The Future of Access Control

Your Essential Guide to Advances in Access Control and Integrated Systems

Mike Sussman
Engineering and Operations Director

Issue 1.1_08/2012
Copyright © 2012 Time and Data Systems International Limited
## Contents

1. Introduction ................................................................................. 3
2. State of the Industry ................................................................... 3
3. Reader Technology ..................................................................... 4
4. Controllers ................................................................................ 5
5. Which Security Credential to Use ............................................ 6
6. Energy Saving ............................................................................ 7
7. The Role of Software .................................................................. 7
8. Cloud-Based Solutions ............................................................... 7
9. Integration and PSIM ................................................................. 7
10. Industry Standards .................................................................. 7
11. Seeing the Bigger Picture ......................................................... 7
1 Introduction

Traditionally the Access Control industry has been fairly stable in its use of technology, but advances in the IP world coupled with new credential technologies, such as NFC and Biometrics, are seeing the industry slowly evolving.

Increasingly IT departments are becoming more involved in security and integration with IT systems, along with Cloud Computing, will bring some exciting challenges in the times ahead.

With a new IEC Access Control standard currently being developed and PSIM (Physical Security Information Management) appearing in almost every article you read on integration, the industry is now beginning to wake up and take note that it needs to catch up with other facilities management technologies such as CCTV and VOIP.

Now is the time for change.

This paper looks at the potential changes that will occur within the industry over the coming years and how these can advantageous in providing higher levels of security and even greater value for money.

2 The State of the Industry

An obvious question to ask is: ‘Is Access Control stagnant or evolving?’ If you look at the Access Control industry and the technology in use, some areas are largely stagnant and have been for many years - for example the Wiegand de facto standard interface between readers and controllers. The industry has been, until recently, reticent about change and a great deal of the equipment that is commonplace today has been available for a number of years. This trend is similar to that traditionally seen in the intruder and fire industry, which has also only seen significant changes in the last few years. Whilst many Access Control systems can be considered ‘fit and forget’ and may last in excess of 15 years, the next few years will see some exciting innovations being launched and presented to the industry.

These changes, which are occurring in both the reader and credential arena (along with the control panels and software), can bring significant benefits to the installer, systems integrator and end user. With the introduction of IP systems and the growing acceptance of them, IT managers are taking more of an interest in the physical security market. In a number of industries, the IT Manager is taking overall control and the security manager’s role may not even exist anymore. The integration between the physical and IT/logical security systems has also increased the role of the IT department within this arena.

The Access Control industry is probably in the position that the CCTV and telecoms industry was five years ago. But will the speed of change match this? Only time will tell. But with the current unsettled political climate and the seemingly ever-present potential for terrorist attacks, security on all levels is only going to increase as time goes on.
3 Reader Technology

Within the Access Control reader market there is little sign of movement with the traditional readers, such as MIFARE and Proximity, which are still very much the main market leaders. However there is a trend towards multi-technology readers and the new entrant is NFC (Near Field Communications); which takes advantage of the mobile phone as a security credential.

Biometric systems are providing the biggest growth sector. There is increasingly widespread acceptance of Biometric readers, which is due to both a change in user perception coupled with increased usability and significant cost reductions. Fingerprint technology is still the main biometric reader method, however facial recognition is growing in popularity, especially in areas where non-contact is required - including sanitised healthcare areas or situations where the environment can affect the condition of user’s hands, such as the construction industry for example.

Biometrics will continue to increase in popularity and with the growing reliability and usability of facial recognition, coupled with the advances in the CCTV world, it won’t be long before these two combine to provide facial recognition as standard from your CCTV system. This will mark a significant change and will increase security greatly. Whilst we may never employ the in-depth methods of ‘CSI’ (and the use of garments such as hooded tops and baseball caps will always impact on reliability), within the corporate environment it will be highly effective and promises to reduce end user cost even further.

One of the new trends is soft biometrics which utilises human descriptions of a subject’s physical appearance. The concept is to be able to recognise individuals based upon a number of physical traits and if you couple this with CCTV this will be an exciting growth area in the coming years.

4 Controllers

Whilst the traditional RS485 communications model still exists, this is quickly being replaced with IP systems which have a number of advantages over the serial methods - not only in the speed of communications but also the ability to quickly interrogate and control the system remotely as well. With Access Control and other systems following the intruder model of remote monitoring, IP adds the advantage of remote diagnostics presented in a more user-friendly manner.

Nearly all new systems are being installed using IP and PoE (Power over Ethernet), which is becoming popular as it saves the cost of running power sockets to every door. The use of POE+ (which provides up to 25.5 watts of power) has the capability to drive locks and this technology and the standards it provides will see the available current increase over the coming years. The latest devices are providing up to 75W through a single CAT5 cable which easily powers a controller and the locks.
With the move towards IT taking control and being involved in physical security, rack based systems will become popular, residing in the same cabinets as the network switches. The drive by IT for diagnostics and customers for any savings they can make is driving integration between Access Control and other security and non-security systems.

5 Which Security Credentials to use?

Whilst there isn’t a great degree of change in the traditional card market, the biggest movement in security credentials is the introduction of NFC (Near Field Communications) on smartphones. This has largely been borne from the acknowledgement that for many people there is no need to carry a separate credential when you always have your mobile with you. This is fine until you realise that you need extra authentication to ensure that the phone as a security credential itself is secure. Whilst PIN is the obvious choice, facial recognition will undoubtedly become standard as an authentication method on phones of the future. Whilst already available in laptops and tablets (and emerging on cutting-edge smartphones) we will see this as commonplace in the next generation of mobile phones.

As already mentioned, biometrics is increasingly commonplace in Access Control readers, but it is growing in acceptance for other authorisation needs as well. Whilst some biometrics systems are better than others, the rate of development promises that the majority of issues that currently effect performance will disappear over the coming years.

Wireless systems are also becoming popular for certain applications, most notably the hotel-type remote door locking systems. However wireless still has to overcome some fundamental issues of connectivity signal. Whilst some of these issues can be mitigated, the basic physics related to radio waves can never be overcome and physical walls will always be a potential problem.

Increasingly though, this connectivity problem doesn’t apply when you look at connectivity for mobile workers. In this arena 3G, WIFI and the forthcoming 4G networks are making it an exciting time to use mobile phones and tablets for remote information access.

6 Energy Saving

Almost every shape and size of organisation is concerned with energy usage and reducing CO2 emissions, from both a cost perspective but also from a corporate environmental responsibility perspective. Switch mode power supplies can make huge savings and with savings of £50 per controller, even a simple 10 door system can save you money which can be better utilised within the business.

This, coupled with energy saving readers to control lighting and intelligent PoE switches that can even turn off specific PoE powered controllers at certain times of the day, can pay dividends. Integration is playing a key part here, with links to control Building Management Systems and lighting systems based upon occupancy.
7 The role of Software

The software aspects of intelligent Access Control systems are also evolving. Whilst we aren’t seeing radical changes, a large proportion of new systems come with embedded software, making remote configuration a lot easier. This enables installers to spend less time on site and allows configuration to be actioned when the customer is off site, thereby minimising disruption.

The downside however is that it can be harder to manage the complete system, especially when a large number of controllers are involved - although this does depend upon the software system chosen.

There is also a trend towards splitting the software and its installation and management between separate interested parties. On the one hand you have the installers and on the other the operational staff. Operationally, exception management and reporting are crucial facets and well-designed, simple to use user interfaces are the key to effectively handling an incident.

The biggest change that is starting to happen in the software aspect of Access Control is hosted systems. Growing numbers of providers are delivering Access Control as a service offering to the end user, thereby minimising server purchase and maintenance and all of the usual patches and upgrade responsibilities that go with this.

8 Cloud-Based Solutions

One of the biggest changes that is happening in the Access Control industry is SaaS (Software as a Service), or as it is often referred to ‘The Cloud’. So what is The Cloud? Microsoft® defines it as an approach to computing that’s about Internet scale and connecting to a variety of devices and endpoints. Essentially it involves hosting some or most (or in some cases all) of your IT services remotely and accessing them through an Internet connection. Some people are reticent when you start talking about The Cloud relating to security; however we all use The Cloud now in some form. Applications such as Skype, Amazon, Skydrive storage and internet banking can all be considered Cloud Computing – many of us already trust The Cloud with our personal information and our money!

So why use Cloud based systems? Firstly it doesn’t require the end user to purchase costly hardware and IT teams to maintain it. There isn’t the hassle of keeping the servers updated, installing software updates or new features. The Cloud also provides the scalability and flexibility that organisations require. If you expand your business or acquire another business you can just expand your SaaS offering to suit.

Many customers are already turning towards the Cloud, as it provides reduced costs both in hardware and resources. The SaaS offering is agile and provides the flexibility when
required. The infrastructure and system is highly automated and simple to install. Disaster recovery is standard within the service providers and this is an area that many businesses, except perhaps large corporations, often fail to implement at the moment. Overall it provides increased end user productivity - you can run your business and reply upon experts to ensure the systems remain reliably operational.

The biggest issue moving forward with the Cloud for Access Control is the ISP backbone and any SLAs that will be required. Whilst the control system will remain autonomous, remote actions and any changes will not occur if the ADSL link between the site and the Cloud system is down. Whilst this downtime is reducing and ISPs are increasing their availability figures, we are unlikely to ever see a guaranteed 100% uptime. If this is a critical matter (and in relation to Access Control and security it probably will be) then dual ISP links can be provided which help to overcome this issue.

VSaaS (Video Surveillance as a Service) has similar issues with regards to the potential disruption of the Internet connection and in this field localised storage can also offer acceptable levels of resilience to overcome any potential downtime in the main link.

For those that want to look at savings now, rather than waiting for Cloud based solutions, then virtualisation is a potential way to go. This allows multiple applications to be spread across virtual platforms all on one physical server. The convergence of physical security with the IT department is driving this forward and this can provide significant power savings for the end user.

9 Integration and PSIM

Access Control software has been typically reactive in its use in the past. Predominately used to configure the systems, aspects such as reporting and alerting weren’t the main driver. Nowadays a more risk-based approach to software is being taken to align it with the way that operational security teams function and to take advantage of the benefits of greater control and reporting. This risk-based approach is prevalent in Middle East markets and is beginning to become more prevalent in the UK and other EMEA countries. Access Control software nowadays needs to provide a holistic view of all systems, both security and non-security related. The realisation of true PSIM (Physical Security Information Management) systems is addressing this need and providing a multitude of benefits.

A PSIM system brings together the physical security system with the automation and intelligence that computing provides. By correlating and analysing the data from disparate systems and applying logic, whether true or fuzzy, potential situations can be identified quickly and presented in a meaningful manner to the operational staff. As the PSIM collects data from non-security related systems as well, trends can be spotted which can not only improve security but also efficiency within the business.

Once a situation has been identified this is presented in a clear manner to the team along with standard operating procedures to follow. This ensures that all members of the team are
adopting the same process and look for any improvements in the process that might help in the future.

10 Industry Standards

Currently the Access Control industry isn’t as regulated in the same way that the intruder and fire industries are. Within Europe the existing EN 50133 standard has been around for a while and isn’t used by everyone because technology has moved on so rapidly. There is, however a new IEC standard which started development about 18 months ago and is currently out for parallel voting. As is usual with a lot of standards when in development, there are some good points and some contentious points. It is refreshing though to see a new standard being developed at the global level and what is encouraging is the speed at which this standard has evolved.

11 Seeing the Bigger Picture

Taking a broad view there are a number of Access Control trends that are emerging. There is definitely a shift to IP based systems and a growing requirement for POE systems, especially from the IT orientated end of the market.

There is a marked convergence of physical security and IT security, both from a management perspective but also from an integration perspective - with closer interoperability between access control and logical IT.

NFC and biometrics will become the main credentials for authentication in the years to come. However, it will be some time before the standard card credentials disappear from product ranges.

The biggest shift though is the move to the SaaS model with cloud based solutions designed to provide the operational intelligence to analyse data and identify potential situations from the myriad of data that they consume.

Overall, there are some exciting challenges ahead for both manufacturers and integrators and all of this will benefit the end user not only within the security field but also energy savings and operational efficiency gains as well.