www.mayflex.com

White Paper

How IP is impacting Physical Access Control

Infrastructure.
Networking.
Electronic Security.

All together.

MAYFLEX
A Sonepar Company

+Background

Installers and end users of security systems have never seen as many exciting product developments as they have in recent years as more and more traditional security systems move across from analogue based to IP-based products. Most recently the video sector has been transformed by the new technologies being adopted resulting in many benefits such as standardisation and compatibility of systems. This paper examines the impact of IP technology on the Access Control Sector of the industry which has yet to fully adopt IP and is still several years behind that of CCTV.

In looking at the adoption of IP-enabled devices on the video surveillance market we can draw parallels as to how the advances of network based technology may follow a similar path in the world of access control. We will examine the reasons for this and look at some of the emerging IP based technologies that are gaining traction in the world of access control.

Let's start by looking at the main types of access control systems being installed in the UK market.

Firstly we have the most commonly installed standalone, single building system, which according to a recent security integrators report consists of 12 doors and around 128 'credentials', that is a unique piece of identification allocated to a specific person.

Secondly there are the larger corporate systems, often referred to as enterprise access control systems. These systems typically protect large campus style environments or multi-site deployments.

Both types of system share the same hardware such as dedicated cabling infrastructure, readers, locks and controllers, but differ at a software level where the large systems have added functionality, scalability and deeper integration with other systems such as video management software and intruder detection.

Both large and smaller systems are traditionally installed on dedicated cabling and are only connected to the corporate network at a client machine level only. These client computers will typically be used to manage the issuing of badges and credentials.

+ Barriers to the early adoption of IP based Access Control

IP technology is still quite new to the access control industry and legacy systems have yet to exploit the advantages of IP technology. There are potentially a number of reasons for this:

+ Existing proprietary hardware/software
+ Manufacturer reluctance to build IP based products
+ Legacy Infrastructure
+ End user reluctance to move to network based solutions

+ Existing proprietary hardware/software

Typical legacy access control systems are dependent on having each device (i.e. Door, Lock, and Card Reader) hard-wired with RS-485 cable into a central unit or server. Furthermore, they are usually proprietary systems, which confine the end-user to a single vendor of hardware and software.

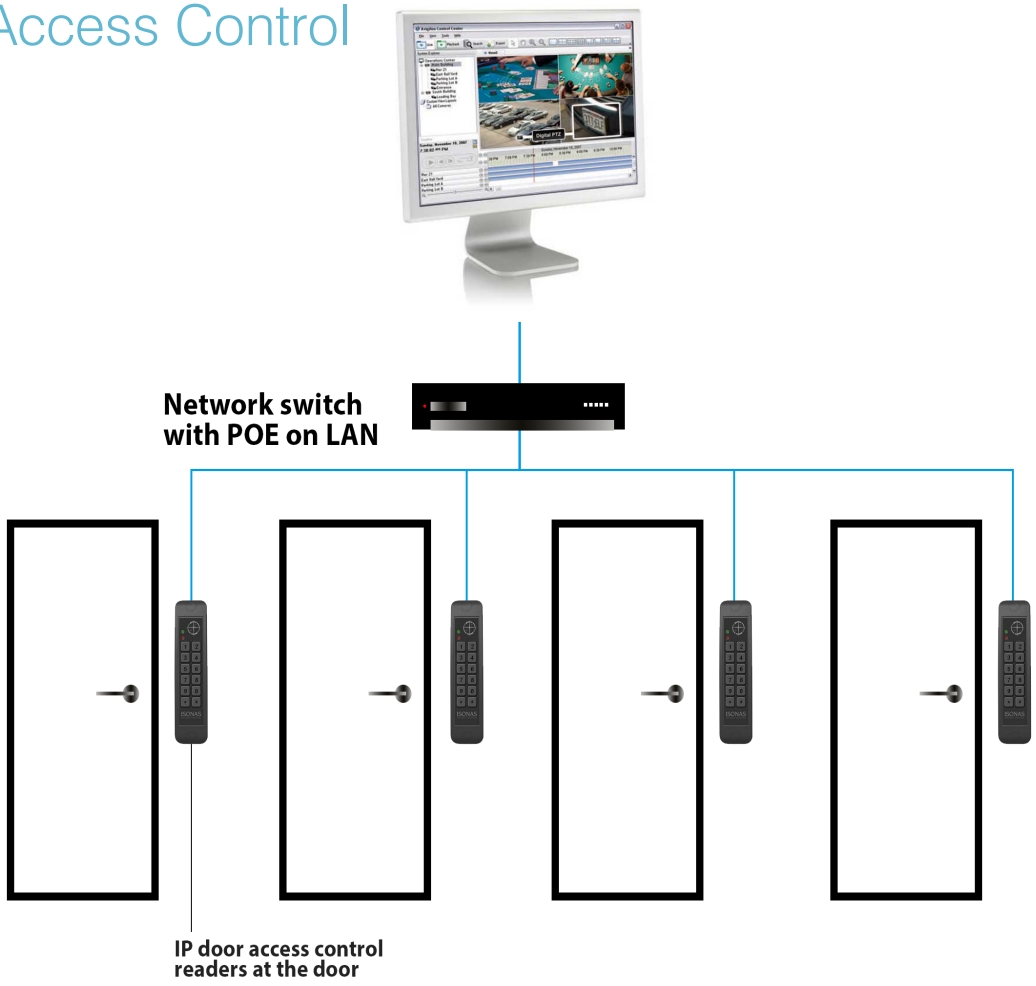
+ Manufacturer reluctance to build IP based products

Whilst this may be a controversial opinion this may well be a reason for slow adoption. If we look at the commercial aspects for a vendor of one of the main enterprise access control systems we can assume that millions of pounds of investment will have been sunk into R & D of proprietary technology that will have thousands of established site deployments across the world. This must represent a significant period before the vendors get a return on their investments in proprietary hardware and software solutions. So the question is, why would they want to move all of their products to IP based open platforms?

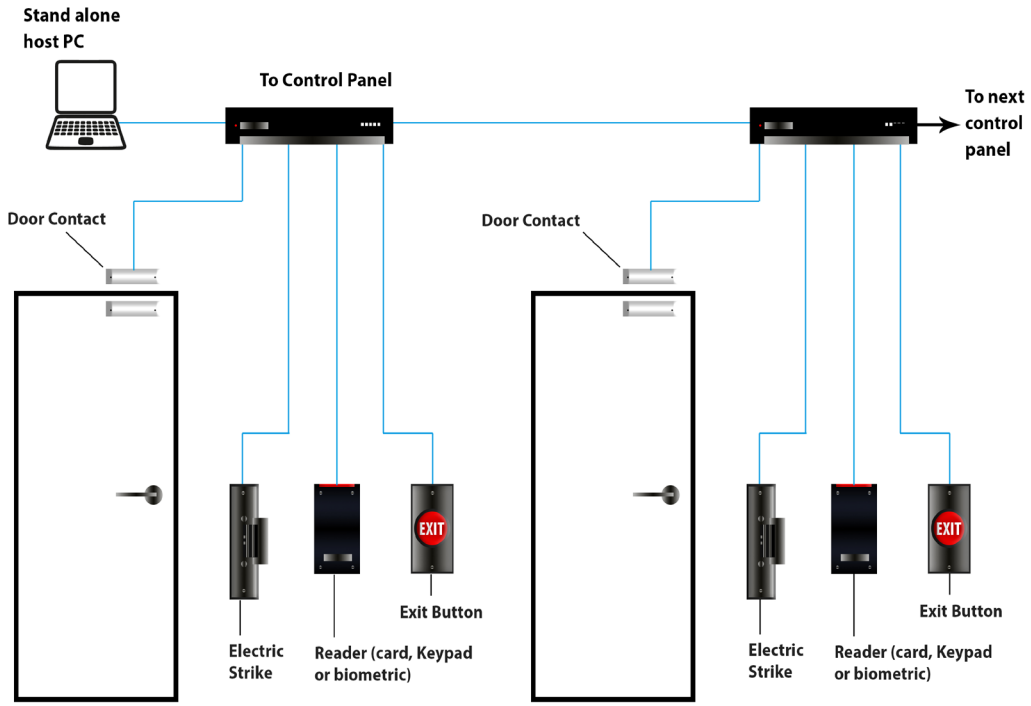
+ Legacy Infrastructure

If you want to expand an existing system, the process can be complicated, as centralised controllers are typically built to accommodate a maximum number of doors, (4, 8 or 16). As a result there are inbuilt limitations to expansion. This coupled with the cabling infrastructure being run in a serial configuration, with localised power requirements, means that upgrading an existing system and adding even a few doors can be expensive.

+ IP Access Control



+ Traditional Access Control



+ End user reluctance to move to network based solutions

End users adopted network based IP video systems over a long period of time. The drivers to this were picture quality, flexibility, storage and the transmission of images. These innovations meant that an end user could have a scalable system with improved image quality on an open platform that provided flexibility of vendor choice.

At the time of writing, these benefits have not appeared across the major ACS vendors and a typical scenario where an end user who is currently using manufacturer A across his estates acquires another site with manufacturer B already installed, means he has to do a complete refit to manufacturer A or make a significant investment in a new overarching control software such as PSIM.

+ Emerging trends in IP based Access Control Systems

The new products coming into the access control sector from new entrants and the younger manufacturer's that don't have enterprise legacy challenges, are negating a number of these issues and are providing new benefits to installers and end users alike, in terms of ease of installation and use, additional functionality and increased flexibility. Efficient scalability 'one door at a time' of an IP based access control system brings down the cost of deployment which greatly assists with an ROI calculation.

These new IP based products impact installers and end users in different ways.

+ Impact of IP based Access control on installers

Network-based Access Control is a simpler way to expand a security system by utilising the existing network cabling. On a new site extra capacity can be added easily as the different cabling topology of an IP based system means the security installer only needs to run cabling to the nearest consolidation point, which in many cases means just a short drop cable to the door.

Since IP networks are now ubiquitous in offices, shops, industry and other facilities, the cost of adding an IP controller is minimal, as opposed to multiple serial connections wired back to a central server.

In addition to this benefit, huge amounts of time and materials can be saved by deploying the use of Power over Ethernet (POE) to power the systems controllers rather than use separate power at the doors.

Furthermore, the traditional type of cabling means that there are several possible points of failure on a typical system that could occur if one or more of the remote units failed. This problem is solved with an IP-based system. Since IP is running over the structured cabling network, the security installer has the peace of mind of knowing that the cabling is certified and therefore proven, before the installation begins.

Finally integration provides another advantage to the installer as the Access Control system can sit on the same network as the BMS and the Video Management System and all can work seamlessly alongside each other, unlike legacy systems which often require a physical interface to communicate.

+ Impact of IP based Access control on End Users

With network-based solutions, the ability to remotely manage a system becomes easier as access control makes the transition from proprietary to open systems, based on international industry standards. We are already seeing a move toward application platform interfaces (API's) which can be used or shared by different manufacturers. New users or credentials can be added instantly to a system from another part of the world under a centralised management function, thereby reducing or eliminating the need for system administrators to be at each site location - reducing costs and increasing the level of security.

Interestingly, at this point, it should be noted the move toward IP based access control systems has already been acknowledged by ONVIF. In 2010, Access Control was added to their scope alongside IP Video, which in the future should enable interoperability amongst different manufacturers.

End users can also benefit from the latest technologies which bring together identity management with video surveillance which ensures the correct physical identities of employees, contractors, suppliers and visitors can be properly authenticated and have the right access to the right areas, for pre specified durations of time. This gives the end user visibility of their site 24/7 and full audit trails of their sites. This is a huge advantage to corporate security people in delivering full compliance and risk management.

Other new technologies that deliver end users advantages include cloud based access control, which has been adopted by some for video and IP to the door, which eliminates the need for control panels at each access point. And a new technology that allows users to manage thousands of readers or IP bridges on a single computer across a widely dispersed network.

+ Conclusions

In conclusion there is an increasing demand for IP based access control systems from both end users and installers alike, as each seek to realise the benefits they have enjoyed from migrating their video systems from CCTV to IP video.

Many of the benefits such as: lower installation costs, flexibility, scalability and open platforms are shared and we will see a trend towards more 'open' ACS solutions that can run on existing networks.

In addition to these benefits, the increasingly larger role that IT departments play in selecting physical security, means that IP based access control systems will inevitably go down the same path as CCTV systems and become more network based in the future.

This means moving access control to IP platforms will bring new and exciting opportunities as installers will begin to appreciate easier installations and increased integration possibilities with other systems.

Furthermore, installers will be free to add access points to their customers systems seamlessly due to the scalability of IP and will become more vendor agnostic as they can choose 'best in class' products from different manufacturers to provide end users with more functionality.

Finally, end-users will be able to take advantage of affordable, flexible, open platform systems that can help them to secure and protect their physical identities and manage access, compliance and risk.

Mayflex UK
Excel House
Junction Six Industrial Park
Electric Avenue
Birmingham B6 7JJ
United Kingdom

Tel +44 (0)121 326 7557
Email sales@mayflex.com
Website www.mayflex.com

Mayflex MEA DMCC
PO Box 293695
Office 11A, Gold Tower
Jumeirah Lakes Towers
Dubai
United Arab Emirates

Tel +971 4 421 4352
Email mesales@mayflex.com
Website www.mayflex.com

Certificate No. FS 547274
Certificate No. EMS 542863
Investor in Customers
CCTV User Group
UserGroup Affiliate Member
FIA Corporate Member
BICSI Corporate Member

All together.

Printed on paper made from 75% recycled fibres.

MF1079_09/18

MAYFLEX
A Sonepar Company