Whitepaper:

Boosting efficiency and streamlining security with an integrated access control solution

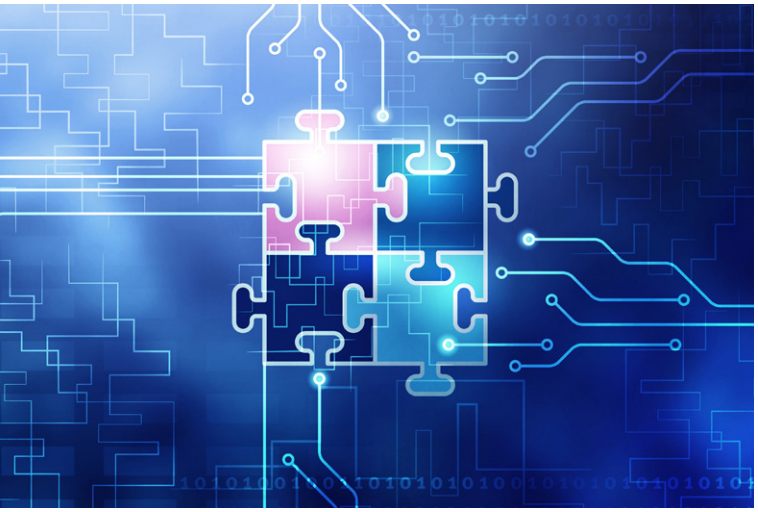
A whitepaper from IFSEC Global and ASSA ABLOY Opening Solutions EMEIA

IFSEC GLOBAL | ASSA ABLOY Opening Solutions

IFSEC GLOBAL

ASSA ABLOY
Opening Solutions

Contents



Introduction

Integration. Integrated systems. Integrators. Interoperability. Connected buildings.

No doubt anyone involved in security, facilities or building management recognises at least one of these terms. Or more likely, reads one of these phrases in industry publications and vendor marketing materials on a weekly basis. In a world where technology and innovation continue to receive plentiful investment, integrated systems are becoming a cornerstone of future development plans.

Secure access management has not been left untouched by the move towards integration. Indeed, access control systems are often viewed as the starting point for a building to shift from operating in separate siloes, towards a more functional, connected and 'integrated' building management system. Technology which provides a facility with data on occupancy levels at any given place, at any given time, enables other systems to respond in tandem, such as lighting, HVAC and power management systems.

Connected systems also provide the security team with a more secure and manageable site. When disparate access, intruder and CCTV systems work together, benefits can be myriad – from reduced false alarms through to the efficiencies created by a centralised platform which all devices are feeding data into.

And, while an integrated system doesn't automatically create a 'smart building', a more intelligent building can't function and provide the necessary data feedback without it.

This whitepaper from **IFSEC Global** and **ASSA ABLOY Opening Solutions EMEIA** aims to assess the growth of integration in security, why demand is growing from end-users and security managers, and why access control systems are considered such an important link in the chain. We speak exclusively to a security systems integrator from **Securitas**, to understand the view of those installing and implementing these systems, and provide interesting case studies for real-world context where ASSA ABLOY's access control solutions have been a foundational part of an integration project.

About ASSA ABLOY Opening Solutions

ASSA ABLOY Opening Solutions leads the development within door openings and products for access solutions in homes, businesses and institutions. Its offering includes doors, door and window hardware, locks, access control and service.

Integration and the central role of access control – A growing trend

In the 2021 **Wireless Access Control Report**, 95% of the 400 respondents cited system integration with other building/security management functions to either be 'somewhat' or 'very' important to their choice of access control system.[1] Vendors have been marketing the benefits of integrated security systems for some time of course, but there now appears to be genuine desire from end-users, such as building and facilities managers, for systems to 'talk to' and connect with each other.

We're not just witnessing this desire in the commercial sector, either. One only needs to look at some of the most popular tech products on the market to recognise that homeowners and consumers are on the lookout for 'smart' devices. A key selling point for these products? Interconnectivity and the ability to 'talk' to other systems, such as Amazon's Alexa or Google's Nest for the smart home environment.

Some believe demand has been accelerated by the COVID-19 pandemic. A greater emphasis on reducing touchpoints and occupancy levels to a minimum has enticed systems integrators to provide new 'frictionless' solutions for end-users. Entrance systems to buildings and offices using cards or mobile devices can be connected to a facial recognition system, for instance, to reduce the requirements for additional security personnel to be present.

Others argue that a move towards integration was taking place already, and that COVID has had little impact. Whatever the case may be, the desire for open, interoperable systems that connect to each other is a trend that's here to stay.

We will take a closer look at the benefits and the reasons behind this in the next chapter, but let's first explore what we mean by 'integration'.

Integration systems – a 'catch all' term?

The term 'integration' in security may refer to several processes and can consequently be somewhat unclear as to its exact definition. Whatever the context, the underlying aim is for disparate systems – be it access control or CCTV – to connect and share data with each other, to create more intelligent and detailed feedback and more streamlined operations.

[1] Wireless Access Control Report, https://www.ifsecglobal.com/resources/wireless-access-control-report-2021/

It can refer to:

- The process of combining two or several different systems or devices into one centralised platform (such as a physical security information management system – PSIM)
- The process of two disparate systems or devices speaking to each other to initiate a required action (such as an ANPR camera identifying an approved vehicle, which then informs the access control barrier to grant access)
- The process of integrating software and hardware solutions together (such as wireless access control hardware devices connecting with a software management system)

Among security professionals, there is growing demand for physical security devices to integrate with each other, and we are seeing regular examples of video surveillance, access control and intruder alarm systems integrating with each other for the benefit of the security teams managing them.

Integrated buildings go further than simply connecting disparate physical security systems together, however. A key driver behind the demand for open platforms and common APIs is the ability to connect with devices outside of the security sphere. This is particularly relevant for access control, where HVAC, lighting and electrical systems may switch themselves on only if the access system is activated by a member of staff or visitor. For instance, meeting rooms only require power when occupants swipe their card for access, supporting organisations and buildings to meet sustainability and efficiency goals.

Crucially, proponents of connected systems stress that any device with which users require integration should be designed on an open, interoperable platform. Standards such as ONVIF promote common protocols for devices and systems from different manufacturers to seamlessly integrate with each other and make it easier for installers and end-users to manage. Indeed, 92% of security and building management professionals consider open architecture, designed for interoperability with similar technologies or products, to be either 'somewhat' or 'very' important.[2]

[2] Wireless Access Control Report, https://www.ifsecglobal.com/resources/wireless-access-control-report-2021/

The recent integration between Genetec's Security Center and CLIQ intelligent key-operated electronic locks from ASSA ABLOY Opening Solutions is a good example of investment which vendors themselves are making in ready-made integrated security technology.

CLIQ and Security Center are now said to work seamlessly together, enabling Genetec software users to broaden access control capability, administer locking more efficiently, and better protect premises from increasingly sophisticated and diverse threats.

Any organisation using Genetec Security Center 5.7 can now deploy CLIQ key-operated wireless locks and padlocks at their premises. Integration via CLIQ Web Manager software extends the access control possibilities of Security Center, enabling programming of CLIQ's battery powered keys with fine-grained access rules – all from a single, familiar interface.

> ***Intelligent keys give customers the ability to expand their access control and management beyond the physical network while maintaining the Genetec unified experience and auditing capabilities,"*** explains
>
> **Jean Philippe Deby, *Business Development Director EMEA at Genetec.***

Integration – Opportunities and challenges

Advocates of integrated systems argue that physical security system siloes are on the way out, as building or site management is becoming more like an ecosystem of interrelated functions, all of which communicate with one another to boost efficiency, while crucially improving security processes. Despite this, deeper integration of building systems is still at the planning or 'wishlist' stage for many companies. On a macro level, the desire for it remains unfulfilled. Why?

Cost and concerns over return on investment were cited as the most common reasons, in our 2021 survey, for failing to upgrade to a more interconnected system. These are answers to be expected for most decisions about investment.[3] Over a quarter of respondents (27%) to the same survey suggest a lack of available solutions developed to compatible standards – though this is a problem many vendors, such as ASSA ABLOY, are overcoming, as the market witnesses an increasing number of open platform, interoperable systems and devices. This migration from proprietary technology to open architecture has likely come as a response to the demand for flexibility from end-users, consultants and systems integrators alike.

Aside from cost, the complexities and understanding of integrated solutions are also said to hold organisations back from adoption. While many large installer businesses have been investing in integration experts and departments for some time, smaller companies may not have the resources or time to develop or hire the networking and programming expertise that connecting disparate systems requires.

Despite these barriers, there is little doubt that the wind is firmly in the sails of a shift towards integrated solutions. Security teams and facilities managers can streamline operations and also develop more intelligent processes using the data gathered from internet-connected devices.

One key benefit of integrating disparate security systems is a more streamlined operations workflow. Whereas traditionally, security personnel had to monitor separate access control, video surveillance and intruder alarm programmes, a security integration platform can aggregate and present data across all these domains. Professionals are only required to manage and understand a single application, and software updates can be delivered directly to one platform, rather than several.

[3] Wireless Access Control Report, https://www.ifsecglobal.com/resources/wireless-access-control-report-2021/

For security departments, the integration of physical security systems remains the most desired application. Crucially, access control is central to this process, where interoperability with door entry systems and visitor management in high demand. The appetite for connected video surveillance and access control, in particular, is prominent, with Omdia analysis indicating that over 80% of all integrated access control is at least partially connected to video surveillance systems.[4]

Other proponents have argued for further development with centralised security platforms, highlighting the benefits of 'converged security centres', whereby cyber security, local news and social media feeds are also integrated within the platform. Particularly relevant for larger event venues, transportation centres and critical national infrastructure facilities, such a solution is designed to provide a holistic viewpoint of threats – both physical and cyber.[5]

In our latest Video Surveillance Report from IFSEC Global, we once more explored the topic: 70% of installers, consultants, distributors and vendors agreed they were witnessing increased demand for integrated solutions from end-users and customers in the past 12-18 months.[6]

Aside from the demand for connected physical security systems we've already discussed, many respondents also highlighted integrated building management processes as important, including fire and smoke systems (43%), lighting (25%), HVAC systems (19%), and audio-based systems (17%). Once again, participants underlined the importance of access control as part of this process.

[4] Omdia, Access Control Intelligence Service, **https://www.ifsecglobal.com/resources/wireless-access-control-report-2021/**
[5] James Willison, Why the UK should adopt a converged security approach to improving resilience, **https://www.ifsecglobal.com/integrated-security/why-the-uk-should-adopt-a-converged-security-approach-to-improving-resilience/**
[6] IFSEC Global, Video Surveillance Report 2021, **https://www.ifsecglobal.com/resources/the-video-surveillance-report-2021/**

What are the key benefits of integrating hardware and software-based access control solutions?

So, if indeed there is a growing trend towards integrated systems, why is this? And in particular for end-users, such as security directors/managers, building and facilities staff, why should they be thinking about connecting disparate systems? We've already touched on some of the benefits of integrating siloed devices, such as access and video surveillance, but what about software and hardware integrations within access control systems themselves? How can this assist end-users? Our four-point list explains more...

1. Support employee efficiency because administrators operate a single interface

Integrating software and hardware solutions can significantly improve efficiencies for daily access management tasks. Whether cloud-based or on-premise, a software platform designed to manage all of a site's existing access points enables regular access management activities to be undertaken in one solution. Credentials can be updated or terminated instantly, access can be given to visitors, and new electronic locks and reader devices can be added or withdrawn via a few simple clicks.

Staff efficiency and system maintenance also becomes easier, with only a single interface to train employees on. New starters aren't required to understand several different systems, meaning they can be given focused training sessions on the interface and quickly get up to speed on how the access management system works.

"Our key-based access system CLIQ offers two distinct options in supporting improved employee efficiency," says Russell Wagstaff, Platform Director, at ASSA ABLOY Opening Solutions EMEIA. "CLIQ Web Manager software may be 'plugged in' directly to an existing platform, making electronic key-operated doors one node in an existing control panel. This was the approach we adopted with our recent Genetec Security Center integration."

"Alternatively, the functionality of CLIQ Web Manager itself can now expand. It can become a hub for multiple processes — managing HR, support ticketing, financial reporting and more alongside daily access control tasks, for instance. The more that can be done from a 'single seat', the larger the business process efficiency gains."

2. Improve security by extending access control to more doors and access points

Integrating hardware devices (such as locks, or card and mobile readers) with software systems, creates greater flexibility and scalability opportunities. Software platforms enable wireless locks and readers to be seamlessly added to and removed from an organisation's overall access management process, as the business scales up or down.

Modern hardware devices – battery-powered locks with RFID readers, for instance – with inbuilt APIs from open platform-based vendors are available for hassle-free integration with an array of software systems. Once integrated, organisations can easily extend their portfolio of locks and access points by installing them and adding them to the system, with no additional keys or wiring required.

The risks when cards or keys are lost are also reduced, as credentials can be wiped from the system immediately. Meanwhile, the access management team has full visibility over who has accessed a given area, room or building, improving accountability if an incident were to occur.

"Aperio wireless locking devices can extend almost any existing access system, from any vendor or manufacturer," adds Russell. "They can broaden site security by integrating seamlessly with an existing control panel or software interface."

"It does not matter which manufacturer a customer chooses for their initial access control installation: Aperio battery-powered devices for doors, server racks, cabinets and many more openings extend management's control to upgrade security for building users and assets."

3. Build a more detailed picture of building use and thereby identify improvements

Integrated systems are inherently designed to collect more data, enabling siloed systems to 'speak' to each other. For instance, if an access control mechanism on a room is unlocked, the system may inform power in that room (lights, plugs etc.) to activate. To do this, data is collected and shared, rather than kept in separate siloes – 'locks over here, and lighting over there'.

In operating in this 'joined up' fashion, organisations could assess building occupancy levels, measure how efficiently spaces and power are being used, or identify 'hotspots' of high activity which could create health and safety risks – in a manufacturing or distribution hub, for instance. Integration across security and building systems can support in gathering this data in a more convenient way and provide building managers with a more complete picture of building use, enabling them to identify potential improvements.

"Greater system interoperability and data sharing is essential if we are to realise the full potential of the 'smart' building," says Russell. "Just like a human brain, the more links we make, the more 'synapses' which are firing, the higher the ceiling for building intelligence. Integrated access, security and building systems are a critical step."

4. Realise new cost-saving opportunities by disposing of mechanical keys and wiring

Another benefit of integrating modern electronic access control devices into a security system is that they are often wireless solutions. Key management workload becomes redundant, as devices are linked to a centralised software management system where credentials on users' cards or mobile devices can be updated instantly. Access rights can also be managed, negating the need for certain users holding tens, or hundreds, of keys at any given time, and reducing security breaches when mechanical keys are lost or misplaced.

As the name suggests, going 'wireless' helps organisations to reduce the volume of wires and cables required in their buildings and sites, and therefore have fewer components to install and service. ASSA ABLOY's own research has found that installation costs for wireless access control can be cut by up to 80%, alongside energy use bill reductions of 70%, when measured against comparable wired access solutions.[7] In addition, some wireless locks are built to open standards, for the very purpose of enabling seamless interoperability with security and building management systems from multiple different manufacturers.

"The hard business reality is that so much of what we aim to achieve with security is constrained by cost," says Russell. "Wireless access control enables security managers to add and integrate control at many more access points, inside and outdoors, than would ever be feasible or affordable with cables."

"Wireless devices powered by batteries or energy-harvesting also help a business to reduce the sometimes overlooked cost of powering their security system. Unlike wired magnetic locks, which draw continuously from mains electricity in order to stay secure, a wireless lock only fully 'wakes up' when presented with a credential. Over a lock's full life-cycle, the energy and therefore cost savings from going wireless really add up."

[7] ASSA ABLOY, Wireless security: Cut costs without cutting corners, https://campaigns.assaabloyopeningsolutions.eu/aperio-cost-savings

Integrated access control systems in action

Despite the benefits touted by vendors and analysts, there remains a significant number of organisations that have not started integrating their disparate building systems. Challenges are myriad; many probably remain unsure whether they'll receive genuine returns on investment.

Here, ASSA ABLOY Opening Solutions provides some examples of successful integration upgrade projects incorporating its solutions.

Dutch university benefits from hardware integration

At the InHolland University of Applied Sciences, a rolling project to upgrade access control has been ongoing for several years. More than 500 Aperio wireless door devices are now deployed at seven separate InHolland campuses. All InHolland's electronic locking devices are integrated with the university's Nedap AEOS access system.

With a single credential, users can unlock all authorised openings managed by the AEOS system, whether wired or Aperio-protected doors.

Cost savings were also made, as the operating cost of running battery-powered wireless locks is said to be much lower than for equivalent wired locks.[8]

Fitting Aperio wireless escutcheons and locks to critical doors ensures university staff, students, visitors and confidential information are safe without impacting site accessibility. Authorised users open relevant secure doors conveniently with a programmable RFID credential. Credentials can be changed by building managers, with the ability to regularly reconfigure user status as needs and usage evolves around the multi-site campus and university facilities.

Based on its experience, InHolland is already planning for the future. A new university site in Amsterdam will become a smart building and will require access control able to integrate with smart building systems. Aperio has a published API and is built for interoperability, so is set to be a natural fit.

"I am very satisfied with the implementation and operation of the Aperio solution and I have every confidence in ASSA ABLOY as a manufacturer," says Frans Bruggeman, Facility Services Consultant at InHolland.

[8] ASSA ABLOY Opening Solutions, Wireless security: Cut costs without cutting corners, https://campaigns.assaabloyopeningsolutions.eu/aperio-cost-savings

Integrating wireless locks to maximise the reach of access control in healthcare

As already noted, the Wireless Access Control Report highlighted that systems integration with other building management systems is important to the vast majority of security professionals. To meet this challenge at the Haute Savoie region's new hospital, managers selected Aperio locking integrated online with an ARD access management system.

The 1300 Aperio readers integrate natively with the central system, so wired and wireless access points at Centre Hospitalier Métropole Savoie (CHMS) are managed together, with real-time logs, remote door opening and free time slot management. Because Aperio locks are battery powered, the hospital could introduce more layers of security and secure doors without incurring excessive installation or operating costs, including for sensitive offices and drug stores. Staff no longer carry big bunches or waste time hunting down keys, with individual permissions all stored on a single, programmable RFID credential.

"Having just a single badge — and not having to carry around heavy keys — has been a major advantage for us," says Béatrice Dequidt, Health Executive at CHMS. "We have implemented internal HR management procedures, creating badges that are automatically integrated into ARD's operating software," adds Alain Gestin, CHMS's IT Systems Architect. Aperio and ARD also maintain compatibility of credentials with the French Government's electronic Health Professional Card (CPS), for added staff convenience.

View from the frontline

As part of this whitepaper, IFSEC Global has conducted an exclusive interview with one of Europe's leading security systems integrator and guarding businesses, to find out the views from those fitting, maintaining and working with end-users to implement interconnected electronic security systems.

Danny Laurier, Sales Business Development Manager at **Securitas** in Belgium, provides his viewpoint on the growing integration trend.

IFSEC Global (IG): Do you believe integrating disparate physical security systems, as well as other building systems, to work with each other is a growing trend? And if so, why?

Danny Laurier (DL): Firstly, I would definitely say it's true that the integration of security technologies is a growing trend – but also with other technologies like IoT, building management and visitor management platforms. The world we're living in has completely changed, as has the way we're doing business – but also the types of threats we're faced with are different than a couple of years ago.

Integration and end-to-end security solutions combining technology and people are key to coping with these developments. At Securitas, we see four key challenges for security professionals.

The first one is the requirement to respond very quickly to incidents. The second is that 24-hour security is required – threats don't just take place in office hours. There are also the growing cyber challenges that IoT and other types of sensors are creating. And fourth is that budgets are tight, so total cost of ownership (TCO) is a key consideration for end-users. Integrated systems and companies like Securitas can really provide support on all four of these challenges.

IG: What are the benefits of integrating access control with other systems for end-users?

DL: Through all of these developments, the amount of data that becomes available for security is huge. Whereas security has mostly been a reactive profession prior to now, integrated solutions and AI platforms allow data to be transformed into knowledge. And, when you have knowledge, you can move from a reactive to predictive risk management approach.

Integration of security systems, such as surveillance, access and intruder, with other data allows companies to bring disparate devices all into one physical security

> *"Without integration, it's not possible to have a good, general overview of your security operation."*

information management (PSIM) platform. Having several different devices feed into a single solution makes life easier for control room operators, as they can respond more quickly and efficiently when an incident is reported. This guarantees a higher level of security for people and assets.

Digital transformation is affecting security, and Securitas invests significantly in this area in order to offer high-end security solutions to our customers.

IG: What level of importance does Securitas place on integrated systems?

DL: Securitas is an integrator, so we place a lot of importance on this area as it is key in order to efficiently protect our customer's assets. Without integration, it's not possible to have a good, general overview of your security operation. It's not stopping at the physical and electronic security level either, as cyber security is now important to consider for digital systems.

Providing an end-to-end solution is really important to us and is our focus, as we offer solutions to our customers for all their security requirements. We'll work on the pre-sales process, understanding customer needs and risks and translating them into a solution and security architecture where we combine security technology with guarding services. Securitas is a holistic security solution provider, integrating people, processes and procedures.

And so that we know these systems are going to work, we only work with 'A' brands with proven, secure, open protocol technology. The products are an important part of this solution, of course, as it helps to sustain an excellent long-term relationship with our customers.

To do this, we need third level support from our suppliers, who can work with us on the various demands placed upon each project and have the right structure in place to do so. We therefore only work with one or two key suppliers in any given area, so we can fully train our integrators and engineers to understand these systems. They get to know the brand and its technology, which enables us to move – like many companies in security – from selling a 'product', to providing a 'solution'.

IG: What advice would you give to an installer of security systems who hasn't undertaken integration projects before but would like to get into the field?

DL: Understanding the customer requirements and risks and having the right expertise on the different security systems is important. But the one thing we did early on in this process was to invest in IT knowledge and skills.

Integrating physical security products requires good IT skills – something that wasn't always necessary with analogue and siloed systems previously. You need someone in your team who invests their knowledge in areas such as networks, cyber security, AI platforms and general IT engineering. We've made a move to become a digital company, and that would be my advice to others looking to develop their business into this field.

Also think about how you can provide an ongoing service to these integrated systems. There's a shift in security directors from managing operational systems, to managing risks. If you can offer a recurring service – Security as a Service, as it's known – many end-users are exploring the option of outsourcing operational tasks such as managing underlying security and IT systems to specialists, or the management of security alarms to a professional control room. It's something we offer at Securitas, and it's enabled us to grow our 'pay per' model.

IG: Why do you use ASSA ABLOY products/solutions?

DL: Well, both ASSA ABLOY and Securitas are international organisations with international footprints, so this is a major benefit to us both – we can deal with customers on a national and international level, and know they'll have the solutions to match.

But they also work at a local level, which is really important to us as well. On any given project, it's important everyone on the team trusts each other – so we trust the supplier, the customer trusts us, and the supplier is trusted by the customer. Having a local presence makes this whole process easy.

And finally, ASSA ABLOY offers the type of support you need when integrating systems. Their products are open platform, for a start, and I believe this is really important as we move away from proprietary standards. And, at some point there is likely to be a requirement of the project that you're not always 100% on, so having the back-up of a trusted supplier to work with you on that and sometimes produce a bespoke solution, is really key.

It's really a partnership, more than a customer-buyer relationship! We need our supplier partners to ensure they're continually evolving their technology to keep up with demands and provide long-term stability for themselves, us, and our customers.

Russell Wagstaff,
Platform Director EMEIA,
ASSA ABLOY Opening Solutions

The future of integration?

Integrations are the blocks on which smart buildings — and eventually, smart cities — will be built. Their value is easy to communicate: When a building 'knows' who is moving around, where they are right now, how many will be in specific areas at certain times, then other systems can react accordingly. The integration is where this begins.

As the way we live and work changes, it seems less useful to think about building management functions in isolation, as this report's analysis of integration shows. Technological change and shifting global work patterns test all building systems simultaneously, every day.

It is no surprise, then, that the desire for smarter solutions is already gathering pace. According to one recent estimate, "The global market for intelligent building (IB) solutions has experienced double-digit growth in the past decade".[9] By 2017, "29.6% of access control equipment shipments — including readers, door controllers and electronic locks — were installed and connected to a BMS platform," according to Omdia.[10]

Analysts at Guidehouse Insights also expect global revenue for intelligent building solutions to exceed €110 billion by 2030.[11]

In other words, this is just the beginning. If 'standalone' digital locks are a missed opportunity to improve the efficiency of building security, the isolation of 'standalone systems' will be viewed similarly.

Growth drivers: From here to… the future

Future-oriented solutions are already essential for any large investment in security — and almost every investment in this field is large. Forward-thinking organisations already plan on a grander scale than technologies, devices and systems. Only a single, all-encompassing ecosystem can deliver the connectivity and convenience required to keep premises secure and filter access to manage the ever-changing movement of people.

As buildings are tasked with getting smarter, this connection between integrated systems becomes more important. According to further Omdia analysis: "Access control integration is essential to unlocking the potential of higher-level BMS platform functionality. As more BMS solutions move towards command-and-control-style features, which allow buildings to adjust building management subsystems to respond to individual occupants' actions, the need for access-control integration grows exponentially".[12]

[9] Guidehouse Insights, Market Data Intelligent Buildings, https://guidehouseinsights.com/reports/Market-Data-Intelligent-Buildings
[10] Omdia, Electronic access control integration is the first stop on the road to smarter buildings, https://omdia.tech.informa.com/OM003090/Electronic-access-control-integration-is-the-first-stop-on-the-road-to-smarter-buildings
[11] Smart Infrastructure Magazine, Intelligent buildings market set for massive growth, https://smartinfrastructuremagazine.com/news/intelligent-buildings-market-set-for-massive-growth
[12] Omdia, Electronic access control integration is the first stop on the road to smarter buildings, https://omdia.tech.informa.com/OM003090/Electronic-access-control-integration-is-the-first-stop-on-the-road-to-smarter-buildings

Protecting the value of an initial investment is another concern. Thus, new ecosystems must create a dynamic hub to which future security products and technologies can connect. They need to be born, and stay, compatible — even with technologies which are not yet mainstream.

Standards, APIs and open platform development are more important than ever.

A building powered by data

Data is the fuel which powers the smart building. Your existing access control system already generates thousands of data-points every day. The question is, what does the system do with all that data? At the moment, the answer is: probably nothing.

Yet data locked inside an access system can help achieve perennial business goals like cost saving and better energy efficiency. Ever more integrated software will streamline decision-making, informing it with data drawn from the security system.

Data-informed automation will also liberate security teams from repetitive manual tasks, leaving them free to do more. Tailored reporting and customisable dashboards can help security managers generate valuable insights and share them with decision-makers and stakeholders around the business. Convenient, data-rich mobile tools will free them from their own desk, too.

New control panels will help security managers to visualize and easily analyse the impact of access on each complementary building and business system. Movement around the site can be monitored and measured to extract insights about building use, while also reinforcing its traditional role by reducing breaches and deterring thefts.

Managing access deeper into a building — far beyond the perimeter or entrance door — provides an opportunity to harness even more of a building's valuable data. Thus, integration can unlock the data that an access system generates every hour of every day. It will be a critical resource and a competitive edge in the quest for better business performance and faster growth.

Are smart buildings also more sustainable?

Of course, growth isn't everything. The question of how we can live and work sustainably is both topical and increasingly urgent. The UN Environment Programme estimates that buildings currently consume around 60% of the world's electricity.[13] Buildings and construction accounted for 37% of global energy-related CO_2 emissions in 2020.[14]

We must always be careful not to over-claim. But the technologies to do better already exist. Implementing building systems which can communicate and interoperate — in short, be 'smarter' — will be a small but important part of the solution. This is integration in action — and its importance is only going to grow.

[13] EU Energy Centre, Energy Efficiency for Buildings, www.euenergycentre.org/images/unep%20info%20sheet%20-%20ee%20buildings.pdf
[14] UN Environment Programme, Pandemic caused dip in building emissions, but long-term outlook bleak – UN report, www.unep.org/news-and-stories/press-release/pandemic-caused-dip-building-emissions-long-term-outlook-bleak-un

THE #1 REUNION EVENT FOR THE SECURITY INDUSTRY

IFSEC INTERNATIONAL | 17–19 MAY 2022 ExCeL LONDON

IFSEC International 2022 is your unmatched opportunity to network and do business with the entire security buying chain, discover solutions and see real products put to the test across access control, video surveillance, cybersecurity and more. Enhance your knowledge and grow your network through our series of online and in-person events.

Official Sponsor:

bsia
british security industry association

Informa AllSecure
This event is produced to the Informa AllSecure Standard

FIND OUT MORE AT WWW.IFSEC.CO.UK

5 INDUSTRY SHOWS. 1 FREE TICKET.

IFSEC INTERNATIONAL | FIREX INTERNATIONAL | SAFETY & HEALTH EXPO POWERED BY SHP | FACILITIES SHOW | INTELLIGENT BUILDING EUROPE