Offline vs. networked access control: what schools need to know

By April Dalton-Noblitt, Allegion
October, 2012

K-12 schools and higher education institutions of all types and sizes are becoming more aware of the security risks posed by unauthorized access and are taking proactive steps to prevent a broad range of potentially threatening or dangerous incidents. They are finding that locks and keys alone are not enough to keep a school's perimeter secure against unwanted or uncontrolled visitors. Multiple buildings on a high school or college campus present a complex situation, with different types of buildings requiring different levels of security. Not every door in any school facility has to be a controlled entrance, nor is it always necessary to have 100 percent, 24-hour control.

Security solutions oftentimes are described as either offline or networked. Offline systems include mechanical key programs, as well as standalone electronic locks that are programmed at the lock. Offline systems do not communicate with one another, and usually are not connected to a remote security command network. Networked access control systems have become common on college and university campuses. Integrated access control systems incorporate online access control, video surveillance with digital recording, alarm monitoring and badging.

Here are some guidelines to follow when considering appropriate applications of offline versus electronic access control solutions:

Mechanical access/egress 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.

Standalone electronic access control – includes devices can be programmed with access data to restrict entry into specific areas to authorized individuals only. Usually, these locking devices are battery-powered and may be able to provide audit trail capability and time-based scheduling for restricting access. These programmable devices are easy to update and provide increased control over who can access certain openings.

Some offline electronic locks can also be programmed by using a simple user management application. User identification information and access rights can be set in the application, then downloaded to the lock through a hand-held device or communicated by authorized credentials when used at the lock. These types of devices control access, track usage and manage data without the need for a facility-wide network. Users are able to use a credential or PIN code to gain access and the lock should have a mechanical key override option.

Networked access control and biometrics – adds a more sophisticated layer of electronic access control. With a hardwired or wireless network, a number of devices can be managed from a single computer using access control software. Users can access areas of campus by using card credentials, entering a PIN or biometric identification. The devices are networked together to allow real-time monitoring and oversight of a large number of users and entrances.

Biometric solutions incorporate devices that can verify hand geometry, fingerprints or face characteristics to ensure that only persons who actually are authorized can gain access to a particular door. In a network, they may be combined with various sensing and monitoring products placed around the opening or integrated into the latching and locking mechanism to detect, deter and delay an intruder and also signal that a breach has occurred.

Facility integration expands the areas managed by software solutions, such as time-and-attendance systems, personnel scheduling systems, and data capture techniques. These measures provide audit trails to resolve problems, speed response time if a problem occurs, minimize maintenance, make it possible to create a central command and control area as appropriate, and allow security staff to focus on other things.

Better security can start with a security and safety needs assessment by a qualified security consulting firm. This should be the first step in taking a proactive approach, rather than one that is reactive. This type of assessment, performed by an outside party, focuses on the school's door openings, key controls, credentials, links with time-and-attendance and personnel scheduling, and other risks inherent with the overall access control system.

Learn more about securing your school

For more information about what type of security solutions are best for your school, 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 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit allegion.com/us

ALLEGION™

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

009058, Rev. 06/14
allegion.com