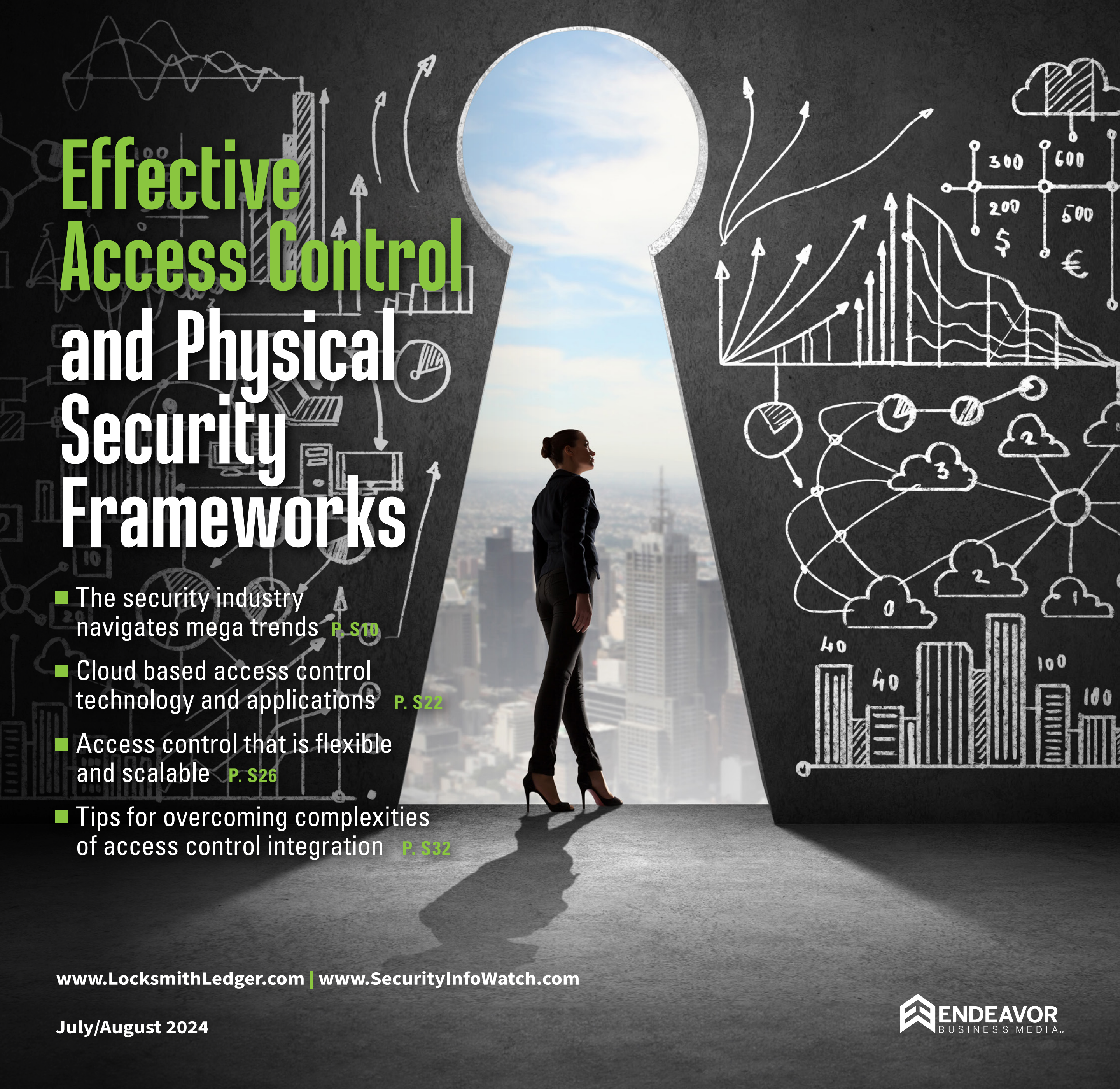
ACCESS CONTROL 2024

TRENDS & TECHNOLOGY

Supplement to Locksmith Ledger International, Security Business, Security Technology Executive



Effective Access Control and Physical Security Frameworks

- The security industry navigates mega trends P. S10
- Cloud based access control technology and applications P. S22
- Access control that is flexible and scalable P. S26
- Tips for overcoming complexities of access control integration P. S32

www.LocksmithLedger.com | www.SecurityInfoWatch.com

July/August 2024

ENDEAVOR BUSINESS MEDIA

Tips for Overcoming the Complexities of Access Control Integration

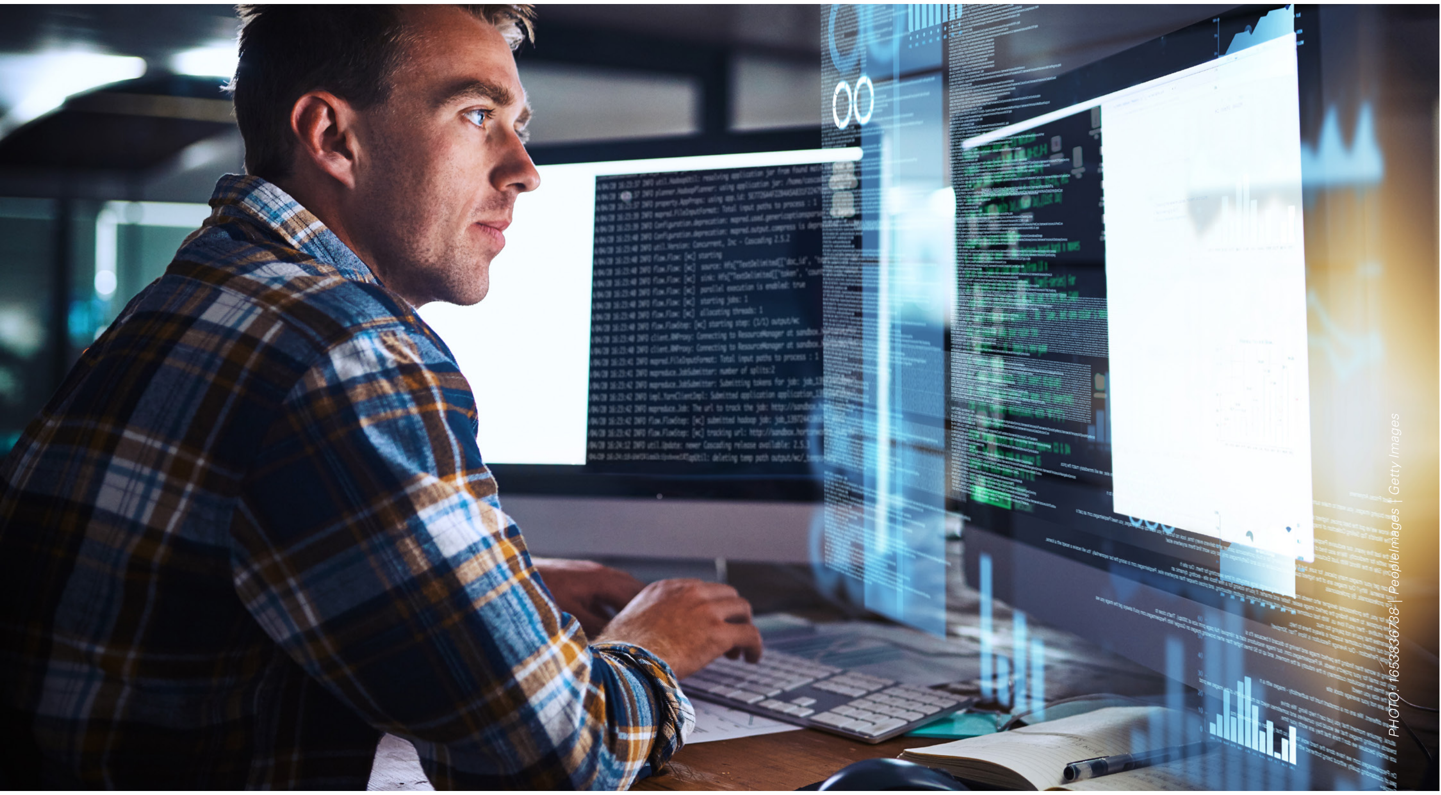


PHOTO 1653836738 | Peopleimages | Getty Images

Many organizations today face legacy technology and migration issues that are compounded by the threats of downtime

BY JAMES CHONG

Understanding the true complexities of access control integration is crucial. It's the first step in overcoming any major challenge. By recognizing the issues or blockers at the core, and understanding all the options and possibilities, we can pave the way for a viable solution. In the realm of security systems, both in physical and cyber security, technical and operational challenges often arise when developing integrations across multiple disparate systems, even within the same category of subsystems, such as access control. The task becomes even more complex in enterprise access control integrations of disparate systems, especially when dealing with proprietary vendor protocols, even when APIs are available.

By delving into the common challenges of access control integrations, we can uncover new methods and innovations that can help end users and systems integrators overcome these long-standing integration pitfalls. The benefits of tackling this challenge are not just theoretical-they can lead to significant cost and operational advantages. This, in turn, can help us better leverage new innovations, such as artificial intelligence and data analytics, in our security systems.

Real-World Integration Challenges

When discussing physical and converged security solutions for enterprise deployments, one of the key subsystems is the access control system (ACS) or physical access control system (PACS). However, in the real world, these systems are far from straightforward. In many multi-site or multi-region environments, it's not uncommon to find non-standard single-vendor or single-version PACS installations. These systems are often deployed gradually over several years, introducing a myriad of challenges for systems integrators and end-users. As the security network expands and evolves, new systems or major software upgrades with new capabilities, such as mobile credentials, biometrics, and other identity management features, are introduced, further complicating the integration process.

Even if the organization initially may have started with one standardized PACS system, through organic growth, mergers and acquisitions or other changes in procurement or management, disparate ACS or PACS solutions that require some integrations are introduced. Please don't worry, getting back to a single standard vendor PACS solution through a rip-and-replace option is typically not feasible due to the high risk of disruption, cost, and support challenges. We will explore more practical and effective solutions.

Many organizations today are also facing legacy technology and migration issues that are compounded by the fact that they cannot afford any downtime. Most are also unfamiliar with new innovations that may be available to leverage to help address these daunting integration and migration challenges. All of these are business issues that add significant layers of complexity and risk both technically and to security operations.

PHOTO: 907564114 | PeopleImages | Getty Images

So Why Integrate?

In our data-driven and hyperconnected world, designing, building, and implementing systems using a truly open architecture platform to integrate, harmonize, and analyze data from disparate sensors, devices, and subsystems is even more critical. There is also more urgency now to leverage new automation tools and innovations, such as artificial intelligence to help maintain the highest level of security, especially with critical infrastructure and other high-risk requirements for organizations. When we talk about integrating disparate PACS or ACS solutions, this requires careful planning and design to help make the execution of the task seamless and successful. One of the many benefits of having your disparate PACS solutions integrated is that, if done properly, it will help ensure that the logical and physical access privileges with an individual or identity will be synchronized across both your IT network and security network.

With seamless integration, the credentials from disparate access control systems can be propagated across the other PACS solutions, simplifying enrollment, on-boarding, and off-boarding. This means that you could enroll an individual or identity in one PACS solution, which will then be enrolled into the other disparate PACS across the enterprise automatically. The same would go for revoking the privileges and access of individuals where this can also be done centrally. Efficiency, accuracy, and compliance can be better achieved through seamless integration across the network.

What Have We Tried to Meet the Integration Challenge?

The security industry has seen many options for integration over the past several decades, including hardware, firmware, and software solutions. Some new, software-based product categories have even emerged over the past 2 decades, including Physical Security Information Management (PSIM), Physical Identity and Access Management (PIAM), Converged Security and Information Management (CSIM), and other subsets or derivatives of custom-developed Command, Control, and Communications (C3). With these software-based integration solutions, the development, adoption and standardization of Application Programming Interfaces (APIs) have also become more common in the industry, especially during the last decade. Today, it would be uncommon to find top-tier or even second-tier ACS or PACS vendors not offering some versions of APIs or Software Development Kits (SDKs) for integrators and third parties to use to gain some level of integration and interoperability.

Over the past 2 decades, the security industry has also developed and introduced standards such as ONVIF (the Open Network Video Interface Forum) for video integration and interoperability and Physical Logical Access Interoperability (PLAI) specification. ONVIF includes protocols and standards that help create connections between disparate video systems and other IP-based security products, while the PLAI specification was introduced by the Physical Security Interoperability Alliance (PSIA) to help promote greater cooperation and interoperability of IP-enabled security devices, including PACS and ACS.

Despite the availability of these open standards and the fact that APIs from PACS vendors have become more commonly available, the challenges are still there. New versions, features, and upgrades can introduce interoperability issues and even backward compatibility issues, which break what used to work or function with their integrations. The sustainment costs and scalability limitations have also become more challenging for integrators and end users.

> Over the past several decades, the security industry has seen many integration options, including hardware, firmware, and software solutions.

What's a Better and New Way to Solve This Problem?

Like many other industries that have been going through digital transformation over the past few years, the security industry has also embraced digital transformation at its core, and some of the new innovations have started to shape some exciting opportunities for meeting today's integration issues. As mentioned above, many products have been developed and introduced over the past two decades to help address the integration challenges by leveraging open APIs and standards. However, the native architecture of the integration products themselves was closed and now has become even a legacy codebase.

This reality is why new innovations are now needed to scale and provide long-term interoperability based on open architecture and new software platforms that can be leveraged by integrators and third parties. To explain this further, software technology has changed dramatically over the past 10 years, and what used to be considered new or innovative back then is no longer the case. From an architecture standpoint, we now have modularized, containerized, and app-based capabilities in software. This allows changes to be made or introduced that can be much more closely controlled and separated to reduce risk and impact if things go awry.

For instance, by separating the core into modularized packages, integration to a new system can be achieved without the integrator or third party having to know all the intricacies of the overall core product. This means that you have a truly open platform that allows third parties to even develop their own integrations and enables an app-store-like community where everyone with development capabilities can use an open API to meet their unique requirements. One example of this innovation is the Advancis Open Platform (AOP) which was introduced to the market in 2023. Any capable integrator or third party can now develop and scale their integrations with third-party security systems by using the same APIs the core engineering team uses for adding new features, functions, extensions, and integrations.

Future changes in integration with other access control systems can be achieved using open APIs and open platforms without solely depending on one application-specific vendor. This is a game changer for our security industry, which has traditionally been siloed and rigid where maintaining or updating integrations was daunting, very costly, and limited only to the software vendor. As more software solutions and vendors develop a new core based on the latest software innovations and standards, the security industry will start to see the benefits of all data sources being connected, integrated, and analyzed for real-time and post-event situation management.

Situational awareness and decision support have been part of security operation centers for decades. Still, now, as threats and risks have increased from all angles, including cyber, we must start planning and implementing new integration strategies that will help ensure security and resilience that embrace digital transformation through the combination of people, process, and technology.

Impact of Integration of Artificial Intelligence

As the evolution and new era of artificial intelligence (AI) is taking almost every market by storm, data integration benefits and needs have become even more important. As data is being generated at levels unseen by IoT sensors and systems, including security devices from door readers, intrusion detection systems, access panels, and more, the benefits of having data being connected, integrated, and normalized allows the application of AI algorithms and modules to be readily applicable.

For instance, computer vision, machine learning, and large language models (LLMs) can all be leveraged by Security Operation Center (SOC) operations where natural language inputs can be used to accelerate real-time data that could help improve response time including resource tracking and management, which could help save lives, time, and limited resources. To help improve the accuracy and reliability of incident detection, AI can be applied to identify suspicious activity and patterns coming from multiple disparate PACS solutions and locations, which would not have been easily possible without automation and correlation.

Undoubtedly, the next decade will be dominated by AI applications in the security industry, which will play a key role in rapidly accessing and analyzing massive amounts of data to help monitor critical security threats, such as detecting anomalies at critical junctions. Fully integrated security solutions will be able to assess video and ACS data to help identify trends and anomalies to enable proactive mitigation measures, which otherwise may have gone unnoticed.

Summary

Today, we have more possibilities for solving access control integration complexities than ever before. New innovations in software technology can now be the new standard for leveraging truly open software platforms that allow integrators and end users to have more control of their integration challenges and futureproof their security operations.

With more options and opportunities to integrate access control and other security subsystems, security operation centers and organizations can better leverage other security tools and future innovations, including AI.

Better and tighter data integration across the enterprise will also result in cost savings, including in training, system maintenance, and overall operational efficiency. Operationally, integrators and users can develop more intuitive workflows and smarter use cases and drive digital transformation opportunities to further increase organizational efficiency and compliance. ***AC***

About the author:

James Chong *is the chairman of Advancis USA.*