SIA
TECHNOLOGY
Insights
Fall 2021
Volume 9, Number 2

WHAT AI SAW AT THE REVOLUTION

Artificial intelligence and automation are remaking security

Page 2

In the Weeds

Cannabis security offers potential – and controversy

Page 18

High Standards

OSDP ensures secure access control

Page 32

Computer Eyes Data

Machine learning will change surveillance

Page 46

Verified. Bench Tested. Proven. Compliant. Trusted.

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

TECHNOLOGY Insights

Fall 2021 Volume 9, Number 2

Artificial Intelligence Will Revolutionize Physical Security

Intelligent, autonomous systems that prevent incidents are coming

Gopal Paripally (gopal.paripally@jci.com) is Global Head of Technology – Vice President for Johnson Controls (www.johnsoncontrols.com).

THE DIGITAL REVOLUTION HAS CAUSED OUR SYSTEMS OF WORK AND PLAY TO EVOLVE, which in turn is pushing the envelope of physical security. Future security systems will be faster, more efficient, and more agile to maintain safety in workplaces, on campuses, and at public venues.

The current state of security technology is often too disconnected to easily adapt to future needs. For security systems to respond to threats in a mixed physical and digital environment, these systems will need to evolve to become centrally managed, easy to integrate, and built with predictive and preemptive automatic responses. The security industry faces critical challenges, including a lack of connection between security solutions, inadequate return on investment, and poor full-environment coverage.

PAST: FORENSIC SECURITY

Security systems of the past were often implemented independently of each other, and they cost more in terms of time, money and resources. These pieced-together systems were unable to grow with businesses and the result was diminished ROI and an increase in resource demand. They also lacked easy access to useful data, leading to a time-consuming process to gather information.

Previously, a convenience store owner might have had a video surveillance system that caught a person on camera during a break-in. But, by the time the authorities arrived, that person and the money were gone. It would take time to sift through the video and a careful eye to catch the thief on camera. Even then, the forensic data would be limited.

TODAY: REACTIONARY SECURITY

Many establishments still use standard security solutions like video surveillance, access control and cloud management, but with better artificial intelligence (AI) analytics and integrations. However, these systems can operate more efficiently to manage physical security threats and improve resource usage. They often exist in silos, lacking connection to broader security technology. These limits increase response times for events and lengthen investigations.

> THE FUTURE OF SECURITY WILL BE FOCUSED ON EFFICIENTLY DETECTING THREATS WITH NEW TECHNOLOGIES LIKE DRONES AND ROBOTS THAT CAN OPERATE AUTONOMOUSLY AND INTEGRATE WITH MORE TRADITIONAL SECURITY SOLUTIONS LIKE VIDEO SURVEILLANCE, ACCESS CONTROL AND OTHER DEVICES, LEVERAGING SENSOR FUSION.

In a situation where someone attempts to enter a building with a weapon, the technology exists to identify the weapon, but it takes time for security personnel to act on the event, especially if they need to first recognize the weapon from a control

room or a video review after a physical witness raises an alert. While systems may be integrated and running analytics, human intervention is still needed to execute critical security responses. The weapon could be inside the building by the time security personnel respond, lock down the facility, and alert occupants to the threat.

> WHEN PROCESSES ARE CONNECTED, THEY CAN PROVIDE PREDICTIVE AND PREEMPTIVE SECURITY WITHOUT HUMAN INTERVENTION, AND OPERATIONAL PERFORMANCE IMPROVES. AS A RESULT, PERSONNEL CAN SPEND MORE TIME MANAGING SECURITY RESPONSES AND STRATEGIES AND LESS ON OBSERVATION AND IDENTIFICATION.

FUTURE: PREVENTATIVE SECURITY

While security goals have not changed, technology has now evolved to enable autonomous responses and monitoring that not only improves the speed of security operations, but increases operational efficiency and creates safer work environments. Autonomous solutions free personnel from the tedium of monitoring and observation while being capable of doing much more than simply triggering alerts that notify people. They can activate security protocols and enable devices to communicate with each other to capture more information and keep people safe without human intervention. This autonomy frees up personnel to focus on strategy, decision making and human response.

In the future, a pan-tilt-zoom camera running AI analytics at an entry point will identify a weapon on a person, zoom in to get a closer look, and direct the access control system to lock the door to prevent entry. Simultaneously, it will send an alert to a security team, occupants or the authorities with this information and maybe even autonomously deploy a drone to find and track the person. In other words, this system will prevent a potentially harmful incident without human intervention.

WHAT DOES THE FUTURE LOOK LIKE?

The future of security will be focused on efficiently detecting threats with new technologies like drones and robots that can operate autonomously and integrate with more traditional security solutions like video surveillance, access control and other devices, leveraging sensor fusion. The future of physical security will result in multiple enhancements.

Improved Security Operations

This starts with leveraging block chain and PKI-based identity management for operators that covers both physical and logical access while addressing cyber and data privacy requirements.

Safer workplaces, faster investigations, real-time detection and easier processes are all the result of improved security operations. When solutions like video surveillance, access control, and new devices such as robots and drones work together seamlessly in a digital environment, businesses are better able to manage security threats.

Command centers can leverage high-definition,

AT A GLANCE: THE FUTURE OF PHYSICAL SECURITY

- Improved Security Operations
- Increased Operational Efficiency
- Flexible On-Premises, IaaS and SaaS Options
- Safer Work and Play Environments
- Autonomous and Intelligent Security

> A COMBINED APPROACH TO CYBERSECURITY AND PHYSICAL SECURITY MAY SEEM TO INCREASE THE THREAT RISK, BUT IT ACTUALLY PROVIDES EXTENSIVE DATA TO TRACE A THREAT TO ITS ORIGIN AND POTENTIALLY NEUTRALIZE IT BEFORE A NEGATIVE EVENT OCCURS.

zero-bezel displays as a flexible canvas for security, all made more intelligent by sensor fusion-driven AI for events. Responses to these events, conducted using natural language processing, natural language understanding, and combined gesture multi-touch control, make interactions fast and simple without the need for a keyboard and mouse.

Increased Operational Efficiency

Organizations are complex environments of people, processes and technologies. When processes are connected, they can provide predictive and preemptive security without human intervention, and operational performance improves. As a result, personnel can spend more time managing security responses and strategies and less on observation and identification.

Flexible On-Premises, IaaS and SaaS Options

Physical security will be able to do more with less, creating more cost-effective solutions and improving operating efficiency. Having the ability to choose between on-premises security, infrastructure as a service (IaaS), or security as a service (SaaS) allows businesses of all sizes and industries to take advantage of the full benefits of security models that are enabled through micro services and container-based deployments.

Safer Work and Play Environments

Maintaining the physical safety of workers, students and the public is critical to preventing loss of life and loss of business. Safety can be improved with more efficient, predictive security systems that allow for better training, compliance and monitoring, along with faster event responses. Leveraging technologies such as body-worn cameras and sensor fusion AI helps to create this reality.

Autonomous and Intelligent Security

Security will move beyond video surveillance and access control with features such as autonomous reporting, monitoring and response. Autonomous security systems will communicate with each other and with people and will act on their own to collect more

information and trigger complex safety protocols.

Security technology will operate with predictive intelligence and will be deeply integrated with building systems, including HVAC, lighting, elevators, and fire alarm and suppression. Remote monitoring capabilities will be the norm and this interconnectivity will bring the Internet of Things (IoT), 5G edge sensors, mobile devices, body-worn cameras, robots, drones, contextual conversational AI, and augmented reality together to provide frictionless access, risk analysis, and predictive behaviors for proactive responses with real-time machine intelligence. Autonomous technologies will include:

- **Drones:** Identify threats from the air and deploy quickly to track in real time, collecting data that a person on the ground does not have. In addition, prevent unwanted drones from violating airspace while being able to track the location of drone pilots who violate safety and security rules.
- **Robots:** An extra set of eyes that can autonomously dispatch and fill in for a camera's blind spot, gain close-up knowledge, or evaluate a situation for safety before allowing human intervention. Additionally, provide facilities with security and safety inspections through sensors,

MAIL SCAN USE CASE

Technology can detect a weapon on a person prior to entry into a business or other establishment. But these autonomous security solutions also help to maintain safety and security in other ways.

Corporations, for example, are already monitoring incoming packages with x-ray mail scan devices that allow for the detection of weapons. Millimeter-wave technology now enables detection of liquids, powders, weapons, explosives, radiation, and other suspect materials without putting people at risk. With new, autonomous technology, a threat found by a mail scanner can trigger a series of events, including shutting off the HVAC system in the case of a potentially harmful airborne substance or triggering a building evacuation if an explosive device is found. The mail scanner can also connect to nearby cameras and deploy a security robot for a closer inspection of the threat.

This process ensures that people in the building remain safe while the potential threat is being evaluated. If a threat is confirmed, the work done autonomously has been recorded and can be used as forensic evidence in an investigation.

security equipment status, audio alerts, measurement of temperature, humidity, combustible gases and air quality, and more.

- **Visual and Audio Detection:** Detect threats like guns from visual captures and gunshots or glass breaks from sound captures. These events can then trigger doors to lock and drones to deploy, while simultaneously sending alerts to security personnel.
- **Facial Recognition**: Whether attempting to identify a person of interest or maintain health initiatives such as mask wearing, facial recognition allows for more efficient investigation and compliance enforcement. The technology can also prevent tailgate and passback violations.
- **Facial Matching:** Rapid, real-time alerts or quick forensic recognition provide the ability to allow entrance to authorized persons and block entrance to unauthorized persons.
- **Re-Identification and Intelligent Person Search:** With a photo or snapshot, video system operators can locate a person of interest based on their appearance in just a few moments.

> TECHNOLOGY CAN HELP EVER-EVOLVING SYSTEMS OF WORK AND PLAY TO BE SAFER AND MORE EFFICIENT WITH LESS REQUIREMENT FOR HUMAN INTERVENTION.

AT A GLANCE: AUTONOMOUS TECHNOLOGIES

- Drones
- Robots
- Visual and Audio Detection
- Facial Recognition
- Facial Matching
- Re-Identification and Intelligent Person Search
- Intelligent Perimeter Detection
- Area Occupancy
- Traffic Monitoring

Searches can also be performed from previously saved images and can be sorted by relevance or time, and selected clips can be saved and exported. In an emergency, live video can also be launched from search results.

- **Intelligent Perimeter Detection:** Detect objects that linger along a perimeter, cross a perimeter, or enter a protected area with the ability to filter out non-critical threats such as animals.
- **Area Occupancy:** With AI technology, people counting can be automated and occupancy alerts can be integrated into a holistic system that can trigger a set of protocols and prevent violations from occurring.
- **Traffic Monitoring:** Traffic cameras can talk to each other to prevent car and pedestrian accidents, as well as to route emergency vehicles as they navigate congestion and intersections.

CYBERSECURITY AND PHYSICAL SECURITY

The landscape of IoT devices and sensors has expanded, which has created more potential for cyberattacks that affect physical security. A combined approach to cybersecurity and physical security may seem to increase the threat risk, but it actually provides extensive data to trace a threat to its origin and potentially neutralize it before a negative event occurs. In this way, technology can help ever-evolving systems of work and play to be safer and more efficient with less requirement for human intervention.

Understanding the impact that the digital space has on physical security allows the creation of new solutions for a safer and more autonomously secure future. These solutions will include better AI analytics, object classification, intelligent searches, frictionless access, and more. Autonomous security systems will provide end-to-end security, free up personnel, and trigger responses to maintain the level of safety that businesses need to move ahead in the age of digital transformation. ◀

The Long Path to True Convergence

Where do things really stand and why have they not progressed further?

Willem Ryan (willem.ryan@alertenterprise.com) is Vice President, Marketing and Communications, for AlertEnterprise (www.alertenterprise.com).

THE ONGOING DIGITAL TRANSFORMATION MEANS LIMITLESS OPPORTUNITIES for those who can harness the digitization of the physical world safely and effectively. But these changes have forever altered the threat landscape, leaving no entity without risk.

According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), today's threats result from hybrid attacks targeting both physical and cyber assets. The adoption and integration of Internet of Things and Industrial Internet of Things devices has led to an increasingly interconnected mesh of cyber-physical systems that expand the attack surface and blur the once clear lines between cybersecurity and physical security.

Any compromise of cyber-physical systems can have a devastating impact on security, operations, profitability and reputation. Experts agree that the current approach of dealing with security in departmental silos is leading to increased risk, rising costs and a climate of mistrust among regulators.

Cyber-physical threats are an everyday occurrence no longer isolated to IT systems. Real-life events, including several high-profile cyberattacks, bear this out. It is a multi-dimensional problem that is rippling through the supply chain, forcing abrupt business changes that are siphoning profitability. Cyberattacks on food and beverage and water supplies can have devastating effects on distribution and quality, potentially affecting the safety of consumers. Ransomware can shut down mission critical operations, like petroleum supplies, and no one knows when the next attack will happen or what the target will be.

The threat extends beyond the organization itself. Research firm Gartner forecasts that liability for cyber-physical security incidents will "pierce the corporate veil to personal liability" for 75 percent of CEOs by 2024, creating even greater urgency to move the needle to true security convergence.

> A THREE-DIMENSIONAL APPROACH TO SECURITY CONVERGED ACROSS IT, OT AND PHYSICAL SYSTEMS STANDS AS THE ONLY WAY FORWARD IN A POST-PANDEMIC WORLD.

THE HACKER THREAT

JBS Foods, the leading beef producer in the world, with operations in the United States, Australia and Canada, was hit by a cyberattack in June. In a statement to the media, the organization revealed that it paid the equivalent of $11 million in ransom in response to the hack.

Three months earlier, Molson Coors had suffered a ransomware attack. In an SEC filing, the beverage giant stated that the incident "has caused and may continue to cause

a delay or disruption to parts of the company's business," including brewery operations, production and shipping.

And a February attack on a Florida water treatment plant that exploited a vulnerability in a remote access software program on a facility computer offered yet another reminder of the growing dangers of cyber-physical threats – and the possibility that employees can be part of the problem.

> WHAT IS PREVENTING CONVERGENCE FROM MOVING FORWARD? BOTH AN ATTITUDE AND A CULTURAL SHIFT ARE NEEDED TO CHANGE PERCEPTIONS AND OUTCOMES.

As every market continues to digitally transform, systems and processes are moving to rapidly connect. Security convergence, focused on identity and access governance, links all of these separate departments and operations, so communications and processes actively and collectively address risk preemptively.

A three-dimensional approach to security converged across IT, operational technology (OT) and physical systems stands as the only way forward in a post-pandemic world. Covid-19 continues to transform access governance, automating across a broader, cross-departmental reach that includes not only security but also safety, health, wellness and the human experience.

BUILDING A HOLISTIC SECURITY AND SAFETY CULTURE

Why are the worlds of cyber/IT, OT and physical security still separate, siloed operations? What is preventing convergence from moving forward? Both an attitude and a cultural shift are needed to change perceptions and outcomes.

Mark Weatherford, chief information security officer at AlertEnterprise, said, "The security divide shouldn't be there. Distinct lines between cyber, OT and physical security teams have resulted in disjointed and ineffective detection, mitigation and response to risk, forged by years of siloed departments."

"As risks have changed, there's now an expectation that CEOs, board members and other executives will be held accountable when bad things happen if they haven't taken the kind of mitigation steps, like convergence, or addressed and invested in cybersecurity, people and policies," Weatherford added. "Wholesale change is occurring and the physical security industry is 'present at the creation moment' as this transition continues."

It is not a new problem. In fact, the vulnerability of critical infrastructure has been discussed for decades. However, people have continued to stay isolated within separate roles in an enterprise. Moving to a converged approach across all departments, including HR, cyber/IT and OT/SCADA can effectively secure the most critical resources while actively enforcing compliance requirements and company policies.

The "CISA Cybersecurity and Physical Security

WHAT IS CISA?

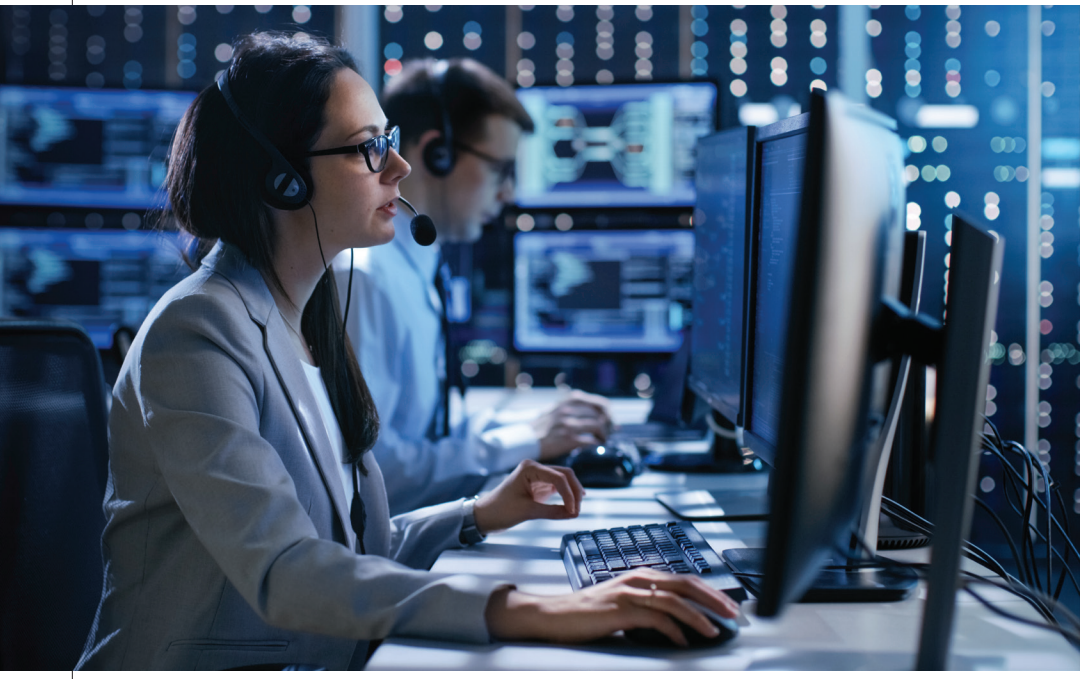
The Cybersecurity and Infrastructure Security Agency (CISA) is a federal agency that works with public and private-sector partners to defend against cyber and physical threats and build secure, resilient infrastructure.

> THE SECURITY DIVIDE SHOULDN'T BE THERE. DISTINCT LINES BETWEEN CYBER, OT AND PHYSICAL SECURITY TEAMS HAVE RESULTED IN DISJOINTED AND INEFFECTIVE DETECTION, MITIGATION AND RESPONSE TO RISK, FORGED BY YEARS OF SILOED DEPARTMENTS.

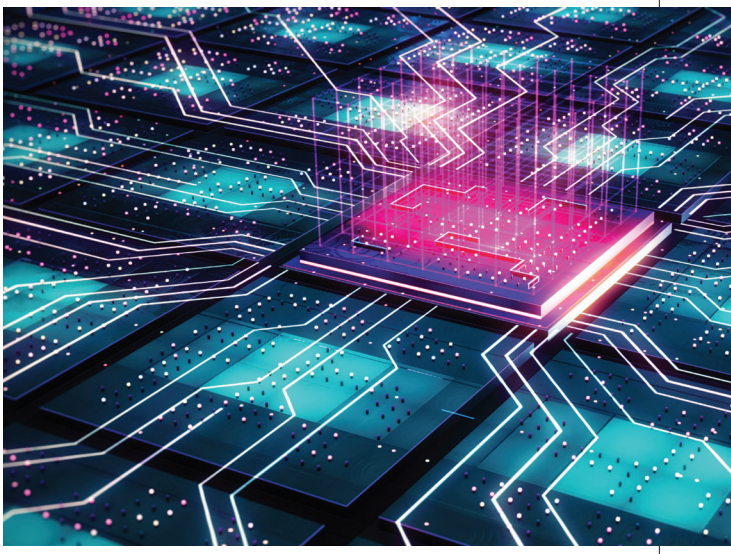
Convergence Guide" describes convergence as "formal collaboration between previously disjointed security functions." The guide states that, "Organizations with converged cybersecurity and physical security functions are more resilient and better prepared to identify, prevent, mitigate, and respond to threats. Convergence also encourages information sharing and developing unified security policies across security divisions."

A culture of inclusivity is vital to successfully converging security functions and fostering communication, coordination and collaboration.

"Security, HR, IT and all departments working together can proactively address risk while caring for the wellness and safety of employees," Weatherford said.



"Wellness scores and risk scores are now part of the identity and access governance process, and we have to have high expectations for our employees to follow through, providing the training and education to understand how security is an important part of business viability and profitability."



THE WAY FORWARD

The only way forward for business is digital transformation. In the past, security was regarded as something that security people took care of, but now it has become a core part of business processes. Security is really business by another name. This approach will bring challenges and opportunities in a post-Covid world in which the rules have changed and technology dominates.

Per CISA, organizations of all sizes can pursue convergence by developing an approach that is tailored to the organization's unique structure, priorities and capabilities.

"That's the era we're in now," Weatherford said. "Being able to trust that the people onsite are who they say they are while facilitating a positive user experience. Fear, uncertainty and doubt has to shift to trust, certainty and assurance. With convergence, we can see that security doesn't have to be a painful, friction-full experience. It can be built into business and actually make these processes better and richer." ◀

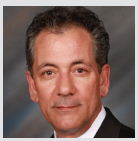
> ORGANIZATIONS WITH CONVERGED CYBERSECURITY AND PHYSICAL SECURITY FUNCTIONS ARE MORE RESILIENT AND BETTER PREPARED TO IDENTIFY, PREVENT, MITIGATE, AND RESPOND TO THREATS.

From Seed to Sale

Securing a cannabis operation poses unique challenges

THE CANNABIS INDUSTRY IS ONE OF THE FASTEST GROWING VERTICALS in the United States, offering a variety of opportunities for businesses seeking to capitalize on continued state deregulation. Amid global shutdowns, shelter-in-place orders, loss of jobs and the ever-present threat of illness, cannabis sales skyrocketed in 2020. A study conducted by Leafly using state tax and revenue data showed cannabis sales were up $7.6 billion over 2019 to $18.3 billion – a 71 percent increase. To date, 19 states have legalized marijuana recreationally, while 36 states have medicinal programs. Some jurisdictions are just now issuing licenses, and more are coming online.

Marijuana's continued status as a Schedule I drug at the federal level, though, certainly does not make it an easy landscape for prospective newcomers to navigate. Whether already operating a facility or planning to open a dispensary, processing or grow operation, there are many regulations to keep in mind – some of which prescribe electronic and physical security requirements. This article describes a few ways that cannabis grow operators, dispensaries and processors can leverage the benefits of a video management system (VMS) in their overall open platform security plan.



Brad Wareham (brad.wareham@salientsys.com) is Director, Key Accounts, for Salient Systems (www.salientsys.com).

LICENSING REQUIRES A SECURITY PLAN

Like any business, a cannabis operation requires certain licenses, approvals and audits before opening the doors. While regulations and security requirements differ across states, almost all require some form of electronic alarm and surveillance system, along with audit trails, whether paper or electronic, that must be archived.

Every location that has legalized medical or recreational marijuana has stringent licensing requirements, whether for grow operations, edibles manufacturing, processing plants, dispensaries, or transportation and the newer delivery services. While these regulations may differ in details, in almost all cases, they include having an acceptable security plan in place. These security plans are heavily weighted in the licensing application process. If the plan is found to be lacking, the business loses points. If the overall grade/number fails to meet the threshold, the business will not be issued a license. This puts pressure on the prospective operation to have an effective, well thought out security plan in place, describing the overall system architecture, including alarm, video and, in some cases, access control that allows the integration of other solutions. In addition, cannabis retailers need an audit trail working in conjunction with seed-to-sale (STS) compliance software, to ensure cannabis operations comply with regulatory requirements.

> SECURITY PLANS ARE HEAVILY WEIGHTED IN THE LICENSING APPLICATION PROCESS.

> NEARLY ALL STATES THAT HAVE FULLY LEGALIZED CANNABIS REQUIRE VIDEO SURVEILLANCE 24/7 THROUGHOUT THE ENTIRE FACILITY.

VIDEO SURVEILLANCE REQUIRED

While rules differ state-to-state, nearly all states that have fully legalized cannabis require video surveillance 24/7 throughout the entire facility. An average dispensary might have up to 40 cameras. A large-scale grow operation could have more than a hundred

cameras to ensure proper surveillance of the product and the harvesting process. No matter the business function, the perimeter needs to be protected and there can be no "dead zones" where a camera's field of view is obstructed. All hard and soft potential physical security threats (customers, employees, delivery people, packages) entering the premises must be tracked using the video system, along with any human or product movement that occurs within the facility.

To have a compliant security system, operators must have archived video footage in the event of an audit by compliance officers. Regulations vary by state, but video retention times of 45 days, 90 days or even 120 days are common. For the owner of a business, this means *everything* is recorded – from the transfer of product to individual product sales and storage – so a robust video solution to archive the footage is a necessity.

If a grow operation moves plants from one end of a facility to another but does not have video footage of the move, it could be a red flag for auditors. While constant video surveillance ensures all operations are compliant, it can also show when crimes – such as employee

theft – are committed. Using video systems, operators can more quickly reconcile inventory and determine if there are any discrepancies. Cameras can also help detect internal theft when items are weighed, as they can alert security personnel if the documented weight of a product does not match what it is estimated to be.

SEED-TO-SALE TRACKING

Seed-to-sale is the process of tagging each and every cannabis plant with a barcode or radio-frequency identification (RFID) marker that allows tracking from a grow operation (seed) to cultivation, processing and final sale. For cannabis customers, everything they buy has a batch number, complete with the lot and date – allowing them to learn the full lifecycle of the product. Such tracking measures exceed those in a pharmacy, where customers rarely find such specifics.

Using a video system with STS integration can drastically reduce the burden of mandatory data tracking on grow operators and dispensaries, as the camera can record an

> USING A VIDEO SYSTEM WITH SEED-TO-SALE INTEGRATION CAN DRASTICALLY REDUCE THE BURDEN OF MANDATORY DATA TRACKING ON GROW OPERATORS AND DISPENSARIES.

image of a plant's barcode as it passes by on its way to processing. The image is scanned and tracked with a barcode reader. While this information is also captured in the seed-to-sale software, video

images provide a valuable individual record of each of these transactions that can be easily retrieved when needed for a compliance audit or investigations.

VIDEO ANALYTICS OPTIMIZES DISPENSARY SECURITY

Cannabis retail dispensaries have faced some of the same challenges from Covid-19 as other retail markets, including long socially distanced lines and decreased occupancy levels. Video analytics can improve operations by using people counting to speed up queues and assist management in ensuring the facility is properly staffed. Video analytics can also be used to monitor the entire facility or operation, inside and out, ensuring the space is secure.

Additionally, integrations with point of sale (POS) and seed-to-sale systems assist dispensaries with reporting. For example, if a customer buys several products, it will be tracked in the POS/STS software and the facility can use the surveillance system that captured the metadata to ensure compliance, complete with an event-stamped audit trail.

REMOTE VIDEO ACCESS AND INVESTIGATIONS

Remote access to systems is in high demand across all sectors of the cannabis space. Even when they are not on site, cannabis operators can have instant visibility into their facilities using the surveillance system. With today's technology, they can have access to video anywhere in the facility via a mobile device. They will be able to see if someone has entered the site after-hours, or if there is an incident that triggers an event in the alarm, access control or surveillance system. This gives operators the ability to decide whether or not to engage internal or external resources to deal with the issue. Additionally, having remote, real-time access to the security and surveillance system can help cannabis operators keep a finger on the pulse of their operations.

As an example, many grow operations are located in remote areas not served by traditional copper or fiber ISPs, or they have facilities across multiple states, so it is vital to have a system that can provide an overview of an entire operation from any location while respecting the pipeline, even if that pipeline is a satellite or 4G cell network.

CASH MANAGEMENT

It is no secret that cash management is a major challenge for cannabis business operators. As cannabis is still illegal under federal law, most banking institutions are

> CANNABIS IS STILL LARGELY CASH-ONLY, WHICH PRESENTS SOME OBVIOUS SECURITY RISKS.

hesitant to venture into the market. As a result, cannabis is still largely cash-only, which presents some obvious security risks. Having large amounts of cash onsite provides an additional incentive to ensure that a comprehensive video surveillance and security solution is in place. Dispensaries must constantly capture POS register information and the entire point of purchase scene, including images of the buyer. Additionally, the VMS, coupled with edge, internal or third-party analytics, can notify local or remote personnel of any suspicious behavior, weapons or other objects that might indicate a potential threat. They can also monitor and record the movement of all cash and product through the entire facility.

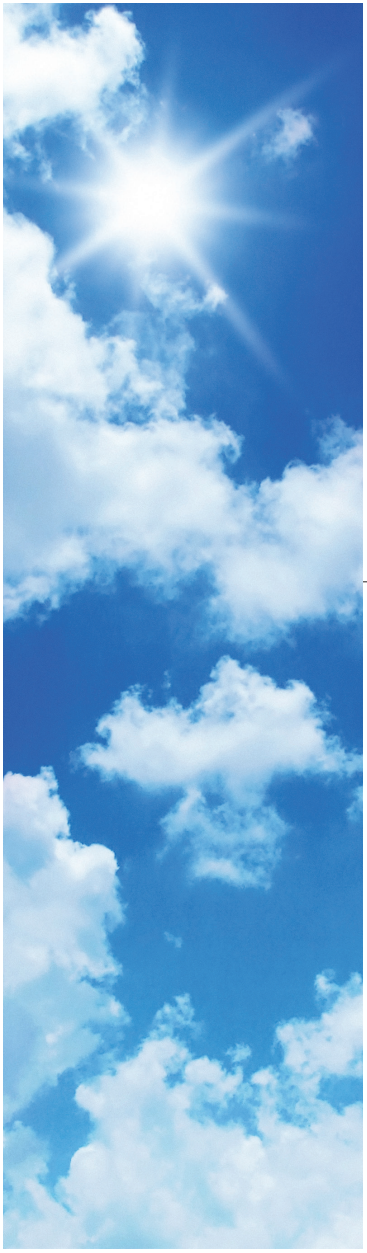
CONSULT A PROFESSIONAL

Security challenges existed long before the Covid-19 pandemic and are likely to continue into

the foreseeable future, as more states legalize recreational cannabis. An influx of sales and customers caused by the pandemic means cannabis facilities face even more pressure to ensure facility security and regulatory compliance. Navigating the strict security regulations imposed on cannabis businesses requires a well thought out plan and a flexible solution that can provide enterprise-level surveillance features and scalability. No matter what state the operation is located in, a security system with the capacity to store video footage and provide remote monitoring capabilities is a must.

Operators looking to open a facility should consider seeking guidance from a security consultant or systems integrator who is well versed in the cannabis space and familiar with the relevant regulations and procedures. The selection of a solutions provider that offers a flexible and open architecture approach to security can help to ensure the business' lifecycle compliance from seed to sale. ◀

> WITH TODAY'S TECHNOLOGY, CANNABIS OPERATORS CAN HAVE ACCESS TO VIDEO ANYWHERE IN THE FACILITY VIA A MOBILE DEVICE.

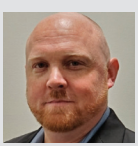


The Flexible Approach to Access Control

Open-source systems and the cloud provide savings and scalability options

JUMPING INTO THE WORLD OF BUSINESS IS NOT FOR THE FAINT OF HEART. In addition to managing employees, overseeing finances, and creating a sustainable plan, there are many other important considerations to be aware of, such as ensuring the comprehensive protection of people and assets inside the facility. Entrepreneurs are responsible for the safety of their business and those that help operate it, which requires making strategic decisions when it comes to what type of security solution will work best now and in the future. It is difficult to accurately predict business trajectory, so it is imperative to have a security system in place that allows for scaling up or down as needs change.

Manufacturers and integrators alike, especially in the access control sector, are responding to this growing concern by offering more customized solutions than ever before. From "as-a-service" offerings to the cloud, the industry understands the need for operational longevity and is continually working to improve the solutions available. When it comes to choosing an access control system that will fit a business's unique



Jeff Bransfield (jbransfield@rs2tech.com) is Vice President of Business Development for ACRE (www.acre-co.com).

needs both today and in the future, there are a few things to keep in mind.

SHOULD ACCESS CONTROL BE IN THE CLOUD?

Over the past few years, the availability of cloud-based security solutions has exploded, and for good reason. The benefits the cloud provides to end users are numerous, ranging from less costly installations to increased scalability potential, making it the number one contender when it comes to future-proofing a system.

The main advantage to selecting the cloud when considering the future of a business is financial. The cloud eliminates the need for a fully local system, which means there is no need to invest in an access control server, which is typically one of the more expensive parts of implementing an access control solution. Capital expenditures become a thing of the past, making system maintenance more cost effective.

In addition, cloud solutions are typically part of a subscription-based model, allowing users to pay a set monthly price for the services they receive. This ensures users are only paying for what they need at present, with the ability to change the services they subscribe to as their business grows. If a business only requires support for four doors when it launches, but experiences growth and later needs support for 10 doors, this can be done easily within the cloud in a cost-efficient way. Alternatively, if a user's business is experiencing slower growth than anticipated, services can be reduced. This ability to scale up or down

> CLOUD SOLUTIONS ARE TYPICALLY PART OF A SUBSCRIPTION-BASED MODEL, ALLOWING USERS TO PAY A SET MONTHLY PRICE FOR THE SERVICES THEY RECEIVE.

> NO WIRES, NO CAPITAL EXPENDITURES AND A DEDICATED TEAM MONITORING THE SYSTEM POSITIONS THE CLOUD AS AN IDEAL OPTION IN TERMS OF AFFORDABILITY AND SCALABILITY.

seamlessly creates cost savings and enables the flexibility necessary to adjust to an ever-changing technological world.

With no software to install and with automatic updates, the cloud ensures delivery of the most up-to-date, secure version of a system possible. Since there is no need to create an entirely new network, installations are streamlined, saving users both time and money compared to traditional access control solutions that require extensive wiring and network configuration. This further reduces installation costs while simultaneously allowing users to add more services without having to pay to rewire the entire network. No wires, no capital expenditures and a dedicated team monitoring the system positions the cloud as an ideal option in terms of affordability and scalability.

WHAT ABOUT OPEN SOURCE?

Open systems are affecting all aspects of physical security, from development to installation. In general, these systems are becoming increasingly accepted and implemented across the industry, though not all companies have recognized the benefits yet.

Open-source systems provide a level of flexibility that is unmatched by other options in the market. Instead of choosing a single manufacturer and getting locked into purchasing products and services from only that vendor, users can mix and match to receive a true “best of breed”

solution. An open system means being able to use equipment from a variety of companies to customize a solution to meet unique needs. There is no cookie cutter approach to access control, and open systems enable integrators to create solutions tailored to clients.

Because of this flexibility, users can start small and add more components to the system as the company grows. With no vendor lock-in, users can find a price point they are comfortable with, while also staying on the cutting edge of new technologies. This is necessary as users grow their businesses and, in turn, need additional equipment. An open-source access control system can easily integrate with video management systems (VMS), human resources, and HVAC systems to provide a full overview of a facility. From there, the system can grant and revoke credentials, schedule lighting and heating based on occupancy, and more. This integration provides situational awareness and ensures that a business is being run in the most streamlined and efficient way possible, with the ability to easily add cameras or other devices as needed.

With proprietary systems, users are forced to make up-front

commitments that do not allow for changes as new technologies are developed. Open systems ensure users are at the forefront of innovation, on whatever scale works best for them, while also providing the freedom of choice to make security decisions based on

> AN OPEN SYSTEM MEANS BEING ABLE TO USE EQUIPMENT FROM A VARIETY OF COMPANIES TO CUSTOMIZE A SOLUTION TO MEET UNIQUE NEEDS.

HOW MUCH DOES DOWNTIME COST?

According to Gartner, the average cost of IT downtime is $5,600 per minute. While there is variance in business operations to account for, this translates to costing companies about $140,000 to $540,000 per hour, with the average being $300,000.

functionality rather than manufacturer agreements.

Some companies have open APIs, which can be modified by integrators depending on what users are looking for. Are they interested in advanced technologies, such as facial recognition and machine learning? Open systems can accommodate that. There are minimal limitations to what can be done when using an open system, ensuring the solution that is implemented can be fully customized to user demands, with the ability to switch out equipment from different manufacturers as needs change. Gone are the days of the build once and maintain forever mindset. Open source provides users with more flexibility to choose than ever before.

IS REMOTE MONITORING NEEDED?

Remote monitoring provides both short and long-term benefits to technology investments and is especially useful for companies that do not have the resources to support full-scale IT departments.

The benefit of remote monitoring is that users have an off-site, dedicated team in place watching over the network to proactively respond to any vulnerabilities that could result in downtime. The moment a potential issue occurs, it is either taken care of automatically or, if human intervention is required, is sent to the correct person and dealt with immediately. This not only reduces downtime but could, actually, prevent the system from going down to begin with, saving the company significant money. Since users pay a set monthly price to receive remote monitoring services, there are no hidden fees incurred when an event arises. Think of remote monitoring like insurance: It is not always needed, but when it is, it pays for itself and more.

Remote monitoring

can also be useful to companies that have an on-site IT team by increasing productivity and allowing users to focus on essential job functions. If employees are constantly responding to every single IT event, that leaves little time for other things to be accomplished. Remote monitoring takes the guesswork out of what tasks need human intervention, streamlining internal operations and allowing employees to use their skills elsewhere.

The benefits of remote monitoring are especially important for companies that are just starting out, as a large financial setback could force a new business to close. For companies that already have an IT team in place, remote monitoring helps users to allocate resources and respond to events in a more streamlined way. In both scenarios, remote monitoring positions businesses to be successful in their responses to threats.

There are many ways to ensure that an access control system is ready for the technological challenges of the future,

> THE BENEFIT OF REMOTE MONITORING IS THAT USERS HAVE AN OFF-SITE, DEDICATED TEAM IN PLACE WATCHING OVER THE NETWORK TO PROACTIVELY RESPOND TO ANY VULNERABILITIES THAT COULD RESULT IN DOWNTIME.

and all the suggestions identified above can be combined. More importantly, all these services provide high levels of cybersecurity. It would not be practical to completely update traditional systems as new technologies are developed, but the cloud and open-source systems provide a way to do exactly that in a cost-effective manner. Combining the cloud, open capabilities and remote monitoring ensures access control systems will stay competitive in an evolving technological landscape. ◀

There Is a Hole in the Boat

Why access control professionals need to move from Wiegand to OSDP

MANY OF THE PEOPLE READING THIS PUBLICATION are, presumably, security professionals who take pride in leveraging their expertise to use technology to protect people and property. A large number likely focus on access control solutions to prevent unauthorized entry into controlled facilities and areas.

As unfortunate as it is to say, statistically speaking, the probability is that many readers are not doing a good enough job. It sounds harsh, but someone must tell the captain when there is a hole in the boat, and when it comes to most access control systems being installed today, the truth is *there is a hole in the boat*.

The problem lies in the fact that most access control systems being installed today still rely on Wiegand-style technology. John Wiegand, grandfather of access control systems, invented this technology in 1974. Needless to say, technology has come a long way since then.

By 1996, Wiegand-style access control had

David Coleman (dcoleman@paigeconnected.com) is Senior Vice President of Business Development for Paige Datacom Solutions (www.paigedatacom.com).

become the de facto standard. Since then, there have been plenty of advancements in the features and benefits of the hardware and software elements of these systems. In many ways, the buildings using these systems have become more secure and more intelligent. However, over the past 10 years, the pace of innovation has also picked up among the bad guys. Hackers have studied these systems, identified vulnerabilities, and created exploits that are simple, inexpensive and fast.

> WHEN INSTALLING A NEW ACCESS CONTROL SYSTEM, THERE REALLY SHOULD BE ONLY ONE CHOICE – FULLY OSDP-COMPLIANT PRODUCTS FROM BOW TO STERN.

HACKING ACCESS CONTROL SYSTEMS

For less than $100, anyone can go online and purchase a device known as an ESP Key. Bad actors can easily take a card reader off the wall and install this postage stamp-sized device on the existing wiring to "sniff" the data that is being transmitted across it. This sensitive data and the vulnerable way it is being transmitted requires attention.

The first problem is that Wiegand-style systems transmit card reader data in one direction, from the card reader to the door controller. Without bi-directional communication, it is impossible to be sure of the status of the card reader. Building owners may not know they have a problem with a card reader until someone tries and fails to badge in. Was it tampered with? Was it vandalized? When did it stop working? These questions are too difficult to answer when there is no immediate alert, which can only be done with bidirectional communication.

The second problem is that the data being transmitted from the card reader to the door controller is sent "in the clear." This means that the data is being sent as simple pulses that equate to unencrypted ones and zeroes. When the ESP Key sniffs these pulses, it sees and stores the credential

data (raw bitstream like a PIN, facility code or user ID). Over the course of a few hours or days, the ESP Key will have collected plenty of data from the unsuspecting users who badged into the door. The hacker needs only to pull out a phone, connect wirelessly to the ESP Key, choose which badge to "replay" and, just like that, they are in the building.

PROTECTED ACCESS CONTROL SYSTEMS

At this point, readers may be wondering, with such a big hole in the boat, how can it be fixed? The answer is simple, and it has been around for several years. The Security Industry Association adopted the Open Supervised Device Protocol (OSDP) as the new access control standard in 2012. In May 2020, OSDP was approved as an international standard by the International Electrotechnical Commission (published as IEC 60839-11-5). The OSDP standard was most recently released in December 2020 as version 2.2.1.

What is OSDP and how does it plug this hole? First, OSDP supports bidirectional communication between the card reader and the door controller, which allows for supervision (the "S" in OSDP). Not only is the card reader continuously monitored, but the data is also sent in a secure channel with AES 128-bit encryption. This means that, even if a hacker installed an ESP Key in an OSDP-compliant card reader, any data that was captured would be unusable, because the encrypted data cannot be converted without a one-time "key" for which there are $3.4x10^{38}$ combinations.

One does not have to search for long to find stories about companies

HOW MUCH IS $3.4X10^{38}$?

Encrypted data from an OSDP-compliant device cannot be converted without a one-time "key" for which there are $3.4x10^{38}$ combinations. That is, 340,28 2,366,920,938,463,463, 374,607,431,768,211,456 or 340 undecillion, 282 decillion, 366 nonillion, 920 octillion, 938 septil¬lion, 463 sextillion, 463 quintillion, 374 quadrillion, 607 trillion, 431 billion, 768 million, 211 thou¬sand and 456 possible combinations.

large and small that fall victim to hackers. And if a system is vulnerable to attack, it is just a matter of time before it is targeted. With attacks focusing on access control systems becoming less expensive to execute, the time is now to take the necessary steps to protect buildings and employees.

> OSDP SUPPORTS BIDIRECTIONAL COMMUNICATION BETWEEN THE CARD READER AND THE DOOR CONTROLLER, WHICH ALLOWS FOR SUPERVISION (THE "S" IN OSDP). NOT ONLY IS THE CARD READER CONTINUOUSLY MONITORED, BUT THE DATA IS ALSO SENT IN A SECURE CHANNEL WITH AES 128-BIT ENCRYPTION.

The security benefits of OSDP will certainly help make buildings more secure, but what about making them more intelligent as well? OSDP supports new features that allow for a richer user interface. Yesterday's "high-tech" card readers boasted the ability to flash more than one LED. With OSDP, the monitor at the card reader can prompt a user to use a different entrance, or even wish them a happy birthday.

TAKING THE NEXT STEPS

Perhaps some of the best news about OSDP is that, while it offers advanced security and intelligence, it does not come with a big price tag. OSDP can be installed for roughly the same price as Wiegand-style systems and there are many great products that make transitioning from Wiegand to OSDP painless.

When installing a new access control system, there really should be only one choice – fully OSDP-compliant products from bow to stern. Some leading manufacturers of OSDP hardware are putting their commitment

to the standard front and center by having their products tested in the SIA OSDP Verified program, which validates that a device conforms to the OSDP standard and related performance profiles.

If upgrading or retrofitting an existing system, there are door controllers that will allow for simultaneous connections to Wiegand and OSDP card readers. This option works for those who might choose to start with the most vulnerable or sensitive areas of the building first. In addition, leading companies in the OSDP space offer solutions to convert one door at a time.

Another area where OSDP shines is upgrading card reader software. Wiegand-style systems require users to physically connect to each device in the field. With OSDP's bidirectional communication, though, it is possible to push an update out to all card readers at once.

In addition to the security benefits noted above, these signals are capable of being transmitted across much longer distances. Standard Wiegand-style card readers need to be located within 500 feet of the door controller. This limitation sometimes requires additional door controllers to be added to a system in order to be within range of the farthest doors. With OSDP, card reader data is transmitted via the RS-485 protocol, enabling signals to be sent 4,000 feet (some manufacturers support even longer distances.) That means the guard shack at the edge of the parking lot and the shed in the back are now within reach.

FOR NON-INSTALLERS

Even non-installers have a responsibility to move the industry in the

right direction. It does not matter what a person's job is on the boat – if they see a hole with water rushing in, they have to tell the captain. A manufacturer who is working on bringing new features or product lines to the market should not allow decisions to be driven by the percentage of Wiegand vs. OSDP systems sold last year. Instead, they should nudge customers in the best direction and offer fewer (or no) options for Wiegand-style readers. Consultants and other influencers of security design should promote the benefits of OSDP and educate clients about the problems of unencrypted, non-supervised transmission of sensitive data.

"CONSULTANTS AND OTHER INFLUENCERS OF SECURITY DESIGN SHOULD PROMOTE THE BENEFITS OF OSDP AND EDUCATE CLIENTS ABOUT THE PROBLEMS OF UNENCRYPTED, NON-SUPERVISED TRANSMISSION OF SENSITIVE DATA.

The security industry was slow to adopt IP video over analog. Certain companies, though, chose to take a leadership position, and by doing so, they catapulted themselves to the leaders they are today, while many of the firms that were slow to adapt are no longer as relevant now. The industry is at a similar crossroads with access control today.

WINNING WITH WIRING

With new hardware and new protocols, some readers may be wondering if new cabling is needed, as well. The short answer is yes. The longer answer is yes, most of the time. To ensure optimal performance, card reader cabling should include two pairs (one for data and one for power) of low capacitance, shielded, 120-Ohm wires. Capacitance is measured in picofarads per foot and something in the ballpark of 12.5 pF/Ft is appropriate. (In contrast, a standard Wiegand card reader typically has a capacitance rating of 47 pF/Ft and an impedance of 39 Ohms.) These types of OSDP card reader cables are readily found at major distributors and can be included as part of

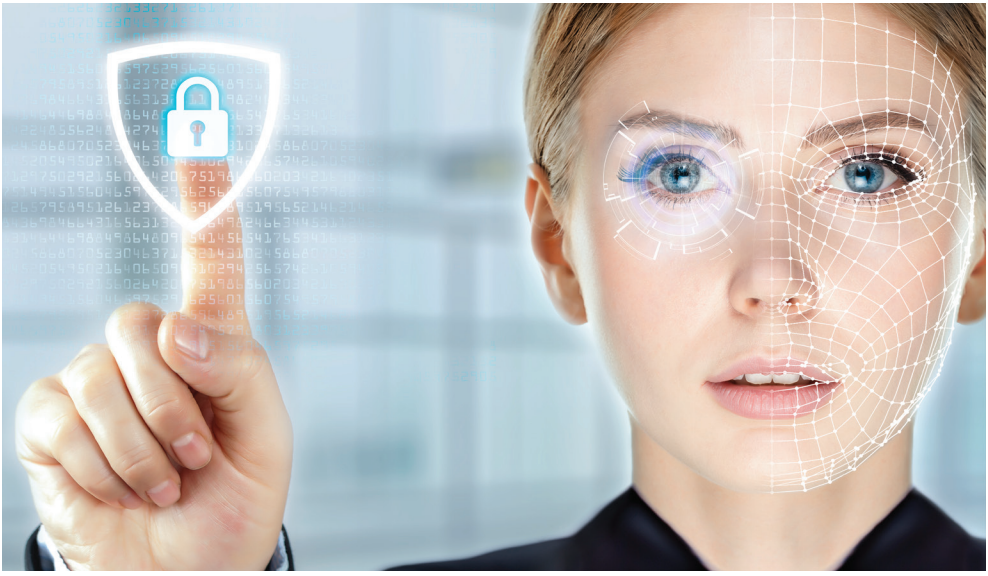
a composite cable that has multiple "legs," all under an overall jacket for door contacts, request for exit buttons, motion detectors, lock power and other accessories in an access control system.

While optimal performance is always going to come from using the appropriate cable for the application, there are going to be short cable runs where the difference is negligible. If an existing card reader cable is less than 200 feet, the risk of using it for OSDP is significantly less than when the cable runs are longer.

Another common question is, "What cable should I run today so my customer is ready tomorrow for OSDP?" If, after educating a customer about the benefits of OSDP, they are still not ready, one forward-thinking strategy is to pull an OSDP card reader cable to each door along with the Wiegand-style composite cable. This way, when the customer is ready to upgrade card readers (and perhaps door controllers), there is no need to waste time installing thousands of feet of new cables throughout the building.

While OSDP is very different from Wiegand, it is not more difficult to learn or install. In fact, the opposite is the case. With fewer wires (two pairs compared to six to 12 conductors), the reduced complexity that comes from long distance support, and the ability to centrally push upgrades to card readers, OSDP can simplify access control projects – all while fixing the hole and keeping the boat afloat. ◀

> WHILE OSDP IS VERY DIFFERENT FROM WIEGAND, IT IS NOT MORE DIFFICULT TO LEARN OR INSTALL. IN FACT, THE OPPOSITE IS THE CASE.



The Future is Autonomous

AI will enable security solutions to analyze and act

James McKnight (james.mcknight@jci.com) is a Product Manager for Tyco American Dynamics (www.americandynamics.net).

ARTIFICIAL INTELLIGENCE (AI) HAS BECOME A PART OF OUR EVERYDAY LIVES. People interact with AI, for example, when shopping online and getting a question answered by a chatbot or having the website recommend additional items for purchase. In addition, AI makes it easy for people to leverage voice-to-text responses on mobile devices quickly and accurately.

AI is also having a dramatic impact on the security industry. It is revolutionizing the capabilities of security technologies and providing decision guidance that makes security operations more efficient and cost effective.

This technology is being incorporated into multiple product categories, including access control, video and building management systems.

Better video compression standards, higher megapixel cameras and greatly improved field of view are just a few of the ways that AI is driving improved image quality and data while reducing bandwidth consumption. It is also enabling accelerated workflows, delivering detailed and actionable intelligence that was not possible just five years ago.

Thanks to AI, security devices and systems have a greater ability to mine data and transform that information into valuable insights. The AI era is here, so how is the technology affecting specific devices and solutions in the security industry?

BETTER VIDEO COMPRESSION STANDARDS, HIGHER MEGAPIXEL CAMERAS AND GREATLY IMPROVED FIELD OF VIEW ARE JUST A FEW OF THE WAYS THAT AI IS DRIVING IMPROVED IMAGE QUALITY AND DATA WHILE REDUCING BANDWIDTH CONSUMPTION.

FRICTIONLESS ACCESS

Frictionless access control has been the talk of the security industry for the past year and a half. This solution uses enhanced facial recognition technology to validate an individual

> AI IS ENABLING ACCELERATED WORKFLOWS, DELIVERING DETAILED AND ACTIONABLE INTELLIGENCE THAT WAS NOT POSSIBLE JUST FIVE YEARS AGO.

and permit access into an area without the individual needing to stop and present a credential. Two imagers in a surveillance camera create a 3D facial topography, which increases accuracy and reduces false positives. When integrated with access control, the system automatically recognizes an individual from a database and determines whether that person should be permitted to enter.

This approach greatly simplifies the user experience with minimal interruption to the flow of access. None of this would be possible without AI and its deep learning algorithms and fast processing speed. Together, they allow the system to concurrently process multiple people in the same frame, accurately detecting and recognizing individual faces from several feet away.

CROWD FORMATION

Being able to quickly identify that a large group of people is approaching – whether in protest or to celebrate a sports victory or for some other reason – is invaluable information for security personnel and police departments. When combined with crowd formation technology, AI can help to escalate actionable tasks. For example, in public transportation hubs such as train stations, AI can detect the number of people waiting in a particular area. If the system detects that the number of people waiting on a platform is approaching maximum capacity, it can alert the operator to activate crowd management protocols and potentially add another train to the schedule.

OCCUPANCY COUNTING

Knowing how many people are in a specific space can assist with occupancy management. Before AI, it was often difficult to tell the difference between a human and a pet in a

> AI MAKES IT POSSIBLE TO EFFECTIVELY MANAGE EXTREMELY LARGE VOLUMES OF DATA AND QUICKLY PROVIDE CONTEXT AND MEANINGFUL INSIGHTS INTO THAT DATA.

> WITH AN AI-ENABLED VMS, MANY OF THOSE DECISION-MAKING FUNCTIONS CAN BE HANDLED AUTONOMOUSLY INSTEAD OF RELYING ON HUMAN INTERVENTION.

crowded setting. AI enables the collection of more detailed information and allows the user to set parameters for the type of data that needs to be analyzed.

When integrated with an access control system, AI can not only confirm the number of occupants in a room, but it can also send an alarm if the count does not match the number of people who used an access control badge to gain entrance into that space. This can help security personnel identify a tailgating issue or other security problem.

SITUATIONAL AWARENESS

Data is becoming increasingly important for security professionals, but sifting through days of raw video footage to pinpoint an event of interest is both taxing and time consuming. AI makes it possible to effectively manage extremely large volumes of data and quickly provide context and meaningful insights into that data.

For example, during manual analysis, a simple event like a person leaving a package near a park bench might be difficult to quickly assess and categorize as a potentially serious threat. By providing simplified context visualization, AI cuts through the noise to help identify the incident and can then aid in determining if the package poses a significant security risk.

AI IN SURVEILLANCE

The digitization of surveillance cameras has made video accessible

on nearly any network. This has evolved to now include video data easily being sent to the cloud for storage and advanced analysis.

Video management system (VMS) capabilities are greatly enhanced with AI. In the most basic system, a VMS enables multiple devices to come together into a single easy-to-use tool, improving data visibility and decision-making. With an AI-enabled VMS, many of those decision-making functions can be handled autonomously instead of relying on human intervention. By continuously monitoring an area, the software can learn what is normal and abnormal behavior. This could include detecting a traffic accident, an illegal U-turn, or even people running in an area where they usually walk.

It is clear that the surveillance industry is at a critical juncture. Technological advancements and the introduction of AI can enable security systems to become the solutions of the future. ◀

Solving Business Challenges with Computer Vision

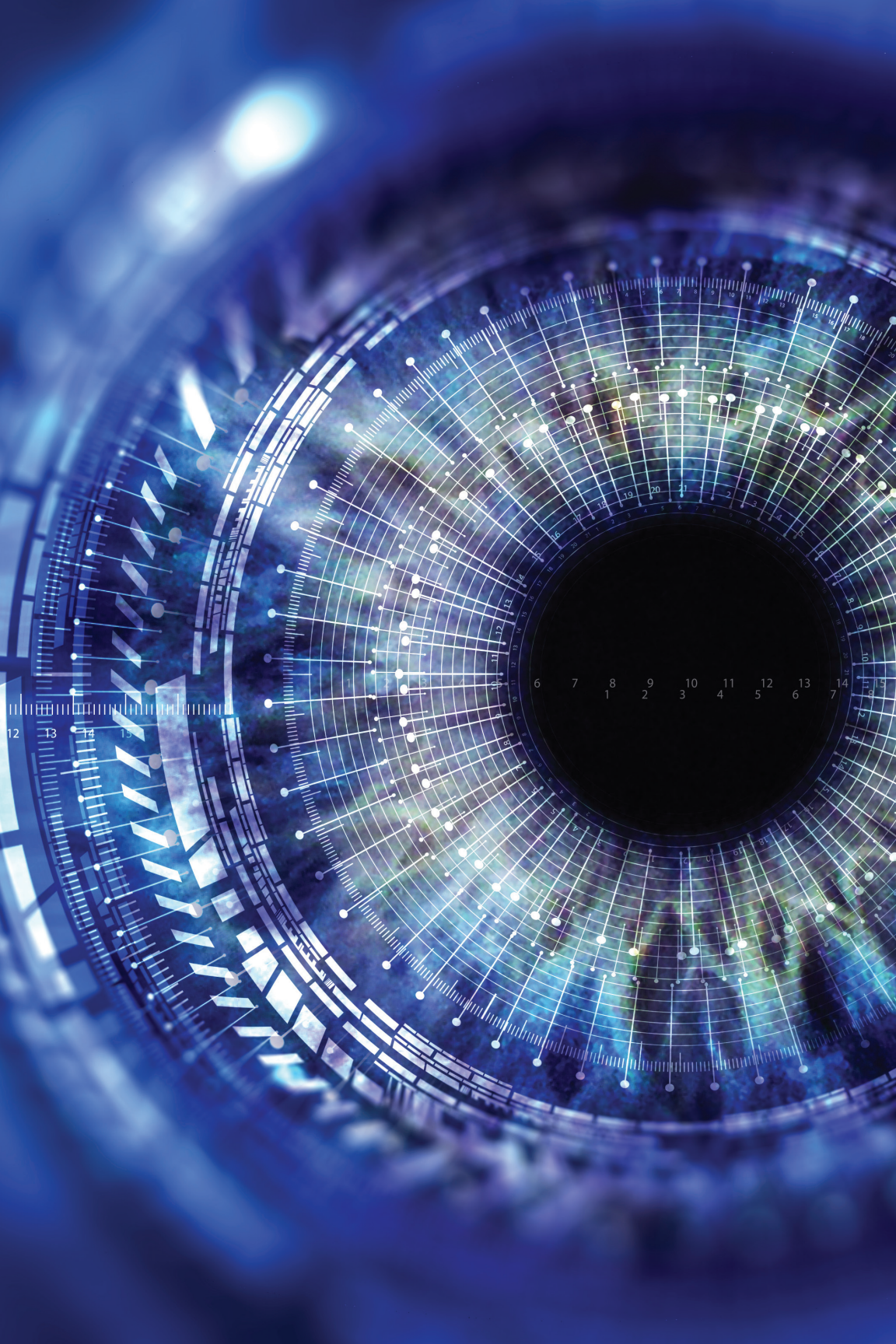
Artificial intelligence technologies will soon be transformative

ALAN TURING IS CONSIDERED TO BE A FOUNDING PIONEER of artificial intelligence (AI), dating back to the 1940s. The role of AI, in particular computer vision, has dramatically increased since then, in part because of the overwhelming amount of digital and visual data in our daily lives.

Computer vision is one of the most advanced fields of AI and involves applying machine learning (ML) models to digital images to identify and label objects and events. This can deliver significant insights into any data captured through any visual medium. Through computer vision, AI can use the "identified" ML data to perform advanced analytics, make recommendations, and deliver insights to make businesses more efficient.

Today, organizations are challenged to increase their ability to perform analytics on large amounts of data. Coupling the inherent "eyes in the sky" nature of surveillance with AI algorithms to identify anomalous events can deliver real-time remediation and produce intelligence and analytics that can transform an enterprise's security, safety and business operations.

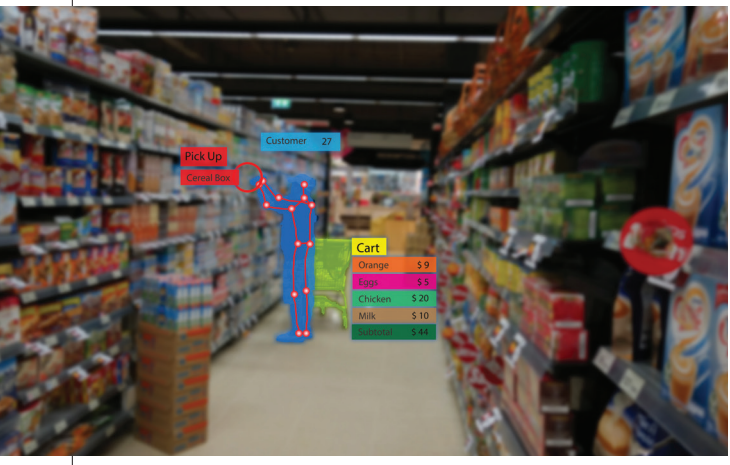
Ron Rothman (ron.rothman@turingvideo.com) is the President of Turing Video (www.turing.ai).



> USING AI IN THIS WAY CAN REDUCE RISK WHILE IMPROVING OPERATIONAL EFFICIENCIES AND INCREASING CUSTOMER AND EMPLOYEE SATISFACTION.

THE EVOLUTION OF SMART SURVEILLANCE

Video surveillance is a mainstay in many industries, from retail to health care to hospitality to corporate offices. Name an industry and surveillance is probably present in some shape or form. It goes without saying that ensuring the highest level of protection and security is vital. Surveillance can "up the ante" by utilizing the analytic features of AI technologies to deliver insights that can improve operations and reduce risk, while getting the highest return on surveillance investments.



Taking the retail industry as an example, instead of having a staff member monitor a multitude of cameras, AI algorithms can automatically identify when a meaningful incident occurs. Imagine if a supervisor could be notified of a long queue in one of the check-out lines. Or store security alerted to a theft as it is occurring. Or a manager informed instantly of a slip and fall so that it could be quickly addressed and documented. Broken merchandise or boxes blocking an aisle could be promptly detected. A potentially dangerous event involving obstructions or hazards in the loading dock, or a forklift being driven too fast or recklessly, could trigger an alert. These are just a few examples of how computer vision AI technology could be utilized in a retail environment, but the possibilities are endless. Using AI in this way can reduce risk while improving operational efficiencies and increasing customer and employee satisfaction.

Another industry that can reap enormous benefits is manufacturing. In addition to keeping a site secure from trespassing and loitering, computer vision can identify operational bottlenecks, helping to increase output. Management teams have theorized and invested for decades in this area, going back to the invention of the assembly line. By applying computer vision AI, new opportunities for efficiencies and savings are available. And, as the manufacturing industry is prone to workplace injuries, AI algorithms can be implemented that identify which employees have been properly trained and authorized to be in an area and confirm that they are using the required protective gear and are adhering to safety protocols. Dangerous activities or obstructions to exits can be identified. Accidents or injuries can be addressed immediately, expediting the dispatch of safety personnel while capturing critical video footage for worker's compensation and OSHA inquiries. Video clips can

be tagged for specific incidents, so what might previously have required hours of searching can now be done in minutes. This is just a brief look at what will become available through computer vision AI, in many cases by leveraging existing cameras and infrastructure.

> WHILE KEEPING A FACILITY SECURE IS IMPORTANT, ENSURING THAT SENSITIVE PERSONAL DATA IS KEPT FROM PRYING EYES IS BECOMING MORE VITAL.

INDUSTRY AGNOSTIC TECHNOLOGY

Any industry can take advantage of computer vision AI-enabled surveillance technologies. Use cases include the following.

> AI CAN BE APPLIED TO IDENTIFY AND SAVE ONLY THE ESSENTIAL VIDEO CLIPS, FREEING UP VALUABLE CLOUD CAPACITY.

- **Hospitals** must comply with privacy regulations while ensuring the protection of patients, employees and visitors. By tapping into AI technology and using advanced algorithms with their surveillance cameras, security personnel can get alerts of entry into restricted areas without having to monitor the locations manually 24/7, thus saving countless security man-hours.

Being notified of an event immediately as it happens, they can investigate and remediate the situation. This provides a deeper level of building security to put both employee and patient minds at ease, while saving on labor costs.

- **Nursing homes** provide critical care during a time in life when people need more hands-on support. Facilities can take advantage of AI-enabled surveillance by employing a people search algorithm to monitor resident locations and get notified in real time if someone has exited the building or their living area. In addition, a slip and fall event could be identified, as could unauthorized visitors. Computer vision AI could be applied to identify abusive behavior, which is, unfortunately, an ongoing concern in this industry. Also, in case of an emergency

evacuation, AI can help determine if a patient is still inside the building and needs assistance.

- **Educational institutions** have been through a lot during the pandemic and have had to significantly change their model of operations. Now that schools are back in session, they are tasked with providing multiple levels of security, from ensuring campus safety to supporting the health and well-being of students. AI algorithms can be implemented that monitor suspicious or dangerous incidents on campus, parking violations, unauthorized visitors, missing students, and fighting and bullying, alerting security to enable immediate response. Other AI technologies can be used for non-contact temperature checks, face mask detection, and social distancing protocol adherence. These types of technologies can be the fastest route to getting back to "normal" school while ensuring both safety and security.

While keeping a facility secure is important, ensuring that sensitive personal data is kept from prying eyes is becoming more vital. It is imperative that NDAA-compliant camera and NVR technologies be implemented to ensure the greatest levels of security, protection and regulatory compliance.

TAKING SURVEILLANCE TO NEW HEIGHTS

One of the most impactful trends in video surveillance over the past few years has been the

> ROBOTS AND DRONES WILL FURTHER DRIVE AI TRENDS AND APPLICATIONS.

shift to cloud-based video storage. Local NVR devices that store surveillance footage often must be erased after 30 or 60 days to make room for new video streams. Being able to store data in the cloud, even in perpetuity if needed, means that more than just a month or two of video clips and incidents are available for review. This can be important in the case of OSHA inquiries and worker's compensation claims, which often do not arise until some time has passed. Most importantly, AI can be applied to identify and save only the essential video clips, freeing up valuable cloud capacity.

As with local storage devices, strong security for the stored data is critical to ensuring privacy and compliance with laws and regulations.

360-DEGREE VIEW OF BUSINESS

The AI transformation is coming, and companies should take action now to capitalize on the intelligence and insights that computer vision AI-driven surveillance can offer.

Robots and drones will further drive AI trends and applications. These mobile autonomous machines will incorporate a variety of 360-degree cameras and environmental sensors while leveraging advancements in laser and mapping technologies. Significant business and operational benefits will be realized by flagging obstructions or incidents on patrol routes.

All of this will bring us ever closer to Alan Turing's vision of smarter machines. ◀

Ready to improve how you manage security projects?

Improve Your Security Project Management Skills with SIA Training and Certification Programs.

SPM
SECURITYPROJECTMANAGEMENT

More than just knowing the technology, successful project management involves budgeting, client management, timeline execution and more.

Learn more at securityindustry.org/spm

CSPM
CERTIFIED SECURITY PROJECT MANAGER

This highly-respected credential can move your career forward and propel your business. The CSPM credential informs clients that you can successfully manage complex, technical security projects.

Learn more at securityindustry.org/cspm

Security Industry Association
securityindustry.org

SIA

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