APPLICATION NOTES

Access Control

Yorkland Controls
+
ENVIRONMENTAL
SOLUTIONS

APPLICATION NOTES

Access Control : Table Of Contents

TABLE OF CONTENTS Page

Yorkland Controls + ENVIRONMENTAL SOLUTIONS

APPLICATION NOTE

Access Control : Introduction

Access control is a means to authorize, restrict or deny entrance or exit of people and/or vehicles into a specific area.
It is used to protect property, employees and other assets such as inventory, equipment, information and cash.
Although access control can refer to any method for achieving this, such as locks and keys or security guards, it specifically describes a more effective, high-tech means of protection.

BENEFITS

- Asset Protection
- Prevention of Illegal Entries
- Enhancement of Personal Safety
- Reduction of Security Costs
- Facilities Management

TYPES

Keys

- Costly to re-key
- Easy to duplicate

Human Guards

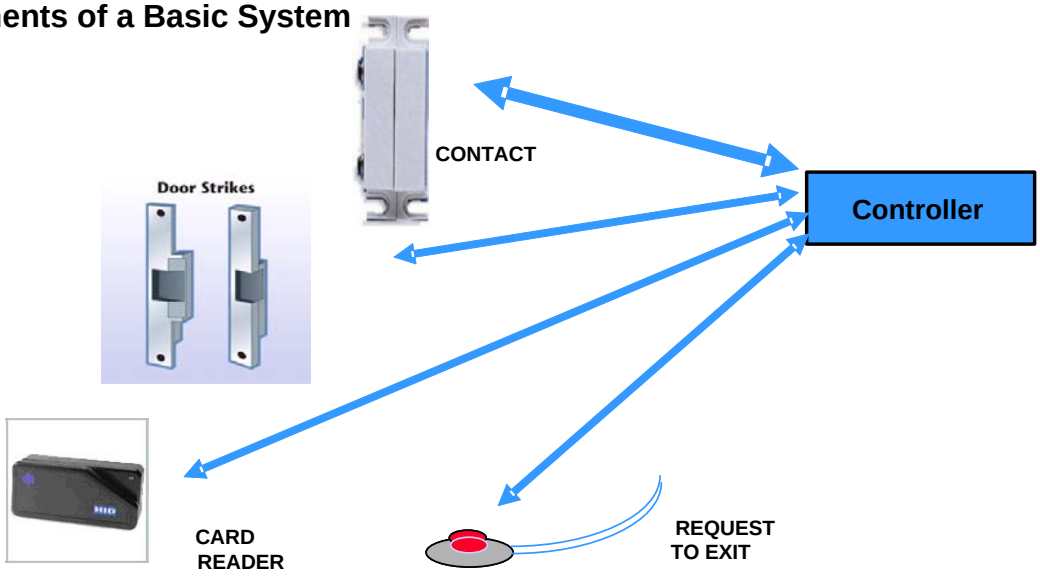
- Expensive
- Possibility of human error

Electronic Access Control

- Inexpensive to maintain
- Difficult to duplicate
- Validate and invalidate a user in seconds
- Identify Who, Where and When (audit trail)
- Readily adaptable to changing security needs
- Temporary users

Access Control : Introduction

Components of a Basic System



How it Works

1. User swipes card
2. Reader sends card data to controller
3. Controller
    a. interprets card data
    b. checks time and date info
    c. makes decision access granted or denied
4. Locking device receives signal from controller to unlock OR remained locked
5. Activity is logged or recorded on output device

Access Control : Basics

To control access to an area, there must be some type of barrier, such as a gate or door, that stops people from entering an area - unless the access system allows them in. The first thing to review is the type of barrier to be connected, and how the entry can be electrically locked and unlocked (such as a door) or activated (such as a parking garage barrier).

DOOR CONTROL HARDWARE

Electric Strikes

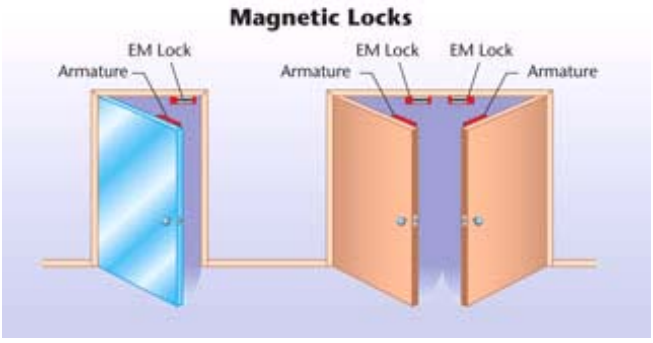
Installed on the mechanical lock side of the door, electric strikes are the most common door control apparatus.

Powered by low voltage AC or DC, strikes can be selected to be fail safe, meaning that the door is open if power fails, or fail secure, where the door remains locked in the absence of electrical power.

Door strikes allow the use of panic hardware, so that a person inside the room or building can push the release bar to exit the building even if the strike is in the closed position.

Electric strikes are typically used on framed wooden and metal doors, and are generally the least expensive way to control doors.

Magnetic Locks



Some door types, such as glass doors or double doors that do not have a center post cannot be controlled with a strike. Magnetic locks use an electromagnet to provide a powerful locking force to a door. The electromagnet is installed in a fixed position, while a metal plate is installed on the moving portion of the door, lined up with the magnet.

Magnetic locks can provide various amounts of holding pressure, from 300 to 1,200 pounds. These devices are by nature fail safe, as removal of power, whether by the access system's controlling relay or by power failure, will release the door. Power supplies with backup batteries are often used to provide emergency power to magnetic locks.

Access Control: Basics

Door Bolt Locks

Some doors cannot have a strike installed, and the usage of a magnetic lock may be impractical or aesthetically inappropriate. (an ornate arched door in a church).

Door hardware vendors supply various types of electrical bolt locks, which throw a smooth bolt typically into the top or sometimes the bottom of a door, providing an electrically controlled locking mechanism.

DOOR POSITION (Status) DEVICES

Door position devices provide status of a door (door is open or closed) to the access control system, allowing it to engage locks, annunciate alarm conditions, and other actions that provide security.
For example, an authorized user may access a door and prop it open, allowing the unauthorized entry of other people and/or the removal of property. A door position device will detect the opening of the door upon the presentation of a valid credential (card), which starts a timer within the access system for perhaps 20 or 30 seconds. When the door position device indicates that the door has shut, the access system can be set to relock the door control mechanism. If the door is propped open past the timer duration, local and remote alarm signals can be set off and transmitted.

The door contact is the most common type of door position indication. These contacts can be magnetic or mechanical, surface mounted or concealed, and are typically wired into the access control panel.
Any type of door contact can be used for this function, but it is important that this device's contacts be used only for the door position function, and not also connected to the intrusion detection system.

Surface Mount Contacts

If only install one contact set on a door is allowed, DPDT (double pole double throw) contacts are available that provide two electrically separate contacts, one for the access system and one for the intrusion system.

In cases where it is difficult to install a door contact, door status can be achieved by installing specific door strikes or *wired hinges* that include a door status output. Status is built in to the locking device. Using these devices can reduce the cost of a system, because they can make the installation of a separate contact unnecessary.

Built-in devices are useful when installing an access system on a fire-rated door. Drilling holes in the fire door for the mounting of a contact set magnet may violate the door's fire rating integrity.

Whether a separate contact or an output from the locking device, door status devices are typically installed on each access-controlled door.

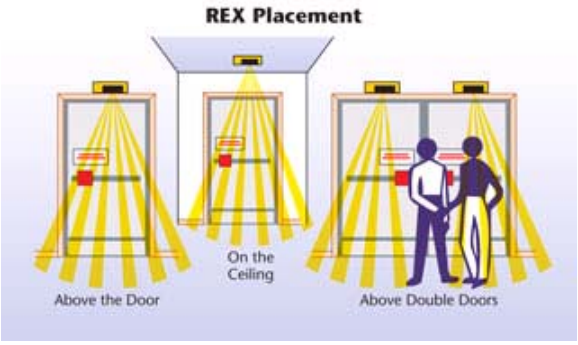
Access Control : Basics

REQUEST TO EXIT DEVICES (REX)

REX devices are installed with the detection device near the controlled door or doors to allow non-alarm exits of individuals.

In the case of an access-controlled door, a card reader is mounted on the outside which allows authorized personnel in. The door is equipped with a position contact (door status) that tells the access control panel whether the door is open or closed. When a person chooses to leave a building through this door, an input must be provided to the access panel, telling it to unlock the door. This REX input can be another card reader on the inside of the door, and the person can present a valid credential to activate the access system. Placing another reader on the inside of the door is costly, and is generally only used in high-security applications where anti-passback functions are needed.

Instead, some type of input device is installed near the door, providing either manual or automatic release of the door when people approach it. This release input also allows the door to be opened from the inside without generating an alarm condition.



In some cases, the request to exit device is a labeled switch that is manually pressed. The request to exit input also can be included in the door's panic release push-bar.

Lower cost REX sensors use motion detection technology, such as passive infrared (PIR) detection, which senses that a person is standing in proximity to the door. When activated, the electronic REX will release the door for a specified time period, perhaps 30 seconds, and automatically relocks the door when the connected door position sensor indicates a closed position. This method provides a *hands-free* door release capability, with no manipulation or credential required to exit the door.

In some applications, the capability of using secondary sensor inputs can provide added security to the door exiting procedure, while reducing nuisance alarms. An additional sensor, such as a PIR or pressure mat, can be located so that people walking towards the door trip the first sensor, which starts a timer in the REX. If the motion detection in the REX detects movement within 10 seconds, the REX will open the door. If the auxiliary sensor isn't tripped first, the REX will not open the door.

PIR

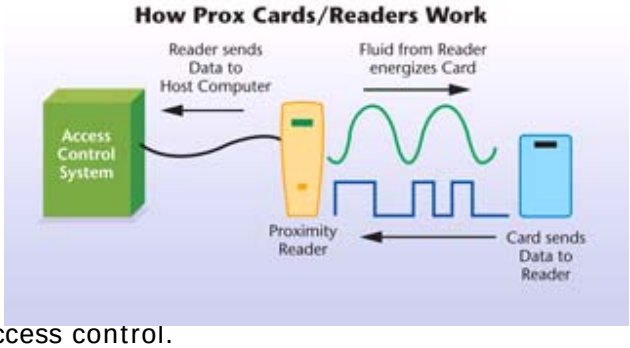
Electronic REXs can provide a variety of door control options, reducing cable runs and labor costs, while providing an easy-to-use system for end users.

Access Control : Basics

CREDENTIAL TECHNOLOGY

Different types of devices can be installed to provide an input for authorized users to open a door or access a specific device. Credential readers take the input from:

- User's Access Card
- Keypad Input
- Biometric Information



Information is transmitted to the access control panel, which decides to allow or disallow the access request based on its programming and database.

Most credential readers, regardless of type, will standard communications protocol such as Wiegand.

PROXIMITY CARD READERS

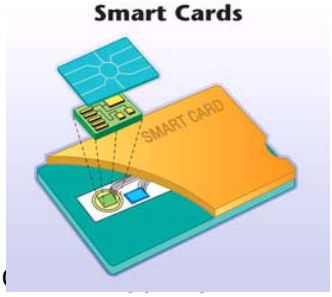
The proximity card is the predominant technology used for access control.
The card reader transmits a specific RF frequency at all times. When a card containing the specific access control credential coding nears the reader, the reader's transmitted energy is picked up by the card, which uses that energy to transmit its coded information to the reader on a different frequency.

Proximity readers can be either short- or long-range, with the long-range units providing a higher RF power output to allow for longer read distances.

ADVANTAGES

- The card can stay within a purse or wallet, not requiring the user to extract them.
- Card read times are very fast because access control information is in a simple, short format. There is no card slot, which can be jammed with glue or ice.
- Cards can be printed with the user's photo and other information, providing a combination ID badge and access control card.

SMART CARDS



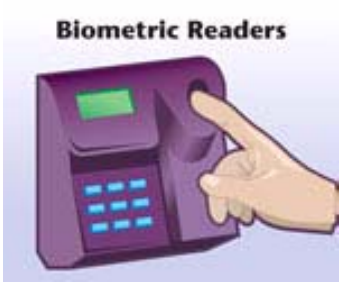
Smart cards contain a microchip with read and write capabilities which, in essence, makes the card a mini-computer with the ability to encrypt and authenticate the data – providing sophisticated levels of security for communication.. These cards can be used to hold biometric access data, debit card functions, and more.

Smart cards can be read using either a contact or contact-less methodology. C where the card physically is inserted in the reader, are a mature technology than contact-less and provide higher security, as the data from the card is not transmitted through the air.
Contact-less provides faster read/write capability and greater memory storage. Contact-less smart cards use RF to transmit data to a reader and provides faster user interface and building access.

An advantage to smart card systems is the ability of a single card to store and transmit separate information for different systems. For example, a single card can be used to access a building via the access control reader, and also provide a separate set of user authentication information to allow access to other resources, such as computers or programs within a computer system. A typical usage of smart cards is to combine access control and debit card functions within single-user cards at universities, hospitals, and other such facilities.

Access Control: Basics

KEYPADS



Keypads provide access credential, without the user having to carry or produce a physical card. Although no physical card exists that could be potentially passed to an unauthorized user- the keypad code itself may be told to another person.

Keypads are slower than card readers, as users must remember their code, punch it into the keypad, and wait for the door release. This issue should be carefully considered if high-volume user entry is required, for example if all employees must enter through one or more specific doors at nearly the same time.

BIOMETRIC READERS

Fingerprints, palm prints, and the human iris possess individually unique characteristics that can be used to verify a person's identity. This *biometric* information can be stored within an access control system and read by specific devices. The primary advantages of biometrics are very high security and the elimination of specific credential devices (cards) and their related costs.

CONCERNS

- Biometric readers are generally higher cost than card readers, and use is planned to include biometrics only at specific locations.
- Biometric personnel records are larger files which can cause slow "lookup" time, which is the time lapse between when the biometric input is provided to the reader and when the door is released. These large files also must be stored within the access control system, which may limit the maximum number of users for a particular system.
- Biometric readers require physical enrollment, so system administrators cannot remotely issue a credential and ship it to a user; the user must be present at the reader for enrollment.

COMBINED TECHNOLOGY USE

The technologies described can be used in various combinations. For example, a user can drive an automobile into a garage, and use a prox card to gain entry for parking. The same user/card combination may be presented at the entry door proximity reader to allow door entry, while the card may be used in combination with a biometric reader to allow entry to a sensitive room.

Smart card technology allows cards to contain the biometric characteristic file of the user. The user first enters a keypad code, presents his or her biometric input (fingerprint, iris), and has the card read. The access system then can verify that the user keypad code presented matches the biometric information contained on the user's card. This can speed up the process of verification, while eliminating the centralized storage of sensitive biometric information.

Access Control : Basics

CONTROLLER PANELS

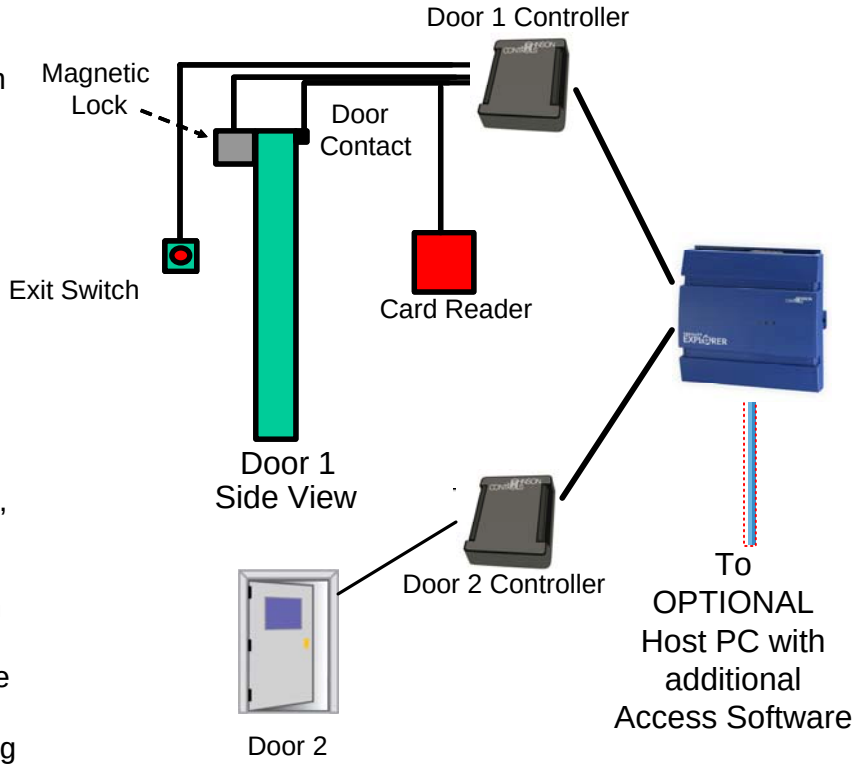
Once the selection of door release, type of credential reader, door release system and REX issues have been made, the type of controllers and system architecture is considered. Access controller panel hardware and system software differ across manufacturer platforms.

The controller panel will typically have electrical connections for the selected credential reader, a relay output to control the door release, door position input, programmable inputs and outputs, and inputs for the REX.

Access controller panels will house an on board software and microprocessor to review incoming information and activate the system's capabilities. An on-board database contains the credential verifying information for the users of that particular controlled door or device. When a credential is presented, the access controller will compare the input to its database to determine whether access should be allowed to a particular door at a particular time and day.

For larger systems, controllers are usually downloaded with a credential database from a central host computer. The decentralized system allows the controller panels to make programmed access decisions regardless of whether there is communication with the host computer.

In most cases, specific host or administration software must be used with specific access controller panels. This means that the same vendor's software and access controller panels must be used within a single system. Credentials may possibly be used in a cross-platform situation, with the same card being programmed into two (or more) separate systems.



SELECTION and INSTALLATION CONSIDERATIONS

- Battery backup is usually required for certain panels.
  Placement of the access controller panels must allow for cabling to reach the controlled doors within the maximum distances of the readers selected.
- Communications between the access controller panels and the OPTIONAL administrative computer is usually carried over Ethernet, which allows for the remote connection of panels using WAN or Internet capabilities.
- Older as well as some current panels provide connectivity via RS485, allowing up to 4,000 feet from the host computer to the remote panel.
- Selection of access controller panels must include considerations of how many credentials a particular panel can store, and of what type (biometric information requires larger file storage space than an access card).
- The processing capability of the panel may affect how quickly the localized access decision is made, which can affect how quickly people can enter and leave controlled areas.

Application Guide

Access Control Basics - Web Based Systems

WEB-BASED SYSTEMS

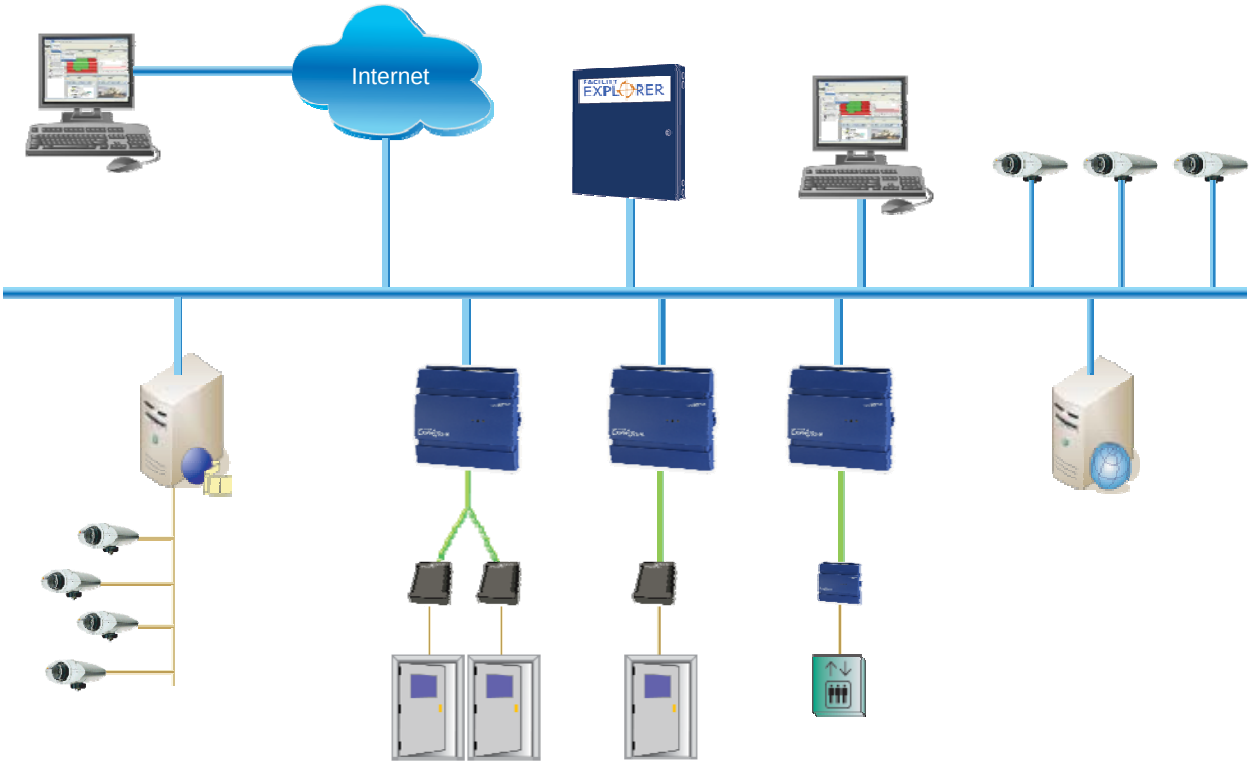
One of the primary issues with many current access systems is that the hosting software must be installed on either a shared or separate PC, which then must be maintained for software updates and integrity. These PC based systems are usually difficult to access remotely and require dedicated and supplier specific software.

ADVANTAGES

Web browser-based systems allow network-connected access controller panels to be accessed and manipulated by authorized users - utilizing a universal Web browser software such as Internet Explorer.
Each controller on the network is ,in essence, a Web server. With this type of system no software is installed or maintained on the end user's PCs. If the access controller panels are connected to a LAN and configured for Internet access, system software updates can be performed remotely.
E-mail alerts of alarm and/or invalid credential presentation can be enabled.
Web-based systems can be a single controller panel, or many spread across multiple buildings and locations.
Cost of ownership by the user is very low, with no separate computers or software to maintain or update.
Built in WEB standards in the product allow adoption by the users' IT department quicker.

CONSIDERATIONS

Installation of these systems will require detailed interfacing with the client's IT department, who will need to allow their connection to the enterprise network, manipulate firewall settings, and provide Internet access if the controller needs to communicate over same network.



Access Control - Retrofitting / Upgrading

Retrofitting /Upgrading Legacy Access Control Systems to WEB Based

Endusers upgrade existing access systems for various reasons:

- Lack of features
- Obsolescence
- Proprietory software
- Increasing service costs

CONSIDERATIONS

Divide the existing system into its components, and carefully review and test their functionality and potential for future use.

Mechanical devices such as door releases, strikes, magnetic locks, existing door position indicators and request to exit (REX) devices can be reused providing they're functional.

Card readers and other credential input equipment, such as keypads, may or may not be reusable. Some devices are no longer manufactured, and such devices may not communicate to newer standards

Existing cabling from the readers to the access controller panels must be checked for compatibility with the new reader technology. If the cabling doesn't meet the new readers' specifications, then it must be replaced. Unless the technologies are matched, replacement of the readers will require replacement of the cards/credentials.

Installation of new access controller panels will require rewiring door electronics and hardware, based on whether existing cabling is functional and any added functions such as replacing mechanical (switch) request to exit pushbuttons to electronic REX (PIRs)

Revisit the local authority requirements regarding exit doors, fail safe or fail secure door releases on power failure, and interconnection of door releases with the fire alarm system.

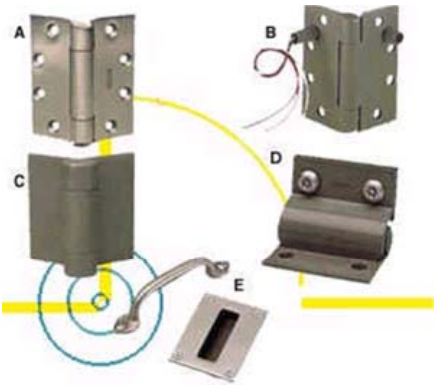
Access Control : Life Safety – Fire Doors

During the design of an access system consideration is to be given to life safety. While access into a building can be denied or controlled, the ability to leave a building cannot be impeded or unduly delayed. If the building is on fire, people in the building must be able to leave quickly without fumbling for keys or access control credentials.

CONSIDERATIONS:

- Can people within the building leave through designated Exit doors without using a key or card? It is likely that they might leave their purse or wallet at their desk in their haste to escape. An audible alarm can sound at the door when it's opened, or the door opening may create an alarm condition on the access and/or intrusion detection system. But the person can still get out the door.
- Will controlled doors unlock or be locked when primary power fails to the building? Can people go through exit doors unimpeded during the power outage?
- What happens when the building fire alarm system is activated? In many cases, the local local authorities will require that door control devices such as magnetic locks be powered down when the fire alarm system has activated. This is accomplished by connecting an alarm output relay in the fire alarm panel to the magnetic lock power supply.

FIRE-RATED DOORS



Doors that are fire rated are designed and built to provide a barrier against the spread of a fire from one room/area to the next. Any modification to a fire-rated door, such as drilling, channeling, or installing a magnet for a door position switch, will violate that door's fire rating as far as the governing authorities are concerned.

Specialized hardware, such as door hinges with b*uilt-in position switches*, can be used successfully on fire-rated doors. It is important to know what doors are fire rated in an , and to approach the application of access devices for those doors so that the door remains intact and is not modified in any way.

Access Control Definition : Anti-Pass Back

Anti-Pass Back

Anti-passback is a feature to prevent an authorized user from presenting a credential card to access an area, and then he or she “passes back” that card, say through a window or another door, to an unauthorized user, who then uses the same card to access the building.

Anti-passback is accomplished by the installation of two credential readers, one on entry and one on exit, at particular doors. Users must present their card to enter, and also to exit the door. The access control system will register when someone has entered, and when he or she has left. If someone enters and passes back his or her credential to another person, the unauthorized user will not gain entry, because the system will know that the proper user’s credential already has been used to enter the building and that he or she hasn’t yet exited. Therefore, the use of the credential by the second user is invalid.
Timed Anti-Pass Back feature allows you to enter a specific time so when the card is used, it will not work again for a specified amount of time.

Anti-passback violations can create local or remote alarm conditions, as well as be logged in the access control event data recording.

CONSIDERATIONS

Applications of anti-passback are to be carefully planned, with the traffic patterns of a client’s users taken into account. A system designed without understanding the clients usage will cause problems. For example, in a a user could present his card at a reader to enter the building, but exit through a REX-enabled door, not having his card read upon exiting. The next time the user presents his card on the outside of the building, the anti-passback logic will deny his entry, because his previous exit wasn’t registered in the system.

Events such as a fire drill may also create havoc for users of an anti-passback system. If large numbers of people quickly exit during a real emergency or planned drill, many users won’t take the time to have their credentials read upon exit. To handle this issue, some access control systems provide an anti-passback reset or forgiveness function that can be activated by the system operator to allow all valid user credentials to be employed to access the building from the outside after such events.

If planning to use anti-passback, installers should make provisions for adequate battery backed up power for all aspects of the access control system, including the door release mechanisms, credential readers, and access controller panels. If any aspect of the electronics fails during a power outage, similar issues can occur.

Anti-passback provides an important employee management feature, as the access system can provide information regarding how many people are within a building or access controlled area at a specific time, as well as their identities.

While anti-passback can be employed on a system-wide basis, it often is used within an overall access control system for specific computer rooms, data storage vaults, and other high-security areas. Biometric readers inherently eliminate the possibility of the unauthorized use of an access card, because there are no cards to pass around.

Access Control : Power Requirements

DEVICE POWER

The planning of an access control application must include the selection of power supplies to provide adequate power to operate the connected door devices. A number of security equipment vendors provide power supplies specifically designed for use with access control devices.

A system that is fail safe will open door release devices in the event of power failure, while a fail secure system retains the door release in the closed position. Installers should consult local authority requirements for the release of labeled exit doors in the event of primary power failure or fire alarm system activation.

Security system dealers need to calculate the amount of current necessary to operate the door release devices, and how much standby battery power should be provided to maintain the operation of the access system in a power failure.

CONSIDERATIONS:

- The cabling type and distance from the power supply to connected door releases must be considered since long cabling distances may require increased conductor size to compensate for current drop.
- Consult local authorities for requirements relative to exit doors. Are exit doors be automatically released when the fire alarm system goes into alarm? This may require interconnection of the access control power supply(s) and the fire alarm system.

Separate Power for Strikes & Mag Locks

Door releases are to be powered separately from other electronics in the system.

Door release devices such as strikes and magnetic locks typically operate at 12 or 24 volts AC or DC. Although the amount of current drawn by a strike (typically 150 mA @ 24 VDC) or magnetic lock (125 - 350 mA @ 24 VDC) is not excessive, electrical spikes and surges occur when the device is energized and de-energized. These issues can create interference, which can hamper the performance of other electronic devices connected to the same power supply.

Access Control : Video Basics

Digital Video Surveillance

Uses either analog or IP cameras for verifying and recording events digital on a Digital Video Recorder (DVR) in real time.

COMPONENTS

Digital Video Recorder (DVR)

A digital video recorder is a similar device to a video cassette recorder (VCR). The difference is that a DVR is a PC or Server based that records video to a hard drive instead of recording to a video cassette.

ADVANTAGES of DVR over VCR

1. Record continuously or on events
2. Link video events to controller events
3. Can be integrated into the an Integrated Environment
4. More cost efficient
5. Easier to recover recorded events
6. Requires less space

Cameras

There are essentially two types of cameras:

- Analog which is connected to the DVR or VCR via a coaxial cable.
- IP (Internet protocol) which can store its video on board the camera or send its video stream to a PC or server

Camera Types

Fixed Box Camera

-Basic surveillance camera.
-Can be installed with multiple types of different lenses.

Fixed Dome Camera

-Has a built in lens and comes in a dome hosing.

CCD Camera

-What is commonly known as the all-in-one camera.
-Has a built in auto focus lens that cannot be changed.

Pan-Tilt-Zoom (PTZ)

-A mechanical camera that can be controlled remotely.
-can be controlled via a joy stick or with the GUI (graphical user interface) in the DVR.
-These types of cameras generally come in a dome enclosure.