

## Access Control and Fire Safety

*Access Control has come a long way from drawbridges, guard dogs, and "Halt, who goes there?" Modern computerised Access Control systems are the fastest growing sector within the security industry. Here Paul Wong, Technical and Product Development Manager at security equipment distributors Norbain, sets out the state of progress of modern Access Control Systems and their operation in the event of Fire Alerts.*



Access Control is most simply defined as 'knowing who goes where and when'. Or more formally, Access Control is 'the electronic control of the passage of people, assets, or vehicles'. At its simplest it is the locked door that needs a pass or code number to open, and from there it gets as complicated as the increasingly sophisticated client base requires.

It's no surprise that, with security ever higher on the corporate agenda, expenditure on Access Control is increasing. But it may come as a surprise that Access Control is the fastest growing sector of the entire security industry, with installations in almost all new buildings, upgrades to existing systems at all levels, and many organisations investing in access control for the first time. Norbain, as an industry leader offering a one-stop-shop to customers, mirrors this industry growth. Last year Access Control accounted for some double digit growth, and this growth is planned to grow – an expanding and important part of Norbain's total service offering.

**Expenditure on Access Control is increasing**

## The core components of an Access Control System

The component parts of an Access Control System are straightforward enough – a **Token** is checked by a **Reader**, a **Control Panel** accepts or refuses entry, and a **Door** opens or remains closed. Looking in more detail at each of these component parts:

**Tokens** – the ‘key’ provided to each individual to gain access. A token may be:

- something you have, such as a Card
- or something you are, such as a Fingerprint
- or something you know, such as a PIN (Personal Identification Number)

**Reader** – the device that reads the token. There are numerous options for Readers, each with its pros and cons for specific environments and applications:

- Mag Stripe
- Infra-Red
- Proximity
- Weigand (a high security option)
- Bar Code
- Biometrics (for finger print or iris recognition, for example)

**Control Hardware** – the ‘brains’ of the system that holds the control information – who can gain access where and when. Local Control Panels hold information for one or a small number of local doors, holding copies of control tables for those doors. These Control Panels are linked to a central PC, which holds the master control table, plus all records of every transaction, both successful and rejected.

**Door/Barrier** - - the physical barriers to entry. Doors and locks are complex and prone to problems if not correctly matched to the application. There are many different types of doors, and Turnstiles and Vehicle Barriers can also be used as part of an Access Control System. The essential access control component of the door or barrier is the lock, of which there are many options, including:

## Access Control priorities change in the event of a fire alert

- Electric Release and Keep
- Magnetic
- Shearlocks
- Solenoid Bolts

## **Access Control systems and Fire Alarms**

Clearly Access Control priorities change in the event of a fire alert. The key issue changes from regulating who enters the building or area to ensuring that everyone who is in the building or area has free exit. The specific features that make Access Control a benefit in times of fire emergency are:

**Fail Safe Doors** – the first requirement in the event of a fire or similar emergency is for all doors to revert to open mode, for easy and safe evacuation. Access Control systems can remove the electronic locking of doors automatically through links to the fire alarm/fire detection system.

**Roll Call** – When a fire evacuation has taken place, it is essential to know who is and who isn't in the building, including visitors. The central PC of an Access Control system can quickly provide a precise list of the names of all building occupants at the exact time of the alarm.

**Networking across the site, and to remote sites** – in addition to knowing who is and is not in a building, it can be important to know where key staff are at the time of an emergency. If an organisation – a company or a university, for example – has a number of buildings in an area, with staff or members moving between them, then a networked system provides a trace on all people in the group of buildings.

**Muster Points** – the roll call itself can be automated, using a reader at a designated safe muster point at which people register their arrival, for quicker and more accurate electronic roll calls.

**CCTV links** – clearly a CCTV control room can use manual control to switch into the camera with a view of the fire. However, there can also be automatic links provided between the CCTV system and the fire alarm/detection system, instantly switching the control room view to that of the camera at the site of the fire as identified by the heat/fire detection system.

As emergency systems, both Access Control and the Alarm System should normally have a UPS – an Un-interruptible Power Supply – that cuts in if the normal supply suffers a failure in the emergency.

## **The practicalities of Access Control Systems**

Although the principles of Access Control are simple, the large number of options for each of the component parts, the need to select the right components for the operating conditions and application, and the requirement for compatibility between components, presents a skill challenge to the system designer and specifier.

For example using the wrong type of locks for a specific door type will result in doors that won't open or close properly. There is also the key consideration of the robustness required under the operating conditions, including physical wear and tear and weather conditions on outside installations.

Different token and reader technologies have different inherent levels of security. PIN Code readers when used alone are considered to be lower security than Proximity, for instance –, but of course Proximity comes at a higher cost. The same comments on security and cost apply to the emerging biometrics technologies, such as fingerprint, iris, and face recognition, which have a substantial software component in them to handle the complex matching that gives access.

In many situations today a new Access Control application is just one more to add to an existing list. To take the example of a university, many already have a card that covers library borrowing, internet use, students union access, and more. Any new Access Control application, such as car parking, will need to use the existing token and reader technology, perhaps a mag stripe card. The costs and the inconvenience of introducing an additional token for a new system are unacceptable.

### **Conclusion**

To sum up, there are three propositions that apply to Access Control and fire safety. First, Access Control Systems and Fire Detection/Alarm systems can now be integrated into a sophisticated automatic system. Second, although each component of the system may not be complex, experienced designers and installers are needed to ensure a full function system that operates effectively under all operating conditions. Third, if this condition of skilled installation is met, the system will provide a powerful aid to the safety of staff and the public in the event of a fire.