WHITE PAPER

IP opens doors to a new world of physical access control

AXIS COMMUNICATIONS

Table of contents

1. A revolution at the door

It is no exaggeration to say that network video has revolutionized the world of CCTV. Now the access control industry is on the verge of a similar, groundbreaking development. Once again, the driving force is the transition to TCP/IP-based systems.
Since the introduction of the first network camera by Axis Communications in 1996, digital network video surveillance systems have developed fast and now delivers a wide variety of advanced features that never could have been be attained by solely relying on analog technology. Today, distributors, integrators and, not the least, end users have come to expect a wide range of useful functionalities, such as remote accessibility, high image quality, event management and intelligent video capabilities along with easy integration, better scalability, greater flexibility and cost-effectiveness.

IP versus traditional access control

The migration of access control systems to a digital environment is sure to bring many comparable benefits, i.e. lowering installation costs, facilitating configuration and management, while simultaneously enhancing the versatility of the systems and opening up for integration with other security products.

Of course, IP-technology is not totally unknown to or unused in the access control industry. But existing systems have not been able to fully exploit the advantages of IP.

Typically, a legacy access control system is dependent on having each device – card reader, handle, door lock, door position switch, etc. – hard wired with RS-485 cable into one central unit or central server. Besides being proprietary systems, which confines the end user to one single provider of hardware and software, these solutions often tend to be very complex and require expert personnel to handle installation and configuration.

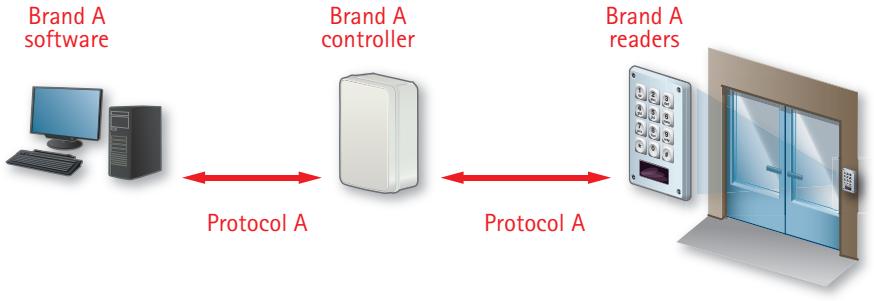

Fig 1. A typical legacy access control system built around a proprietary technology from one single supplier.

Further more, when expanding traditional analog systems the process is complicated by the need to consider that a typical central controller is built to accommodate a certain maximum number of doors, normally 4, 8, 16 or 32. Not only does this limitation make the system inflexible but also makes it difficult for the end user to match his requirements with products available, e. g. if there is a want for access control at, say, 9 or 17 doors. The lack of flexibility also brings high marginal costs, which can make the addition of one extra door unjustifiably expensive.

2. Small basic systems

All in all, conventional access control products and systems are normally designed and optimized for large installations with a lot of doors and maybe thousands of credentials (cardholders). The actual market looks very different. According to Sales & Security Integrator gold report (2013), the average installation consists of 10 doors and have about 128 credentials. Only about 20% of the installations have more than 10 doors.

Without the need for hard wiring to a central control unit or central server, IP-based systems enable installations that are non-proprietary, flexible and scalable. This means not only a more versatile solution, but also a more cost efficient one. Freed from the constraints of enlarging the system in certain multiples, a network-based system can - should it be necessary - be enlarged by one door, and one reader, at the time.

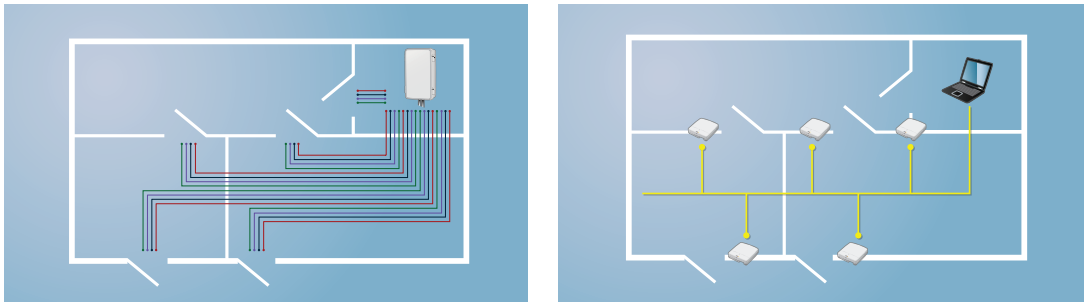

Fig 2a. Traditional installation with one central unit and proprietary cabling to the accessories at the door.
Fig 2b. IP Solution with network switch. AXIS A1001 Network Door controllers are placed at each door with cabling to door accessories.

Furthermore, TCP/IP enables "edge" solutions. An edge solution has one controller for each door, which then is connected to the existing local Ethernet through a regular network switch. Since IP networks now are ubiquitous in offices, stores, factory plants and similar facilities the cost of adding an IP-based door controller would be minimal, as opposed to multiple serial connections wired back to a central server. Cabling work can be even further facilitated. By employing a PoE (Power over Ethernet) supported controller at each door, the need for separate power cables for door equipment such as locks and readers can be eliminated. This reduces the total installation cost. In addition, support for Uninterruptible Power Supply (UPS) makes it possible to avoid having battery back-up for door equipment.

3. Large and more advanced systems

The transition to IP-based solutions will make implementation of access control systems far more attractive. It will also resolve many of limitations of existing traditional systems, and bring additional functionalities that go far beyond conventional door control. Integration with video is one example of a very common requirement which will be much easier to meet with IP-based solutions. In fact, a common, standardized digital environment has the potential to create countless opportunities to integrate other systems such as intrusion detection, fire detection, and so on into uniform, manageable and user-friendly systems

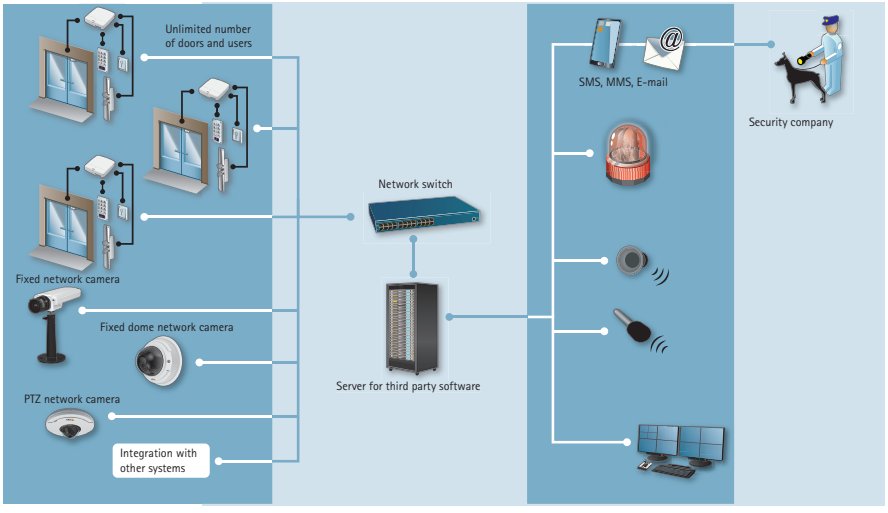

Fig 3. A schematic view of possible integrations between an access control system and a network video surveillance system and other IP-based third party applications. Note that also management functions can be distributed.

High security requirements do not make the system less manageable. On the contrary, IP-based access control systems enable remote management, which clearly is an advantage on very large or dispersed sites. This ability also makes it easier and simpler to configure, test and verify a whole new or partly new system, as adjustments can be made from the closest network connection.

Deploying systems – regardless of their size – is therefore quicker and less labor-intensive than installing a corresponding analog system.

The distributed "intelligence" of such a system makes it less vulnerable to power shortages and network failures. Uninterruptible Power Supply (UPS) and local buffering of events in combination with encrypted communication contribute to the highest degree of reliability and security.

4. Benefits of standards

Very much like in the video surveillance market a shift into IP in the access control industry will surely also mean a transition from proprietary systems to open solutions. And these solutions will most likely be based on international industry standards.

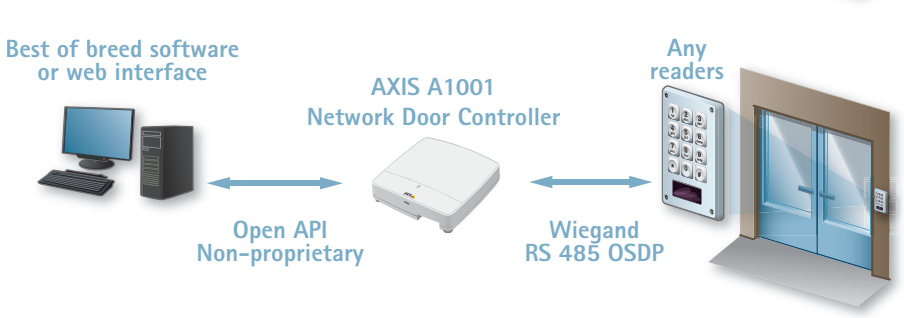

Fig 4. An example of a non-proprietary access control system.

Open solutions and standardized interfaces are a prerequisite in any industry that want to establish their own equivalent of "plug-and-play". There are many gains from such development also in access control. It will allow end users to freely pick and choose between components – reader, door controller and software – that best satisfy their needs and preferences. This freedom of choice makes the system future-proof and means the end user no longer has to rely on a single brand or supplier. Equally important, it can also enable integration with other security related systems and third party applications, without the need for costly hardware boxes to make the "bridge" between the different systems.

In the network security systems market there is already a clear trend to develop open or standardized application platform interfaces (APIs), which can be used by all competing market participants on fair, reasonable and non-discriminatory terms. Naturally, this will increase supply and promote competition and bring a new level of innovation to the industry, while simultaneously making it even easier for end users, system integrators, consultants, manufacturers and others to take advantage of the different possibilities offered by network solutions.

For example, the Open Network Video Interface Forum (ONVIF), which is a global and open industry standards body with the goal to facilitate the development and use of IP-based security products, announced in 2010 an extension of the organization's scope of standardization to cover physical access control. Ideally, access control devices from manufacturers that comply with the ONVIF standards will in the near future interoperate effortlessly and seamlessly with each other, as well as with other video surveillance products and systems conformant with the standard.

5. New business opportunities

Making access control systems based on TCP/IP will bring new and exiting business opportunities. Integrators will, for instance, appreciate the easy installation and the possibility to integrate access control with other systems. Distributors will find new markets and new customers when they are free to bundle different components from different manufacturers to create useful and attractive business offers. And end customers, finally, can take advantage of an affordable, yet flexible, future-proof and adaptable technology that can help to secure and protect valuable assets.

www.axis.com

53812/EN/R1/1309

About Axis Communications

As the market leader in network video, Axis is leading the way to a smarter, safer, more secure world - driving the shift from analog to digital video surveillance. Offering network video solutions for professional installations, Axis' products and solutions are based on an innovative, open technology platform.

Axis has more than 1,400 dedicated employees in 40 locations around the world and cooperates with partners covering 179 countries. Founded in 1984, Axis is a Sweden-based IT company listed on NASDAQ OMX Stockholm under the ticker AXIS. For more information about Axis, please visit our website www.axis.com.

AXIS COMMUNICATIONS