



# HOW CAN IP TECHNOLOGY REVOLUTIONISE ACCESS CONTROL

The use of Internet Protocol (IP) has been a game changer for many security systems. You only have to think about the advancements made in CCTV to see the benefits - principally the ability to monitor and control devices remotely from any internet-enabled location. Mass adoption has also led to improved standardisation and compatibility of systems.

However, the majority of access control systems are yet to make the leap from analogue-based to IP-based installations. There are a number of reasons for this, which will be explored in this paper, but there are also similarities that can be drawn between access control and CCTV to identify the path that needs to be taken to benefit from the latest developments in technology.

## THE BIG PICTURE

The current access control landscape leans towards two scenarios that most businesses will find themselves in. Firstly, there is the single building system that has around 10 doors, to which staff will be given a unique ID pass that will allow them access to specific areas.

Then there are enterprise access systems that usually include larger sites or multiple deployments.

From a hardware perspective, these two deployments will be extremely similar with readers, locks and controllers all being more or less the same. It's at the software level where the enterprise deployment will have more sophisticated functions such as integration with other systems as well as easy scalability.

The crucial similarity though, is that both systems will ultimately be connected to a corporate network via

dedicated cabling to a client machine only. So what's stopping these businesses from going digital?

## STRINGS ATTACHED

Although it has achieved great success in some sectors, IP technology is still relatively new to many in the analogue world and as such there are many legacy systems yet to take advantage of the latest developments.

So what is preventing IP technology from having an impact on access control in the same way that it has for CCTV?

Well, there are several factors and most businesses will be able to strongly identify with one, if not more.

The most common issue will be that legacy access control systems will have been installed that are dependent on each device being hard-wired to a central control system. To further complicate matters, these are often proprietary systems that lock the user to a single vendor.

To expand this problem, centralised controllers are usually limited to the number of access points they can control. This can often lead to an expensive upgrade just to add even a couple of access points.

Of course, the change to IP enabled CCTV didn't happen overnight. One of the key issues that will be encountered during any change will be end user reluctance to adapt to a new system. With CCTV, the benefits of improved picture quality, flexibility, easy storage the ability to quickly share content meant the transition was inevitable. It won't be long until the benefits of IP access control are equally overwhelming.



Thanks to an injection of clever products and great design from new entrants to the access control sector, many of these benefits are now becoming clear. These range from ease of installation and use, extra functionality and flexibility, efficient scalability and lower cost of deployment, which provides great ROI.

#### **IP IMPACT**

Network-based solutions make managing an access control system easier, but also put more power into the hands of users. For example, new users or credentials can be added to a system from anywhere. This removes the need for administrators to visit different locations - reducing costs but increasing the level of security.

IP-based systems also remove the danger of multiple possible points of failure on a typical system that could occur if one or more of the remote units failed. Integration is also simplified as access control systems will be on the same network as CCTV and other systems, rather than legacy systems that often require a dedicated interface.

This upgrade improves identity management and ensures only those with the right credentials will be able to access protected areas, delivering better compliance and risk management.

The fact is that installing a network-based access control system is simple and will save time and resources.

Installation is often straight forward as existing cabling can be utilised and connected to the nearest

**FOR MORE INFORMATION ON  
ACCESS CONTROL AND IP TECHNOLOGY,  
VISIT THE TOUCHSTAR WEBSITE NOW.**

**[www.touchstar-atc.com](http://www.touchstar-atc.com)**

consolidation point. As most businesses, large or small, have IP networks, the cost of adding an IP controller is very small compared to the task of connecting multiple connections to a central server.

#### **CONCLUSION**

As installation cost are lower, there will be little to hold back the implementation of IP access control systems. This will result in many benefits for businesses, including easy scalability, flexibility, improved security and management, open platforms and more.

The improvements also make the system more user-friendly and easier to assign credentials and admin functions, while IT departments can remain confident that overall security is tight and all details are logged and easily shareable.

What's more, access points will be able to be added without issue as new systems will become vendor agnostic, allowing businesses to choose the best solution as they see fit rather than relying on legacy systems.

