



# Entrance Control in Smart Buildings

Balancing security, design and flexibility  
in a hybrid world

**GUNNEBO**<sup>®</sup>  
*Entrance Control*

# Entrance Control in Smart Buildings

## Balancing security, design and flexibility in a hybrid world

For today's public and commercial buildings, smart represent the convergence of technology, user experience and operational efficiency.

With this advancement comes new vulnerabilities. This white paper explores the critical role entrance control plays in addressing these challenges. Drawing on the latest research on cyber-physical threats to building management systems (BMS), we examine the need for seamless security integration that supports hybrid working models, respects design aesthetics and ensures continuous operational readiness.

We explore how entrance control contributes to broader goals of wellness, resilience and smart infrastructure efficiency. This paper aims to provide a balanced, informative perspective on how entrance control can evolve to meet the complex demands of smart, connected buildings in 2025 and beyond.

In doing so, Gunnebo Entrance Control wishes to stimulate debate and encourage contributions. We look forward to engaging with you and your colleagues in this dialogue and would be pleased to share additional points of view and insights. Feel free to contact your local representative to start the conversation.

### The Cyber-Physical Threat Landscape of Smart Buildings

Smart buildings rely on interconnected systems for lighting, HVAC, surveillance, security and access control – all managed through increasingly complex Building Management Systems (BMS).

This integration poses serious risks. According to a 2025<sup>1</sup> study, 75% of organisations are currently operating BMS infrastructure with known

### About the author



**Tina Hughan**  
Global Marketing & Sustainability Director

Tina is a marketing professional with over 20 years experience serving industry sectors as diverse as retail to manufacturing.

Tina has a Masters Degree in Marketing, is a Fellow of the Chartered Institute of Marketing (FCIM) and a member of the Institute of Digital & Direct Marketing (MIDM) as well as holding Chartered Marketer status.

<sup>1</sup> Exposed and unaware? Smart buildings need smarter risk controls. Published 4th July 2025: <https://www.helpnetsecurity.com/2025/07/04/building-management-systems-bms-risk/>



Glass barriers, speed style gates, low-profile turnstiles and embedded biometric systems are being favoured for their ability to integrate with architectural intent

exploited vulnerabilities.

Many of these systems remain accessible via unsecured internet connections, dramatically increasing the risk of targeted attacks.

**“Many of these systems remain accessible via unsecured internet connections, dramatically increasing the risk of targeted attacks.”**

The Royal Institution of Chartered Surveyors (RICS) found 27%<sup>2</sup> of UK businesses experienced a cyber-attack in the past year – an increase from 16% the previous year. And 59% has been highlighted on a global basis<sup>3</sup>. 73% of business leaders

expect cyber disruption within the next two years<sup>4</sup>.

These statistics highlight the urgency with which the security of BMS and associated systems, including entrance control technologies, must be addressed.

This heightened threat landscape requires a broader cultural shift in how we view physical security. No longer can security be considered in isolation either technologically or architecturally.

The interdependence between physical and digital environments means a breach in one area often translates into risk in another. For example, if an intruder gains physical

access to a server room through a compromised entrance control system, the cyber implications could be severe.

Inversely, cyber exploitation of entrance systems can lead to unauthorised physical access. This hybrid threat environment calls for bespoke entrance control solutions that operate securely, consistently and contextually.

### **Blending Security Seamlessly with Design**

Modern smart buildings are as much about experience as they are about functionality. Architects and designers place emphasis on aesthetics, flow and user comfort.

<sup>2</sup> 27% of UK businesses hit by cyber-attacks in the past year, says RICS – could your infrastructure be at risk? Published 02 July 2025: <https://drlogic.com/article/27-of-uk-businesses-hit-by-cyber%E2%80%91attacks-in-the-past-year-says-rics-could-your-infrastructure-be-at-risk/>

<sup>3</sup> How many cyber attacks occur each day? (2025) Published 6 June 2025: <https://explodingtopics.com/blog/cybersecurity-stats>

<sup>4</sup> The new biggest risk to business owners: cyber attacks. Published July 1 2025: <https://www.romeroinsurance.co.uk/news/the-new-biggest-risk-to-business-owners-cyberattacks>

In this environment, entrance control technologies must tread a fine line. They need to enforce robust security protocols without disrupting the visual or spatial harmony of the building.

Traditionally, security infrastructure has been designed to stand out -

**“Security infrastructure that blends into its environment supports a perception of trust, seamless foot flow, professionalism and smart use of technology.”**

metal detectors, turnstiles, guards - but today, the trend is towards subtlety.

Glass barriers, speed style gates, low-profile turnstiles and embedded biometric systems are being favoured for their ability to integrate with architectural intent. This approach not only enhances the visual appeal of the space but also promotes smoother user experiences and free flowing movement, where security does not feel obstructive or confrontational.

Security infrastructure that blends into its environment supports a perception of trust, seamless foot flow, professionalism and smart use of technology. This matters in line with increased focus on mental health and in sectors like hospitality, corporate headquarters, universities and healthcare, where first impressions are critical and anxiety must be minimised.

Innovative materials and manufacturing methods are also

expanding the possibilities of designed security. Minimalist aluminium housings, LED indicators and sensor-driven gates can be coordinated with bespoke interiors.

Touchless entry options reduce contamination risk while maintaining

aesthetic fluidity. In combination with sustainable materials and modular designs, entrance control can now meet high standards for visual appeal and environmental responsibility simultaneously.

### **The Role of Smart Infrastructure in Enhancing Well-being**

A critical evolution in smart building design is the integration of well-being-focused infrastructure. As highlighted by industry experts, smart infrastructure, particularly when powered by IoT, can improve occupant well-being, resilience and overall building intelligence.

Entrance control systems are no exception. When embedded into a smart ecosystem, they can collect environmental data, support air quality monitoring and manage occupancy in ways that promote comfort and safety.

For example, IoT-connected entrance systems could detect CO<sub>2</sub> levels and signal HVAC adjustments or offer visual feedback when a space is

## **SpeedStile FLs Max**



SpeedStile FLs MAX supports a wide range of third party authentication and verification devices

**Gunnebo SpeedStile FLs MAX is a premium speed gate combining sleek aesthetics with cutting-edge security.**

Offering a compact footprint, a high level of integration capabilities, and advanced detection technology to prevent tailgating and piggybacking, it ensures seamless entrance control without compromising design or user experience.

With a choice of square or round cabinet shapes, SpeedStile FLs MAX seamlessly blends into any architectural environment. The high transparency glass wings maintain minimal visual impact, ensuring an open and welcoming entrance and exit to your office reception or leisure facility while supporting security and design intent. SpeedStile FLs MAX has an independently verified EPD.

[Find out more on our website](#)



Entrance control systems should serve as practical solutions that enhance user confidence without sacrificing convenience

nearing capacity. These features are not only about comfort, but they are also increasingly tied to public health and confidence in shared spaces.

Touchless access and mobile credentialing support hygienic entry,

**“Smart infrastructure has the power to change how people perceive and interact with the built environment. When well-being is embedded into the function of every system the building becomes an active participant in maintaining health and well-being.”**

reducing touchpoints in high-traffic areas. In environments conscious of health risks, these systems serve as practical solutions that enhance user confidence without sacrificing convenience.

In emergencies or crises, smart entrance control becomes a tool of

resilience. It can guide occupants to safety, control ingress and egress dynamically and integrate with wider safety protocols. This functionality aligns with a growing recognition that smart buildings must not only be efficient - but they must also protect

and support the well-being of those within.

Smart infrastructure has the power to change how people perceive and interact with the built environment. When well-being is embedded into the function of every system the building becomes an active

participant in maintaining health and well-being.

### **Prioritising Sustainability in Modern Entrance Control**

Sustainability is no longer a future goal; it is a current imperative. As organisations strive to meet environmental, economic and social targets whilst reducing carbon footprints, every system and its supply chain within a smart building must contribute positively to the overall agenda.

Entrance control systems are increasingly designed with environmental impact in mind. This includes the use of low-energy hardware that operates efficiently without compromising performance. Energy-efficient motors, sensors and control boards are reducing power consumption across access points that operate continuously throughout the day.

Equally important is the choice of materials. Manufacturers are moving toward sustainable alternatives - recycled metals, low-emission coatings and responsibly sourced components- reducing the embodied carbon of the system and.

Modular construction and maintenance schedules allow components to be replaced without discarding entire units, while systems designed for disassembly and recycling ensure materials can be repurposed rather than sent to landfill. This circular approach is

becoming practice in responsible manufacturing.

Data-driven access control supports wider sustainability goals. By linking entrance data to HVAC and lighting systems, buildings can adjust environmental settings based on real occupancy patterns, reducing energy consumption.

Real-time data analytics can inform building managers when and where to allocate resources, optimising both energy use and user comfort.

A sustainable entrance control system is one that secures and supports the building's environmental performance. As smart buildings evolve, sustainability and security must go hand in hand - working together to create spaces that are safe, efficient and future-ready.

### Supporting Hybrid Work Through Adaptive Access Control

The shift to hybrid working has permanently altered how buildings are used. With employees arriving at staggered times, attending only part-time, or using flexible desk arrangements, the traditional 9-to-5 office model no longer applies. This unpredictability poses new challenges for security, fire safety regulation and access management.

Entrance control technologies must accommodate 24/7 access needs, often with minimal on-site supervision. Buildings that once operated on fixed schedules are



Employees expect buildings to work around their schedules

now expected to be available around the clock. This means entrance systems must provide not just secure access but also real-time verification, automated alerting and seamless remote management.

This model of flexible access has implications for workforce productivity. Employees expect buildings to work around their schedules – not the other way around. Seamless, personalised access can improve punctuality, enhance satisfaction and reduce frustration. When employees are confident, they can access what they need, when they need it and it encourages greater trust in the workplace infrastructure.

It adds to the nature of resource, budget and cost restricted Facility and Security Managers looking to remotely manage sites.

Visual verification becomes especially important in this context. Security teams need the ability to confirm identities without physical presence, which has led to an increase in the use of facial recognition, behavioural analytics and AI-assisted surveillance. These technologies enable proactive response to irregular access attempts while maintaining the convenience and speed required by modern users.

Flexibility in access control supports a growing contingent workforce. Contractors, freelancers and service providers may only need limited

or temporary access. Dynamic credentialing systems - where permissions can be granted and revoked instantly - ensure building managers maintain precise control without disrupting daily operations.

Integration with visitor management systems ensures a smooth and secure flow of guests through shared workspaces.

Data gathered from entrance systems plays a crucial role. Analysing entry and exit patterns can help organisations optimise space usage, reduce energy consumption and improve employee well-being.

For example, real-time data can be used to trigger HVAC systems only when rooms are occupied, or to avoid overcrowding by redirecting traffic to less busy areas. These capabilities align entrance control with broader goals of ESG compliance, energy efficiency, and digital workplace transformation.

### **Implementing Best Practices for Secure and Resilient Access**

Securing entrance control in smart buildings requires a multi-layered approach that addresses both physical and cyber vulnerabilities. One foundational measure is network segmentation.

Entrance systems may operate on isolated networks, protected by firewalls and monitored for anomalies. Where remote access is required, it should be mediated through secure

VPNs or zero-trust frameworks.

Credential management is equally vital. Default passwords must be replaced, and multi-factor authentication should be standard. Role-based access control ensures only authorised personnel can manage or alter system configurations. Where possible, integration with corporate identity providers streamlines provisioning and deprovisioning, reducing the risk of orphaned access points.

Beyond basic protections, a culture

**“Entrance systems may operate on isolated networks, protected by firewalls and monitored for anomalies. Where remote access is required, it should be mediated through secure VPNs or zero-trust frameworks.”**

of continuous improvement is necessary. This includes regular red team testing, patch management protocols and participation in threat intelligence sharing networks. It also means educating facilities and IT teams about emerging threats, ensuring the human layer of defence is as strong as the technical one.

Encryption and secure communication protocols are another layer of defence. Legacy protocols such as unencrypted BACnet should be phased out in favour of secure alternatives. Entrance devices must support encrypted data transmission to protect against interception or tampering.

Monitoring and incident response

procedures should be embedded into daily operations. Every access attempt, successful or not, should be logged and reviewed regularly. Anomalies such as repeated failed entries, access outside normal hours, or unusual user behaviour must trigger alerts. Physical devices should be tamper-resistant and equipped with sensors to detect forced entry.

Routine updates and audits are essential for long-term resilience. Firmware should be kept up to date, and hardware nearing end-of-life must be replaced proactively.

Security postures should evolve in tandem with emerging threats and technology standards.

### **The Future of Entrance Control in Smart Workplaces**

As smart buildings continue to evolve, entrance control will become even more integral to their functionality, style and security. The convergence of identity management, behavioural analytics and AI-driven decision-making will enable predictive access systems that respond to context as well as credentials.

Systems may one day grant access not just based on who you are, but why you're there, who you're with and what your typical behaviour looks like. By correlating access data with

calendar events, occupancy sensors and usage patterns, buildings can make more informed decisions about when to allow or deny entry.

Sustainability will continue to play an evolving role. Low-energy hardware, materials with minimal environmental impact and systems designed for disassembly and recycling will become standard. Entrance control will be expected to safeguard assets and people and contribute positively to the building's overall environmental footprint.

New developments in spatial intelligence could further augment entrance control. By mapping occupant movements over time, buildings can adapt to peak

hours, adjust layouts, or pre-empt congestion. This spatial feedback loop creates an environment that responds to its users in real time, bridging physical and digital infrastructures.

Entrance control will continue its evolution into a user-centric experience. As the boundary between physical and digital workplaces becomes more fluid, the act of entering a building will feel less like a checkpoint and more like a seamless transition – one where safety, convenience, and design coexist harmoniously.

### **Conclusion**

The transformation of our buildings into intelligent, connected

environments demands a new approach to security - one that is integrated, unobtrusive, stylish and adaptable.

Entrance control is at the heart of this shift. By embracing technologies that align with architectural design, support hybrid work patterns, uphold sustainability goals and meet rigorous security standards, organisations can create safer, more responsive spaces.

**Contact us for more information on our solutions for smart buildings.**

**01825 746101**  
**[gunneboentrancecontrol.com](https://gunneboentrancecontrol.com)**

## Gunnebo Entrance Control: Supporting the Smart Building Lifecycle

Gunnebo Entrance Control is working closely with commercial environments to support the growing demands placed on smart buildings. From cybersecurity and hybrid working patterns to sustainability and design integration, our approach is grounded in delivering adaptable, secure and future-ready entrance control systems that function as part of the wider building ecosystem.

As buildings become more connected, so do the risks. Gunnebo's entrance control systems are designed to operate securely within networked environments, supporting protocols that align with IT and cybersecurity best practices.

Our systems can be deployed on segmented networks, support encrypted data transmission and integrate with identity management platforms to prevent unauthorised access. This ensures the entrance point itself doesn't become a weak link in the building's overall cyber-physical architecture.

Hybrid working has introduced a new set of operational requirements. Office buildings are no longer used on fixed schedules, which places pressure on entrance systems to provide secure access across extended timeframes. Gunnebo Entrance Control solutions are engineered to offer high availability. Features such as biometric verification, mobile credential integration and remote monitoring allow security teams to maintain control without always needing to be physically present.

Gunnebo Entrance Control is working on the focus on sleek design and ensuring solutions seamlessly blend with surroundings by developing entrance lanes that can be customised with a wide range of finishes, lighting options, and form factors. The result is a smoother, more intuitive user experience that supports both brand image and occupant wellbeing

Service is captured through proactive maintenance, remote diagnostics and rapid response capabilities. Data from entrance systems helps identify wear trends, enabling pre-emptive servicing and reducing the likelihood of sudden failures.

Gunnebo Entrance Control is focused on creating tailored systems that serve buildings, operators and users - safely, reliably, and unobtrusively. As the demands on smart infrastructure continue to evolve, we remain committed to supporting buildings that are intelligent, secure, sustainable and welcoming.

For more information:  
[gunneboentrancecontrol.com](http://gunneboentrancecontrol.com)

**GUNNEBO**<sup>®</sup>  
*Entrance Control*