



Access Control Explained

6620-4019 Issue 2 M5315

Contents

Introduction	3
Why Electronic Access Control?	3
Is access control difficult to specify and install?	3
How to survey a site and assess risks.....	4
A word about identification	5
PIN-only entry systems	5
Token-based systems	5
Biometric systems	6
Components in a token-based system	7
Card	7
Reader	7
Lock.....	7
Door sensor.....	8
Egress	8
Door Ajar Sounder	8
Controller.....	8
Software	8
Types of System	9
Intelligent readers.....	9
Separate Controllers	9
Networked systems.....	9
Summary – Pros and Cons of different types of system.....	10
Special situations.....	10
Car Parks	10
Elevators (Lifts)	10
Remote sites	10
Alarm management.....	11
Employees versus Visitors	11
Integration.....	11
Cabling.....	12
Other Benefits from Access Control systems.....	12
Don't forget.....	12

Introduction

This document is designed to help you specify an electronic access control system. This has been considered a minefield in the past by people more familiar with intruder alarms and CCTV – but these days manufacturers strive to supply “usable” products that require little, if any, training. Common sense and this document are all you should need!

Why Electronic Access Control?

Old-fashioned locks and keys leave much to be desired in anything other than a domestic environment, because:

- Standard keys are easily copied
- Each person may require several keys
- Lost and stolen keys represent a major security risk, requiring time and money to solve

But with a modern electronic system these problems are a thing of the past.

Electronic systems can provide additional security by enforcing time rules, by raising an alarm in the event of an unauthorised attempt to gain access, and by recording all access movements, in and out, for analysis in the event of later discovery of a security breach.

Is access control difficult to specify and install?

If the customer’s basic requirements are known, then the choice of system can be quickly narrowed down. Basic questions regarding the number of doors people will usually indicate a particular system type (see “Choosing a TDSi System”). Some customers – if they have an understanding of access control principles – will be able to assess their own risks and be quite positive about what features they require, while others will require guidance. The next section talks about site surveys and risk assessment.

How to survey a site and assess risks

There is one golden rule that must be followed, otherwise we'd go mad:

THERE IS NO SUCH THING AS TOTAL SECURITY

Total security is something we can aspire to, but most commercial organisations – as opposed to the government, the military etc. – have to evaluate how much security is appropriate to the risk, and this will inevitably involve placing a limit on the budget. The best systems are the ones that reduce the immediate risk while allowing for non-redundant expansion as needs grow – not just the need for more doors and more people but also the need for more security. Unfortunately, we do live in a time when each year, the risk increases.

So a site survey will involve assessing where and what are the highest risks, and establishing how the risk may be reduced. This is exactly the same principle as for intruder alarms – work on the principle of “dissuading” the potential violator so that they go elsewhere.

The highest risk will be where there is a combination of the following factors: an un-secured door, with no people about on either side of the door, leading to an area containing something of value.

Once you have established which doors need to be controlled, you have to establish how much control to apply. This is rarely a case of “all-or-nothing” – where any person with a card can gain access wherever and whenever they want – and so it's worth looking at the various enhancements to establish which ones can be applied:

Feature	How it works	Where it is of benefit
Access Levels	Each person can only go through certain doors.	If some areas in the organisation are felt to need higher protection than others, for reasons of, for example, theft or confidentiality. This is probably true for most organisations.
Time Zones	Each person can only go through certain doors at certain times.	If there are times of day or days of the week when certain people should not be present – for example, a business whose normal office hours are 9-to-5 might wish to allow access only during the hours of 8 a.m. until 6 p.m.
Card+PIN	After using a card, a person must type in a PIN before the door will open	If there is a risk of lost or stolen cards being used. This risk may be at its highest when the number of people in the area is at its lowest – in which case this feature can be scheduled automatically.
Anti pass-back	After a card has been used to gain access to an area, it cannot be used again for a given time (“timed anti pass-back”) or until the card has been used to leave the area.	Where there is a risk of one person inside an area handing a card to someone outside the area. The risk is higher where turnstiles are installed, because ordinary doors allow “tail-gating” anyway.
Man traps	A door will not open unless another door is closed.	Where there is an “air-lock” situation – e.g. dust-free zones – or where tailgating can be prevented by two doors close together with room for only one person in between them.
Alarms	Any “unexpected” event or “abnormal behaviour” can be notified to a supervisor, who can then establish what happened and decide how to respond.	This can benefit every installation. For example, if a door is left open too long, or a person tries to gain access where they are not allowed, then these represent risks that can and should be eliminated. There are many different types of event that can be detected and dealt with – too many to list here.
Point-monitoring	“Spare” inputs on the access control system can be used to monitor windows, fire exits and the like.	If there is a risk that open windows and fire exits could allow people to by-pass the access control system.

A word about identification

All electronic access control systems work on the bases of identifying a person before deciding whether to unlock the door. The means of identification fall into three categories.

PIN-only entry systems

These are the least secure. Those with a common code – where everyone uses the same number – are the cheapest and least secure.

Slightly better are unique PIN systems, where each person has a different number, and these do at least allow you to delete a single code if it has become “compromised”. But there is still the risk of deliberate or accidental passing on of a code, and little way of knowing that this has happened.

Token-based systems

This type of system is the most popular, and the type that the remainder of this document focuses on.

Token based systems, using cards, tags etc., provide much better security. Each token is usually unique – or as near to unique as makes no matter – and if you are concerned about stolen tokens you can require a PIN number in the way that cash machines do.

The choice of card technology can seem bewildering at first, but each technology has its own set of unique characteristics and pricing structure. Fundamentally, there are two types – those that you have to insert or swipe, and those where the card is read at a distance. The latter kind are mostly short range (i.e. proximity) working from 2cm up to 60cm. But there are true hands-free systems where 1 or 2 meter range is quite possible and you don't need to get the card out of your pocket as you approach the door.

Biometric systems

After several years in existence, biometric systems are only now starting to find acceptance in the general, as opposed to specialised, security market. Fingerprint recognition seems to be the most popular at the moment in terms of cost, accuracy and acceptability. But facial recognition is a technique that has been proven and when the price/performance ratio starts to improve we can expect to see significant market change in favour of such systems. Iris recognition is being trialled by some banks for increasing security at ATMs.

Components in a token-based system

Card

This is what the person carries in order to identify himself or herself to the system. It may be credit-card-sized, or it may be more like a fob on a key-ring. It may have to be “swiped” through a slot in the reader or merely brought to within a few centimetres (“proximity”). Some work from a metre away and don’t even need to be removed from the pocket (“hands-free”).

If there is no pre-existing reason for choosing one technology over another (e.g. if the cards have to also be used in an other system such as a time-and-attendance recorder) then the choice of technology will be based on cost of readers, cost of cards, level of security offered and personal preference:

Technology	Reader cost	Card Cost	Security *	Other issues
Mag-stripe	Low	Low	Low	Mis-reads are common. Readers are usually not weatherproof. Cards are easily damaged through accidentally erasure of the coding.
Wiegand	Medium	Medium	Medium	Old technology; often site-specific so long lead-times at manufacture
Infra-red (Microcard)	Medium	Medium	Medium	Small readers, mis-reads are rare. Cards are more secure and more robust than mag-stripe.
Proximity	High	Medium to High	High	Easy to use and rapidly growing in popularity as prices come down. Most cards are “passive” (i.e. contain no battery) and therefore have an unlimited life.
Hands-free	High	High	High	Can read when you don’t want them to; e.g. walking down corridors past doors. Most cards are “active” (i.e. contain a battery) and therefore have a limited life.
Smart Card (e.g. Mifare)	High	High	High	Can be useful where several different systems are installed and only one card per person is wanted.

* Card security – the risk of copying - is not a single issue. It relates to the need for time, equipment, money, and special material. It also relates to the risk of the copying being detected.

Reader

This is what identifies the person to the controller, by reading the card and sending its unique identity.

Some readers are more prone to vandalism than others, so risk-assessment needs to be carried out. If a reader is attacked, it may result in unauthorised access (see “intelligent readers”) but usually will result in authorised people being denied access. Some proximity readers can be hidden behind panels so that being invisible better protects them.

Two readers may be required on some installations – either to enforce anti pass-back rules or to monitor everyone’s whereabouts. But this only works if turnstiles are used...

Lock

The choice of lock depends firstly on the door – electric strikes or bolts, magnetic locks, turnstiles or barriers are all options depending firstly on the architecture – and secondly on the required resistance to attack.

As the “lock” is normally located on the edge of the door furthest from the hinge, double-doors represent a particular problem unless one door is fixed closed during normal operation (i.e. it is normally opened only for emergencies or to allow large objects to pass through).

Another problem situation is a door that “swings” – i.e. opens both inwards and outwards so it can be pushed open from either side. Frameless glass doors also require specialist solutions.

All lock types have their advantages and disadvantages – if you are unsure which type to choose then gather as much information as possible about the door and seek advice from a supplier.

Magnetic locks

Magnetic locks have become very popular as they provide rapid solutions in a wide variety of circumstances – often without the need for major surgery to the door, frame or pre-existing “furniture”.

There are two types: face-to-face for outward opening doors and shearlocks for inward opening and swing doors. These locks are available in a range of strengths and designs. Note that some designs will reduce “headroom” and may have health-and-safety implications if there is a risk of injury from the metal edges of the mechanism.

Door sensor

The door sensor is an optional piece of equipment, which serves two purposes:

- For access control, the door sensor provides an extra level of security, in the following way. If the lock release time is set to, say, 10 seconds, it is quite possible for someone to get through the door in only two or three seconds after using their card. This leaves seven or eight seconds of 'un-expired' time, during which (if no door sensor was fitted) the door could still be opened. However, if a door sensor is fitted, then as soon as the door opens the lock release is de-energised. The door re-locks as it closes.
- For access monitoring, having a door sensor fitted means that all occurrences of the door opening and closing can be monitored if a printer or PC is part of the installation. Also, relays can be set to operate – and thereby sound an alarm – if a door opens when it shouldn't (i.e. the access control system had not released the lock), or stays open for too long.

Egress

This is an optional piece of equipment, which allows people through a door – from the secure area to a less secure area – without the use of a card or PIN. Pushing the button causes the lock to be released, just as if a card had been entered (i.e. for the pre-programmed 'lock release time').

This is sometimes used as a 'reception' button, where someone inside the building can let someone else in.

More commonly, the egress button permits a person to exit the building or room. Although certain types of door lock mechanisms permit egress by turning the handle on the inside, this may be detected by the ACU as a 'door forced' situation. In other words, the door has opened but no card or PIN was used. Installing an egress button gets round this problem.

Note that fire regulations may also require people to be able to exit an area without depending in any way on electrical systems.

Door Ajar Sounder

An access control system is useless if the door is propped open. If a door sensor is fitted, then a sounder can be used to alert anyone in the vicinity that this has happened. Loud buzzers are very effective at persuading people not to do this in the first place!

Controller

Controllers may be built-in to a reader or be separate. Separate controllers may control one door or several. See “types of system” later for guidance on how to choose which is best.

Software

Software provides a means of programming cards and setting the rules for the system – normally this information is sent to the controllers so that it is the controller(s) that makes the decisions. These rules are also stored in a database on the computer so that (a) you can see what you have programmed and (b) if a failed controller has to be replaced then it can be re-loaded with the necessary information.

Software will normally also monitor the system, recording events (e.g. who has gone through which door and when) and saving the information to disk so that reports can be printed. Normally, you will be able to view these events in “real-time” so that you can watch as people move around.

You cannot buy access control software from one manufacturer and use it with controllers and readers from another manufacturer.

Types of System

It's worth looking briefly at the types of systems that exist.

Intelligent readers

At the simplest level, a combined reader/controller provides a convenient all-in-one package that can be installed quickly to control access at a single door. You could install more than one if you have more than one door, but then every time you needed to add or erase a user, you would have to do this at several locations.

There is a security risk with these products, in that the controlling electronics is on the insecure side of the door, and therefore open to attack. Consideration needs to be given to the likelihood of attack, and if the risk is high then either some form of tamper protection will need to be fitted or a different type of system installed.

Separate Controllers

When protecting a single door, fitting a controller on the secure side of the door is more secure in high-risk situations. No matter how the reader is attacked, the door will not open.

For multiple door situations, there are controllers that can control several doors each. This can represent cost savings because there is only one controller, and it can also be more convenient because you can programme cards in for multiple doors with a single action. But the practicalities and costs of cabling up between the doors can outweigh the benefits depending on the cabling distances.

Networked systems

Intelligent readers and separate controllers fall into the category of "stand-alone" systems because they do not need a computer and software to manage and monitor them. Computer linked systems should be considered where any of the following apply:

- more than one stand-alone system would have to be installed to secure the number of doors required (in such cases you would otherwise have to perform programming operations at multiple locations)
- there are more than just a couple of different combinations of access rights (imagine the complexity of programming a 16-door stand-alone system where some people are allowed through all doors, some through some of the doors, others through a different selection of doors...)
- more than one person can be expected to administer different aspects of the system (multiple workstations make this easy and convenient)
- a remote site needs to be controlled and monitored (either dial-up modems or a permanent network connection can be utilised)

Such systems provide the ultimate in convenience and flexibility, and healthy competition ensures high performance at sensible prices. Modern systems are intuitive and user-friendly and require minimal training for administrators.

Summary – Pros and Cons of different types of system

Type of system	Pros	Cons
Intelligent reader	Low cost, easy installation	System is on the “insecure” side of the door and can be attacked to gain unauthorised access.
One-door controller	More secure than intelligent readers in vulnerable locations.	If more than one door is to be controlled, cards will have to be programmed in each controller.
Multi-door controller	Single point of programming up to the capacity of the controller (2-16 doors typically)	Sophisticated features can complex to set up.
Networked system	<p>Central programming and monitoring regardless of number of doors.</p> <p>User-interface much more intuitive and flexible.</p> <p>Multiple workstations can administer the system.</p> <p>Sophisticated filtered reporting, alarm management, interface with other systems.</p>	<p>None (except cost!).</p> <p>Note that a small minority of computer-linked systems use the computer to make the decisions – this may mean a computer failure means failure of the whole system.</p>

Special situations

Car Parks

People don't want to get out of their cars so that they can use their card to raise the barrier – this is an ideal situation for mid-range proximity readers. Up to 60 cm can be achieved with “passive” tags and if this is acceptable it means that the readers used in the building may well be cheaper than if active tags were used.

If a car park cannot hold all the cars that might want to use it, then some form of occupancy control needs to be implemented. This can sometimes be part of the barrier system, where a counter can be reset when the car park is empty, and from then on counts all the cars in and all the cars out. The barrier will not be raised if the counter is above a set limit. This form of control can also be applied by the access control unit, which counts cards rather than cars and can be cheaper to implement as it may reduce the need for vehicle loops.

Elevators (Lifts)

Several systems offer the possibility of elevator control. Typically, this involves placing a reader in the elevator car and when a card is presented, only the floors to which that card is allowed can be accessed. This is achieved by re-wiring the floor call-buttons through relays in the ACU. When a card is used, the appropriate relays change over and for the next few seconds the call-buttons may be pressed. Some more modern elevators allow the relays to be wired into a command interface instead of having to re-wire the call buttons. In high-rise elevators (30 floors and over) there sometimes a data interface through which commands may be sent to enable and disable call-buttons.

Remote sites

Remote sites can be considered as being of two types – those where local administration and monitoring is required, and those where it is not.

If local administration is required, then usually the two sites will have to be linked together by a permanent-available connection – for example a Wide Area Network (WAN). This is because in any system there is usually only one database – and any administration terminal must be linked to the database.

If local administration is not required then an occasional connection may be implemented – for example, dial-up modem over conventional telephone lines. The central computer will connect to the remote site whenever there are commands and card numbers to be sent, and will also connect on a regular basis to collect event data. The access control units on the remote site will connect to the PC whenever there is an alarm to report.

Alarm management

An access control system can generate a huge amount of event data that may be useful in analysing what happened after an incident has occurred. However, nobody is likely to want to sit in front of a screen watching this happen in “real time”. This is where alarm management comes in – this is the principle of notifying someone only as and when a specified event occurs.

The general principles of good alarm management systems can be summed up as follows:

- it must be hard to miss the fact that an alarm has been raised
- it must be easy to establish what the event was, and where it happened
- if there is more than one alarm, it must be easy to establish which is the more important one (importance is pre-defined by the system administrator)
- the operator must be able to find out what he or she is supposed to do about the alarm
- the system administrator must be able to find out what alarms have occurred, which operators dealt with them and how quickly they did so.

Employees versus Visitors

Even trusted employees should be controlled. Essentially, by giving them a card you are saying, “I trust you”. But even if you have thoroughly vetted all your staff, and have done psychological profiling to establish trustworthiness, circumstances change.

So, by restricting access only to those areas and only during those times decided by the system administrator decided, the risk is minimised. Also, if someone has been told exactly where they can and can't go, and they try to “bend the rules” by trying their card in a prohibited area – or if someone has stolen their card and is trying gain unauthorised entry because they don't know where that card is allowed – the system can make the most almighty row about it!

Anti pass-back also prevents a dishonest employee from gaining access through a turnstile and then passing their card through the bars to someone else.

And if you don't discover until much later that a security breach has occurred – the event log will show you all events from the system – doors opening, closing, being left open too long, fire doors propped open. It may well be that the monitoring is as useful as control in providing deterrence.

Not all electronic systems provide these additional features and they naturally have a price attached – it's up to the customer to decide if they are important.

Un-attended visitors should be treated in the same way as employees, with one extra consideration – if a visitor does not return his or her card then it should be voided. Some systems can do this automatically.

Integration

Integration with other security systems – particularly CCTV – is becoming a common requirement. In an unattended situation, rather than having the CCTV system switch through the cameras on a programmed sequence, it is possible for the access control system to react to an unusual event occurs by sending a command so that pictures are recorded of the location of the event for later analysis.

Another possibility is for high-security low-traffic situations, for example late at night, where you might want a guard to decide whether to allow access or not. If the guard is not close to the point of access, which is quite possible where more than one point of access exists, then when a user swipes their card, the system can:

1. alert the guard that someone wants to gain access
2. bring up a picture stored in the access control database of the true owner of the card
3. switch a CCTV camera so the guard can see the live picture of the person standing there

The guard can check that the two images match, and release the door by simple command to the access control system. This need take no more than a few seconds – and the guard might be many miles from the door!

Where guards provide security, they may well be responsible for dealing with alarms generated by the access control system. If they are on tour round the site, they could be alerted by a message sent to their pager or mobile phone. Also, while on tour, if they fail to use their card at a certain point by a certain time, the system could raise another alarm to summon help in case they have been attacked.

Intruder alarms are normally active out-of-hours, while the access control system is mainly used during work hours. However, at the point where these two overlap – e.g. first person in and last person out – the access control system can over-ride the intruder system by shunting intruder detection contacts or arming or disarming the system. Also, if a security incident occurs, comparing event logs from the two systems can provide useful evidence.

Cabling

The limitations and economics of running cables needs to be considered:

- Reader cables have limitations due to signal degradation over distance. Typically, 100 metres is the limit – but it may be less depending on the reader technology, the specification of the controller and also the amount of electrical noise in the vicinity.
- Low-capacitance cable will normally be required for reader and communications cables.
- Lock-strike cables have limitations due to voltage drop. Simple calculations will tell you what specification of cable to use.
- All cables should be screened, with separate “functions” carried down separate cables. Sometimes you might get away without using following these rules – but if the installation doesn’t work reliably you’ll need to re-cable, and this may be costly in man-hours!
- Typical requirements per-door are:

- 6-core cable for Reader
- 2-core cable for Door Sense
- 2-core cable for Lock Strike
- 2-core cable for Egress Button
- 2-core cable for Door Ajar sounder

Other Benefits from Access Control systems

There are many ways in which an access control system can benefit an organisation.

Security can be further enhanced if the access control card also bears a picture of the rightful holder. If staff members are instructed to challenge anyone not wearing a card, or if the picture doesn’t match the face, then every employee suddenly becomes an additional security guard.

Because the system can record all comings and goings, the data can be used for other purposes. For example, calculation of the time spent on the premises can be used for attendance totals, and this in turn can satisfy the requirements of the working time directive or be used for payroll. Further, in the event of a fire alarm or other catastrophe, the system can list all those people on the premises and also those who have presented themselves at muster points. Beware though – this does require significant enforcement of rules requiring every person to swipe in as well as out even if someone holds the door open for him or her.

Don’t forget...

In closing, let us remember one vital thing:

Don’t forget the people who have to use the system. If the system makes it hard for them to do their job – in particular through queuing to get through turnstiles, or being refused access where they should have been allowed - eventually it may have to be de-commissioned or significantly revised. Fortunately, many of the aspects we have covered are of benefit to the employees as well as the employer, and problems like this are rare.