Mobile phones or QR codes can be given to casual visitors entering common areas or to enable access

Picture credit: Axis Communications

ACCESS DENIED

Pia Hantoft *explains why access control is the fastest growing sector in physical security*

Access control has, for the second year running, been the fastest growing sector in the physical security industry, with an increase of around 5 percent compared with 2016. Access control now accounts for 24 percent of the total market. The technology, which can be integrated with audio and video to complement and strengthen security offerings, helps organisations manage personnel movement throughout a building and premises by granting or denying people access to specific areas.

In recent years, with the move to Internet of Things (IoT) system structures, access control has seen its uses expand into different industries. With everything on the same network working in harmony, it maximises a system's effectiveness and capability to identify, alert and deal with security breaches.

Additionally, the move to open, non-proprietary access control, instead of closed, proprietary access control, has opened the possibility to create large systems with best-of-breed technology, which often comes from various providers. This allows organisations to select their products from the best supplier and easily add or remove new hardware or software to an existing setup, future proofing the system.

Advances in access control, IoT solutions and open systems, have enabled different elements to be integrated into one security system. Open management systems bring a vast array of benefits. By connecting multiple different sensors and software into one system, organisations can create a comprehensive security network.

Door controllers can, for example, be connected to cameras. This enables security operators to ensure that the person that has entered the premises using an ID card, or other identification methods, is in fact who they claim they are.

SOUNDING OFF

It's possible to include an audio element to access control systems. Much like an intercom at the entrance of an apartment block or shared office space building, it serves as a method of communication and an extra layer of security. This active communication pathway can be used in case of problems with accessing buildings. The person can simply push a buzzer and be linked to security operators who will be able to assist. Alternatively, it is possible to combine the access control system to networked speakers. This allows operators to perform a public address via a SIP mic or choose a specific zone to alert the public of any particular issues, such as alarms.

Access control can even be integrated with Human Resources (HR) software. By integrating access control to HR's time and attendance software, it is possible to keep track of an employee's comings and goings, to establish when they have been in the building. On the other hand, it can help alert security teams monitoring an organisation's security if the ID card of a person who is supposed to be on annual leave is being used.

Network and system managers will only have to be trained how to use the open system interface once. The interface will then remain the same no matter what technology gets added further down the line or sits on the network. This means that organisations will only need to pay and spend money on one training session, ultimately saving money.

Open systems are easily scalable and flexible depending on needs. New applications simply need to be added or removed from the system without much difficulty. Network-based systems don't have a large centralised control panel. As a result, the system can continuously grow to encompass more and more different technologies.

These types of solutions are easy to install, maintain and upgrade. Encouraging and working towards sustainable partnerships between hardware, software and application technologies and products will deliver organisations tangible benefits.

The number of mobile phone users is set to reach 4.7 billion this year, with over 60 percent of the world's population already owning a handset. These handheld electronic devices are replacing everything, from payment processes and music devices to cameras and now as key cards.

It is widely expected that by 2020, as many as 20 percent of organisations will be utilising their mobile phone handsets as tools to enable admittance through access control. Seeing as mobile phones are already used for identification, authentication, authorisation and accountability, it seems fitting that they should be extended to be used in situations such as access control.

For companies, using their employees' mobile phones as access authentication eliminates the costs of handling, printing, distributing and disposing of physical badges and key cards. In addition, few people ever go anywhere without their mobile phone, which means there is less chance of someone getting stuck outside a building waiting for somebody to give them access.

Much like mobile phones, QR codes can be used by casual visitors entering common areas or to enable access for late deliveries. As with mobile phone access, using this system, organisations can save money on providing one-off access cards, as well as lessen the impact of environmental damages from discarded passes.

License plate recognition access control systems require the collaboration of several technologies working in perfect harmony. This means that access control technologies can be used to streamline, for example, access to a secure car park. It is a cog in an open system that will determine whether a vehicle is allowed to enter a secure area.

In such a situation, the vehicle enters a camera's detection zone, which will trigger embedded software to check the license plate. That data can then be sent to a gate controller who will check against a database and decide whether the vehicle can be granted access. Cameras optimised for this type of scenario usually come with special firmware with optimised settings for the picture quality.

> SYSTEMS CAN COME WITH CARD, FINGERPRINT AND FACIAL ID TO MONITOR RESTRICTED AREAS

However, if the vehicle's license plate fails initial safety screenings, video connected to access control could help the operator establish if this person can be given access. Alternatively, the person trying to enter the premises could have a pre-sent QR code, which can be scanned by a door station in the access control system to grant them access.

Operators can pre-set the systems to allow vehicles access during certain hours. Organisations do not need to employ costly security guards around the clock, but could instead use access control technologies to their full capacity.

DATA ANALYSIS

The intelligence and processing are all done on the edge. This is where data produced by IoT devices is processed closer to the sources, meaning organisations can analyse data in real time, without sending it along routes to data centres. It also saves organisations from investing heavily in expensive servers. Furthermore, by using the edge, users save on their bandwidth and storage use, further reducing avoidable expenditures.

Hospitals are, by their very nature, facilities open to everyone, which makes them among the most difficult areas to keep safe due to the multitude of people that enter and exit the premises in all sorts of conditions and emotional states.

▶

An ENA survey of 7,169 nurses found that nurse abuse was, unfortunately, commonplace, with over 54 percent claiming that they had been a victim of it at some point. Access control systems can be placed around the hospital to help manage the flow of patients and visitors around the facilities. In doing so, security operators can keep a close watch, through video connected to network door stations, and deal with someone if they act in an aggressive manner.

Healthcare facilities are often filled with lots of valuable equipment and drugs. Access control systems can come with card, fingerprint and facial ID to monitor restricted areas where these valuables are kept. This can assist hospitals as they will spend less time having to replace any of the stolen goods.

KEEPING PEOPLE IN

Access control systems can be used to keep people out as well as in. The vulnerable such as those that are suffering from mental health conditions or dementia can be placed in special sections of the hospital to keep them safe. This is to make sure that they do not wander out of the grounds and put themselves in danger.

In addition to this, access control can work with RFID chips. By putting chips in infants' or babies' clothes or bracelets, access control systems can make sure that children do not leave specified areas. Or, if a chip, attached to a baby, does try to pass through a specific designated area then cameras can then be triggered to record what's happening and help security officers assess the situation and determine the best course of action.

With hospitals often facing a tight squeeze on their budgets, it is important to make sure that they have access to security systems without large overheads. By using technologies such as access control, that is open, IP based and works together with different software and hardware, hospitals can use the money they would spend on extra security staff, on other essentials such as patient healthcare.

Although IoT and connected systems come with a wealth of benefits, they can leave organisations vulnerable to cyber attacks. As everything is in some way connected to the internet, leaves numerous avenues for access, some more heavily secured than others. Hackers take advantage of these back-door channels, meaning that they can steal important and valued data, costing organisations an average of $3.5 million in 2017.

ADVANCES HAVE ENABLED DIFFERENT ELEMENTS TO BE INTEGRATED INTO ONE SECURITY SYSTEM

It is important for organisations that choose to apply extensive IoT systems to protect themselves with an equally smart cyber security system. In doing so, they will not only be protecting the company's reputation but also any personal information it has on employees.

Access control as a service (ACaaS) is a growing part of the offering. By utilising cloud-based services, companies can reduce, the time spent by IT departments on developing and maintaining their own expensive servers and infrastructure. This will help companies reduce expenditure, lowering the total cost of ownership.

Not only can access control reduce an organisation's expenditure on security products, but it also helps secure entry and exit points in a variety of ways. Technology is constantly evolving, and with access control growing year on year, it will be interesting to see how this technology can be used in the future ●

Pia Hantoft – Axis Communications guiding force in Access Control – has nearly 10 years' experience in the security industry, with a specific area of expertise around access control.

It is possible to keep track of an employee to see when they have been in the building

Picture credit: Axis Communications