SECURITY AND INTEROPERABILITY

THE CORNERSTONES OF ACCESS CONTROL

Two principles have become paramount for any successful deployment: robust security and seamless interoperability. A system that excels in one area but fails in the other is incomplete. True value is realized when a solution offers strong security while integrating effortlessly with other building management technologies

By: Gaurav Mahajan, Regional Sales Director, Middle East & Africa, ICT
gmahajan@ict.co

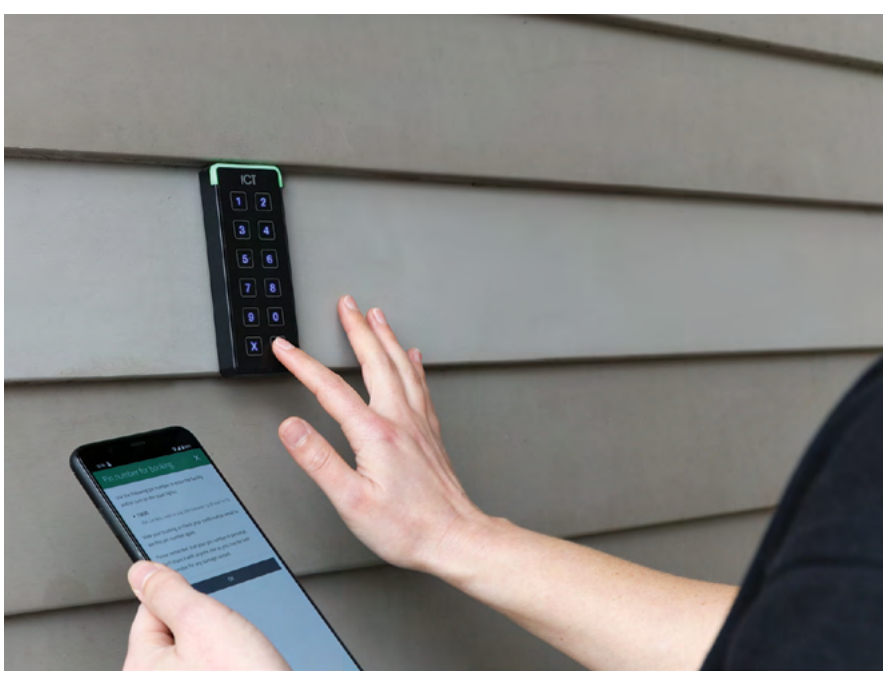
To avoid any vulnerabilities in the access control system, it is crucial to look at the security of the credentials, the communication protocol between readers and controllers, and the cybersecurity of the entire system.

Secure Credentials

The first line of defense in access control is the credential itself. Legacy technologies, such as 125kHz proximity cards, are notoriously easy to clone, leaving facilities exposed to unauthorized entry. Transitioning to advanced credential technologies is essential. High-security smart cards using Desfire EV3 and mobile credentials utilizing AES 256 encryption offer superior protection. These technologies create a secure, encrypted link between the credential and the reader, making duplication practically impossible and providing a reliable foundation for the security infrastructure.

Secure Communication Protocols

The integrity of communication between readers and controllers is just as critical as the credentials. Unsecured protocols are susceptible to interception and manipulation. Implementing RS-485 or the Open Supervised Device Protocol (OSDP) provides encrypted, bi-directional communication, ensuring that data transmitted between system components is protected from eavesdropping and tampering. RS-485 is proprietary, while OSDP is an open industry standard. This secure protocol verifies that commands are authentic and have not been altered, adding a vital layer of protection essential for high-security environments.



Cyber Security Measures

Cybersecurity is a constant, evolving threat. Mitigating the risk starts with deploying access control systems that are secure by design from reputable security manufacturers who comply with ISO 27001:2022, such as ICT. However, technology and compliance alone are not sufficient. Installation companies and customers must also implement proactive cybersecurity measures, including

A unified access control system does not operate in a silo. Its ability to integrate with other platforms and systems is what unlocks its full potential, transforming it from a security tool into a comprehensive building management solution

regular, mandatory training on best practices, phishing awareness, and more. By fostering a culture of security awareness, both security installers and end-users empower their teams to become an active part of the defense strategy, ensuring the system's integrity against sophisticated attacks.

The Power of Interoperability and Unification

A unified access control system does not operate in a silo. Its ability to integrate with other platforms and systems is what unlocks its full potential, transforming it from a security tool into a comprehensive building management solution.

Unifying access control and intrusion detection is the foundation of interoperability, as both are intrinsically linked to building access management. It allows you to manage a single database of users, making it easy to enroll them with the right access level and disable them, reducing the risk of errors. It also enables dynamic scenarios such as automatically arming an area if all employees have exited it or automatically disarming it when a person with the right access level swipes their credential in. It increases security as well as efficiency.

Open Platform

An open API (Application Programming Interface) system lays out the groundwork for endless possibilities. By integrating the access control system with other systems and platforms, it creates a more cohesive operational environment and improves overall efficiency. Whether it's synced with HR software, visitor management systems, room booking systems, or IoT devices, integration empowers the access control system to deliver smarter, more innovative solutions tailored to customers' needs.

The Value of Native Integrations

Native integrations elevate system performance by enabling access control platforms to communicate directly with building systems such as lifts, intercoms, and visitor management solutions. This direct compatibility removes the need for complex custom development, reduces integration risks, and ensures system reliability. For property managers and onsite teams, native integration delivers a unified interface, faster deployment, and seamless scalability, driving operational efficiency while consistently meeting both security and business objectives.

ICT sees how the robust security and the openness of their access control platform have been the foundation to provide their customers with a tailored solution. Unifying access control and intrusion detection and supporting it with secure credentials and a suite of readers and controllers brings enhanced security and better user database management. ICT's open API and DataSync software simplify database synchronisation and offer easy integration with third-party systems, equipping security and facility managers as well as installation companies with an adaptable and reliable solution. ■