SIA
TECHNOLOGY
Insights
Spring 2024
Volume 12, Number 1

Smart Is Secure

Artificial intelligence is the next stage in perimeter security Page 48

Going Mobile

In access control, smartphones are replacing keycards **Page 22**

***AI*ntegrators?**

Artificial intelligence creates new integration opportunities **Page 38**

To Wire or Not to Wire

Wireless plus wired approaches can end a sea of troubles **Page 84**

SIA thanks Wesco for supporting SIA Technology Insights.

We Build, Connect, Power and Protect the World.

You drive productivity and progress. We power the path forward. As a leading global supply chain solutions provider, we use inspiration to drive innovation. Every day we seek out opportunities in the unexpected to deliver creative approaches that help build, connect, power and protect our world.

Your partner in productivity and progress, Wesco.com.

wesco

Ingenuity delivered.

Wesco.com

SNG

SECURINGNEWGROUND

Oct. 8th – 9th, 2024 | NYC

The Security Industry's Executive Conference

Once a year, the security industry's brightest minds, biggest players and most driven entrepreneurs come together in New York City for two days of information sharing, top-level networking and security industry business analysis. At Securing New Ground trends are spotted, connections are formed, and minds are opened. Join us at SNG!

About Securing New Ground

- Founded in 1996
- The executive conference of the Security Industry Association (SIA)
- 2 days of intelligence sharing, education, analysis and networking
- Attended by 250+ senior-level industry leaders

Attended by Leaders

Luminaries. Entrepreneurs. CEOs of the Leading Companies. Global CSOs. Investors. They're all at SNG.

Securing New Ground has a reputation for attracting the people who drive growth and change – those who will reshape the future of the industry.

THE GLOBAL SECURITY MARKET IS EVER EVOLVING and to stay ahead, you have to understand the market trends and network with the people influencing those trends. That is why **I ALWAYS GO TO SECURING NEW GROUND.**

Fredrik Nilsson, VP Americas
Axis Communications

SECURINGNEWGROUND.COM

TECHNOLOGY Insights

Spring 2024

Volume 12, Number 1

SIA Technology Insights is published twice a year, in the spring and fall, by the Security Industry Association in Silver Spring, Md.

All editions are available at no charge at www.securityindustry.org/techinsights.

Questions, comments and article proposals may be submitted to the editor, Ron Hawkins, at rhawkins@securityindustry.org.

Surveillance and Beyond

Autonomous indoor drones address multiple security and operational challenges

Gil Brudner (gil@indoor-robotics.com) is the Director of Product at Indoor Robotics (www.indoor-robotics.com).

THE SECURITY INDUSTRY FINDS ITSELF at the heart of a technological renaissance. Indoor drones, in particular, herald a new era of security solutions. These aerial devices are redefining the boundaries of surveillance and safety in real time, showcasing the fusion of technology and practical application in meeting today's security challenges.

THE EVOLUTION OF INDOOR DRONES

Drones have evolved significantly from rudimentary, manually-operated devices to highly sophisticated, autonomous systems that embody the pinnacle of artificial intelligence (AI) integration in security operations. State-of-the-art drones now carry out complex security tasks with unparalleled precision and efficiency, a far cry from earlier, less reliable incarnations that were prone to navigational mishaps.

Equipped with cutting-edge algorithms and advanced sensor technology, indoor drones

> STATE-OF-THE-ART DRONES NOW CARRY OUT COMPLEX SECURITY TASKS WITH UNPARALLELED PRECISION AND EFFICIENCY, A FAR CRY FROM EARLIER, LESS RELIABLE INCARNATIONS THAT WERE PRONE TO NAVIGATIONAL MISHAPS.

can autonomously analyze environmental data, make informed decisions, and conduct surveillance without human intervention. This technological leap forward merges the precision of modern innovations with adaptability and problem-solving capabilities akin to human reasoning. It signifies a transformation in which drones move from peripheral players to central figures in comprehensive security strategies.

NAVIGATING ECONOMIC TURBULENCE

In the current, unpredictable economic environment, the security industry faces unprecedented staffing challenges. Finding and retaining qualified security personnel has become increasingly difficult, as fluctuations

in the market exacerbate already high turnover rates. The lack of a stable workforce has propelled the search for innovative solutions to the forefront of industry priorities. Indoor drones have emerged as a response to these challenges, offering a reliable and efficient alternative to traditional security staffing. These autonomous agents work tirelessly, unaffected by the economic pressures that complicate human staffing, providing invaluable consistency in a time of widespread uncertainty. By integrating indoor drones into their security strategy, organizations across many sectors can not only address immediate staffing challenges but also lay the groundwork for a more resilient and adaptable security infrastructure.

Warehouses and Logistics

In the complex and expansive environment of logistics and warehousing, indoor drones have become essential assets, navigating through aisles and over obstacles with precision. These drones ensure the security and accurate placement of every package and pallet, operating with a level of efficiency and reliability that traditional methods cannot match. They play an important role

> THESE AUTONOMOUS AGENTS WORK TIRELESSLY, UNAFFECTED BY THE ECONOMIC PRESSURES THAT COMPLICATE HUMAN STAFFING, PROVIDING INVALUABLE CONSISTENCY IN A TIME OF WIDESPREAD UNCERTAINTY.

in maintaining order and safety, offering a sophisticated solution to the challenges of security surveillance. Their integration into warehousing operations marks a significant advance in how goods are stored and protected.

Self Storage Facilities

Indoor drones are transforming security and operational practices in self-storage facilities, where they patrol and monitor to ensure unit security and to identify unauthorized access. Beyond surveillance, these drones, powered by advanced AI, efficiently check unit occupancy and conduct maintenance inspections, pinpointing unsecured units and potential safety hazards. This dual functionality not only fortifies the facility's security but

also aids in the proactive management of space and maintenance issues, streamlining operations and safeguarding both customer belongings and the facility's integrity in a single, efficient sweep.

Retail and Commercial Spaces

After the store closes and the lights are dimmed, indoor drones assume their vital role, patrolling the quiet aisles with efficiency and accuracy. They serve as important components of nighttime security operations, with their flights providing a vigilant presence that safeguards the premises. Their deployment demonstrates the evolving nature of security, where technology complements traditional methods, not just on the ground but also in the air.

Office Spaces

In office environments, indoor drones offer a nuanced security solution, serving as adaptable cameras by day and autonomous guards by night. These drones navigate areas where traditional cameras cannot be installed, due to privacy concerns. Utilizing advanced AI, they can detect a range of

> THIS INTEROPERABILITY EXTENDS THE UTILITY OF DRONES BEYOND MERE SURVEILLANCE, TRANSFORMING THEM INTO PROACTIVE AGENTS OF SECURITY THAT ENHANCE THE CAPABILITIES OF EXISTING FRAMEWORKS.

anomalies, from potential fire hazards to compliance violations, such as missing safety equipment or OSHA infractions. This dual functionality ensures comprehensive surveillance and safety oversight, illustrating drones' capability to adapt to the specific needs of an environment while respecting privacy and enhancing overall security.

Critical Infrastructure

With high voltages and hazardous materials presenting significant risks, drones navigate through areas that pose dangers that are too great for human security personnel, providing a reliable layer of protection for the nation's most critical utilities.

BRIDGING THE GAP WITH EXISTING SYSTEMS

Indoor drones are able to integrate seamlessly with existing security systems, both cloud-based and on-premises. They

can effortlessly connect with video management systems (VMS), Internet of Things (IoT) devices and more through various interfaces such as dry contacts, web APIs, and other protocols. This ease of integration means that drones can become an integral part of the security infrastructure without the need for extensive overhauls or replacements.

Drones can autonomously navigate and interact with other systems and can, for example, trigger alarms based on specific detections or initiate lockdown procedures in response to verified threats. This interoperability extends the utility of drones beyond mere surveillance, transforming them into proactive agents of security that enhance the capabilities of existing frameworks.

Indoor drones can be an effective countermeasure against both physical and cyber threats. On the physical front, they offer a versatile surveillance solution, capable of accessing and monitoring hard-to-reach areas without putting human lives at risk,

while on the cyber front, they are secured with advanced encryption and cybersecurity measures, ensuring that the data they collect and transmit is protected against unauthorized access and other threats.

While drones have established their value across traditional sectors, emerging technologies and creative applications are pushing the boundaries of what they can achieve in security. The integration of drones with AI and machine learning is enabling autonomous decision-making, predictive analytics, and sophisticated threat detection capabilities that were previously unattainable. Additionally, the use of drones in emergency response scenarios, such as for disaster assessment, exemplifies their potential to not only observe but actively contribute to crisis management. Future innovations may also see drones collaborating with ground-based robots or leveraging augmented reality to provide immersive security training experiences.

The autonomous drone industry emphasizes safety through advanced collision-avoidance systems, privacy through strict data protection practices, and compliance

by working closely with regulatory bodies. These proactive measures ensure that drones are a responsible and effective solution for modern security challenges.

LOOKING AHEAD

The transformative power of indoor drones can be seen in diverse environments, demonstrating their broad impact on security and operational efficiency. At logistics centers in Nevada, for example, indoor drones have led to a 30 percent reduction in inventory discrepancies, while retail chains in California have experienced a 40 percent decrease in after-hours break-ins.

Innovations in AI, autonomy and collaborative operations hold the promise of further expanding drone capabilities. As the regulatory landscape evolves alongside public acceptance, drones are set to become even more integral to the security and surveillance infrastructure. ◀

> THE INTEGRATION OF DRONES WITH AI AND MACHINE LEARNING IS ENABLING AUTONOMOUS DECISION-MAKING, PREDICTIVE ANALYTICS, AND SOPHISTICATED THREAT DETECTION CAPABILITIES THAT WERE PREVIOUSLY UNATTAINABLE.

Amplifying School Security with Gunshot Detection Systems

Solutions can speed response to the threat

Rich Onofrio (ronofrio@shooterdetectionsystems.com) is the Chief Technology Officer of Shooter Detection Systems (www.shooterdetectionsystems.com).

GUN VIOLENCE IN AMERICAN SCHOOLS is a topic that no one likes to think about, much less discuss. Preventive measures should be priorities, including security practices and technologies, and resources should be provided to help students and staff deal with mental health and anger issues before they escalate. But schools must also prepare for when these efforts are not enough.

Nearly 60 percent of active shooter incidents at educational institutions since Columbine in 1999 have occurred in high schools, and about 21 percent have occurred in middle schools or junior high schools. The remainder have happened in elementary schools, K-8 schools and K-12 schools.

The number of individuals killed or injured in school shootings in 2023 was more than double the number of casualties in 1999.

Gunshot detection systems have emerged as a meaningful component of a comprehensive security strategy that can have a significant impact on the outcome of active shooter incidents. These systems can be leveraged to quickly alert everyone of a dangerous situation, enabling them to react and respond before it is too late.

THE LIMITATIONS OF CURRENT RESPONSE SYSTEMS

During gun violence incidents, knowing exactly where the incident is happening in real time is critical so that building occupants can quickly get to safety and first responders can rapidly mitigate the threat.

> DURING GUN VIOLENCE INCIDENTS, KNOWING EXACTLY WHERE THE INCIDENT IS HAPPENING IN REAL TIME IS CRITICAL SO THAT BUILDING OCCUPANTS CAN QUICKLY GET TO SAFETY AND FIRST RESPONDERS CAN RAPIDLY MITIGATE THE THREAT.

At Virginia Tech in 2007, an active shooter managed to go undetected for two and a half hours after his first two shots were fired in a dormitory. He later shot 47 people that he locked inside of an academic hall. After this incident,

the implementation of more robust mass notification systems became commonplace. However, these systems often rely on human action to trigger them, which can result in errors and delays, highlighting the need for better technological solutions.

The premise behind gunshot detection is that the system will alert first responders faster than any current method so that they can get to the scene faster, armed with critical incident details they might not otherwise have. Providing vital location information, including where in the building the incident is happening, cuts through typical alert delays and enables a more immediate response to be initiated. To maximize effectiveness, a gunshot detection system should be capable of sending real-time data and updates to 911 operators – and it must be reliable enough that law enforcement agencies will accept the technology into their workflow.

Both speed and accuracy are paramount. The average length of an active shooter incident is around five minutes,

with an average of one death occurring every 5 to 15 seconds while active shooting is taking place. Ultimately, a school needs to be able to rely on the gunshot detection system to automate the alerting process as early as possible and with the highest level of accuracy to make a real impact.

When integrated with other technologies already in many schools, such as video surveillance, metal detectors and electronic locks, gunshot detection systems provide a crucial layer of detection that can instantly alert staff if a determined shooter is undeterred by other countermeasures. This layered approach is recommended by leading school safety organizations, such as the Partner Alliance for Safer Schools (PASS), and is included in the Cybersecurity & Infrastructure Security Agency's (CISA) Guidelines for School Safety.

A GUIDE TO EVALUATING SYSTEMS

Much like other security technologies, not all gunshot sensors and alerting systems are created equal. At their core, indoor gunshot detection systems include one or more sensors, strategically positioned within a facility, that transmit gunshot alerts through a communications platform.

> THE PREMISE BEHIND GUNSHOT DETECTION IS THAT THE SYSTEM WILL ALERT FIRST RESPONDERS FASTER THAN ANY CURRENT METHOD SO THAT THEY CAN GET TO THE SCENE FASTER, ARMED WITH CRITICAL INCIDENT DETAILS THEY MIGHT NOT OTHERWISE HAVE.

When evaluating sensor types, it is important to understand how the sensor functions. The simplest approach is to ask some very basic questions: How is a gunshot identified? How is the information getting to key stakeholders on campus? How long does that take? Is the information accurate?

Acoustic-Only Solutions

It is not technically difficult to simply place a microphone on a wall and calibrate it to detect an acoustic signature that meets a certain criterion. This approach, however,

> WHEN EVALUATING SENSOR TYPES, IT IS IMPORTANT TO UNDERSTAND HOW THE SENSOR FUNCTIONS. THE SIMPLEST APPROACH IS TO ASK SOME VERY BASIC QUESTIONS: HOW IS A GUNSHOT IDENTIFIED? HOW IS THE INFORMATION GETTING TO KEY STAKEHOLDERS ON CAMPUS? HOW LONG DOES THAT TAKE? IS THE INFORMATION ACCURATE?

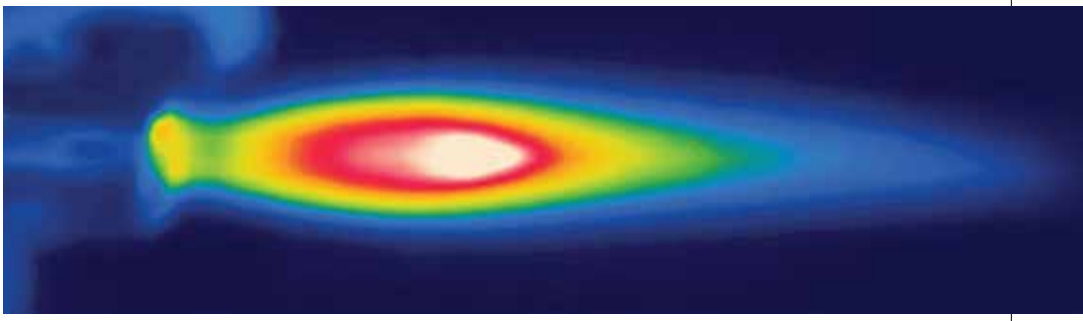
will lead to a high number of false alerts.

Multi-Mode Solutions

Since every gunshot creates both an acoustic signature (bang) and an infrared signal (flash) (including most suppressed weapons), a sensor that uses both signals to detect shots will be the most effective. If a vendor claims to detect a gunshot through a physical barrier (like a wall), it is likely the system is not using the infrared signal to assess the event. The infrared flash should be detectable even if the shooter is not in the line of sight of the sensor – for example, is facing away from it.

Calibration

Some sensors require calibration to the environment. For example, a calibration-required sensor in a large gymnasium may need a different setting than one in a school lobby. Manual



calibration involves close monitoring and analysis before sensors are fine-tuned to sounds in the environment. A plug-and-play sensor that does not require calibration will be the most reliable and will be less susceptible to human error.

External Validation

Systems that rely on acoustics alone can potentially produce false alerts resulting from innocuous loud noises. In these cases, external validation measures are needed to verify a gunshot before an alert is sent to authorities. Some systems send audio files to human analysts or stream audio to the cloud to confirm "possible" shot events. Audio clips sent outside of a local server, however, can raise privacy concerns. Additionally, sensors that rely on any type of external validation inherently slow down the notification process, weakening the benefit of real-time alerting.

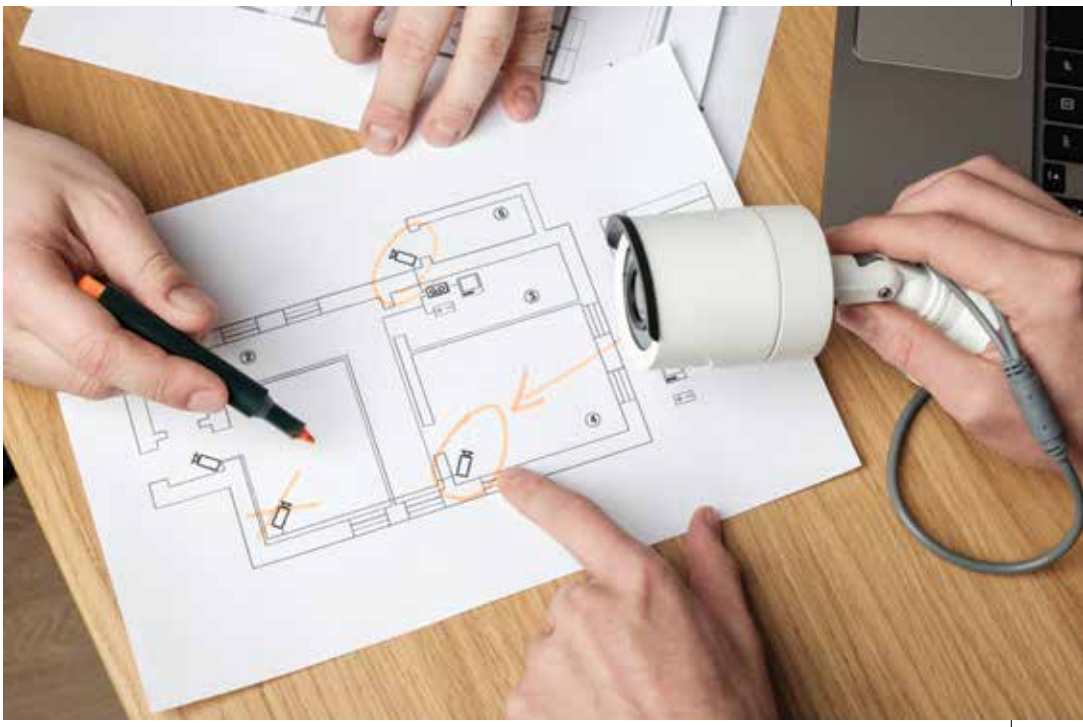
NAVIGATING THE LANDSCAPE OF GUNSHOT DETECTION SYSTEMS

More than 20 years of realistic active shooter drills being conducted in schools and other environments have shown that these drills are potentially more traumatizing than they are beneficial. Gunshot detection systems that have simulation and training modes can activate shot detection in the software without needing to present a weapon into the environment. Like fire alarm drills, a simulated active shooter drill can help organizations initiate a calmer, more organized, less traumatic training experience.

> MORE THAN 20 YEARS OF REALISTIC ACTIVE SHOOTER DRILLS BEING CONDUCTED IN SCHOOLS AND OTHER ENVIRONMENTS HAVE SHOWN THAT THESE DRILLS ARE POTENTIALLY MORE TRAUMATIZING THAN THEY ARE BENEFICIAL.

School safety administrators need to understand the uses of multiple technologies and how they can be effectively deployed without breaking the budget. Manufacturers that cannot clearly describe how their technology works, that rely on downplaying competitor products, or that do not embrace the added work of third-party verification are only creating more confusion about what solutions will deliver the best results.

For all the benefits that gunshot detection can bring to an organization, one of the difficulties with system selection is that there is no central governing body that regulates the industry or monitors marketing claims. Until that day comes, one important resource that schools should use is the Department of Homeland



Security's SAFETY Act program. Technologies that are SAFETY Act certified bear the agency's red seal of approval. This indicates that the solution is listed on the DHS Approved Products List for Homeland Security and has been vetted by the DHS Science and Technology Directorate.

Schools can look to experts like security consultants or integrators to advise them on system selection, implementation and integration, as well as funding vehicles. If a school does not have a relationship with a trusted security consultant or integrator, administrators should seek out security systems providers that specialize in video, access control and emergency notification systems. In addition to national solutions providers, there is a growing number of smaller, regional systems integrators who offer an indoor gunshot detection product.

By employing gunshot detection systems, schools can add a crucial layer to their existing security and crisis response plans that is purpose-built for fast response and mitigation of loss of life. ◀

A Seamless and Sustainable Approach to Access

As mobile credentials become ubiquitous, mobile access systems become more powerful

Sanjit Bardhan (sanjit.bardhan@hidglobal.com) is Vice President & Head of Mobile for HID Global (www.hidglobal.com).

PICTURE GOING TO THE OFFICE AND QUICKLY ENTERING by just tapping a smartphone against a digital reader. There is no searching for keycards or badges, just seamless access granted. As you make your way through the building, from the lobby to your designated floor, the lighting adjusts automatically to your presence. Behind the scenes, security managers have peace of mind knowing that access is tightly controlled and managed remotely through a cloud-supported platform, while building owners have confidence that their buildings are operating efficiently and securely.

This shift in how individuals navigate modern building environments is the essence of mobile access control. Around the world, a growing number of organizations are leveraging the benefits of mobile access technologies to enhance

security and employee access management. And as credentials are integrated with digital wallets, mobile access is taking on new dimensions.

CONVENIENCE MEETS SECURITY

Mobile access through digital wallets simplifies controlled access to buildings and elevates the user experience. While digital wallets have been around for payment transactions for some time, they are now holding medical prescriptions, travel documents, driver's licenses, ID cards, insurance information and more. With the integration of employee badges into digital wallets, individuals can authenticate themselves to their employers using their smartphones or smartwatches and seamlessly access office doors, elevators, turnstiles, parking lots and many other building locations and amenities. There is no need to carry physical plastic badges or keycards, lowering costs associated with printing, maintenance and replacement. This shift to digital credentials also aligns with sustainability goals by reducing plastic waste.

> THIS SHIFT TO DIGITAL CREDENTIALS ALIGNS WITH SUSTAINABILITY GOALS BY REDUCING PLASTIC WASTE.

With mobile devices now ubiquitous, particularly among younger, digitally native generations, mobile access is a logical step for organizations seeking seamless and enhanced access control.

The 10 questions below can help security

10 QUESTIONS FOR SECURITY PROFESSIONALS CONSIDERING MOBILE CREDENTIALS

1. Have you considered all of the opportunities in the organization?
2. Do you understand all of the elements in a mobile access system?
3. Have you assessed your specific needs?
4. Do you understand mobile access communication standards?
5. Are you considering an end-to-end system?
6. Are the subsystems interoperable?
7. Are all of the stakeholders aligned?
8. Have you considered the total cost of ownership?
9. Are you addressing data privacy concerns?
10. Have you chosen the right partners?

> MOBILE ACCESS CAN BE INTEGRATED WITH SMART BUILDING CONTROLS TO MANAGE FACILITIES MORE SUSTAINABLY THROUGH REAL-TIME LOCATION SYSTEMS.

professionals and decision makers better understand how these systems work and how to deploy them successfully.

1. Have you considered all of the opportunities in the organization?

Access systems are not just about building entry and exit. For example, mobile access can be integrated with smart building controls to manage facilities more sustainably through real-time location systems. By sharing pertinent occupant data, the smart building system can optimize operational efficiency by adjusting temperature settings, particularly in underutilized areas of the building. This not only enhances comfort but also contributes to achieving green building goals by reducing energy consumption.

Mobile access systems can also be used in various scenarios. For example, employees, tenants and visitors may now use a mobile identity for building access but have to use a plastic card to

check in at a time clock. Companies can achieve the greatest implementation success by allowing mobile access use for every application in their environment.

2. Do you understand all of the elements in a mobile access system?

When starting a deployment, it helps to review the essential elements that go into a mobile access system. Typical systems usually consist of four main components.

- *Hardware* – This includes the credential reader units placed on walls, doors, elevators, turnstiles, etc., wherever access is required.
- *Mobile credential* – This is the actual credential that is downloaded onto the user's device.
- *Cloud platform* – A mobile, cloud-based service stores and processes data, helping administrators easily and efficiently manage user enrollment, credential provisioning, lifecycle management, data

> ALONG WITH SELECTING READERS AND LOCKS, MOBILE ACCESS DEPLOYMENT ALSO REQUIRES CREATION AND MANAGEMENT OF MOBILE IDS AND THE BUILDING OF MULTILAYERED AUTHENTICATION FOR PHYSICAL AND LOGICAL ACCESS CONTROL.

privacy and other tasks.

- *Delivery technology* – This is what provides system capabilities and functionality, either directly or via a customized app provided by a technology partner.

3. Have you assessed your specific needs?

Every deployment is unique, and security practitioners and integrators should consider several factors.

- *Readers* – Determine whether readers are already enabled for mobile deployment or need to be upgraded. Some readers can easily be made mobile-capable by adding a small device, while older legacy readers may need to be fully replaced. Check with the manufacturer for mobile readiness, as more modern readers can be easily reconfigured, even if they were originally installed for traditional card access.
- *End user preference* – Identify preferences, such as iOS or Android.
- *Number of credentials* – Determine how many mobile licenses will be needed now and in the near future.
- *Use cases* – Some organizations may

need a mobile access system to only open doors or secure areas. Others may need a system that covers a range of uses, from doors and turnstiles to secure printing and network access.

- *Implementation* – Is it possible to transition to mobile in a single phase, or should it be implemented over time? It is important to remember that the readers should be as interoperable as possible to support mixed use of access control technologies.

4. Do you understand mobile access communication standards?

A mobile system relies on one of two types of communication standards to connect the mobile device with the reader: Bluetooth Low Energy (BLE), which can operate both at close range and from longer distances, and near-field communication (NFC), which operates at very close range, making it ideal for applications of less than 10cm. Both standards support iOS and Android devices. Because building environments and readers vary, the ability to fine-tune the reading distance depending on the desired opening mode – such as long-range, tap or gesture-based – can be an important feature.

5. Are you considering an end-to-end system?

From smart devices and mobile credentials to readers and locks, creating a secure environment should include a holistic view of the system. Along with selecting readers and locks, mobile access deployment also requires creation and management of mobile IDs and the building of multilayered

authentication for physical and logical access control. Organizations must also ensure secure, seamless provisioning with the ability to monitor and modify security parameters.

6. Are the subsystems interoperable?

Within mobile access, interoperability allows different products and technologies to exchange usable information. For example, an effective system works across multiple applications, from accessing a conference room to entering a parking garage. Direct application programming interfaces (APIs) within the mobile access system allow integration with multiple types of mobile devices and backend systems.

7. Are all of the stakeholders aligned?

In the past, access system buying decisions might have been handled by the security department alone. Now, particularly in larger organizations, many more stakeholders, including IT and HR, are involved. Providing information

for these stakeholders to better assess the value and functionality of a mobile access system helps make it easier to achieve cross-department cooperation.

8. Have you considered the total cost of ownership?

Pricing a mobile access system may require a different approach from what is typically used because a 1:1 comparison with card-based systems can be misleading. While plastic credentials are typically a one-off cost, mobile credentials operate on a subscription-based model. Reputable manufacturers will provide cost of ownership tools that allow organizations to compare expenses in a standard use case.

For stakeholders interested in meeting sustainability goals, a mobile access system

PROVIDING INFORMATION FOR STAKEHOLDERS TO BETTER ASSESS THE VALUE AND FUNCTIONALITY OF A MOBILE ACCESS SYSTEM HELPS MAKE IT EASIER TO ACHIEVE CROSS-DEPARTMENT COOPERATION.

accelerates the path toward eco-friendly operations by eliminating plastic cards. Look for mobile access systems that carry independent certifications to validate their contributions. Mobile access systems can also contribute to LEED certification.

9. Are you addressing data privacy concerns?

The adoption of mobile access significantly reduces the risk of credentials being lost or cloned. Mobile access solutions that have earned third-party certifications ensure the system is highly secure and reliable. If an enterprise spans different regions, it is important to make sure the system has country-specific compliance certifications.

10. Have you chosen the right partners?

The transition to mobile access requires an ecosystem of partners, from the manufacturer of the system to the integrator that installs the readers and integrates the various software and hardware platforms in the facility. Range of experience, verified security credentials, and a wide solutions portfolio

all matter when it comes to mobile access deployment. Whether at a regional real estate company or a large university, it is important to select partners that understand the site's unique needs, provide customer-driven solutions, and make the transition as seamless and cost-efficient as possible.

Mobile access experts can help to assess needs and recommend future-proof components, making it easier for the system to evolve along with mobile technology. Likewise, the right partner can provide regional expertise at the global level, which enables scaling solutions from one part of the world to another.

Mobile access control represents a pivotal evolution in security applications, offering a potent combination of convenience, security and adaptability. From a seamless end user experience to making progress toward sustainability goals, these solutions provide many benefits to organizations of any size. Understanding the fundamentals of the system, as well as key factors to make the deployment successful, can help security practitioners open doors in new, more efficient ways. ◀

New Solutions for Multi-Family Access Control

Cloud platforms and mobile credentials offer convenience and security

Jennifer Lytle (jennifer.lytle@liftmaster.com) is Vice President and General Manager, Emerging Business, at LiftMaster (www.myq.com/community).

ACCESS CONTROL SYSTEMS FOR APARTMENTS, CONDOMINIUMS AND GATED COMMUNITIES have evolved from traditional methods such as keys, cards and fobs to more advanced solutions. Smart access control presents an opportunity to foster new client relationships, and security integrators who are serious about growing their business should get in front of the transition from traditional legacy approaches. The new standard for convenient and secure entrance control is a cloud platform that automates entry requests and gives residents an app that controls every entrance.

WHAT TO KNOW ABOUT CLOUD ACCESS CONTROL SYSTEMS

For multifamily property managers, it can be time consuming to grant entry to large numbers of visitors, including delivery drivers, service people,

maintenance crews, and guests. Whether the entrance to be secured is a gate, an outside door, an interior door like a package locker, or a resident's front door, there are too many people and deliveries for managers to oversee on top of other responsibilities.

A cloud access control platform automates entry management for busy multifamily buildings. The benefits of such a platform are many and include the following.

- *Scalability* – It is flexible, accommodating changes in the number of doors to secure and the number of users, as well as adjustments to access levels without having to update the software.
- *Flexibility* – It can be accessed and managed from anywhere using a web browser, tablet

> FOR MULTIFAMILY PROPERTY MANAGERS, IT CAN BE TIME CONSUMING TO GRANT ENTRY TO LARGE NUMBERS OF VISITORS.

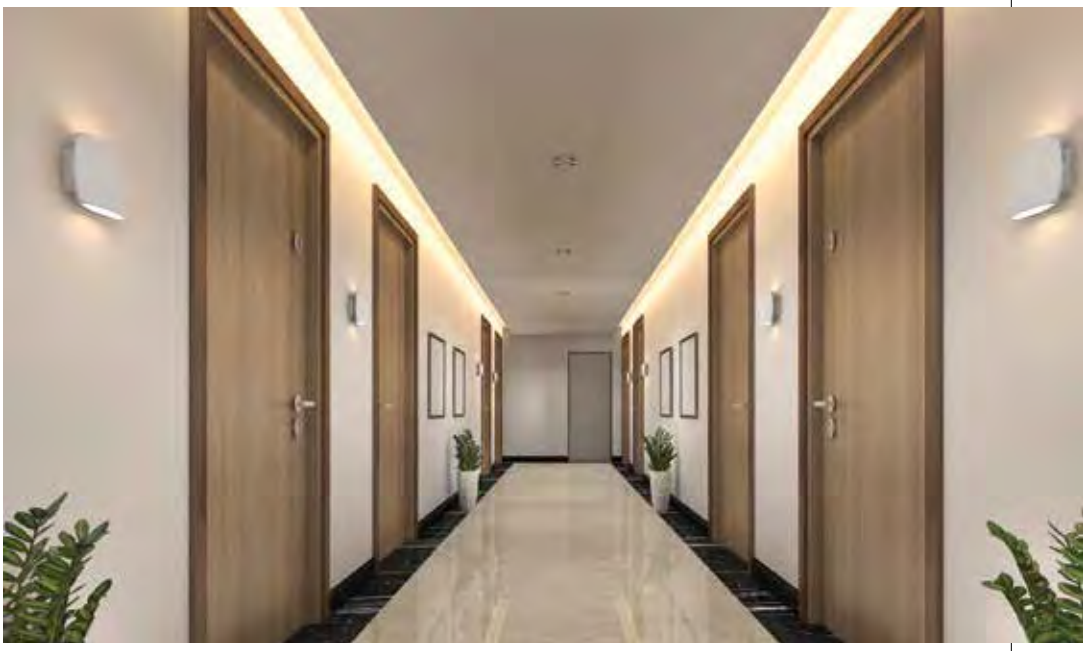
> A CLOUD ENTRANCE CONTROL PLATFORM ENABLES MOBILE CREDENTIALS AND ALLOWS RESIDENTS TO USE A SMARTPHONE APP AS A DIGITAL KEY.

or laptop for property managers and a smartphone app for residents. Property managers can grant or revoke access to anyone from anywhere.

- *Cost effectiveness* – It is sold "as a service," with a monthly subscription, which avoids large capital expenditures.
- *Security* – It uses encryption and authentication protocols to protect the data and communication between the devices and the servers.

WHAT TO KNOW ABOUT MOBILE CREDENTIALS

A cloud entrance control platform enables mobile credentials and allows residents to use a smartphone app as a digital key. Using wireless technologies such as Bluetooth or near-field communication (NFC), mobile credentials communicate with either smart card readers or video intercoms installed at property entrances.



They are a convenient and secure alternative to physical keys, cards and fobs, especially for Millennials and Gen Z, who use their smartphones for everything.

According to a report by MarketsandMarkets, the global market for mobile access control is expected to grow from $1.2 billion in 2020 to $3.6 billion by 2025 at a compound annual growth rate (CAGR) of 23.9 percent.

The report cites the increasing adoption of smartphones, the rising demand for contactless access control solutions, and the growing awareness among property managers that today's renters value entry control apps and will pay higher rents to get them.

Mobile credentials provide multiple benefits, chief among them convenience and security. Encryption and authentication protocols prevent unauthorized access and card cloning and allow property managers to revoke or send new credentials remotely and receive notifications of access events.

DEMAND DRIVERS

Three trends are contributing to the increasing use of mobile credentials.

BENEFITS OF CLOUD-BASED SOLUTIONS AND MOBILE CREDENTIALS:

- Enhance appeal and value of property with modern and convenient features
- Improve operational efficiency and cost effectiveness by eliminating keys, cards and fobs
- Increase security and compliance through real-time control of access

MOBILE CREDENTIALS PROVIDE MULTIPLE BENEFITS, CHIEF AMONG THEM CONVENIENCE AND SECURITY.

Demand for smart home technology and security

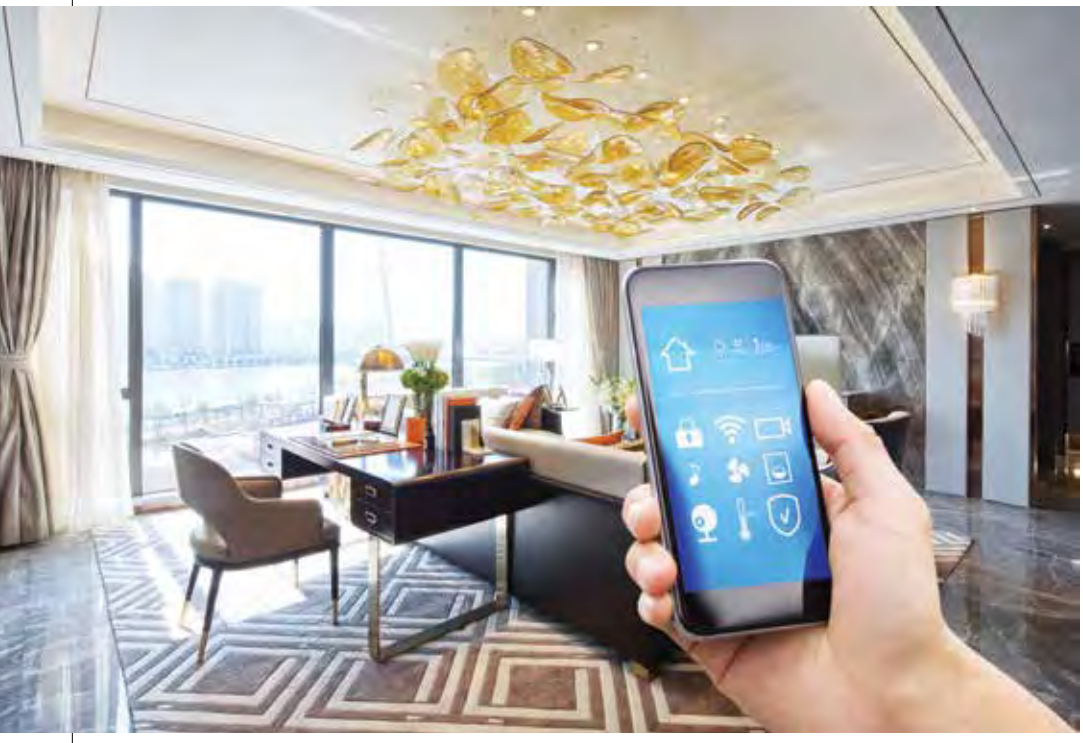
According to Statista, the global smart home market reached $141 billion in 2023. More renters want smart home features that enhance comfort, convenience and security, such as voice control hubs, smart thermostats, smart video intercoms, and smart locks.

Shift to contactless solutions

The Covid-19 pandemic accelerated the interest in contactless solutions to reduce the risk of infection. Although surface transmission is not the threat it was once thought to be, a preference for touchless solutions remains.

Rise of remote work

The pandemic also increased the number of people who work from home or have hybrid schedules. According to a report by Upwork, 36.2



million Americans will be working remotely by 2025, an 87 percent increase from pre-pandemic levels. As a result, more residents need to manage access for guests from their home office.

CHOOSING A TRUSTED ACCESS CONTROL BRAND

Not all cloud access control platforms and mobile credentials are created equally. Security integrators add value to their business when they recommend products that are designed for a flawless customer experience and are built to last in high-traffic areas. It is essential to provide customers with a trusted brand that will deliver the best solutions and support.

Cloud platforms and mobile credentials are the most important security trends shaping the future of multifamily access control. By improving and expanding their service offerings and encouraging the adoption of these solutions, security integrators can add value to their business through bundled product purchases, installation and maintenance support. At the same time, they are helping property managers increase their property's appeal and value, improve operational efficiency, and increase net operating income by attracting renters who value smart tech and will pay more to get it. ◀

CLOUD PLATFORMS AND MOBILE CREDENTIALS ARE THE MOST IMPORTANT SECURITY TRENDS SHAPING THE FUTURE OF MULTIFAMILY ACCESS CONTROL.

Can AI Reverse Security's Declining Margins?

Repurposing and expanding video surveillance infrastructure may be the key to long-term success

Matt Powell (matt@issvs.com) is Managing Director for North America at ISS (www.issivs.com).

THE LAST SEVERAL YEARS HAVE BEEN A BIT OF A ROLLER COASTER RIDE for the security industry. On one hand, the uncertainty created by the global spread of Covid-19 was a bit of a boon initially to the market, creating demand for solutions, such as remote video monitoring, that organizations could use to keep tabs on what were largely vacant facilities at the time. Another benefit brought about by the pandemic was that it allowed integrators to get into buildings to work without having to worry about disrupting the day-to-day activities of employees or tenants.

However, as weeks turned into months and months dragged on into years, the global supply chain issues brought about by on-again, off-again lockdowns created significant project backlogs and inventory challenges and even affected the ability

of integrators to provide basic levels of service. If these impacts were not bad enough, the pandemic also significantly contributed to skyrocketing inflation rates across all manner of products, including security solutions.

In fact, according to the *Security Business* State of the Security Industry 2022 report, 60 percent of integrators surveyed reported being affected in some way by rising interest rates and inflation, with responses ranging from being unable to secure loans and funding to delaying a potential sale of the business to having to cut back on wages, raises and benefits for employees. Additionally, 46 percent of integrators said that every manufacturing partner

> THIS COMBINATION OF INCREASED COMPETITION AND A RELATIVE LACK OF PRODUCT DIFFERENTIATION HAS RESULTED IN WHAT SEEMS LIKE EVER-SHRINKING MARGINS FOR INTEGRATORS AS THE MANUFACTURING COMMUNITY HAS EMBARKED ON A "RACE TO THE BOTTOM."

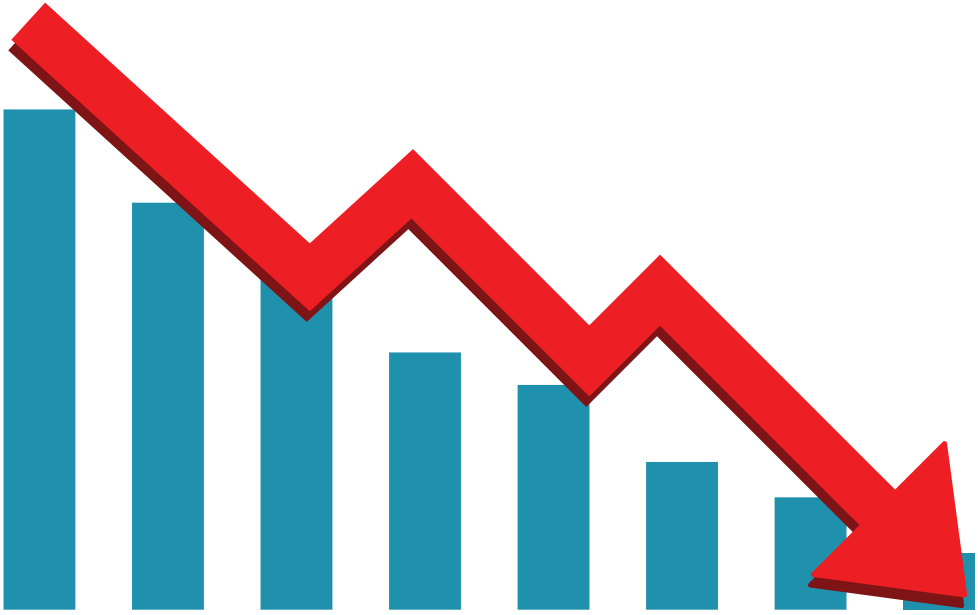
they worked with raised their equipment prices in 2022, while another 34 percent said that 75-99 percent of their vendors increased prices.

These challenges have exacerbated one of the industry's biggest challenges – declining margins on security hardware. Surveillance cameras, in particular.

THE RACE TO THE BOTTOM

It may seem counterintuitive, but some of the greatest innovations in video surveillance technology over the past few decades – which have simultaneously served to propel adoption across nearly every market imaginable – have now been incorporated by most manufacturers into their own product lines, thereby making cameras a commodity. The proverbial IP tipping point, in which sales of network cameras exceed analog, seems to have come and gone without anyone taking much notice.

No one really talks about IP vs. analog that much anymore because IP has become the de facto standard. Similarly, high-resolution and multi-sensor cameras are now widely available from a majority of



brands. The meteoric rise in the 2010s of China-based video surveillance manufacturers that provided parallel or even superior functionality to many industry stalwarts also served to drive prices lower.

This combination of increased competition and a relative lack of product differentiation has resulted in what seems like ever-shrinking margins for integrators as the manufacturing community has embarked on a "race to the bottom" where the winner is whoever can provide the best camera at the cheapest possible price.

The consequences of this new business paradigm are finally coming home to roost for many companies that thought they could ride the hardware gravy train over the long term. The aforementioned State of the Security Industry report, for example, found that while nearly three quarters of integrators reported revenues being "significantly" or "slightly" up in 2022 compared to 2021, less than 60 percent of respondents polled said that their gross profit margins increased similarly over the same time period.

So, rather than acting in the best interest of their clients and building a

> EDGE PROCESSING IS CURRENTLY NOT AT THE POINT WHERE IT CAN CONSISTENTLY AND RELIABLY DELIVER THE SAME PERFORMANCE THAT ONSITE SOLUTIONS DO, NOR WILL IT HAVE THE CAPABILITY TO DO SO ANYTIME SOON.

solution that is truly "best-of-breed," a significant number of integrators have resorted to discount shopping among their vendor and distribution partners as a way to squeeze an extra point or two of margin out of their project pipeline.

This is not only dangerously myopic for integrators as they look to build long-lasting relationships with end users, but it has also incentivized vendors to look into ways of bypassing the channel to sell direct, as they too have experienced a significant shift in the profitability of their businesses. Many integrators have decided to hedge their bets against this ongoing trend by exploring new technologies and service offerings that will enable them to charge a premium above and beyond simple hardware sales.

LIVING ON THE EDGE

One area of heavy emphasis within the video surveillance market for a while now has been the development of cheaper, more powerful processors embedded within the cameras themselves as a way to reduce the infrastructure footprint. If all of the image processing and prerequisite capabilities needed for a deployment can be done inside the camera, then the need for things like specialized servers, cabling and other products that quickly add up on a video install should be greatly reduced. Or so the thinking goes.

The problem with this notion is that edge processing is currently

not at the point where it can consistently and reliably deliver the same performance that onsite solutions do, nor will it have the capability to do so anytime soon. The ability to process high-resolution images alongside other data-intensive applications like video analytics inside of cameras is still years away from becoming a realistic possibility. Therefore, any potential cost savings a business would realize by leveraging a surveillance network with edge-based processing would quickly be wiped out by the performance issues and the inability of operators to get the data they need.

In fact, during an event at ISC West 2023, security technologist and SIA Public Safety Interest Group Chairman Steve Surfaro cautioned against the market looking to the edge as a way to run artificial intelligence (AI), analytics and other tools. "Right now, most solution providers in the industry are looking to do edge AI. Absolutely ridiculous right now," he said. "You should be focusing on offloading the CPU cycles off of your VMS platform and using an AI processor."

THE 'AS-A-SERVICE' TRAP

Another popular way the industry has looked to offset declining margins is through the use of video surveillance as a service (VSaaS), access control as a service (ACaaS) and other hosted/managed offerings. This enables businesses to swap large, upfront capital expenditures for a monthly operational cost, similar to the residential market where dealers provide alarm systems and sensors for free in exchange for creating a recurring monthly revenue (RMR) generating account.

This has largely been painted as a win-win for both integrators and end users. RMR enables integrators to reap the benefits of steady and

> WHILE THE FIRST ANALYTICS THAT HIT THE MARKET IN THE MID-2000S LARGELY OVERPROMISED AND UNDERDELIVERED, TODAY'S AL SOLUTIONS ARE STARTING TO PAY DIVIDENDS AS A FORCE MULTIPLIER FOR END USERS AND A MONEYMAKER FOR INTEGRATORS.

reliable income streams, as opposed to having to rely on one-off projects with long sales cycles that are becoming increasingly affected by a wide range of economic factors. In addition to not having to invest in video or other security hardware, end users can also rest easy from a maintenance perspective, knowing that all of their updates will be done automatically by the service provider.

With what seem like so many benefits for all involved, where's the rub? The issues are actually myriad for both integrators and end users. With regard to the integrator, they are largely outsourcing the customer relationship to a third-party provider – be it a cloud solution vendor or a video monitoring firm – who can then take the customer direct or possibly harm the integrator's reputation should they provide a poor level of service. And the end user, since they do not own the equipment outright, is forced to use whatever hardware has been specified for the project

and cannot scale with the same level of flexibility that comes with system ownership.

AI AND VIDEO'S THIRD WAVE

Yet another area that integrators are turning to as a way to increase their profit margins is through the adoption of AI-powered video analytics, which hold enormous potential for businesses even beyond traditional security applications and use cases. Looking at video surveillance innovation in terms of waves, with the first being analog cameras and DVRs and the second being IP cameras and video management software, the industry appears to now be in the third wave, with AI-driven software algorithms and neural network training methodologies. While the first analytics that hit the market in the mid-2000s largely overpromised and underdelivered, today's Al solutions are starting to pay dividends as a force multiplier for end users and a moneymaker for integrators.

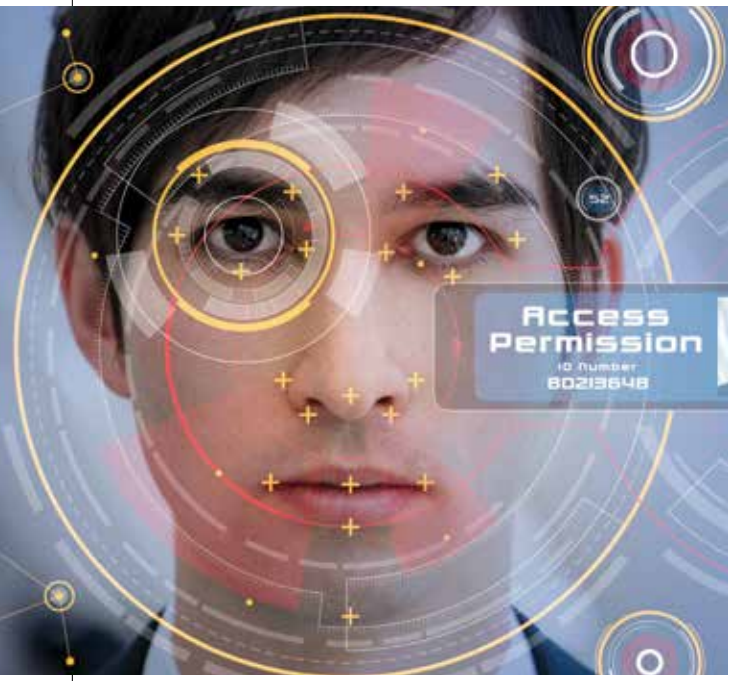
Not only can analytics be tailored to help organizations mitigate specific types of risks depending on their operating environment, they also represent a potential windfall for the security industry as a whole. The 2023 *SDM* 100, for instance, quoted several integrators who see significant opportunities for their businesses in providing AI analytics to the market.

"The market was generally strong, but not much different than 2021,"

according to one alarm company. “CCTV was strongest and analytics were key.”

Another alarm company reported, “In its commercial and national account business units, [the company] experienced growth in most verticals in 2022 as employers made efforts to bring employees back to the office safely. These employers were also seeking new ways to efficiently manage multi-site locations and overcome labor shortages, evidenced by new investments into AI and cloud-based systems.”

A majority of integrators (56 percent) who took part in the State of the Security Industry survey reported having a strong interest in adding AI-based technologies to their offerings. And though some think of AI as only being a video surveillance tool, the technology is being increasingly used in access control, since facial recognition can be leveraged as a secondary or even primary method of authentication in certain circumstances.



Despite the varied applicability, increased product differentiation, and higher profit margins that AI and video analytics bring to the table, many integrators remain fixated on simply selling more cameras as the best way to grow their business and overall footprint in the market. Perhaps unsurprisingly, the vast majority of integrators (77 percent) in the State of the Security Industry survey reported that IP cameras were their top performing video surveillance product offering in the previous year, with all other product categories – including video management software (45 percent), video storage and playback (39

percent) and cloud/hosted video (31 percent) – far behind.

The number of camera options that integrators have to choose from continues to dwindle, which will further amplify the margin crunch. According to a 2023 report from market research firm Novaira Insights, demand for both video surveillance hardware and software remains strong as the global market, excluding China, grew by more than 13.2 percent in 2022. However, with each passing year, the industry's largest vendors continue to increase their portion of the video surveillance pie. The research firm noted that the combined market share of the world's 10 largest vendors grew from 61 percent in 2020 to 64 percent in 2022.

As consolidation intensifies in the years to come, there will likely be fewer and fewer options for integrators to mark up. Resorting to bargain hunting is not a business model for long-term, sustained success, nor is investing in largely unproven technology and service offerings.

THE PROLIFERATION OF IP AND HIGH-DEFINITION CAMERAS MEANS THAT ANALYTICS CAN USUALLY BE ADDED TO A SYSTEM WITHOUT THE NEED FOR ADDITIONAL HARDWARE.

AI and the current generation of video analytics provide integrators with a key advantage over many of these other alternatives: pre-existing infrastructure. The proliferation of IP and high-definition cameras means that analytics can usually be added to a system without the need for additional hardware, providing integrators with the ability to resell them without having to invest time and manpower resources in ripping and replacing the current technology stack.

Artificial intelligence is fundamentally transforming the way companies do business and it will revolutionize how they think about and approach security and safety. The industry will be anything but "business as usual" for the foreseeable future and AI is a big reason why. ◀

Tightening the Perimeter with Technology

AI and other solutions can turn security from reactive to proactive

Jamie Bradford (jbradford@evolontech.com) is the Director of Technology Solutions at Evolon (www.evolontech.com).

IN RECENT MONTHS, THERE HAS BEEN A NOTICEABLE EVOLUTION within the security sector, a transition from traditional physical defenses to technological solutions. This significant shift has greatly enhanced the scope and effectiveness of perimeter defense strategies, propelling solutions beyond the conventional reliance on physical barriers and personnel toward a future of increased efficiency, precision and adaptability.

The infusion of cutting-edge technology into perimeter defense mechanisms represents a pivotal advance toward more sophisticated, effective and reliable security monitoring

systems. It marks the dawn of an era where the advantages of modern solutions far exceed those of conventional security measures.

The heightened interest in a more technological approach is driven by several factors, including the need for instantaneous monitoring and analysis, minimization of false alerts, and improvement in the promptness and efficacy of responses to security threats. Surveillance systems equipped with the latest technological advancements are at the forefront of addressing these needs. As these technologies continue to mature, they hold the promise of revolutionizing security protocols, contributing to the creation of safer and more secure environments.

> TRADITIONAL METHODS COME WITH THEIR OWN SET OF CHALLENGES, INCLUDING ONGOING MAINTENANCE EXPENSES, THE POTENTIAL FOR HUMAN ERROR OR OVERSIGHT, AND THE DIFFICULTY OF SURVEILLING EXPANSIVE AREAS.

> THE ADOPTION OF STATE-OF-THE-ART TECHNOLOGIES WITHIN THIS MARKET SEGMENT MARKS A SIGNIFICANT SHIFT TOWARD AN ANTICIPATORY SECURITY STANCE, MOVING FROM A REACTIVE RESPONSE TO INCIDENTS AS THEY UNFOLD TO A STRATEGY THAT PREEMPTIVELY IDENTIFIES POTENTIAL THREATS.

REVISITING TRADITIONAL SECURITY APPROACHES

Historically, the foundation of perimeter defense has been physical barriers and the presence of security personnel tasked with preventing unauthorized entry and responding to incidents. These traditional methods, though, come with their own set of challenges, including ongoing maintenance expenses, the potential for human error or oversight, and the difficulty of surveilling expansive areas.

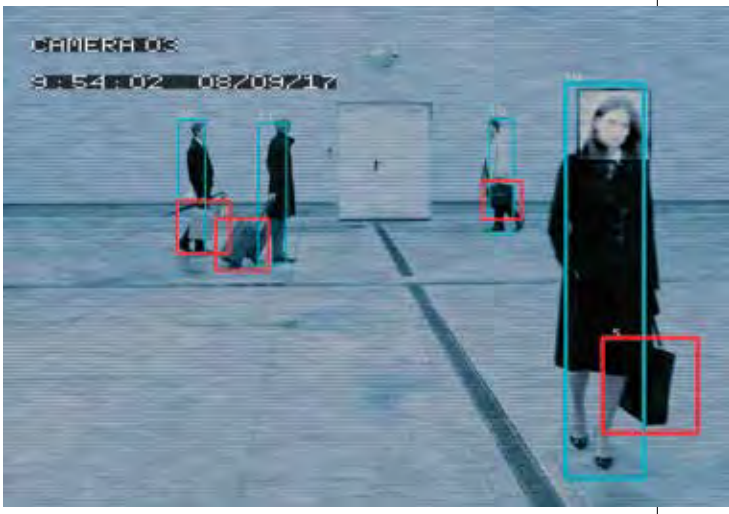
New technologies offer a novel solution to these challenges, leveraging the ability to process and analyze extensive data sets

for informed decision-making. These advanced systems are capable of real-time video monitoring, anomaly detection, and threat prediction with a level of accuracy and speed unattainable by human operators alone.

One of the standout benefits of incorporating the latest technological innovations into perimeter security is the superior ability to detect objects. While the role of security personnel in risk identification is indispensable, the integration of modern technology can significantly amplify their efficiency by automating routine tasks and spotlighting potential threats. The continuous analysis of video and security data helps differentiate between normal occurrences and genuine security incidents, thereby reducing unnecessary alerts.

LOOKING AHEAD WITH PROACTIVE INSIGHTS

The adoption of state-of-the-art technologies within this market segment moves security from a reactive response to incidents as



they unfold to a strategy that preemptively identifies potential threats. This is powered by the detailed analysis of behavior patterns and the spotting of incidents that stray from expected norms. Using the capabilities of data analytics and artificial intelligence, these advanced systems are designed to forecast possible security breaches, allowing for early intervention to minimize damage and

> THESE INNOVATIONS SIGNIFICANTLY BOLSTER SECURITY ARCHITECTURES, ENHANCING RATHER THAN REPLACING THE ESSENTIAL COMPONENTS OF CONVENTIONAL FRAMEWORKS.

> THE UPFRONT INVESTMENT IN SUCH TECHNOLOGY CAN YIELD SUBSTANTIAL LONG-TERM COST BENEFITS BY DIMINISHING THE DEPENDENCE ON ELABORATE PHYSICAL STRUCTURES AND LABOR-INTENSIVE SURVEILLANCE, WHICH ARE TYPICALLY RESOURCE-INTENSIVE TO MAINTAIN.

loss. Transitioning to this anticipatory model of security is a notable progression in asset protection and safety enhancement, steering clear of the confines of reactive methods.

These innovations significantly bolster security architectures, enhancing rather than replacing the essential components of conventional frameworks. For instance, sophisticated monitoring technologies can seamlessly integrate with existing physical deterrents like gates and barriers, introducing intelligent access control methods that adaptively react to threats flagged through ongoing analysis. Such integration may result in the automated securing of vulnerable areas upon threat detection or the adjustment of access rights reflective of the risk level determined by the system. Security teams stand to gain immensely from these technologies, as they deliver essential, actionable intelligence that

aids in strategic decision-making and streamlines response protocols. This melding of human insight with technological advancements elevates the overall efficiency of security measures, forging a more fortified and resilient environment.

Dispelling prevalent assumptions, the transition to these sophisticated technologies is not synonymous with exorbitant expenses. Rather, they emerge as a cost-efficient and scalable alternative to traditional security measures. The upfront investment in such technology can yield substantial long-term cost benefits by diminishing the dependence on elaborate physical structures and labor-intensive surveillance, which are typically resource-intensive to maintain. The scalable nature of these solutions also ensures that they can be tailored and extended to accommodate evolving security demands without requiring a comprehensive revamp of the existing setup. This adaptability guarantees that security protocols can advance in step with new threats and technology developments, maintaining robust protection measures without leading to spiraling costs.

The leveraging of advanced technology within perimeter security opens the gateway to a new chapter of proactive and intelligent safeguarding. The continuous evolution of these technologies will lead to even more refined solutions that are predictive, autonomous and capable of directly addressing threats, setting a new benchmark for the security industry. The security landscape is moving toward a future focused on prevention and foresight, powered by the latest technological advances, signaling the arrival of a transformative era in perimeter defense. ◀

Data from recent market research indicates a market valuation for advanced video analytics of $5.6 billion in 2023, with projections suggesting a climb to $16.3 billion by 2028.

Improving Visitor Management with Lighting Technologies

External illumination boosts accuracy of biometric solutions

Eddie Reynolds (eddier@iluminarinc.com) is the President and CEO of iluminar Inc. (www.iluminarinc.com).

VISITOR MANAGEMENT IS A CRITICAL ASPECT of every physical security plan. Verifying the identity of patrons and guests before granting access to a facility is essential for maintaining a safe environment. Over the last decade, airports, government facilities, banks, data centers and other institutions have increasingly adopted contactless, biometric technology systems, such as facial and iris recognition. In fact, according to Cognitive Market Research, the global contactless biometric technology market size was estimated to be $48.2 billion in 2023 and is forecast to grow at a

compound annual growth rate of 19 percent through 2030.

These technologies are attractive options as they offer a reliable, accurate and unintrusive means for identity validation. They are used to authenticate travelers going through custom checkpoints, verify security clearance prior to granting employees access to restricted areas, confirm when a high-paying patron is in the building so that staff can provide optimal customer service, and bar individuals who have violated company policies and are not allowed to enter the premises.

However, in order for biometric technologies that rely on a visual scan to work effectively, it is essential that security cameras are optimized to capture the highest quality video. This is where infrared (IR) and white light are important.

HOW FACIAL AND IRIS RECOGNITION WORK

Facial recognition analytics use video cameras to scan images, then use algorithms to map faces and detect unique features. This information is translated into hundreds of data points to replicate the geometry of a person's face. The face print is then used as a reference point for employees or visitors who seek to enter a building.

> STUDIES FROM NIST AND OTHER ORGANIZATIONS HAVE ANALYZED THE IMPACT OF LIGHTING ON FACIAL RECOGNITION PERFORMANCE AND FOUND THAT VARIATION IN BRIGHTNESS AND DIRECTION OF LIGHTING IN REFERENCE IMAGES CAN NEGATIVELY AFFECT DETECTION RATES.

Studies from the National Institute of Standards and Technology and other organizations

> CAPTURING CLEAR VIDEO IN LOW OR NO LIGHT SCENARIOS IS EXTREMELY CHALLENGING. EVEN HIGH-QUALITY CAMERAS STRUGGLE WITHOUT CONSISTENT, ADEQUATE ILLUMINATION.

have analyzed the impact of lighting on facial recognition performance and found that variation in brightness and direction of lighting in reference images can negatively affect detection rates.

In scenarios where surveillance cameras are placed outdoors at various entry points, changes in lighting conditions are inevitable. Capturing clear video in low or no light scenarios is extremely challenging. Even high-quality cameras struggle without consistent, adequate illumination.

Iris recognition works similarly to facial recognition in that a camera scans or photographs a person's unique iris structure, creates an iris template, and stores it for future comparison. In order to capture the specific attributes of the iris

structure, however, the system needs both IR lighting and a camera that is sensitive to IR.

LIGHTING FOR INCREASED DETECTION ACCURACY

To increase detection accuracy for facial and iris recognition applications, security professionals can install external IR and white light illuminators. Built-in LEDs on cameras, while convenient, have limitations. Typically, camera LEDs emit light up to 150 feet and cover a 30-degree field of view, despite the cameras themselves typically having a field of view of 90 degrees or more. The coverage gap creates hotspots in the image. Built-in LEDs can also generate heat, which, over the long term, degrades the camera lens. The heat might also attract bugs, which can block the camera's field of view.

> BUILT-IN LEDS ON CAMERAS, WHILE CONVENIENT, HAVE LIMITATIONS.

> ULTIMATELY, THE VALUE OF EXTERNAL LIGHTING SOLUTIONS IS THAT THEY ARE DESIGNED TO CREATE EVENLY ILLUMINATED SCENES, WHICH IS ESSENTIAL FOR VIDEO-BASED BIOMETRIC SYSTEMS.

In contrast, external lighting solutions, such as IR and white light illuminators, offer expanded emission ranges extending to hundreds of feet. Many illuminators emit light at four times the standard range of cameras with integrated LEDs. External illuminators also offer greater angle flexibility, with common options available in 30, 60 and 120 degrees, to name a few options.

Ultimately, the value of external lighting solutions is that they are designed to create evenly illuminated scenes, which is essential for video-based biometric systems. For example, when IR illuminators are paired with specialty cameras, the system yields sharp, crisp and detailed images for iris recognition. Deploying white light illuminators alongside cameras

for facial recognition, meanwhile, minimizes the appearance of shadows, increases the visibility of facial features, and enables greater accuracy in color representation.

CONCLUSION

Facial and iris recognition systems for employee and visitor management will continue to see steady deployment in the years ahead. However, the accuracy of these systems depends on the accuracy of the images they read. Security teams can increase detection rates and reduce the risk of false positives by optimizing video capture capabilities. This starts with investing in external IR and white light technologies designed to enhance the performance of video-based biometric technologies.

By improving image detail and video capture, lighting leads to more precise detection and actionable data that allows for more informed decision making, all of which increases the overall functionality, performance and return on investment of facial and iris recognition systems. ◀

How AI Can Transform Integrated Security

The potential is great, though challenges remain

James Segil (james.segil@motorolasolutions.com) is Vice President of Marketing and Inside Sales, Video Security & Access Control, at Motorola Solutions (www.motorolasolutions.com).

THE PHYSICAL AND CYBERSECURITY WORLD IS DYNAMIC AND FAST-PACED, with security experts constantly looking for ways to automate, optimize and enhance their security efforts. In the rapidly evolving landscape of security services, one trend is clear: the move toward artificial intelligence (AI).

Since the invention of the Internet, there has not been a new technology that has captivated its audience as quickly as AI. From healthcare to retail to education to manufacturing, AI has already affected nearly every industry, so it is no wonder that security would quickly seek to adopt the capabilities that it offers.

That said, the rapid development of AI tools includes a fair share of questions. How will this impact the way we work? What does it mean for the future? What is the role of AI in physical security? Will AI create jobs or eliminate them? For

security leaders, the No. 1 question is: How can AI protect people, premises and assets.

To answer that question, it is useful to look at how AI has taken security from a reactive to a proactive era, making systems smarter than ever and boosting safety while improving convenience.

THE ROLE OF AI IN SECURITY

An integrated security system is a centralized platform combining various security solutions such as alarm systems, access control, video cameras and video analytics. The next-generation solution combines human expertise with cutting-edge automation to identify potential threats, respond with precision, minimize labor-intensive processes and improve overall security.

AI enhances security by providing real-time analysis, predictive capabilities and automation of routine tasks. AI for security solutions empowers security professionals and IT leaders to protect their organizations more effectively and streamline security operations.

THE NEXT-GENERATION SOLUTION COMBINES HUMAN EXPERTISE WITH CUTTING-EDGE AUTOMATION TO IDENTIFY POTENTIAL THREATS, RESPOND WITH PRECISION, MINIMIZE LABOR-INTENSIVE PROCESSES AND IMPROVE OVERALL SECURITY.

AI plays a significant role in enhancing security across various sectors.

Threat detection and mitigation

When it comes to detecting threats, AI supports security efforts by analyzing patterns and identifying unusual activities that may lead

> NOT ONLY CAN AI DETECT UNUSUAL ACTIVITIES AND POTENTIAL THREATS IN REAL TIME, BUT ANALYTICS CAN PREDICT SECURITY ISSUES BY EXAMINING HISTORICAL DATA AND IDENTIFYING PATTERNS THAT INDICATE VULNERABILITIES.

to potential problems. With intrusion detection and prevention systems, AI helps to identify and respond to threats instantly, preventing incidents and mitigating damage and loss.

Adaptive systems

Adaptive systems are technologies that can dynamically adjust and respond to changing conditions and potential attacks. Here, AI plays a crucial role in spotting anomalies in a wide variety of environments with precision.

For example, AI-powered analytics can be trained to identify specific objects and people and closely observe their movements. With access control, AI can identify individuals through facial recognition and authorize or deny entry.

Predictive analysis

Not only can AI detect unusual activities and potential threats in real time, but analytics can predict security issues by examining historical data and identifying patterns that indicate vulnerabilities. This proactive approach helps organizations anticipate and prevent threats, reducing the likelihood of security incidents.

For instance, when securing a large venue with big crowds, AI can analyze crowd dynamics and detect unusual movements and overcrowding. This helps tackle potential issues before they escalate while regulating traffic flow. To secure a perimeter, AI analyzes data from sensors

and security cameras, responds to unauthorized access attempts such as fence climbing, and triggers responses accordingly.

Proactive security

AI enables proactive surveillance by analyzing video and flagging unusual activities, allowing operators to review the footage and take immediate action when a possible breach is detected. AI-powered analytics like real-time object and gun detection bring potential crimes to the attention of security teams, allowing them to immediately activate alarms or contact the authorities.

In access control solutions, AI can enhance security while streamlining management by analyzing entry attempts and preventing unauthorized access.

THE ROLE OF AI IN CYBERSECURITY

AI can significantly enhance the efficiency of physical security and streamline processes. Similarly, security leaders can strengthen their cybersecurity programs and solve real-world problems by leveraging AI in multiple domains.

Network security

AI can monitor and analyze network traffic in real time, strengthening network security and identifying suspicious activities like unauthorized access attempts or unusual data transfers. When these activities are detected, users can take immediate action to block or contain potential threats.

Endpoint protection

Machine learning can identify and block malware, ransomware and other malicious software. It can also analyze user behavior to identify anomalous activities that could indicate compromised accounts or insider threats, helping to detect and prevent unauthorized access and data withdrawal.

AI-powered firewalls

Next-generation firewalls use AI to analyze networks and make real-time decisions on what traffic to allow or block. This dynamic approach enhances security by adapting to evolving threats. AI identifies potential threats using historical data and emerging trends to help firewalls prepare for new cybersecurity risks.

AI also leverages cloud-based security

services to enhance firewall capabilities. Cloud resources are used for threat analysis, real-time updates and heavy computing tasks, providing a more scalable and responsive security infrastructure.

Incident response

AI assists in the analysis of cybersecurity incidents and security breaches, helping IT teams to understand the scope, impact and origin of an attack. It also automates responses to incidents by isolating affected systems, blocking malicious activities and reverting systems to a secure state. Automating responses streamlines the process of mitigating and containing cybersecurity threats, putting a stop to an attack the moment it is detected and preventing it from impacting an entire network.

> SOME SYSTEMS FULLY EXPLOIT THE POWER OF AI TO DESIGN WORKFLOWS FOR EVERY PROCESS.

Vulnerability management

AI is used to identify weak points in systems and applications. Automated vulnerability assessment tools powered by AI can analyze complex systems and help IT teams focus on addressing the most critical issues first.

> HUMAN INTELLIGENCE COMPLEMENTS THE CAPABILITIES OF AI BY PROVIDING ETHICAL JUDGMENTS, CONTEXTUAL UNDERSTANDING, AND ADAPTABILITY TO NAVIGATE COMPLEX AND DYNAMIC REAL-WORLD SITUATIONS.

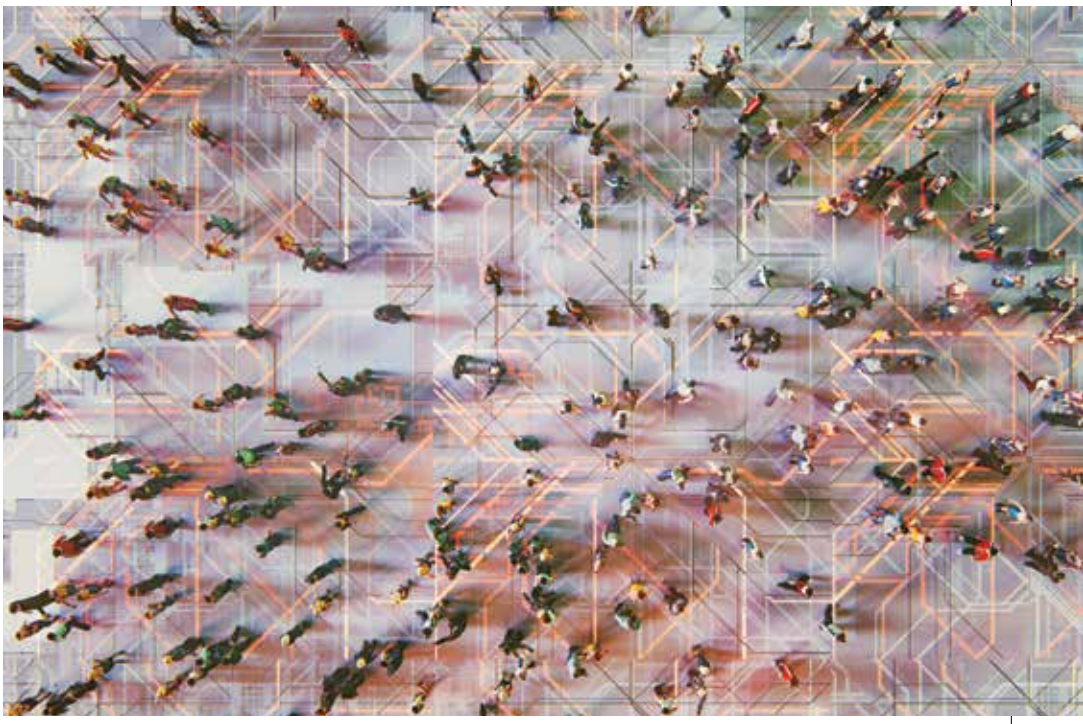
Personalized security recommendations

AI prevents breaches by analyzing user behavior and preferences to provide personalized security recommendations. This includes making suggestions for stronger passwords, advising on privacy settings, and recommending updates tailored to users' specific needs.

Improving business operations

AI can help enhance security by automating processes, from threat detection to incident response to identifying unauthorized network access. It can also be used in ways that significantly improve areas outside of security, such as business operations. This can lead to increased revenue as a result of greater efficiency and productivity.

Some systems fully exploit the power of AI to design workflows for every



process. For example, AI can automate operations with a system that connects data, video, voice, software and analytics to significantly streamline processes and allow users to focus on the bigger picture.

AI-powered analytics can also detect events such as heavy foot traffic and congestion in a building. This insight helps businesses assess current processes and create procedures that facilitate seamless operations. Additionally, AI-powered analytics can provide valuable data on capacity that informs business owners when it is time to downsize or relocate to a larger building.

CHALLENGES OF AI IN INTEGRATED SECURITY

Although AI can improve security, this does not come without challenges. Some drawbacks include vulnerability to attacks, limitations in integrating with legacy systems, restricted scalability, and difficulties in complying with regulations.

- *Security breaches* – AI systems can become targets for

cyberattacks. That is why developing AI systems that are robust and resistant to threats is crucial.

- *Interoperability* – Integrating AI with legacy systems can be challenging. Consider compatibility and interoperability when connecting AI with existing security infrastructure.
- *Scalability* – Performance and scalability are critical as data volume increases. AI might present challenges in handling the growing demands of integrated security environments.
- *Compliance* – Compliance with standards is essential to avoid legal issues, but adhering to various national and international regulations governing the use of AI in security is complex.

Addressing these issues might require consulting with AI, cybersecurity and regulatory compliance experts. Finding vulnerabilities in AI systems can also encourage ongoing development to

improve the capabilities of the technology in such systems.

THE FUTURE OF AI AND INTEGRATED SECURITY SOLUTIONS

AI holds tremendous promise as organizations seek more holistic and advanced approaches to safeguarding assets. From providing a cohesive and centralized management system to enhancing protection against cyberattacks on critical infrastructure, systems with advanced AI capabilities will be essential to creating comprehensive security ecosystems. Organizations that invest in these integrated solutions will be better prepared to address evolving security threats.

That said, however, there remains no substitute for sound human judgment. Human intelligence complements the capabilities of AI by providing ethical judgments, contextual understanding, and adaptability to navigate complex and dynamic real-world situations. While AI offers efficiency, human oversight is crucial to ensure responsible and effective execution. ◀

How to Improve the Integrator-End User Relationship

A cloud-based business software solution ensures accuracy and accessibility

Maureen Carlson (maureen@systemsurveyor.com) is the Co-Founder and Vice President of Growth for System Surveyor (www.systemsurveyor.com).

IN THE WORLD OF PHYSICAL SECURITY INTEGRATION, simply installing equipment and providing passable customer service along the way is not enough. As integrated systems grow more complex and intelligent devices require more consistent lifecycle maintenance to perform at their best, it will be up to integrators and end users alike to adopt business software solutions that are designed to enable more efficient collaboration and streamline operations.

While business software has become indispensable to many companies' core operations across verticals and industries, certain questions remain. What kind of business resource software application makes the most sense for the physical

security industry? What should system integrators and end users look for? And, also, what should they avoid?

> IN THE PHYSICAL SECURITY INDUSTRY, MANY INTEGRATORS STILL DO THEIR WORK UNASSISTED BY SOFTWARE SOLUTIONS.

THE GROWTH OF BUSINESS SOFTWARE

As early as 1961, the first large-scale computerized systems revolutionized the way business was conducted. In the decades prior, most processes, from record-keeping to finance and accounting, were performed by hand. With the introduction of enterprise-wide systems capable of automating these processes, however, even small business owners who had little experience with things like accounting were able to lean on tools designed to perform basic business functions accurately and efficiently.

By the turn of the 21st century, software had been developed to address nearly every business operation, from project management and payroll to front-facing functions,

> AT EVERY STAGE OF A PHYSICAL SECURITY SYSTEM'S LIFECYCLE, A DYNAMIC SYSTEM DESIGN, MANAGEMENT AND OPERATIONS PLATFORM ENABLES INTEGRATORS AND END USERS TO ACCESS EVERYTHING THEY NEED FROM A MOBILE TABLET OR LAPTOP COMPUTER.

such as customer relationship management and e-commerce. In the physical security industry, however, many integrators still do their work unassisted by software solutions. This can mean taking notes on physical blueprints and drafting proposals by hand or sending PDFs, photos and spreadsheets via email. Doing this work without relying on business software that is designed to simplify, standardize and secure collaboration between parties invariably slows things down and opens the door to unnecessary complications.

In order for integration firms to grow and end users to get the biggest return on their investment in physical security solutions, it is vital that both parties embrace intelligent and purpose-built business

software. For integrators, field service software applications can be a driving force behind optimizing sales and operations, improving internal processes and customer interactions, and enhancing competitiveness and profitability. For end users, leveraging a dynamic, digital platform ensures that operations teams have a single, secure place to document and manage a system in real time.

THE BENEFITS OF BUSINESS SOFTWARE

When it comes to facilitating a healthy and sustainable relationship between integrators and end users, business software truly excels. At every stage of a physical security system's lifecycle, a dynamic system design, management and operations platform enables integrators and end users to access everything they need from a mobile tablet or laptop computer, using applications designed to keep these resources organized in one central location.

The immediate benefit to this kind of security system design platform is accessibility. While

a technician may need to access a building's blueprint in the field, a project manager seeking the same information might spend more than 80 percent of their time working in an office. The moment a slight alteration is made by a technician in the field, whatever documentation a project manager has in their hands in the office is rendered obsolete. A cloud-based software solution, however, would allow this same team to work together seamlessly, from the field to the office to anywhere in the world.

More broadly, efficient collaboration is the key to maintaining a positive working relationship. Most operations teams will say that one of their biggest pain points is the handoff from sales to operations. In other words, everything goes smoothly until the time comes for different teams to collaborate. As most integrators now provide ongoing services to their customers, the interactions between integrators, sales

representatives and end users can be frequent. Not to mention that operations teams often tap several key people when overseeing systems, from procurement, vendors and project managers to technicians, subcontractors and the customers themselves. Ultimately, the goal is to get this operations delivery team on the "same sheet of music," as they say. Failure to do so can lead to miscommunication and unmet expectations.

To make sure all of these stakeholders are working with identical information, business operations software facilitates collaboration between stakeholders across multiple disciplines.

> THE IMMEDIATE BENEFIT TO THIS KIND OF SECURITY SYSTEM DESIGN PLATFORM IS ACCESSIBILITY.

SELECTING THE RIGHT SOFTWARE

When choosing business application software, the most important thing is to identify the problems that the team is looking to address. An integrator whose

> WHEN CHOOSING BUSINESS APPLICATION SOFTWARE, THE MOST IMPORTANT THING IS TO IDENTIFY THE PROBLEMS THAT THE TEAM IS LOOKING TO ADDRESS.

sales team has trouble putting a system design and proposal together quickly and consistently can prioritize a software-based solution that is designed to automate bills and streamline collaborative design. On the other hand, an end user whose biggest pain point involves outdated tools and processes for system documentation, device maintenance and communication between stakeholders might look for a business software solution that produces digital as-builts that make it easy to drag-and-drop elements, take installation photos and capture baseline information that all partners and stakeholders can access.

By simplifying and visualizing every aspect of a system design, end users can improve

lifecycle management and guarantee that key resources are easily accessible and digitally secure.

KEY TAKEAWAYS

For many businesses, investing in the future means addressing yesterday's problems today. Now is a good time to look at security system design, management and operations software that offers teams a better way to document all aspects of a physical security system in one place.

When evaluating the benefits of integrating software into a business's workflow, it is necessary to have a clear understanding of what the team needs before seeking out software designed specifically to meet those needs. Sometimes, getting the right answers depends on asking the right questions. In the end, integrating business software that is purpose-built for a given industry will save a lot of time and will generate immediate value. ◀

Security Shifts: The Technology Trends Creating a Safer World

Cloud and AI are remaking video surveillance

IT IS QUITE CLEAR THAT TECHNOLOGY IS UNDERGOING SIGNIFICANT CHANGES, and it is largely thanks to major advances in artificial intelligence (AI) and cloud computing. These developments are in line with what experts like Bill Gates have been predicting: a significant boom in technology over the next few years, driven by the increasing power of AI.

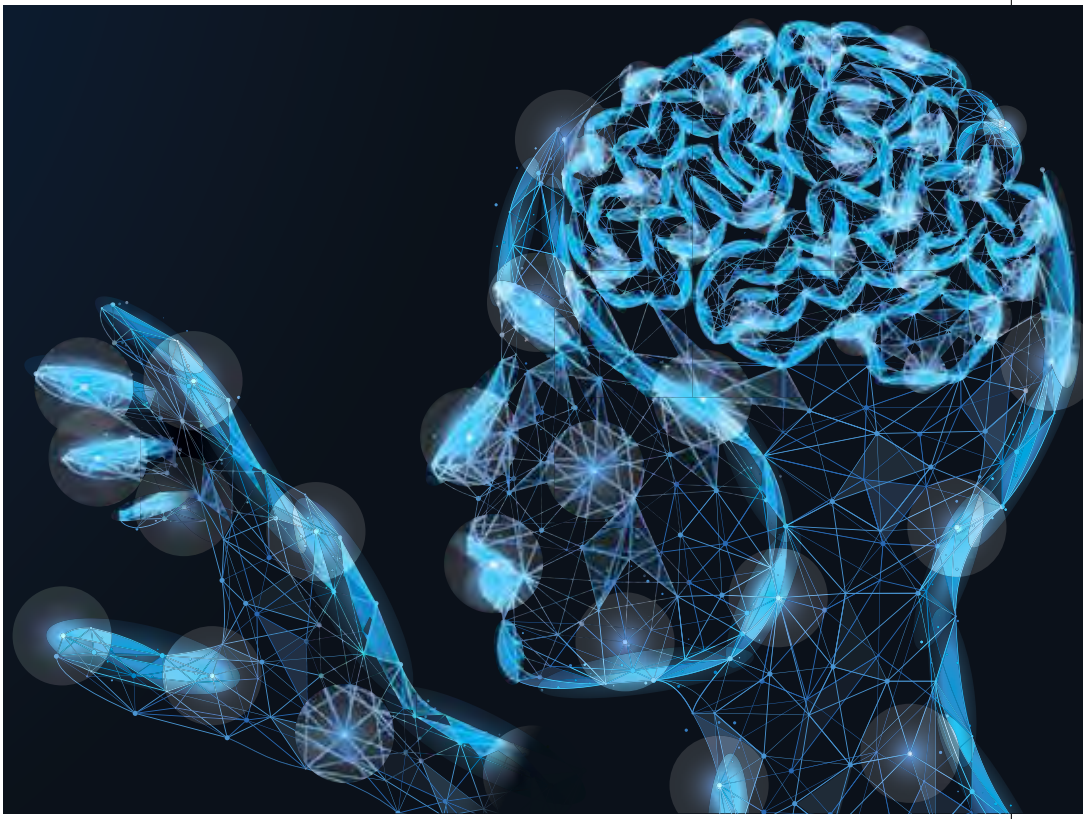
AI is revolutionizing industries by enhancing efficiency and fostering new innovations. At the same time, cloud computing use is growing because of its ability to deliver a scalable and flexible infrastructure that allows data to be stored, processed and accessed from anywhere in

Steve Prodger (steve.prodger@arcules.com) is the Chief Revenue Officer for Arcules (www.arcules.com).

the world. Together, AI and the cloud are changing the way we work, live and even dream. They are preparing us for a future filled with endless possibilities. And as these technologies continue to evolve, they are expected to boost productivity, improve connectivity, and offer more intelligent solutions to some of the world's most challenging problems.

The year 2023 proved to be a pivotal point, as it saw AI evolve from early experimental stages to practical applications in the real world. It was Gates who emphasized this transition, noting that the first serious, work-related use of AI represented a significant development in our understanding of what it can achieve, and of its limitations. As we look

THE YEAR 2023 PROVED TO BE A PIVOTAL POINT, AS IT SAW AI EVOLVE FROM EARLY EXPERIMENTAL STAGES TO PRACTICAL APPLICATIONS IN THE REAL WORLD.



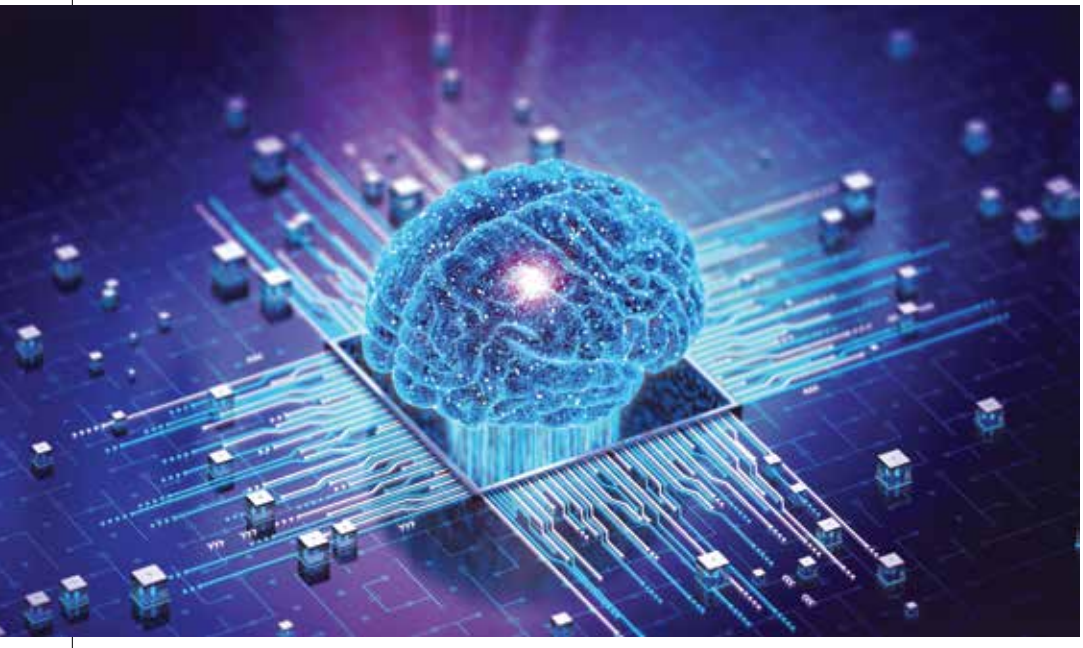
> THE IMPACT OF AI ON SECURITY IS BECOMING MORE EVIDENT AS THE INDUSTRY MOVES AWAY FROM TRADITIONAL METHODS THAT RELY HEAVILY ON HUMAN INTERVENTION TO MORE SOPHISTICATED STRATEGIES.

ahead, the coming year is expected to be a period of rapid progress in the refinement and use of AI, along with other emerging technologies.

THE INDUSTRIAL REVOLUTION, REIMAGINED

The technological revolution is transforming industries such as security and video surveillance significantly. The introduction of AI into video management systems (VMS) changes how they operate by bringing in advanced analytics. These technologies improve the way IT and security leaders use video data, making it possible to recognize objects, detect anomalies, and analyze behavior more effectively. As a result, the use of analytics in security video deployments has increased, reducing the need to have large teams of specialists and making it easier to develop and refine models.

The impact of AI on



security is becoming more evident as the industry moves away from traditional methods that rely heavily on human intervention to more sophisticated strategies. Large language models play a key role in this change, improving how we interact with and understand data. New ways to create and enhance visual content are also being adopted, showing how AI is becoming more integrated into this sector. This change reflects a wider movement toward using AI to rethink the way we analyze and use data and leverage it to create a safer world.

INTO THE CLOUD

The adoption of cloud technology in video surveillance represents a departure from traditional, localized, and often complex on-premises VMS. Despite the bandwidth concerns inherent in streaming real-time, high-definition video, the benefits of cloud

> WITH AI-POWERED ANALYTICS, CLOUD PLATFORMS ENABLE THE PROCESSING OF VAST VOLUMES OF DATA EFFICIENTLY, PROVIDING ACTIONABLE INSIGHTS FOR BOTH SECURITY AND BUSINESS INTELLIGENCE.

> THERE IS THE OPTION TO DEPLOY A CLOUD SOLUTION THAT INCORPORATES BOTH STRUCTURED AND UNSTRUCTURED DATA, BLENDING EDGE AND CLOUD COMPUTING TO CREATE A DYNAMIC, VERSATILE ENVIRONMENT FOR DATA MANAGEMENT AND ANALYTICS

solutions – scalability, adaptability and the ability to meet evolving business and security needs – are difficult to ignore. And with AI-powered analytics, cloud platforms enable the processing of vast volumes of data efficiently, providing actionable insights for both security and business intelligence.

Cloud solutions offer significant benefits for a wide range of environments, contrary to the belief that they are best suited for smaller operations. For example, video surveillance as a service has been proven to be equally beneficial for large, geographically dispersed deployments as it is for smaller ones. While challenges such as bandwidth demands and transition costs do exist, they can be navigated effectively with proactive planning and infrastructure development. Large enterprises, in particular, can benefit from cloud-based systems'

scalability and reduced hardware reliance, supporting expansion and minimizing edge hardware requirements. There is also the option to deploy a cloud solution that incorporates both structured and unstructured data, blending edge and cloud computing to create a dynamic, versatile environment for data management and analytics. This hybrid model supports analysis of traditional or AI-driven video, offering the opportunity to achieve deeper, actionable insights into security data.

The fusion of advances in cloud and video surveillance technology with the broader AI movement marks the beginning of a new era in security. These innovations promise to revolutionize video surveillance systems by enhancing efficiency, intelligence and adaptability. These technological leaps will enable leaders to adopt a proactive rather than reactive approach to risk management, significantly improving security. This shift not only echoes the technological progress anticipated by people like Gates but also heralds a new era in fostering a safer, global community. ◀

Balancing Wireless Innovation with Wired Reliability

Integrating both approaches advances convenience, security and sustainability in smart buildings

Richard Kasslack (richard.kasslack@nvtphybridge.com) is Senior Vice President of Sales and Corporate Development at NVT Phybridge (www.nvtphybridge.com).

IN THE REALM OF SMART BUILDING TECHNOLOGIES, the evolution of the Internet of Things (IoT) has led to a significant transformation in networking needs, bringing forth not only the question of data connectivity but also the crucial issue of power delivery to each endpoint. There is an intricate balance between wireless flexibility and the cost-effective, power-efficient nature of wired networks, particularly Ethernet. Examining both the data and power dimensions of network infrastructure can provide a comprehensive view of modern networking solutions in the context of evolving smart building demands.

THE EVOLUTION OF IOT AND SMART BUILDING TECHNOLOGY

The landscape of smart building technology has been revolutionized by the rapid evolution of IoT. This transformation is not just a trend; it

> WHILE WIRELESS TECHNOLOGY HAS MADE REMARKABLE STRIDES IN CONVENIENCE AND ACCESSIBILITY, THE BACKBONE OF A RELIABLE AND SECURE NETWORK IN A SMART BUILDING ENVIRONMENT IS PREDOMINANTLY WIRED.

is a fundamental shift in how we interact with and manage our physical environments. The proliferation of IoT devices has led to buildings that are not only structures of concrete and steel but also dynamic ecosystems brimming with sensors, devices and systems that communicate constantly.

This communication is not merely for convenience. It is a critical component of building management, energy efficiency and security. Smart buildings leverage IoT to optimize heating, ventilation and air conditioning (HVAC) systems, enhance security through intelligent surveillance, and provide a more responsive and adaptive environment for occupants. This has implications for how we design and manage

building infrastructure, pushing us beyond traditional concepts of wiring and networking.

Furthermore, the data generated by these devices is vast and invaluable. It requires robust, reliable infrastructure to transmit, process and store. This is where the interplay of wireless and wired networks becomes crucial. While wireless technology offers flexibility and ease of deployment, it often cannot match the reliability and speed of wired connections, especially in environments dense with IoT devices.

In addition, the management and security of these IoT devices present unique challenges. The network must not only support a large number of devices but also ensure their security and manageability. This includes making regular updates, monitoring for anomalies, and ensuring seamless integration with existing systems.

The evolution of IoT in smart buildings demands a re-evaluation of network

infrastructure. It calls for a holistic approach that considers the strengths and limitations of both wireless and wired technologies.

THE CASE FOR ROBUST WIRED INFRASTRUCTURE

In the dynamic landscape of IoT and smart buildings, the importance of a robust wired infrastructure cannot be overstated. While wireless technology has made remarkable strides in convenience and accessibility, the backbone of a reliable and secure network in a smart building environment is predominantly wired. This is primarily due to several inherent strengths of wired connections.

First, wired networks offer unmatched reliability and stability, both of which are essential in environments where consistent connectivity is critical. In smart buildings, where systems such as security, HVAC and lighting rely heavily on uninterrupted data transmission, the steadiness of wired

networks ensures that these systems function optimally without the risk of interference or connectivity issues common in wireless networks.

Second, wired connections are inherently more secure than wireless ones, as they are less susceptible to eavesdropping and unauthorized access. In an era where cyber threats are increasingly sophisticated, the enhanced security of wired networks offers peace of mind, especially for critical infrastructure within smart buildings.

Furthermore, the bandwidth and speed of wired networks are generally superior. For the huge amounts of data generated by IoT devices in smart buildings, wired networks provide the necessary capacity and speed for efficient processing and transmission. This is particularly important for applications that require real-time data analysis or high data throughput.

Moreover, wired infrastructure lays the foundation for a scalable and adaptable network. As smart buildings evolve and the number of connected devices grows, a wired network can be scaled and modified more easily to accommodate these changes, ensuring longevity and future-proofing investments in building infrastructure.

WIRED NETWORKS, WITH THEIR LOWER ENERGY CONSUMPTION PER DATA UNIT TRANSMITTED COMPARED TO WIRELESS NETWORKS, CONTRIBUTE TO THE OVERALL ENERGY EFFICIENCY OF SMART BUILDINGS, ALIGNING WITH THE GROWING EMPHASIS ON SUSTAINABILITY.

Environmental considerations also play a role. Wired networks, with their lower energy consumption per data unit transmitted compared to wireless networks, contribute to the overall energy efficiency of smart buildings, aligning with the growing emphasis on sustainability.

POWER AND COST EFFICIENCY IN NETWORK DESIGN

In modern smart buildings, any discussion of network infrastructure

> WHEN DESIGNING NETWORK INFRASTRUCTURE FOR SMART BUILDINGS, CONSIDERING THE DUAL ROLE OF ETHERNET IN PROVIDING BOTH DATA AND POWER IS CRUCIAL.

is incomplete without addressing power delivery and cost efficiency. These factors become particularly crucial when considering the many endpoints in a smart building, each requiring both connectivity and power.

Consider two IP endpoints in a smart building: a security camera and a VoIP (Voice over Internet Protocol) phone.

Security cameras need a stable data connection for video streaming and power. With Power over Ethernet (PoE) technology, a single Ethernet cable can provide both high-speed data connectivity for streaming high-definition video and the power needed to operate the camera. When upgrading an analog camera to IP, there are high-quality PoE over coax managed, unmanaged and extender solutions available that

can transform the existing coax infrastructure into a robust and secure PoE path for the new IP camera. These approaches eliminate the need to have separate power sources near each camera, allowing for flexible placement throughout the building.

VoIP phones, similarly, require both a stable network connection for clear voice transmission and power to function. Again, PoE enables the phone to be powered and connected to the network through one Ethernet cable. Like the coax example above, there are innovations that deliver PoE over a single pair of wires with extended reach that can transform the point-to-point infrastructure into a robust and secure PoE path. This simplifies the installation process, reduces clutter and allows for easy relocation of phones if needed.

The cost-benefit analysis of wired versus wireless networks takes a decisive turn when considering PoE. The initial investment in Ethernet cabling is often offset by the savings from not having to install separate power lines. Additionally, wireless endpoints typically require more complex and expensive hardware

> THE INTEGRATION OF WIRELESS TECHNOLOGY INTO THE EXISTING WIRED INFRASTRUCTURE CAN PROVIDE THE BEST OF BOTH WORLDS – THE RELIABILITY AND SECURITY OF WIRED NETWORKS AND THE FLEXIBILITY AND USER-FRIENDLINESS OF WIRELESS SOLUTIONS.

to enable connectivity, adding to the total cost of ownership.

Furthermore, the power efficiency of PoE-enabled networks is significant. By centralizing power distribution, it is easier to manage and monitor energy usage, contributing to the overall energy efficiency of the building. This centralized approach also facilitates better power backup solutions, ensuring uninterrupted service.

In summary, when designing network infrastructure for smart buildings, considering the dual role of Ethernet in providing both data and power is crucial. This approach not only enhances the cost effectiveness and efficiency of the network but also aligns with the environmental sustainability goals of modern infrastructure development.

WIRELESS TECHNOLOGY – COMPLEMENT, NOT REPLACEMENT

Wireless technology plays a pivotal role in smart buildings, but it should be viewed as a complement to, rather than a replacement for, wired infrastructure. The allure of wireless is undeniable – it offers flexibility, mobility and ease of installation that wired networks can seldom match. This makes it ideal for areas where wiring is impractical or for devices that need to be mobile or reconfigured frequently.

However, the inherent limitations of wireless technology must be acknowledged. Wireless networks are more susceptible to interference, which can impact reliability, particularly in environments with a high density of devices or physical obstructions. Additionally, while advances in wireless technology have significantly improved its speed and bandwidth

capabilities, it still generally falls short of the high-speed, high-capacity performance offered by wired connections.

Security is another crucial factor. While wireless networks have made strides in security protocols, they inherently have a larger attack surface because they transmit data through the air. Wired networks, by their very nature, offer a more controlled and secure environment for data transmission.

Wireless technology often serves as an extension of the core wired network. It relies on a robust wired backbone to function effectively, particularly in smart buildings where a multitude of devices require a steady and reliable connection. The integration of wireless technology into the existing wired infrastructure can provide the best of both worlds – the reliability and security of wired networks and the flexibility and user-friendliness of wireless solutions.

In the context of smart building design and IoT integration, then, wireless technology should not be seen as an all-encompassing solution, but rather as a valuable

component of a broader, hybrid network strategy. This approach aligns well with the principles of modern local area network (LAN) design, where flexibility, security and efficiency are paramount.

SECURITY CONSIDERATIONS IN NETWORKING

Security is a cornerstone in the architecture of smart building networks, especially in an era where cyber threats are evolving rapidly. In the context of networking, this encompasses both the physical security of the infrastructure and the cybersecurity of data transmission.

Wired networks, with their physical connections, provide an inherent level of security. Data is transmitted through cables, making it more challenging for unauthorized entities to intercept. This physical security is crucial in areas where sensitive information is handled or critical systems are in operation.

On the other hand, wireless networks, despite their convenience, introduce vulnerabilities through their broadcast nature. The data transmitted can potentially be intercepted or disrupted. However, advances in wireless security protocols have significantly mitigated these risks. Implementing robust encryption and authentication measures is essential to safeguarding data integrity and privacy.

A hybrid network that intelligently integrates both wired and wireless elements can enhance overall security. This approach allows for the segregation of network traffic based on sensitivity and vulnerability. For instance, critical systems can be run on wired networks for enhanced security, while non-critical, user-facing systems can leverage the flexibility of wireless networks.

Network management also plays a critical role in security. This includes continuous monitoring for unusual activities, regular updates to firmware and software, and adherence to best practices in network security. Such proactive management is crucial in both wired and wireless networks to identify and

mitigate potential security threats promptly.

While both wired and wireless networks have their unique security considerations, a balanced approach that leverages the strengths of each can provide a more secure and robust solution for smart building networking. This aligns with the evolving landscape of cybersecurity and the diverse needs of modern smart buildings.

PREPARING FOR THE FUTURE

Future-proofing building infrastructure is a necessity. The key to achieving this is flexibility and adaptability in network design, ensuring that buildings can keep pace with evolving technologies and changing requirements.

The integration of both wired and wireless networks is crucial in this endeavor. Wired infrastructure, with its reliability and high-speed capabilities, forms the backbone, ensuring that the core functions of the building are uninterrupted and secure. It provides the robust foundation necessary for the heavy-lifting tasks of data processing and transmission.

Concurrently, wireless networks offer the agility to adapt to new technologies and user

> THE CONCEPT OF SUSTAINABILITY CANNOT BE IGNORED. FUTURE-PROOF NETWORKS MUST NOT ONLY BE TECHNOLOGICALLY ADAPTABLE BUT ALSO ENVIRONMENTALLY CONSCIOUS.

needs. They allow for the easy addition of new devices and systems, catering to the ever-changing landscape of IoT and user preferences. This flexibility is crucial in environments that must constantly evolve, such as smart buildings.

Moreover, the concept of sustainability cannot be ignored. Future-proof networks must not only be technologically adaptable but also environmentally conscious. Wired networks often provide a more energy-efficient solution compared to wireless networks, contributing to the overall sustainability goals of modern infrastructure.

Future-proofing building infrastructure requires a thoughtful blend of the stability and security of wired networks with the flexibility and adaptability of wireless networks. This hybrid approach ensures that smart buildings are not only equipped to handle the demands of today but are also prepared for the technological advances of tomorrow.

CONCLUSION

A harmonious integration of wired and wireless technologies in smart building infrastructure is essential. Embracing the strengths of both, rather than choosing one over the other, offers a more comprehensive, secure and sustainable approach to building networks. This strategy not only caters to the current demands of IoT and smart technologies but also positions these infrastructures to adapt and evolve with future developments.

The principles of modern LAN design combined with the pivotal role of wireless technology can create networks that are robust, flexible and forward-looking. In an era in which technology continuously reshapes environments, such a balanced approach ensures that smart buildings remain at the forefront of innovation and efficiency. ◀

SICC™

SECURITY INDUSTRY CYBERSECURITY CERTIFICATION

THE CYBERSECURITY CERTIFICATION FOR SECURITY INDUSTRY PROFESSIONALS

Why Earn the SICC?

The only credential focused specifically on cybersecurity for physical security systems

Validate your understanding of essential topics like:
- Infosec principles
- Networking and network security
- Device security
- Software security
- Social engineering

Accelerate your career and build trust with your colleagues, partners and clients

We will be making the SICC certification part of our essential staff training to ensure everyone in our organization has the skills and knowledge they need to face changing cybersecurity challenges and build innovative, secure solutions for our customers.

– Courtney Gibson, SICC, chief technology officer and chief information security officer, BioConnect

Learn More About the SICC

www.securityindustry.org/sicc

SIA SECURITY INDUSTRY ASSOCIATION

Co-developed with support from

PSA SECURITY NETWORK

security specifiers

VERIFIED OSDP™ VERIFIED

When you need interoperable, high-security access control solutions, ask for products that bear the OSDP Verified mark.

OSDP Verified means these products have been tested by the Security Industry Association as conforming to one or more profiles of the OSDP standard. For you, that means peace of mind knowing these solutions can communicate securely and seamlessly.

To learn more about OSDP and find a guide to OSDP Verified products,

visit securityindustry.org/OSDP

Security Industry Association
securityindustry.org
SIA