

Access Control: Delivering Security, Life-Safety and Convenience - Overview of Door and Hardware Components -

By T.J. Gottwalt, AHC/CDC, CSI, CDT for *Architectural Record*

Designing a building without considering the placement of plumbing, heating ducts or electrical wiring would be impractical, yet it happens all the time with another critical building component. Access control has traditionally been treated as an afterthought in building construction—a design approach that can lead to additional installation expenses and compromises in aesthetics, not to mention poor integration of security components that were hastily lumped together.

This oversight causes problems for building owners. Doors and hardware—essential elements of an access control system—constitute less than two percent of overall construction expenses, but statistics show they figure in about 25 percent of all punch list items at project closeout. Most of these punch list items can be eliminated by simply devising an effective access control system that is incorporated into the overall building design.

Making Buildings Safer by Integrating Equipment and Procedures

Think of security as a circle, a closed loop without gaps. A building may have numerous security components in place, but a single interruption breaks the loop and compromises the whole system. For that reason, it is vital to take a comprehensive approach to security so every possible risk is minimized.

Regardless of the building type (school, hospital, office), components of the access control system will fall under the categories of design, hardware and procedures. These components should be meshed together to create an access control system that delivers security, convenience and life-safety.

Much to the delight of architects and design professionals, today's door control hardware is capable of performing a given task with a certain degree of stealth. In other words, properly functioning hardware is able to go unnoticed as it performs the basic tasks of providing security, life-safety and convenience. There is no need for safety and security to be difficult or obtrusive, at least not with the locking hardware options now available.

This stealth-like effect is created by seamless integration of the door control hardware with the rest of the building's security controls. When working in tandem the security controls should deliver uninterrupted service and facilitate easy access and egress. Much like a traffic light, properly functioning doors should allow orderly flow of traffic. A broken or malfunctioning traffic light at a busy intersection creates backups, delays and safety hazards. Likewise, a mish-mash of hardware controls leads to doorways that impede safety and security.

Access Control Components

Locking hardware controls who enters the facility by limiting the number of access points. This funnels all building occupants and visitors through central doorways that can easily be monitored to keep out unauthorized individuals. Internal doorways can also be configured to only allow access to authorized personnel. The options available for accomplishing this task are numerous.

A mechanical lock and key system is the simplest from a technology standpoint, but requires extensive upkeep. Meticulous record keeping is needed to track all keys. If one key is lost or stolen, it will be necessary to look back in the records and determine which locks are accessible with the missing key. The cylinders on those locks would then be replaced and new keys would have to be issued to anyone with access to those doors.

Key duplication is another concern, but can be easily rectified by selecting a patented high-security key system that offers factory protection of key blanks. This means the manufacturer of the key system will not distribute key blanks without written permission from authorized facility personnel. Even if electronic hardware is used, a master key override is employed on most locking systems.

Electromechanical door controls—either stand-alone or hardwired locksets—sidestep the key control issue and allow even greater levels of access control. Stand-alone locks are battery powered, require no hardwiring and, therefore, are generally less expensive to install. A stand-alone lock can be operated by magstripe card, key fob, keypad or a combination of card and keypad or fob and key pad. The locks can be interrogated for security purposes and programmed to allow varying levels of access privileges. Unless the locks offer wireless networking capabilities, however, most stand-alone locksets on the market are unable to communicate directly with other building security controls.

Hardwired door hardware offers the ultimate in door control. A hardwired opening can be linked to a network, allowing user access privileges to be changed instantly. Important security tasks - interrogation of door locking hardware, changing user profiles, identifying possible security breaches and issuing lockdowns - can all be completed from a centralized computer. In addition, hardwired openings can be linked with the facility alarm controls. If a fire alarm is activated, the control panel will send a signal to automatically close all fire doors and bypass delayed egress exit devices. This versatility makes hardwired openings ideal for facilities that require tight control over security and life-safety.

The type of hardware used will vary. Mechanical hardware will usually consist of mortise locks, cylindrical locks and exit devices, while stand-alone locks are typically available as mortise locks, cylindrical locks or exit devices. Electromechanical hardware will also include mortise locks, cylindrical locks and exit devices along with electric strikes, magnetic locks, keypads, card/prox readers, automatic openers and door position switches.

When and where should each type of hardware be employed? Following are some basic guidelines.

Door Locking Hardware

Mortise locks fit into a mortise in the door edge, and typically feature levers to operate a latchbolt. They provide greater torque resistance, security and variety of functions than typical cylindrical locksets and are recognizable by the separate key cylinder above the lever. Mortise locks can be applied to any door in a facility that requires latching or locking that doesn't require panic hardware. The brute strength of a mortise lock makes it a popular choice for securing sensitive areas such as, executive offices, storage closets, computer/medical labs and stairwell doors.

Cylindrical locks are a step down from the strength and durability of a mortise lock and are more appropriate for securing interior openings. A cylindrical lock requires less door preparation than a mortise lock and is also less expensive and easier to install.

Exit devices, also known as panic hardware, allow safe egress while restricting access from outside a building. Exit devices consist of a push pad or bar which extends across the push side of the door. When depressed, the device retracts a latchbolt to allow the door to be pushed open. Think of these as a one-way valve through which people can exit but not enter unless authorized. Life-safety codes establish occupancy or space requirements that dictate which doorways must be equipped with an exit device. Generally speaking, rooms within education, healthcare, and assembly occupancies with an occupant load greater than 50 persons will require panic hardware.

Electromechanical versions of mortise locks, cylindrical locks and exit devices enhance access control by requiring ID credentials such as a keypad, card/prox reader, key fob or biometric identification device. They also feature fail safe or fail secure options in the event of power loss. A fail safe device becomes unlocked in the event of a power failure, while a fail secure lockset is automatically locked. Linking the locks into a centralized computer system permits constant monitoring of the doorways. If a door is propped open, for example, the computer will immediately detect the anomaly and warn of the possible security breach. This requires the use of a door position switch.

Exit devices offer the greatest number of electromechanical functions. Delayed egress exit devices, for example, sound an alarm and remain locked for 15 seconds when the push bar is pressed. After the 15 second delay, the push bar is unlocked and egress is allowed. This is an ideal application for openings where material can be snuck out the back door. In the past, the best available option was an exit alarm, which would merely alert facility personnel when someone had walked off with something. Delayed egress devices give time to apprehend a would-be thief, and become a significant deterrent against theft.

Another electronic exit device function is the electric latch retraction exit device. This device operates as a normal exit device, until power is applied. When power is applied to the device, its latchbolt is retracted, and the door can be pulled (or pushed) open without depressing the push rail or operating any trim, such as a lever. This can be applied to an entrance which may either have a card reader for access, or be remotely controlled by a time clock or other switching device. Some manufacturers' devices actually retract both the latchbolt and the push rail on the exit device, making the device completely silent when operated. This is ideal for auditoriums, theaters, music rooms, or any other space where acoustics and quiet door operation are important.

Strikes and Maglocks

Electric strikes or magnetic locks can be used to further regulate who passes through access points, providing an even greater level of protection.

Electric strikes are door locking devices, usually solenoid-operated, that will unlock the door when electrical power is applied to it. An opening that requires a person to be "buzzed in" is equipped with an electric strike. The buzzing sound is created when a button is pushed, sending an AC current through the device. This action disengages the device and allows the door to open. The operation just mentioned is a fail secure mode of operation, the most common function of an electric strike. A fail safe configuration will operate in the reverse condition; normally locked when power is applied and unlocked when power is interrupted. If desired, the buzzing sound can be eliminated by using a DC power source.

Magnetic locks are electromagnets that mount on the fixed frame and a strike plate that mounts on the moving door or gate. When the door closes, the strike plate automatically aligns with the magnet. The magnetic force then takes over, strongly securing the door. Release is achieved by switching of the power to the magnet. Magnetic locks are available in a range of holding forces. Facilities that demand greater security, such as a detention facility, will need magnetic locks with holding forces that approach 2,000 pounds.

Since electricity is required to power the magnet, all magnetic locks are fail safe unless they are equipped with a back-up power supply. Magnetic locks operate on DC power and, unlike electric strikes, are silent when locked or unlocked.

Both electric strikes and magnetic locks are commonly operated with a push-button switch, making them ideal for personnel-monitored openings such as office suites and hospital ward entrances. Be sure to check with the local code authority before applying magnetic locks to openings, as there are specific regulations governing their application.

While technically not a lock, automatic operators are an important component in an access control system. With the simple push of a button a door can be opened, held open to allow passage and then closed. Most buildings have at least one entrance that is required to be accessible in such a manner to meet ADA/accessibility codes. These entrances are not only for physically disabled persons, but for many situations when a person may not have their hands available to push or pull a door open.

Switches

The types of switches that can be used in conjunction with electromechanical hardware add to the diversity of access control options. Switches send a signal that activates or deactivates the lock. Several types of switches can be used in an access control system. The options available—some have already been mentioned—include push buttons, keypads, key switches, signal switches, card readers, electronic key readers, motion sensors and biometric readers.

Push button switches are located at the opening, such as a handicap door opener, or are remotely operated by a person. A simple push of the button unlocks the door and allows access.

Keypads require a numeric code to activate the lock. A keypad can be programmed to uniquely identify each user or to function similar to a combination lock where each door, rather than the user, has a unique code. Keypads can serve as the exclusive identification device, or they can be used in conjunction with other credential switches such as a card/prox reader.

Key switches are mounted at the opening and are operated by a conventional key. The device allows authorized personnel to control or signal from various locations within a facility.

Signal switches are mounted within the lock, exit device, door frame, hinges or magnetic lock and are used to initiate operation of the system, monitor the state of the doorway (open or closed) or request to exit. Every door in an access control system needs to include a door position switch in order to monitor the status of the door (open or closed). Whenever a door has a door position switch, the system needs to know when it's alright for someone to exit, therefore a switch is required as a "request to exit", also known as REX. This can be a switch on the inside lever of a mortise lock, a switch in the push rail of an exit device, a touch sense bar, or a motion sensor.

Card readers are probably the most commonly used access control switch. A variety of technologies are available with card readers including magnetic stripe, proximity and smart cards.

Electronic keys offer the same convenience as conventional keys. Older versions of this technology relied upon direct contact with a mated surface. Newer systems use passive technology and are gaining popularity.

Motion sensors operate by way of input from an infrared sensor that detects heat, a motion sensor that detects movement, or a combination of both.

Biometric readers authenticate the identity of system users by scanning unique physical characteristics such as fingerprints, hand prints, retinas or facial geometry. The readers can be mounted by the opening or incorporated into a handheld proximity device. Biometric readers usually require a large database of user information in order to authenticate each user.

Non-Locking Components

Locks and switches are only part of the access control system. Doors, frames, and door closers and holders also deserve consideration, particularly in the area of life-safety and code compliance. All these components must work together, for example, to create a fire-rated opening. The closer/holders can be tied into the building's alarm controls and serve to automatically close a door if the alarm is activated. This creates a smoke and fire barrier that can contain and limit damage from a fire.

Hinges and pivots also fall outside the realm of locks, but are essential to security. Both should be of the proper weight to fully support the door and prevent damage to the rest of the opening. Electromechanical versions of each may be needed to hardwire an electrified opening.

While these measures help control doorways throughout a building, separate tools can also be employed to enhance safety within the facility. The installation of strategically placed CCTV cameras will not physically prevent a crime but can still act as a deterrent by capturing illegal activity on film. Alarms work in the same manner. This is where building design can also play a role in creating a more secure environment. CPTED (Crime Prevention Through Environmental Design) offers a practical resource for security and crime prevention practitioners. The layout and design of a facility can greatly enhance, or detract from, the overall security and safety of its occupants.

A major factor to consider when designing an access control system is location: what part of the country will the building be located? If it will be in Florida, the Gulf states or anywhere along the coast, windstorms codes must be figured into the building plans. A windstorm-compliant building must use products that have been tested and approved for the geographically-specific maximum wind speeds. A high-rise building in New York City will have to meet life-safety codes that require an egress marking system on exits.

Being Prepared

Hardware is just part of a comprehensive security plan and must be supported by policies and procedures. The latest access control devices can be used to secure a building, but they are worthless if occupants hold the door open for a stranger. Establishing a visitors' policy and requiring all students/employees to wear ID badges will help protect against this type of intrusion. Identification policies should be enforced at all entry points, including the often-overlooked shipping and receiving areas.

Procedures are the final piece that completes the security puzzle. While hardware and policies are preventative measures, procedures are reactionary strategies that protect building occupants during an adverse event.

Schools, for example, use lockdown procedures to secure students inside classrooms when a risk is detected. But an effective lockdown requires appropriate locking hardware, such as a classroom security lock. This demonstrates the tie-in between procedures and hardware and why security must be viewed holistically.

A truly effective security plan must consider all possible risks and dangers as well as the best way to address these problems without turning the facility into a fortress. A well-planned access control system should deliver seamless safety and security, all while remaining largely invisible.

© ASSA ABLOY SALES & MARKETING GROUP INC.