Cube Training - Vocational Training Centre

Education is key, if it’s success you wish to see.

Cube Group Limited, Thames Innovation Centre, 2 Veridion Way, Kent, DA18 4AL
Tel: +44 3330064005, E-mail: sales@cctvdvrsystem.co.uk

Table of contents

How to control access to a specific area: An Introduction. 2
Doors 2
The Electric Strike Door. 2
The Magnetic Locking Door 3
Door Bolt Locks 3

Door Position Devices. (Also referred to as Door Status Devices). 4

Request to Exit Devices (REX) 4
Credential Technology 5

Proximity Card Readers 5
Smart cards 6
Keypads 6
Biometric Readers 7
Combined Technology 7

Controller Panels 8
Controller Panel Selection and Installation Considerations. 8

Web Based Access Control System 9
Web Based Access Control Systems. Advantages and Considerations 9

Upgrading and Retrofitting Access Control Systems 10
Upgrading your Access Control System. Things to Consider. 10

Access Control Life Safety and Fire Doors 11
Life Safety. Things to Consider. 11
Fire Rated Doors 11
Anti-Pass Back 12

Access Control Power Requirements 13
Device Power 13

How to control access to a specific area: An Introduction.

In order to maintain security and safety within any controlled public or privately owned space or area, that area must have some form of physical barrier, namely a door or gate, securely installed and permanently in place. This will prevent either overcrowding or, in the case of privately owned spaces or areas containing either hazardous or valuable items, unwanted or uninvited guests or visitors.

With the age of a simple 'lock and key' door now behind us, there are many electronic based doors, gates and barrier systems that employ a number of different activation methods to ensure that only the right people gain access to whatever space or area the owner wishes to control.

This guide will help to explain the various different electronic activation methods any individual, business or organisation can choose to keep themselves, their homes, offices, products and belongings safe and sound. Once you have decided which system works best for you, you can literally lock yourselves up and throw away the key!

Doors

Despite the long standing view that any door with a simple lock and key mechanism is at risk of being smashed and broken into, there is still a fear that many of the new-age technology electronic style door locking systems will work perfectly well until there is a power cut, and the user will be either locked in, or out, of their building, home or yard, until the power returns.

The thought of being left potentially trapped, increasingly helpless and possibly even in danger without a way of solving the issue can result in many property owners unnecessarily putting their homes and/or business premises at a heightened level of risk. But electronic door technology has come a long way and those fears should be dispelled in the following pages.

The Electric Strike Door.

The **Electric Strike Door** is now the most commonly used electronic door control method. Powered by low voltage AC or DC, Electric Strikes are installed on the side of the door with the standard mechanical locking system and, critically for those with safety concerns, Electric Strike Doors have a 'fail safe' mode. This means that in the event of a power cut the

door can be set to either ‘locked’ or ‘unlocked’ with the added bonus of a special ‘panic hardware’ mode whereby any person(s) inside a building can push a release bar to open the door even if the Electric Strike is set to ‘locked’ during a power failure.

Electric Strikes are typically used on metal doors and doors with wooden frames and are generally the least expensive ‘door control’ method.

The Magnetic Locking Door

Not every door has a centre post that Electric Strike Doors require and for these types of door, typically a glass door or double doors, the most cost effective method of secured control is a Magnetic Lock.

Using a powerful electromagnet to provide the locking force, **Magnetic Locking Doors** can provide anywhere between 300 and 1200 pounds of holding pressure. Installation is simple with the electro-magnet placed in a fixed position on the door frame and a metal plate installed on the door itself in line with the magnet and, like the Electric Strike, Magnetic Locking Doors are fundamentally fail safe as the removal of power either manually or in the event of a power cut, automatically releases the magnetic lock and opens the door.

Magnetic Lock Doors also have backup batteries, which act as an emergency power supply to ensure that the door remains locked in the event of a power failure.

Door Bolt Locks

But these two solutions still cannot cater for every type of entrance way. For example doors on certain historical listed buildings cannot be adjusted or modified in any way that wasn’t possible at the time of construction and therefore many ornate arched doorways such as those found in churches and cathedrals cannot have Electric Strikes or Magnetic Locking systems put in place for practical and aesthetic reasons.

Likewise, much smaller doors such as those on medicine cabinets, which need securing to keep children from gaining access but that don't require electromagnetic locks, also need a practical and cheap method of control.

With that purpose in mind, any D.I.Y or hardware shop can supply simple yet effective electrically controlled **Door Bolt Locks**. Typically these are smooth in appearance and are driven by long life solenoid 'direct throw' mortise bolts with special right angle bolts available for particularly narrow door frames. This is the most basic of all electrically controlled locking mechanisms.

Door Position Devices. (Also referred to as Door Status Devices).

For users wishing to bypass traditional or magnetically operated locking systems altogether, **Door Position Devices** can not only communicate to the main access control system to give it information on its 'status' (for example whether the door is open or closed), but also remotely engage the locks themselves, trigger any attached alarm system and even prevent unauthorised people from entering an area via a timing system.

Many Door Position Devices require users to swipe or scan a validated credential card (most commonly used in a workplace setting), before it can be opened and to prevent an authorised user from unintentionally allowing access to unauthorised persons, a pre-programmed timer will then kick in and close the door automatically. If the door remains open longer than the standard timing system, usually between 20-30 seconds from acceptance of the Users' credentials, the access system can trigger an alarm both locally as an immediate deterrent and in many cases remotely to the business owners home address or even a local police station.

While this can be inconvenient if the door needs to be left ajar to allow the loading or unloading of goods, the unique timing system can be altered to suit specific scenarios before being reset to their standard timing duration. Once the door is closed safely, the Door Position Device will automatically re-lock and re-set the door control mechanism until another validated credential card is swiped or scanned.

Door Position Devices that perform dual functions like this are referred to as DPDT's or 'Double Pole Double Throw' due to the fact that they require two electrically separate contacts. This type of built-in device can be especially useful on fire-rated doors where any modification, attachment or drilled-in holes would compromise its safety certificate.

However not all Door Position Devices are fully integrated with remote alarm triggers. The most common type of DPD's are single purpose Door Contacts that can be magnetically or mechanically controlled. Standard Door Contacts are wired directly into the access control panel of the door and focus solely on the status of the door and not any additional alarm system. The single purpose Door Contact is the cheaper of the two options but a separate electrical contact, door strike or wired hinge can be added even in the narrowest or awkwardly positioned door as a simple way of upgrading the entire system to include local and remote alarm triggers.

Request to Exit Devices (REX)

Predominantly used in high-security areas due to the extra costs involved, **Request to Exit Devices** can be added to doors that already have an external Door Position Device installed for the specific purpose of monitoring the departures of any authorised person who has already entered their credentials to get in to a secured area.

In the event that someone has been able to bypass the entrance control panel without the correct credentials, any attempt made by that person to exit the secured area would result in the door either remaining in a locked position or triggering an alarm when an attempt to open it without swiping the REX Card first.

In certain cases the Request to Exit Device differs from the standard 'card swipe' panel and can either come in the form of a clearly labelled button or a built in part of the doors emergency exit push-bar.

Lower cost REX Device solutions use motion detection technology, such as passive Infra-Red sensors which activate the doors' release mechanism for a set period of time when a person is standing in close proximity. The Infra-red sensors then detect when the user has walked through the door and then automatically closes and relocks the door, creating a hands-free solution without the need for additional access panels and credential cards.

Taking the increase in costs to one side, the addition of a secondary REX access control panel provides added security and reduces nuisance alarms while Passive Infra-Red Sensors and pressure mats located on the approach to a door have the advantage of avoiding

unnecessary door openings as the built in release mechanisms won't open the door if the initial sensor is triggered but then after a set period of time, no contact with the door is made. This is extremely helpful if a person happens to remain standing by a REX equipped door but with no intention of exiting the secured area.

Electronic REXs can provide a variety of door control options whilst reducing the need for large amounts of extra wiring and the associated fitting and labour costs and are seen as an easy-to-use solution for the owner.

Credential Technology

The first generation of electronic Door Position Devices used pre-programmed credit card style **User Access Cards** to transmit information about the user to the control panel to either allow or deny access to a secured area. However the continual advances in **Credential Technology** means that there are now a number of options available to the mass market from **Keypads** where each user has a unique access code to **Biometrics** where Users can only gain access to, or exit from a controlled area by having their fingerprints, voices or even their eyes scanned by the access panel.

Proximity Card Readers

The **Proximity Card Reader** is still the most widely used method of Credential Technology used for access control. The card reader transmits a constant and specific Radio Frequency (RF) and when a card containing the specific access control credential coding nears the Reader, the Readers RF is picked up by the card, which then transmits its own unique coded information back to the Reader on a different frequency.

Offering the quickest solution to controlling access to a specific area owing to the fact that Proximity Readers can communicate either at short or long range and don't require the user to physically swipe their access card, Proximity Cards can double up as an ID badge containing the Users photograph and other relevant information.

Bypassing the need to physically swipe the Proximity Card also negates the risk of a User dropping their card, having it snatched from them at the point of entry or being denied access in the event that the card slot is either jammed or damaged.

Smart cards

Like the name suggests, **Smart Cards** provide very sophisticated levels of security information and are essentially mini-computers thanks to their built-in microchips that can encrypt and authenticate numerous forms of data that can be transmitted by either physically inserting the card into the Reader or, as is becoming increasingly common, as a Contact-less solution.

The Contact type system where the User must still enter his or her data into the Access Device is still the most established and secure method as no data is transmitted solely through Radio Frequencies, which can be intercepted by hackers. However the pace of improvements in security is such that the much quicker and easier to use Contact-less Smart Cards are swiftly becoming equally as secure as the 'old' technology.

The main advantage of a Smart Card system is its ability to store and transmit a number of totally separate pieces of unique and sensitive information for different systems. For example a single card can be used to access a building via the access control reader, and then also allow the User to access their computer, laptop and other internally controlled areas with different access panels and different authorisation requirements to the main entrance. This is especially useful in a workplace such as a hospital where only certain staff members are authorised to enter specific areas.

Keypads

Whilst **Keypads** bypass the need for a User to carry or produce a physical card that can be stolen, passed on to another User or, as is increasingly common, cloned, the use of Keypads as an access control method carries several increased risks.

Whereby a single card and all its data has to be reproduced with 100 per cent accuracy or held by a single individual at any one time, there is very little to stop a User passing on their Unique Keypad code to any number of unauthorised Users. Also in cases where the User does not require regular access to a controlled area there is an increased risk of that User forgetting their unique code and being prevented from gaining entry to an area that they are entitled to be in.

Keypads are also much slower to operate than Card Readers as each User must punch in their multiple digit code, and then wait for the door release mechanism to begin which can pose a major problem if a large number of Users/Employers have to enter or exit a building through a single door at roughly the same time.

Biometric Readers

Of all existing forms of Credential Technology, **Biometric Readers** are the most advanced, secure and expensive solutions. The potential advances in the development of Biometric technology also outweigh all other forms of Credential Technology making this method the most favoured when maximum security is required by the Owner.

Each User possesses many individually unique characteristics that cannot be realistically stolen, borrowed or cloned such as their fingerprints, palm prints, voices and even their iris. These pieces of biometric information can all be stored by a Biometric Reader access control panel to verify a person's identity and automatically recognise which specific areas of a building that User is permitted to enter.

Despite the advantages in terms of security over all other forms of Credential Technology, Biometric Readers do have drawbacks, not simply the higher costs involved compared to other solutions.

Biometric personnel record files are usually larger than Card Readers, and therefore have a generally slower 'lookup' time, which is the amount of time taken between the initial biometric input from the User and the eventual release of the door control mechanism. Due to the fact that each file has to be stored within the access control system this can also reduce the maximum number of Users permitted to use a particular system making a single access control panel impractical for larger businesses. Biometric Readers also require physical enrolment by the User, so system administrators cannot remotely issue a credential, creating a longer set-up process when the system is first installed.

Combined Technology

As there is no 'one size fits all' solution to Credential Technology, many businesses, organisations and individuals use a combination of the currently available technologies to satisfy the security needs of their premises. A common example of this would be a Keypad controlled car park gate to allow staff into their designated parking area, a Proximity Card Reader to allow them to gain general access to the building and then a Biometric Reader for certain individuals who require access to a particularly sensitive area of the workplace.

Controller Panels

Once an organisation has selected their specific type of Door Position Device, Credential Technology (or Combined Technologies), Door Release System and REX, they must then consider what type of access **Controller Panel** they wish to use as an overall platform to host all the software.

Controller Panels differ from one manufacturer to another and in most cases manufacturers have bespoke administration software that can only be used in conjunction with their access Controller Panels. While End Users have to decide on which manufacturers' product best suits the needs of their business, all Controller Panels generally have many similar methodologies behind their 'unique' operating systems. Starting with their chosen form of credential reader, which is electronically activated, Controller Panels will have a relay output to control the door release, a door position input, programmable inputs and outputs, and inputs for the REX. It is possible however that Credentials be used in a cross-platform situation, with the same card being programmed into two (or more) separate systems.

Access controller panels will also house an on-board software microprocessor to review incoming information and activate the system's capabilities. This built-in database contains all the various credential verifying information for each authorised users of that particular controlled door or device. When a credential is presented, the access controller compares that unique input to its database to determine whether access should be allowed or denied.

For larger systems, the credential database is housed on a centralised 'host' computer, which receives and then responds to the Controller Panel. Not all systems require this however and Controller Panels are capable of holding enough data to negate the need for a centralised computer system for both individual premises as well as small and medium sized businesses.

Controller Panel Selection and Installation Considerations.

As with every element of access control and credential technology, each operator will have their own individual requirements and financial restrictions meaning that there are plenty of options to consider when choosing **which Controller Panel to install**. Likewise each Controller Panel comes with its own set of requirements that may make them perfectly suitable for one operator but completely impractical for another.

The types of credential technology being employed and the number of Users required to use the system will dictate certain choices and regardless of the amount of file storage space and processing speed, the vast majority of Controller Panels require a back-up battery. In every installation, the final placement of the Panel requires a certain amount of wiring and cabling to be put in place to ensure the door being used isn't too far away from the Panel, thus rendering the sensors useless.

In the cases of larger organisations that require access data to be held on a central computer, communication between the access controller panel and the host computer is usually carried over Ethernet. Despite living in the 'internet age' there are still areas where strong wireless internet capabilities are not available although many older panels provide connectivity via RS485 with a maximum range of 4000 feet between host computer and remote panel.

Web Based Access Control System

One of the primary issues with the current generation of access system is that the hosting software must be installed on either a shared or separate PC, which will require regular software updates, additional maintenance to ensure GDPR compliance and continually evolving anti-virus protection. The ability to access the hosting software remotely via a **Web Based Access Control System** can make life a lot easier for the owner despite the heightened potential for the system to be compromised and the necessity for potentially expensive and complex manufacturer specific software.

Web Based Access Control Systems. Advantages and Considerations

One of the key advantages to a web based Access Control System is that a Controller Panel connected to the internal network of a business can easily be updated and maintained by a suitably qualified member of the IT Department. This can be done for either a single Controller Panel or for multiple Panels spread across different buildings and locations. If an alarm is triggered or an invalid credential presented at any access point, the User can receive an instant email or message specifying the type of breach and the location, which massively reduces costs and foregoes the need for separate computers or software

Each Controller Panel on an organisations 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. Built in WEB standards in the product allow quicker and easier adoption by the Users' IT department.

But there are still many things to consider with any Web Based Access Control System that could make them unsuitable for certain Users. For example installation requires detailed interfacing with the client's IT department, potentially opening up the client's internal data-sensitive information to being accessed by the overall network. This could also require the altering of certain firewall settings and the safety concerns that that could pose, especially if the Controller Panel and those Users operating it via a Web Based System need to communicate over the same network.

Upgrading and Retrofitting Access Control Systems

Older, non-remote 'Legacy' Access Control Systems can be updated to operate as a Web Based System although in certain cases, a completely new ACS is required if the software used by the existing system is on an operating system no longer supported by any of the major web browsers or is simply obsolete.

As technology continues to provide new solutions in the quest for security and peace of mind, Users are always seeking ways to maximise security and tweak and upgrade their existing access systems.

A lack of security features, obsolete technology and operating systems, increasing service and maintenance costs, the changing nature of an individual business and availability of

proprietary software are among the many reasons why Users upgrade their systems and move towards remote Web Based solutions.

However there is a risk that any User could needlessly spend unnecessary money upgrading a system when they have yet to explore ways of maximising their current security control methods.

Upgrading your Access Control System. Things to Consider.

Before making a final decision to upgrade there are several important areas to consider.

Begin with divide the existing system into its components, and carefully review and test their functionality and their 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 re-used and recycled into different areas of the business providing they are still fully functional. On the other hand card readers and other credential input equipment, such as keypads, may or may not be reusable as they are no longer manufactured and do not conform to modern data protection and security standards. These may also house sensitive User information and would need to be disposed of in specific ways

The existing wiring from the Reader to the Access Controller Panels may still be compatible with the technology used by the upgraded Reader, especially if it is made by the same manufacturer. However if the cabling is not fully synched to the new Reader then full functionality of the new system won't be possible and the entire wiring system will need replacing. There is no point upgrading to a new system if it can't be used to its full potential.

Even if the wiring is still compatible, if the User is employing Card Based Credential Technology it is likely that the cards will need replacing as the internal microchips will be out of date as will the door electronics and hardware and any additional functions such as a mechanically operated Exit button, or an electronic Passive Infra-Red Request to Exit sensor.

The rules laid out by local authorities and individual industries regarding exit doors, fail safe or fail secure door releases on power failure, and interconnection of door releases with the fire alarm system are also constantly evolving and so if a User is looking to combine some of their existing technology with a new upgraded system, careful checks would need to be made to ensure they remain compliant with the latest Health and Safety requirements.

Access Control Life Safety and Fire Doors

During the design of an access system, paramount consideration is 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.

Life Safety. Things to Consider.

Every business, organisation or individual using any kind of electronically controlled Access Control System must be able to answer a number of potentially lifesaving questions before installing any type of security measure.

Can everyone inside the building leave through designated Exit doors without using a key or card? All Fire Safety guidelines deter people from returning to their workstations to pick up items such as wallets or purses that usually contain their card readers or key fobs. Opening a door without them may trigger an alarm but at least any person can still get through the door without his or her credentials.

If there is a power failure, do all controlled doors have a manually operate override to unlock them and allow people through in an emergency? Keeping unauthorised Users outside is one thing but trapping authorised Users inside is equally as dangerous.

What happens when the fire alarm is activated? Does the Access Control System have the ability to instantly 'power down' in the event of a fire, meaning that all locking systems cease to operate automatically to allow anyone inside a safe an unimpeded passage to safety? This can be 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 to provide a barrier against the spread of a fire from one room or designated area to the next. Modifying any Fire Rated Door is highly frowned up as even the most minor of modifications such as drilling a hole in order to install a magnet for something as basic as a Door Status Switch can render all insurances for the Business Owner null and void. Specialist hardware, such as door hinges with built-in position switches, can be used successfully on fire-rated doors but it is important to know which doors in the building are fire rated so that the approach to controlling access to those doors is dealt with differently to any entrances or exits that are not designated as fire-rated.

Anti-Pass Back

One commonly used but difficult to prevent method used to get unauthorised people into any secure area is when an authorised user enters a building with their credentials and then passes their card, or keypad code out to an unauthorised user via another door or even an open window. The unauthorised user then simply uses the same credentials to gain access to the building.

However Smart Card technology and many modern Access Control Systems now have **Anti-Pass Back** features built into them to prevent this from happening.

Anti-Pass back is accomplished by installing two separate credential readers on particularly vulnerable doors or access points, one on entry and one on exit. Users must present their card to enter, and also to exit and the access control system registers when someone has entered, and when he or she has left. While this does not deter anyone from the physical act of passing back their card reader to a second unauthorised User it will instantly prevent that second User from gaining entry to a building as the secondary Ant-Pass Back credential reader has not been told by the initial user that he or she has left the building via the User swiping their card on the Exit Controller Panel. Anti-Pass Back violations can also trigger local or remote alarms and attempted unauthorised entries can be logged against the cardholder's records through the access control systems data recording facilities.

Applying Anti-Pass Back features still need to be carefully planned as the existing Access Control System needs to have a pre-programmed awareness of the overall pattern of every Users usage, effectively meaning the ACS can pinpoint a User's location. In organisations with multiple layers of internal security, this location can be pinpointed more accurately whereas in single system buildings, the 'understanding' of the ACS is merely whether the User is 'In' or 'Out.'

Without placing a pre-programmed 'understanding' into an Access Control System, a User could present their card at a reader to enter the building, but exit through a REX-enabled door, not having been required to scan or swipe their card upon exiting. Unless a programme is in place within the ACS to let the system know that the User is no longer in the building, the next time the user presents their card to gain access to the building the Anti-Pass Back logic will unnecessarily and incorrectly deny them entry.

Events such as a fire drill may also create havoc for users with an Anti-Pass Back system especially if a large number of people leave the premises at once during a real emergency or even a planned drill.

To take this scenario into account, some access control systems provide an Anti-Pass Back reset or 'forgiveness' function that can be activated by the system operator to allow all Users with valid credentials to be allowed to re-enter the building without their credentials.

Providing the Owners have made adequate system back-up provisions for all aspects of the access control system, including the door release mechanisms, credential readers, and access controller panels in the event of a power cut, Anti-Pass Back 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.

Anti-Pass Back systems are capable of being installed to control an entire building or wider area but they are generally used in more specifically controlled area with fewer authorised Users just because of their understandably slower and more rigid swiping protocols. Impractical in places like factory floors with hundreds of workers, where a less time consuming method is preferred, Anti Pass Back finds more regular usage as a specific part of a wider Access Control System, which requires A-PB for certain high security areas with very few authorised Users.

Access Control Power Requirements

Device Power

During the very first stages of planning the installation of any form of Access Control device the operator must ensure that the building they wish to be protected has the correct means of powering even the smallest of systems without causing issues in other areas. There is no use in installing an ACS if it drains power from other critical areas or, at worst, causes the overall power supply to collapse.

To this extent a number of electricity providers provide power supplies specifically designed for use with access control devices to ensure that a business or organisation has enough power to safely run the additional device with no risk to the rest of the building or business activities the ACS is designed to protect.

Any Access Control System from a reputable manufacturer will have clearly defined instructions and guidance as to the amount of power required not only for everyday use but also all 'emergency' situations such as the fail-safe settings that will open door release devices in the event of power failure and then maintain their operation until power is restored and the instant release of all designated fire exits.

For the Door Release mechanisms themselves the type of wiring and the distance between the power supply and the Door itself need to be factored in to any considerations as the longer the cabling, the more compensation is required to counteract any current drop

It is also advisable to have a separate power supply for Strikes and Mag Lock Door Releases that is kept away from all 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.