ASSA ABLOY

White Paper

Smart Infrastructure Integration and Access Control

ABLOY®

The global leader in
door opening solutions

Introduction

From the wheel to the World Wide Web, the way we live and work has always been shaped by advances in technology. One of the most exciting and revolutionary trends currently making its mark is the growth of connectivity, microelectronics and the so-called 'Internet of Things'.

The impact of this technology is already being felt in sectors ranging from home appliances to entertainment, but one of the areas with the greatest potential to be transformed is security and access control.

Innovative software and cutting-edge hardware can combine to create keys and locks designed to match an organisation's specific needs. Access rights can be issued, denied and monitored in real time with no need for wires or power, offering the very best in both flexibility and security.

More than this, access technology is increasingly forming part of a greater, fully integrated infrastructure system that links every aspect of a building together. Heating and lighting controls can be set to activate in areas where staff are working, or stock control systems linked to key fobs and storeroom locks. Building management systems (BMS) already do this but integrating into access control adds health and safety benefits as well as security.

Successfully integrating our digital automation and control systems, smart devices and data analytics with our physical infrastructure can offer exciting opportunities for businesses, communities and governments. Next-generation Smart Integrated Infrastructure (SII) offers new prospects for effectively managing the way we live, work and grow, whilst remaining safe and secure.

In this report we explore how organisations in all sectors can take advantage of cutting-edge security and access controls, and how they can link into a wider connected ecosystem, to deliver operational efficiencies to potentially under-resourced businesses.

The Technology of Now

For many consumers and businesses, technology based around the Internet of Things still seems futuristic and distant. However, research predicts that business-to-business spending on IoT technologies, apps, SaaS solutions will reach €250 billion by 2020, and this is expected to keep growing by around 20% each year.

Indeed, there are many game-changing systems out there already, demonstrating that they are both effective and robust. In the access control environment, one of the leading examples of this is CLIQ® technology from Abloy UK.

This wire free system (PACS) allows individual keys to be programmed and updated to provide access to specific areas at specific times and dates. When the system administrator or automated decision making process integrated with HR changes an employee's access rights, the employee can update their key using a smartphone, allowing them to control security and compliances at remote sites or facilities.

Furthermore, advances in system-level architecture allows PROTEC2 CLIQ to be integrated with wider (PIAM)[2] controls and networks such as inventory management, health and safety, permit to work (P2W), HR, contractor operator licensing, training and site induction protocols[2].

According to the British Royal Academy of Engineers, the number of connected devices may be as high as 50 billion by 2020.

[2]PIAM Physical identity and access management.

Integrating Infrastructure

One of the most important things to acknowledge from the rise of integrated systems is the vital nature of useful information.

In all modern businesses data is key but most businesses could be referred to as "DRIP'S" - Data Rich and Information Poor - and therefore don't use the data as it's too complicated and time consuming to analyse.

In the most successful systems, the flow of data shouldn't just go one way. While information from BMS and maintenance can inform access controls, the data generated from doors and locks can also be used to inform other systems, highlighting anomalies which are much easier to analyse and therefore automate logical actions, including managing access rights.

The logs and audit trails provided by systems like CLIQ can be exported and analysed, providing invaluable information on how employees and contractors are operating and their whereabouts.

Knowing how often and at what times certain areas or equipment is accessed can allow management to streamline processes, spot trends, boost synergies and deliver operational efficiency. It can also allow human resources specialists to check on employee activity and ensure that staff fatigue is also managed.

What is Smart Integrated Infrastructure (SII)?
The point where physical infrastructure meets with digital communications and data analytics, unlocking system-wide synergies.

Managing Success

When we think of integrated building systems we naturally think of them tying together pieces of physical equipment, such as lighting or heating. However, the benefits start to deliver when they are linked into all manner of databases and information sources that improve security, operational efficiency and health and safety compliance.

For example, an access control system can be linked to a database of employee work permits. When the employee attempts to use their CLIQ key to open the lock to a work site, it can check to see if they have the necessary permissions in place, including competencies to carry out the work.

Similarly, it can be used to restrict access to restricted areas depending upon the employee's current competencies, assigned task or clearance level.

The Keys to Unlock SII

- Pervasive, reliable wireless coverage
- Miniaturisation of processors, allowing all devices to become smart
- Abundant, cheap and reliable cloud storage and computing
- Access to wide data streams
- Agile, modern application development and intuitive user designs
- The use of the latest AES encryption
- SaaS
- Multi-Tenancy and Scalability
- Automation and Integration

Smart and Secure

One of the challenges faced by innovators of integrated IoT technology is that of security. Connecting a system to the wider internet creates another potential access point for criminals and vandals to try and break.

Naturally this is a concern for all systems, but it is of particular importance for access control technology. This means that all smart access control systems need to not only be physically secure, but also highly resistant to cyber-attacks.

There are several ways to increase the security of the system, but some of the most important are:

- Ensuring that data transfers between the different parts of the system are strongly encrypted, using a minimum of 3DES but preferably AES so even if the information is intercepted the wider network remains secure.
- Automatically creating and maintaining a detailed, reliable audit trail of which keys have been used to access which locks, providing comprehensive traceability.
- Make sure that lost or stolen keys can easily and quickly have all access rights denied.
- Hosting data associated with the system securely, potentially by using a highly trusted third party so that it is not stored on-site.
- Ensuring that the mechanical security is just as strong as the electronic system, with reliable cylinders and the latest patented lock technology.
- Use of three factor authentication i.e. "something you have and something you know"
- Automation of on-boarding and off-boarding processes to ensure credentials are active and inactive seamlessly in line with business needs.
- Integration with existing applications ensuring minimum access is required – access where you need it when you need it rather than everywhere you might one day need it.

Conclusion

It's hard to see when the next "big thing" will become the current standard, but when it becomes clear that a major shift is on the way the winners are always those who understand, adapt and adopt technology early on.

Whether you refer to it as the Internet of Things, Smart Systems Integration or intelligent buildings, our networks and equipment is going to become increasingly linked. Access control is one of the areas with the greatest potential to not only benefit itself, but to help other areas of infrastructure become more operationally efficient and streamlined.

The technology needed to achieve this is already out there, proving its reliability and effectiveness every day. The possibilities it offers right now are huge, but so can be the risks – so it's crucial that as the integration of systems increases, the protection of those systems and the data contained is vital.

About

Abloy UK is the UK's leading expert on high security quality door locking and functionality.

Its product range includes electric locking, cylinder, padlocks, door operators and more. Together, the solutions offer secure, compliant and lasting solutions trusted by organisations throughout the UK, Ireland and worldwide, across a variety of industries – wherever compromise is not an option.

Abloy has the capability to offer you a complete security solution; from initial surveys and fact finding, to assessments, problem solving and planning through to specification.

All Abloy staff are friendly, fully engaged and willing to put in that extra commitment to find the correct solution to suit your needs.

Abloy UK are the UK's leading experts on high quality door locking and functionality.

abloy.co.uk

Abloy UK
Portobello Works
School Street, Willenhall
West Midlands WV13 3PW

+44 (0)1902 364500