide an audit trail so that you will know who has accessed the lock and when. These solutions are a good starting point for moving to EAC because they are typically less expensive to install and operate than a networked solution.
- Online or networked EAC devices are connected to a central system that you can use to manage users and schedules, update credential rights and more. These systems may be Web-based or may run via software that is installed on your existing network. The locks and readers are then linked to the network either through a hardwired or wireless connection. You may choose devices with a variety of credential types, including PIN, magnetic stripe, proximity cards and smart cards. Changes to lock data are made quickly and easily from a single point because all the locks are connected to the network, and reports can be downloaded from the software for quick and easy information gathering. While not every business has the budget to implement a fully networked solution, it does offer the convenience of managing all your openings from a single point.

Just like there are different levels of security systems, the type of credential you choose also impacts the security of your system and the personal information of your employees.

- Biometrics offers the highest level of security because they do not require a physical credential for identification. Instead they identify people using unique biometric information like hand geometry or fingerprints to ensure that the person is who they say they are. For extra security, in addition to the biometric information, the user may be required to present a credential or PIN number to gain access.
- Systems using smart card credentials offer a sophisticated level of security. Smart cards actually exchange information with readers through a process known as mutual authentication. It's an added level of security and it ensures communication between the reader and the credential is unique and cannot be compromised.
- Proximity credentials are today's standard for most access control applications today. They are easy to use – both for the card holder and the system administrator.
- Magnetic stripe credentials are an ideal choice when it's required to have unique information stored on each credential and to have read/write capabilities.
- PIN codes are the simplest of credentials used in electronic security applications. Users only need to remember a 3-8 digit code to gain access. Because these codes are easily passed on to others, using a PIN code alone is not the most secure choice.

Why should you move from mechanical to electronic access control?

- Using keys as a credential has long been a standard in the industry. While keys do offer a good level of security, unauthorized duplication, lost and stolen keys and the lack of information about the use of the doors mechanical locks secure can cause extra work and reduced productivity.

Better security can start with a security and safety needs assessment by a qualified security consultant. A security professional can help you plan your migration from mechanical to electronic access control in a way that fits your building, your schedule and your budget.

Learn more about electronic security

For more information about planning your migration to electronic security, please contact a professional security consultant in your area by calling **888.758.9823** or fill out the **Contact Us** form on our website at allegion.com.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a \$2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit allegion.com/us

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN



© 2014 Allegion
009031, Rev. 03/14
allegion.com