TECHNOLOGY
Insights

Spring 2023

Volume 11, Number 1

Fans of Security

Crowdsourced intelligence at major events can be a force multiplier Page 18

Visualizing Success

New data presentation tools enhance security, operations

Page 24

Lights, Camera, ALPR

External lighting improves license plate recognition

Page 28

Park Places

AI makes garages, lots safer, easier to navigate

Page 34

SNG™

SECURINGNEWGROUND

Oct. 17 – 18, 2023 | 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*

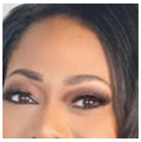
SECURINGNEWGROUND.COM

SIA

TECHNOLOGY insights

Spring 2023

Volume 11, 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.

The Future of Physical Security and Risk Management

Digital twins provide new, dynamic views of building operations

ARTIFICIAL INTELLIGENCE (AI) IS BECOMING UBIQUITOUS. However, when it comes to the enterprise, physical security has remained within the domain of forensics, with outdated manual methods and tools keeping these departments in the dark ages. The result: Facilities are managing expensive, inefficient and wasteful physical security protocols.

Beyond cameras and controlled access, enterprises are now, for the first time, able to harness the gold mine of data held in their security systems, Internet of Things (IoT) devices, IT infrastructure, internal regulations, and regulatory compliance documentation. This data can be used to visualize all systems and map them to an organization's physical security risks, both internal and external, and show how they are interconnected within the facility and the business operation.

Stephane Levy (slevy@beamup.ai) is the founder and CEO of BeamUp (www.beamup.ai).

111100001

RISKY BUSINESS

The outdated, manual, analog tools that enterprises have been using are not fit for purpose. Ill-equipped contractors using legacy tools and methods expose enterprises to physical and cyber risks that can cost them millions of dollars.

Tools like spreadsheets and CAD files are not only static, error-laden and stored locally, but they are also siloed. Companies that are still working with these tools face knowledge gaps, lost documentation, and duplicated efforts from design through the entire lifecycle. Leveraging data is critical for efficiency, performance and savings in security system design and operations.

Today's technology advances, such as cloud computing, deep learning and IoT, enable the application of enterprise data to mitigate risks and accurately and efficiently manage facilities' security systems.

During the past 10 years, enterprises have started to apply AI and deep learning to building systems, in some cases reducing management costs by 70 percent and system design

time by a massive 90 percent.

With the role of data central to the operations and planning of security systems, security executives must work closely with data scientists and expand their skill sets if they want to keep up.

By using convolutional neural networks, graph neural networks and other deep learning architectures, solutions can automatically and quickly classify floorplans and detect features (doors and windows) and objects (desks) within each space in a facility, then generate outputs including recommendations, 3D models or building system designs.

All changes are documented and stored, and any iterations are already automatically compliant with regulations. As a result, security systems within multi-facility enterprises are efficient, compliant and secure at a fraction of the cost of previous methodologies.

> “TODAY’S TECHNOLOGY ADVANCES, SUCH AS CLOUD COMPUTING, DEEP LEARNING AND IOT, ENABLE THE APPLICATION OF ENTERPRISE DATA TO MITIGATE RISKS AND ACCURATELY AND EFFICIENTLY MANAGE FACILITIES’ SECURITY SYSTEMS.

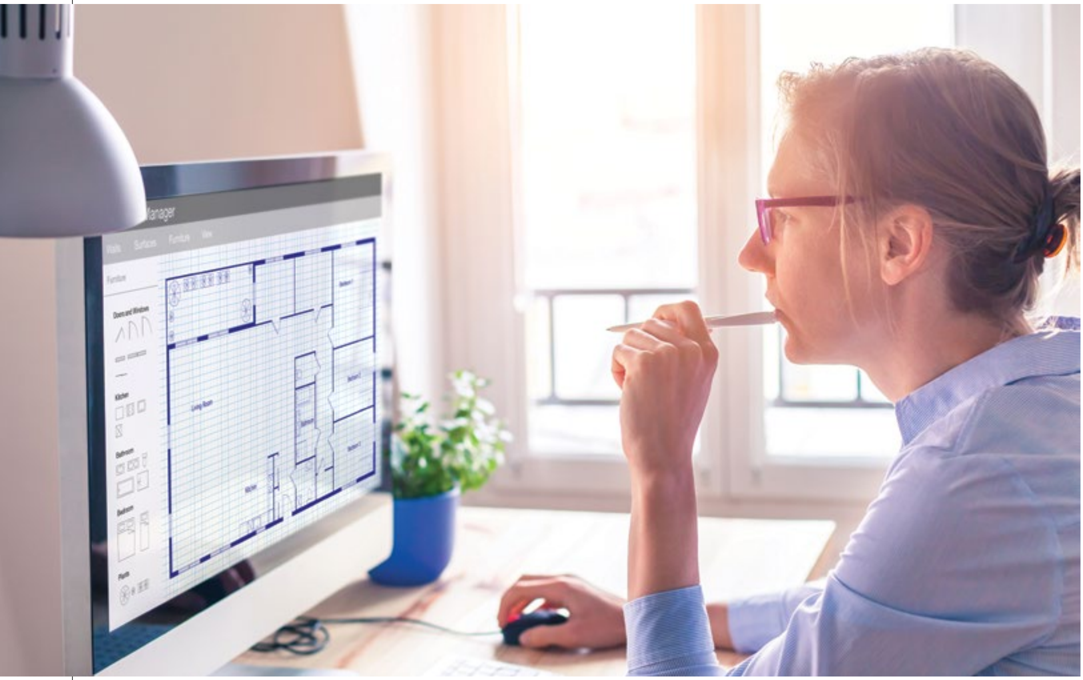
WHY ARE DIGITAL TWINS NEEDED?

Building data can be used to develop a 3D model, which, when combined with real-world data, creates a “digital twin” – a virtual representation of the physical environment. This functionality is changing the game for security teams.

Big picture visualization of data across hundreds of facilities – floor plans, devices, furniture, door types – provides security professionals with a macro view of all system components across the global network of buildings.

The combination of digital twin technology with AI unlocks the true promise of the technology – the ability to both see and automate key processes for managing security systems. Now, arduous tasks such as vendor management, warranty renewal, and budget projections and modeling can be completed with precision in much less time than when done manually.

Not only can the technology identify risks, it can also immediately provide remediation alternatives. For example, if there is a compliance issue, an alert is sent to



the security team, which can then easily access floor plans, add or move a camera, arrange for a device's installation, and automatically update the documentation.

TECH-ENABLED READINESS FOR ANYTHING

The adoption of digital twin technology will change the management of real estate. Security executives will need to work closely with the CTO and develop new skills to manage and plan multi-level security strategies. This new technology makes it possible for them to model and evaluate physical security system performance under specified conditions of threat and system operation.

> WITH THE ROLE OF DATA CENTRAL TO THE OPERATIONS AND PLANNING OF SECURITY SYSTEMS, SECURITY EXECUTIVES MUST WORK CLOSELY WITH DATA SCIENTISTS AND EXPAND THEIR SKILL SETS IF THEY WANT TO KEEP UP.

For example, security system design might require an analysis of the interactions of basic security functions within a facility. During an event, personnel must be able to determine how many entrances and exits a building has and what kind of locking mechanisms are in place.

In an emergency, floor plans and vendor information must be easily and quickly accessible, which is impossible if they are only stored locally on someone's desktop. Equally, if there is a change of use of the facility, the security team must be able to see floor plans, device information and regulatory guidelines in order to document the changes and make sure they are compliant.

Security is dynamic, and digital twins ensure that appropriate personnel have access to all relevant building data as they need it, and that documentation is readily available. Full oversight of a facility's system data enables always-on security teams to keep up with changes and company needs.

CONSIDERATIONS FOR SYSTEM DESIGN

Designing a building's security system is a complex process in both new builds and retrofits or renovations. There are countless considerations and data points that are

virtually impossible to manage manually or with analog technology, from usage, layout or location of different departments to security camera placement and door types.

This is where working with digital twin technology presents the most significant impact for security system designers. The technology can model the features of a building in accordance not only with a company's internal rules and guidelines but also with government regulations. For instance, server rooms must only have one entry point, so not every space within a facility would be appropriate for this function. If a server room was planned with AI and digital twin technology in a location with two doors, it would be automatically flagged.

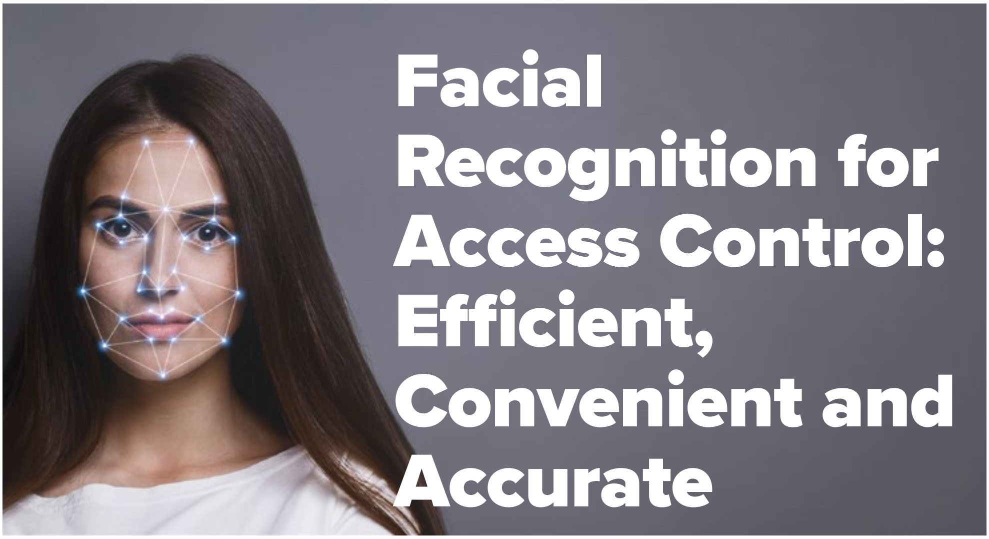
This technology reduces system and infrastructure design time from months to days. It also mitigates operational costs associated with outside contractors, errors, rework and compliance breaches.

Beyond design and management of security systems, AI and machine learning streamline workflows and provide valuable insights for internal processes. The technologies automate approvals for changes and iterations and integrate with existing company systems for full visibility and access. Further, they unlock critical business and industry landscape insights by benchmarking operational performance against other facilities within the same region, business or industry. The C-suite can use these insights to make informed business strategy decisions.

> THE COMBINATION OF DIGITAL TWIN TECHNOLOGY WITH AI UNLOCKS THE TRUE PROMISE OF THE TECHNOLOGY – THE ABILITY TO BOTH SEE AND AUTOMATE KEY PROCESSES FOR MANAGING SECURITY SYSTEMS.

From everyday maintenance to design, business strategy and internal operations, AI and digital twins are improving the performance of security teams around the world as they design, plan and manage safe, secure and compliant buildings. ◀

Facial Recognition for Access Control: Efficient, Convenient and Accurate



Systems that identify enrolled individuals are the most effective and least controversial

LIKE SO MANY OTHER SECTORS OF THE ECONOMY, THE SECURITY INDUSTRY CANNOT FIND WORKERS. Even steeply rising wages are not attracting enough candidates to fill access-related security positions. Fortunately, help is here, in the form of facial recognition (FR) solutions. With the ability to provide safe, effective and cost-efficient identity verification, FR technology can close the security industry's labor gap.

FR has come a long way fast. In the early 2000s, the Los Angeles Police Department tested very early handheld devices. Officers would stand a suspect against a wall and take a picture, then wait as long as five minutes while the software tried to match the image against a database of fewer than 150 people who had injunctions against them. It was kludgy and ineffective, but the promise was evident.

In 2006, the first Face Recognition Grand Challenge, an event created to encourage innovation within the industry, found the best algorithms at that time to be 10 times more accurate than just four years earlier and 100 times more accurate than in 1995. Fast forward

Steve Reinharz (steve.reinharz@radsecurity.com) is the president of Robotic Assistance Devices (www.radsecurity.com).

to today, and the National Institute of Standards and Technology (NIST) reports that current high-performing algorithms are “close to perfect” in matching faces against a database of 12 million people.

Facial recognition technology is having an impact at both the state and local levels across the United States. At last count, seventeen state police departments and 744 local police departments utilize FR, and facial recognition is used by the U.S. Customs and Border Protection’s Global Entry system at airports to verify the identity of enrolled individuals who are returning to the United States.

FR’s less accurate rate of identifying the faces of non-white individuals, however, has driven some public distrust over its use as a policing tool. Innocent black men have been arrested and accused of

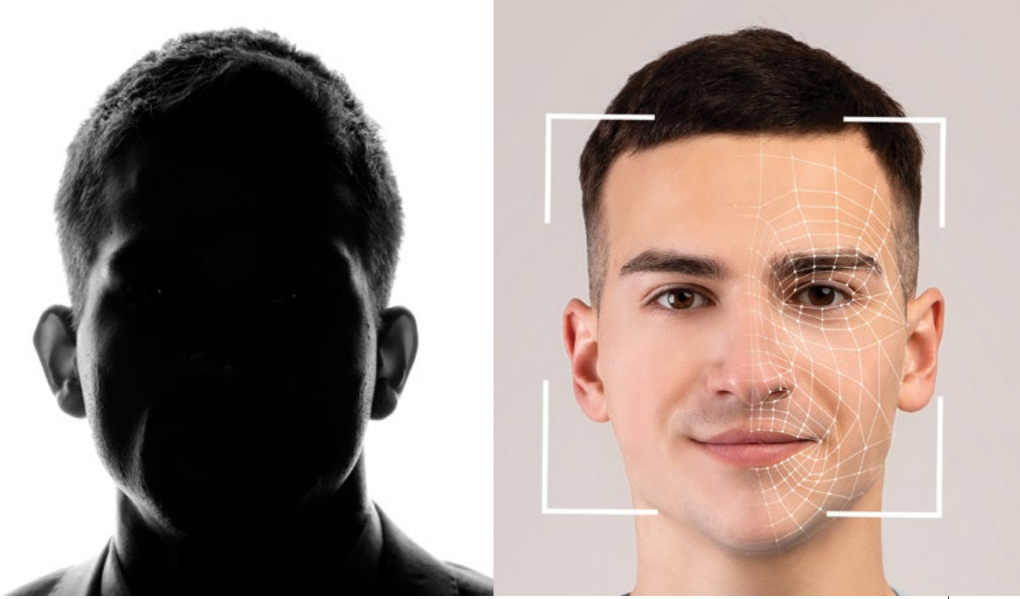
> WITH THE ABILITY TO PROVIDE SAFE, EFFECTIVE AND COST-EFFICIENT IDENTITY VERIFICATION, FR TECHNOLOGY CAN CLOSE THE SECURITY INDUSTRY’S LABOR GAP.

> USING SURVEILLANCE VIDEO IN CONJUNCTION WITH FR APPLICATIONS – WHERE INDIVIDUALS HAVE NOT AGREED TO SHARE THEIR BIOMETRIC DATA – IS QUITE DIFFERENT THAN DEPLOYING BIOMETRIC IDENTITY SOLUTIONS IN ACCESS CONTROL ENVIRONMENTS.

crimes based on mistaken FR matches.

But using surveillance video in conjunction with FR applications – where individuals have *not* agreed to share their biometric data – is quite different than deploying biometric identity solutions in access control environments. The many state laws restricting the technology's use do not pertain to the ways that the security industry leverages it for worker/visitor/resident/traveler/guest/you-name-it screening purposes.

FR access control relies on "cooperative subjects." Individuals agree to enroll in programs that use their faces to enter a workplace, visit a hospital, board a plane, use a hotel elevator, or gain access to some other restricted area. They "cooperate" by submitting



to a benchmark reading (ideally, a digitized, 3D "mug shot" encrypted with proprietary algorithms), then, when seeking entry to a location, look at an FR-enabled camera to provide a match. Under these conditions, error rates of the best FR solutions are near zero. Furthermore, the top 20 algorithms accurately identify black faces equally as well as white faces.

Much of the bad rap associated with FR comes from applications that use "non-cooperative" subjects. These are individuals whose faces have been captured surreptitiously by surveillance cameras, often in less-than-ideal lighting and from an awkward angle. A 2020 study of a top FR vendor found that its system's error rates jumped from 0.1 percent when matching faces to a high-quality headshot to 9.3 percent when comparing them to surveillance video in which the subject was not looking directly at the camera or was obscured by shadows – a nearly 100-fold difference. As the security industry expands the use of FR solutions in access control applications, it needs to educate the public on this vital distinction.

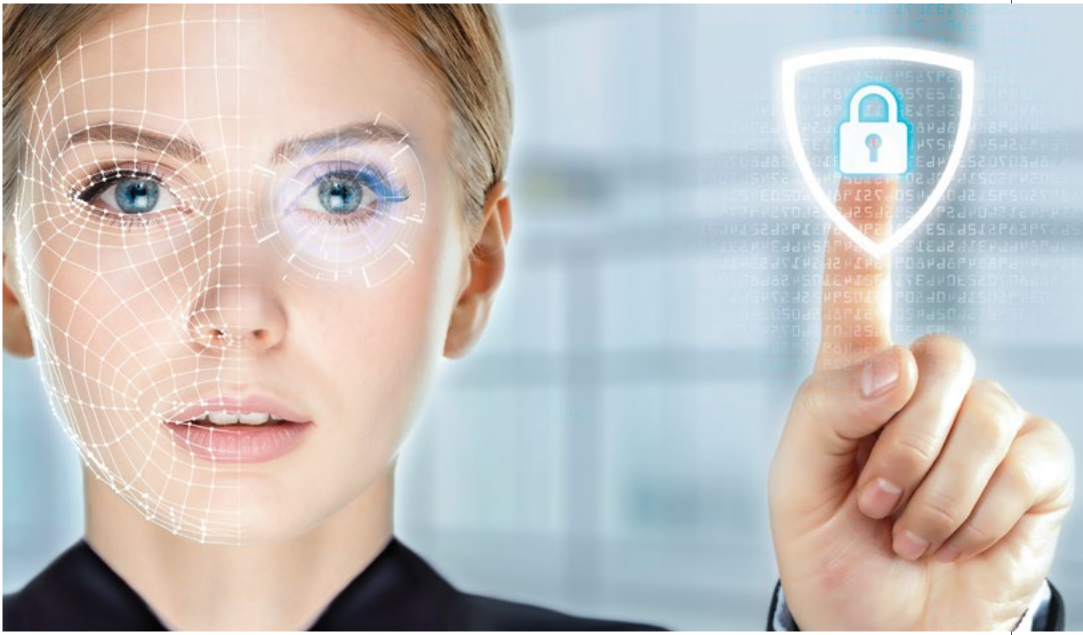
Convenience will also play a role in adoption.

In 2015, the global market for FR solutions was $2.3 billion. In 2021, that number had more than doubled to $5.1 billion. By 2028, it is projected to more than double again to $12.67 billion.

WHEN PEOPLE WAITING IN LONG LINES TO INTERACT WITH AN OVERWORKED SECURITY OFFICER SEE OTHERS WHIZZING BY, BARELY PAUSING TO VERIFY THEIR IDENTITY AT A BIOMETRICS-ENABLED CAMERA, MANY WILL LIKELY BE PERSUADED.

Companies hoping to win public acceptance should make participation in FR systems optional. When people waiting in long lines to interact with an overworked security officer see others whizzing by, barely pausing to verify their identity at a biometrics-enabled camera, many will likely be persuaded.

Finally, the public needs to feel confident that, when enrolling in FR systems, their biometric data will be used only for the designated applications. The European Union is already taking an aggressive stance in establishing oversight. Its proposed "AI Act" will restrict the use of biometric recognition systems to networks in



which participants have expressly agreed to share their data. Furthermore, biometrics cannot be used to profile users, such as scoring trustworthiness or predicting the potential for criminality. While the AI Act is an EU initiative, there will undoubtedly be a spillover effect beyond member countries, just as has occurred with the union's General Data Protection Regulation (GDPR).

The AI Act does permit matching a consenting individual's face to a stored, encrypted record to verify identity and grant access through a point-of-entry. There is no ethical ambiguity for such applications. Acceptance will come by informing the public about how opt-in FR systems work, winning them over with attendant conveniences, and creating sufficient oversight mechanisms to ensure proper system use. ◀

> THE PUBLIC NEEDS TO FEEL CONFIDENT THAT, WHEN ENROLLING IN FR SYSTEMS, THEIR BIOMETRIC DATA WILL BE USED ONLY FOR THE DESIGNATED APPLICATIONS.

Using Crowdsourcing to Secure Events

Deployment of a reporting app can vastly increase situational awareness, responsiveness

Sheryl Pinckney-Maas (spmaas@guardianzone.com), is the CEO of Guardian Zone (www.guardianzone.com).

NOW THAT THE EVENT INDUSTRY HAS REBOUNDED FROM THE COVID-RELATED DOWNTURN, THE LANDSCAPE OF IN-PERSON EVENTS HAS CHANGED SIGNIFICANTLY. Festivals, sporting events, concerts, exhibitions and conferences all look and feel much different than they did before the pandemic. Not to mention, horrific instances of mass violence have become all too familiar. With all of this in mind, it is vital that event security teams take advantage of every available tool to keep attendees safe.

WHAT 'SAFETY' MEANS TO EVENT ATTENDEES

Potential threats related to attending large events are not limited to gun violence. Fights, thefts, alcohol and drug abuse, crowd surges, sexual assault, and medical emergencies remain persistent problems for sports arenas, concert

At the end of 2022, the number of mobile phones in use around the world was 7.26 billion in a global population of 8 billion.

venues and convention centers alike.

Implementing security measures to keep event attendees safe must follow a holistic approach. If security personnel do not have the ability to communicate directly with fans in real time, they will most likely be unable to intervene and stop an incident in a timely manner.

THE SHORTCOMINGS OF TRADITIONAL SECURITY TECHNOLOGY

Many venues still suffer from fundamental problems related to limited security staff and uncoordinated crisis response. For example, facilities that deploy surveillance cameras as a standalone solution might still find themselves unprepared to address events quickly, as not all surveillance systems are continuously manned. Regardless of the number of cameras a venue deploys, if personnel lack the ability to verify reports, communicate with attendees and disseminate mass alerts, security will remain underequipped.

To address emergencies

in real time, it is critical that venues integrate crowdsourced intelligence software that gives patrons the ability to share information directly with security personnel so that they can then assemble a complete picture of an incident. Venues must also adopt evidence-based practices, which means taking advantage of available data and research findings to help make informed decisions on resource allocation.

Integrating real-time, two-way communication capabilities between security staff and event attendees acts as a force multiplier without requiring additional personnel. Individuals attending conferences, festivals or games simply download a free, easy-to-use app through which they can provide critical intelligence.

> TO ADDRESS EMERGENCIES IN REAL TIME, IT IS CRITICAL THAT VENUES INTEGRATE CROWDSOURCED INTELLIGENCE SOFTWARE THAT GIVES PATRONS THE ABILITY TO SHARE INFORMATION DIRECTLY WITH SECURITY PERSONNEL.

they often lack – resources.

In addition, because crowdsourced intelligence platforms rely on cloud-based software, integrating them into existing security systems does not require a major overhaul. For event security accustomed to operating on traditional systems, folding crowdsourced intelligence into an emergency operations plan better equips them to do their jobs without forcing them to learn an entirely new system.

With a crowdsourced intelligence platform, event staff can tailor security to their needs using agnostic,

INTEGRATING REAL-TIME, TWO-WAY COMMUNICATION CAPABILITIES BETWEEN SECURITY STAFF AND EVENT ATTENDEES ACTS AS A FORCE MULTIPLIER WITHOUT REQUIRING ADDITIONAL PERSONNEL.

THE BENEFITS OF CLOUD-BASED, GEOFENCED, CROWDSOURCED INTELLIGENCE

Using crowdsourced intelligence takes the guesswork out of keeping individuals safe, putting power in the hands of the people who need it most and equipping security personnel with something

customizable geofencing technology to extend their perimeter into surrounding parking lots and neighborhoods, not only broadening a security team's footprint, but also protecting patrons well before they arrive. It is a tool that offers peace of mind to community members and fans alike.

KEY TAKEAWAYS

Much like how navigation apps crowdsource traffic information, event security can leverage critical information from thousands of attendees. Equipped with a cloud-based platform built on insights from evidence-based research, venue personnel can enhance their responsiveness and effectiveness by putting tools in the hands of every spectator and showing them that their safety and security is a top priority. ◀

> FOR EVENT SECURITY ACCUSTOMED TO OPERATING ON TRADITIONAL SYSTEMS, FOLDING CROWDSOURCED INTELLIGENCE INTO AN EMERGENCY OPERATIONS PLAN BETTER EQUIPS THEM TO DO THEIR JOBS WITHOUT FORCING THEM TO LEARN AN ENTIRELY NEW SYSTEM.

Delivering Data to Enhance Situational Awareness

Visualization solutions can enable better and faster decision making

CRITICAL DECISION MAKING REQUIRES ACCESS TO INFORMATION. Organizations rely on data visualization to present a common operating picture for more efficient assessment, faster analysis, and improved responses. It can also play an essential role in enhancing surveillance systems that use cameras, as they generate large amounts of data that can be difficult to analyze manually.

Data visualization has evolved considerably since its beginnings. Early systems were as simple as line graphs and bar charts that were primarily used to display statistics to help people understand complex numerical data. The advent of the Internet led to a proliferation of data visualization tools and the development of interactive and

Courtney Mamuscia (courtney@rgb.com) is the marketing director for RGB Spectrum (www.rgb.com).

real-time visualizations.

One of the major developments in recent years has been the introduction of interactive and dynamic visualizations, allowing users to explore data in real time and gain insights that were previously difficult or even impossible to realize through traditional static charts and graphs.

Another key development has been the integration of machine learning and artificial intelligence into data visualization tools, which allows users to generate predictive models and perform advanced data analytics.

There are numerous benefits to seeing a comprehensive view of operations through modern data visualization tools. Organizations can make better decisions when they have a more complete and more accurate picture of their operations. By presenting data in an easy-to-understand format, modern visualization tools allow decision-makers to identify patterns, trends and anomalies that might have otherwise gone unnoticed.

> THE INTEGRATION OF MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE INTO DATA VISUALIZATION TOOLS ALLOWS USERS TO GENERATE PREDICTIVE MODELS AND PERFORM ADVANCED DATA ANALYTICS.

LEVERAGING DATA TO IMPROVE OPERATIONS

Data visualization tools can help organizations improve operational efficiencies by identifying bottlenecks, inefficiencies and potential areas for improvement. For example, a manufacturing plant might use data visualization to track its production process and identify where delays occur, allowing for adjustments and increased productivity.

Current data visualization tools communicate complex ideas and information to a broad audience using a visually appealing format and delivering a comprehensive view of operations. They allow organizations of all sizes to share insights with stakeholders and customers in an informative way, increasing engagement and enabling decision-makers to quickly comprehend situations.

Visual quality, 24/7 reliability, intuitive user interfaces, and good workspace ergonomics all play a part in ensuring that crucial data is available and readily actionable. A key

> “ BY PRESENTING DATA IN AN EASY-TO-UNDERSTAND FORMAT, MODERN VISUALIZATION TOOLS ALLOW DECISION-MAKERS TO IDENTIFY PATTERNS, TRENDS AND ANOMALIES THAT MIGHT HAVE OTHERWISE GONE UNNOTICED.

component of visualization for monitoring and collaborating across an enterprise is the use of video walls, which are found extensively in public safety, commercial enterprises, defense, energy, transportation, education, infrastructure, and military applications. Typical installations include such sites as control rooms, command centers, process control systems, security operations centers, traffic management centers, and emergency operations centers.

Effective visualization solutions combine data from various sources, reliably and securely disseminating mission-critical information to multiple destinations across an enterprise and between organizations, from a video wall in a control room to a computer monitor across a campus or a cellphone anywhere in the world.

There should be a modular network of decision support components and systems, such as an AV-over-IP platform that excels even in bandwidth-constrained environments, KVM-over-IP, recorders, desktop multi-viewers, and video wall processors to meet any requirement.

Finally, simpler, unified control can be achieved by consolidating multiple keyboards and mice into a single keyboard and mouse for all applications. This results in improved operational efficiency, streamlined workflow, and reduced operator fatigue. ◀

“

EFFECTIVE VISUALIZATION SOLUTIONS COMBINE DATA FROM VARIOUS SOURCES, RELIABLY AND SECURELY DISSEMINATING MISSION-CRITICAL INFORMATION TO MULTIPLE DESTINATIONS ACROSS AN ENTERPRISE AND BETWEEN ORGANIZATIONS.

More Light Equals Improved Analytics

License plate recognition benefits from external illumination

INVENTED IN 1976 AT THE POLICE SCIENTIFIC DEVELOPMENT BRANCH IN BRITAIN, AUTOMATED LICENSE PLATE RECOGNITION (ALPR) represents one of the first applications of artificial intelligence (AI) and machine learning. At the most basic level, ALPR systems capture an image of a vehicle's license plate and transform the picture into alphanumeric characters using optical character recognition.

Eddie Reynolds (eddier@ilunimarinc.com) is the CEO of iluminar (www.iluminarinc.com).

THE APPLICATIONS OF ALPR TECHNOLOGY

Around the world, police departments use ALPR systems to compare detected plate numbers to databases of vehicles of interest. Departments of transportation also use ALPR systems for electronic toll collection and as a method of tracking the ebb and flow of traffic.

In the past decade, with developments in AI, machine learning, surveillance cameras, and related innovations, ALPR systems have progressed. For example, many ALPR systems today use infrared (IR) lighting to enable a camera to perform at any time of day or night. Algorithms used to identify a license plate have also become more complex, which has helped to make ALPR systems more accurate.

And yet, even as these technology components have evolved, many ALPR

> USING EXTERNAL ILLUMINATION SOURCES – ESPECIALLY IR ILLUMINATORS – TO REBALANCE LIGHTING IN VIDEO IMAGES NOT ONLY IMPROVES DETECTION ACCURACY BUT ALSO ENSURES THAT AN ALPR SYSTEM CAN OPERATE AROUND THE CLOCK.

operators today face the same issues they did in the late-1970s, including object misidentification and high error rates. The good news is that these problems are solvable.

SIMPLE PROBLEMS CALL FOR SIMPLE SOLUTIONS

There are generally three common roadblocks to successful ALPR software performance:

- Blurry images, particularly as a result of motion blur
- Poor image resolution when a plate is too far away from a camera
- Poor lighting and low contrast because of ambient light, glare, and/or harsh environmental conditions

Surprisingly, the solution to these problems is relatively simple. Using external illumination sources – especially IR illuminators – to rebalance lighting in video images not only improves detection accuracy but

Many countries now use license plates that are retroreflective, which means they are designed to reflect light back to its source, thereby improving the contrast of an image. In some countries, the *characters* on a plate are designed *not* to be reflective, providing an even higher level of contrast.

also ensures that an ALPR system can operate around the clock.

THE MAGIC OF EXTERNAL ILLUMINATION

Most issues that ALPR software encounters come down to the cameras being deployed. For systems that produce blurred images at dawn, at dusk or during hours of darkness, for example, the problem is often the result of a camera automatically slowing its shutter speed in order to capture more light. For static or slow-moving objects, such as parked cars or sluggish traffic, a slower shutter speed does not create any problems. When a car drives past that same camera at high speed, however, a slower shutter speed will produce an image that is too blurry to read. In this scenario, integrating external

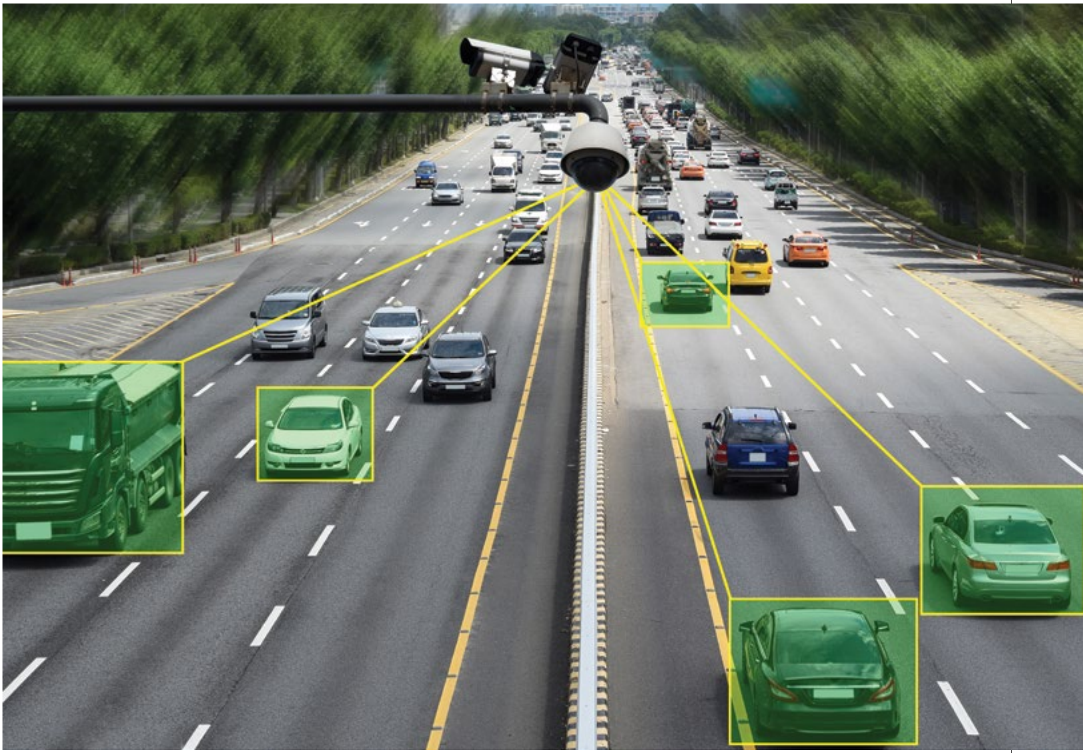
> ACROSS APPLICATIONS, BETTER ILLUMINATION HAS BEEN PROVEN TO EXTEND THE DETECTION RANGE OF MANY VIDEO ANALYTICS.

illumination is an effective and quick fix.

The situation is similar for systems that struggle to detect license plates at longer distances. Across applications, better illumination has been proven to extend the detection range of many video analytics. The science is simple: If an area is properly illuminated, a camera will produce higher contrast images, making it easier for analytics to differentiate between multiple objects in frame. This equally applies to letters and numbers on a license plate.

IMPORTANT INSTALLATION CONSIDERATIONS

Successful deployment of an external illumination device alongside cameras in an ALPR application depends on several factors. For systems using a dedicated ALPR camera, for example, it is often useful to deploy external illuminators to supplement onboard illumination sources, especially to address problems related to

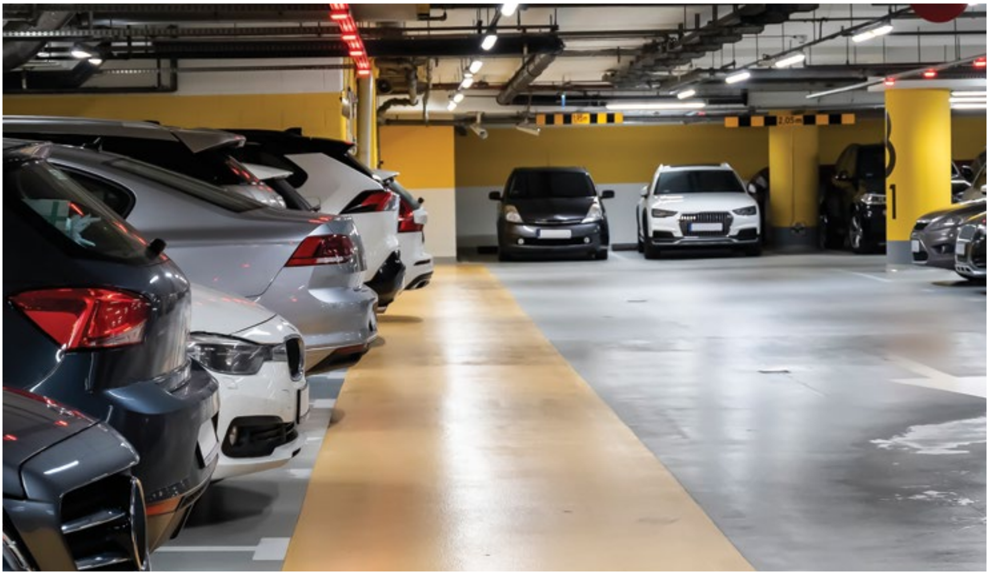


long-range detection and motion blur.

For ALPR applications involving cameras that are also being used for other purposes, such as perimeter intrusion detection, integrating a white light illuminator can improve both intrusion detection and license plate recognition performance. For cameras installed at a significant height in order to avoid obstructions, integrating IR illuminators can provide greater visibility over longer distances than visible light. IR light is also invisible to the naked eye, which may be preferable in some security applications.

Regardless of the specific requirements of a given application, there is an external illuminator purpose-built to meet every need. ◀

> FOR CAMERAS INSTALLED AT A SIGNIFICANT HEIGHT IN ORDER TO AVOID OBSTRUCTIONS, INTEGRATING IR ILLUMINATORS CAN PROVIDE GREATER VISIBILITY OVER LONGER DISTANCES THAN VISIBLE LIGHT.



Making Parking Lots Smarter – and More Secure

Artificial intelligence solutions promote a better, safer customer experience

PARKING LOTS AND GARAGES ARE THE THIRD MOST CRIME-PRONE AREAS IN THE COUNTRY, according to the U.S. Department of Justice. More than one out of every 10 property crimes occurs in these areas, totaling about 1,400 incidents *every day*. Property owners, city officials and campus administrators have a responsibility to keep people and cars safe. A parking area that gains a reputation as a place where violent crime occurs or where parked cars are regularly burgled or damaged will quickly become a place that people avoid.

PARKING LOT SECURITY CHALLENGES

Parking facilities in city centers and on college campuses are vital to attracting customers and students. These facilities offer a necessary service; however, they often have limited security with poor lighting, and are ill-designed with many blind spots.

Harry Yang (hyang@meritlilin.us) is the general manager of Lilin Americas (meritlilin.us).

In addition, many parking lots have poorly maintained shrubbery that can provide cover for potential criminal activity. The major challenge for parking lots, especially large ones, is keeping cars and people visible. Criminals who target parking facilities are usually opportunists looking for an easy target – one that is away from witnesses and security guards – so they go to parking lots that lack security measures.

Security systems in campus and city parking lots provide a variety of benefits. First, they help protect vehicles, deter theft, and offer a sense of safety and security for customers. The systems can also be used to monitor and control access to the lots.

> “ CRIMINALS WHO TARGET PARKING FACILITIES ARE USUALLY OPPORTUNISTS LOOKING FOR AN EASY TARGET – ONE THAT IS AWAY FROM WITNESSES AND SECURITY GUARDS – SO THEY GO TO PARKING LOTS THAT LACK SECURITY MEASURES.

Solutions range from simple cameras to more sophisticated

> TODAY'S SMART IP CAMERAS WITH ONBOARD AI DELIVER ADVANCED ANALYTIC ALGORITHMS AT THE EDGE, DECREASING REACTION TIME AND IMPROVING SECURITY.

deployments, including motion detectors, access control, and the latest analytics using artificial intelligence (AI). A few of the more popular options are examined below.

Traditional Surveillance Cameras

Surveillance cameras are the most common type of security system used in campus and city parking lots. These cameras provide a visual deterrent to potential criminals, enable monitoring of parking lot activity, and provide evidence for law enforcement if a crime is committed.

One difficulty with cameras in parking facilities is the sheer size of the area that must be monitored. Parking garages often have multiple levels, and stadium-sized parking areas are vast; covering the entire area would take numerous cameras, driving up costs. A solution to this is to use wide-angle and fisheye lens cameras to monitor large areas with the fewest number of devices, which also saves money on cabling and licenses.

Smart IP Cameras

Smart IP video surveillance cameras offer a decided advantage over traditional cameras, which provide only basic analytics. Today's smart IP cameras with onboard AI deliver advanced analytic algorithms at the edge, decreasing reaction time and improving security. A few examples of AI functions include:

- License plate recognition (LPR): This analytic detects and reads license plates, which can allow entry to a parking lot and enable operators to track the time a vehicle remained in the facility.
- Vehicle/people counting: This analytic counts the number of vehicles and people entering and exiting a parking facility. It can analyze the capacity of a facility and provide statistics to traffic flow management systems.
- Vehicle identification: This analytic detects and records the type of vehicle (bicycle, motorcycle, car, bus, etc.) and its description. Such information is useful for identifying

> AI-DRIVEN CAMERAS CAN ANALYZE ENORMOUS AMOUNTS OF DATA, MAKE DECISIONS ABOUT THREAT LEVELS, AND RESPOND TO THINGS THAT, IN THE PAST, WOULD HAVE REQUIRED HUMAN INTELLIGENCE.

vehicles that are in violation of parking lot regulations and assisting law enforcement officials investigating vandalism or theft.

Access Control Systems

An access control system allows only authorized personnel to enter the lot. This gatekeeping reduces the risk of crime and can be used to prevent cars from outnumbering available spaces. Many access control systems easily integrate with traditional or smart IP surveillance cameras, offering single-pane-of-glass functionality for control centers or guard stations.

Access control systems, however, can be costly to install and typically require badges or credentials, which, all too often, are lost or stolen.

Lighting

Proper lighting deters criminals by making it more difficult for them to hide or operate in darkness, thus providing

a safer environment for drivers and pedestrians. Additionally, lighting can improve security by making it easier for law enforcement officers to identify suspects or witnesses who are captured on video when a crime is committed.

Alarm Systems

Alarm systems alert authorities when an unauthorized person attempts to enter the lot. They can also use motion sensors that detect any suspicious activity within a given area. As with access control systems, alarm systems easily integrate with surveillance cameras to offer a complete record of incidents.

ARTIFICIAL INTELLIGENCE OPENS THE DOOR TO IMPROVED SECURITY

State-of-the-art video cameras are equipped with the latest in AI software. Today's AI-driven cameras can analyze enormous amounts of data, make decisions about threat levels, and respond to things that, in the past, would have required human intelligence. Recently, smart IP cameras with onboard AI have hit the market, and they offer a distinct advantage over traditional cameras that require a dedicated server to perform AI functions. AI edge devices reduce latency – the time it takes for data transfer – which enables quicker responses.

Perimeter defense cameras using AI analytics can create a virtual fenceline around a parking lot. These cameras can recognize the difference between a false alarm, such as a stray cat, and a real threat, such as a human prowling in an area where they should not be.

The latest cameras can also detect objects left behind, track traffic levels, spot cars that have been in the lot for an extended period of time, and use facial recognition technology to identify people who have been flagged as potential threats.

Where appropriate, a camera can automatically initiate responses, such as turning on a spotlight, playing a loud recording telling a person that he or she is trespassing and authorities are being notified, and alerting a guard at a security hub.

AI-enabled cameras also offer video categorization features that enable easy and quick searches for specific footage.

ENHANCING SATISFACTION

In addition to security, AI can provide automated

customer service in parking lots. AI-enabled chatbots can answer customer questions about parking availability and fees, point customers to available spaces, and even offer directions to nearby businesses or attractions. One useful solution combines vehicle detection and counting algorithms with LED signage for parking guidance. This powerful system alerts drivers to the number of available parking spaces in a given area.

All of this makes it easier for customers to find what they need quickly and easily while reducing the need for onsite staff. As AI continues to develop, it will become increasingly important for businesses, city planners, and campus administrators to use this cutting-edge technology to enhance their security measures. ◀

> AI-ENABLED CHATBOTS CAN ANSWER CUSTOMER QUESTIONS ABOUT PARKING AVAILABILITY AND FEES, POINT CUSTOMERS TO AVAILABLE SPACES, AND EVEN OFFER DIRECTIONS TO NEARBY BUSINESSES OR ATTRACTIONS.

Mitigating Risk and Enhancing Productivity with AI Technology

Software can relieve workers of an increasing number of tasks

Dr. Daniël Reichman (danielr@ai-rgus.com) is the CEO and chief scientist of Ai-RGUS (www.ai-rgus.com).

ARTIFICIAL INTELLIGENCE (AI) IS BECOMING INCREASINGLY PREVALENT IN DAILY LIVES. Unlocking a phone with facial recognition, using voice assistants such as Siri or Alexa, traveling in self-driving cars, and relying on fraud detection algorithms are examples of people using AI without necessarily recognizing it as such.

AI is being implemented all over the world across many industries to advance other technologies. Enhancing worker safety, ensuring compliance with regulations, and saving time and money are a few of the ways the technology can help to reduce risk and benefit organizations.

AI FOR WORKER SAFETY AND WORKERS' COMPENSATION

> THE TECHNOLOGY CAN ANALYZE VIDEO CAMERA STREAMS ON A MANUFACTURING FLOOR TO IDENTIFY SAFETY VIOLATIONS, SUCH AS THE MISHANDLING OF EQUIPMENT OR OTHER HAZARDOUS CONDITIONS.

AI can be used to improve worker safety by detecting hazardous conditions in the context of non-human physical danger. The technology can analyze video camera streams on a manufacturing floor to identify safety violations, such as the mishandling of equipment or other hazardous conditions. For example, AI can spot loose electrical wires, open fires, smoke, liquid spills, messy conditions, workers entering restricted areas, or even workers not wearing protective equipment like hardhats and safety vests.

The use of AI to monitor camera feeds, meanwhile, can be helpful for determining how situations arose. It can also provide real-time notifications of safety concerns.

With regard to safety in the context of human contact and personal violence, AI can help by identifying guns, weapons, crowding and loitering, and can aid in investigations by showing how an unauthorized person gained access to a building.

AI can further be used to summarize video content. In many of the above situations, the story evolves over an extended period of time covering multiple camera views. AI can analyze video streams and pick out the specific segments of interest, greatly reducing the amount of time it would otherwise take to comb through many hours of video recordings.

The technology can help in similar ways in workers' compensation cases, by providing visual documentation of accidents and other incidents. However, if a company's security cameras are not properly managed or are not recording optimally, this diminishes the chances

that they will be beneficial. Installing AI software to monitor for blurriness or obstructions is an effective way to address this issue. Deploying cameras that can be easily maintained and monitored through such use of AI is an easy way to reduce the likelihood of major problems and the resulting financial and reputational damage to an organization.

AI FOR COMPLIANCE

The first required step to compliance is setting up a system to meet the rules. The second step is constantly monitoring that everyone in the organization is following those rules, avoiding all deviations, both accidental and intentional. AI can remove the burden of having multiple people trying to supervise every situation throughout

> DEPLOYING CAMERAS THAT CAN BE EASILY MAINTAINED AND MONITORED THROUGH SUCH USE OF AI IS AN EASY WAY TO REDUCE THE LIKELIHOOD OF MAJOR PROBLEMS AND THE RESULTING FINANCIAL AND REPUTATIONAL DAMAGE TO AN ORGANIZATION.

the workday. Getting too close to heavy equipment, dumping waste where it is not allowed, and theft are just some of the situations in which AI can assist with detecting and assessing the situation. This allows workers to focus on other duties.

Compliance regulations and laws vary across industries and states. College campuses, prisons, cruise ships, gun stores, marijuana dispensaries, and liquor stores are all regulated differently, and AI is adapting to keep organizations compliant.

AI FOR TIME AND MONEY SAVINGS

AI software helps to make tasks more efficient and reduce the risk of human error. It can also identify areas of inefficiency, which can reduce costs.

New tools and programs such as cybersecurity, data management and AI software are all ways to boost productivity and save time that businesses can use on product development. These new technologies enable organizations to operate at a higher level than before.

For example, when sorting through video content for a specific incident, AI can highlight where and when to look for evidence. Allowing AI to take over repetitive tasks reduces the amount of time an employee has to spend on mundane projects, giving them the opportunity to focus on more productive activities.

LOOKING TOWARD AN AI-FOCUSED FUTURE

AI can be used in several ways, such as monitoring for worker safety, meeting compliance requirements, and saving time and money to improve productivity. As new technology and software become available, AI will be integrated into many new advancements.

Taking charge and implementing AI software into everyday life will help companies stay ahead of the competition. It will also help to mitigate risk and make the business more efficient. ◀

> AI SOFTWARE HELPS TO MAKE TASKS MORE EFFICIENT AND REDUCE THE RISK OF HUMAN ERROR. IT CAN ALSO IDENTIFY AREAS OF INEFFICIENCY, WHICH CAN REDUCE COSTS.

FICAM Revisions Enable New Security Solutions in Government Sector

Face biometrics now equivalent to fingerprints under FIPS standards

David Smith (david.smith@identityone.net) is the CEO of Identity One (www.identityone.net).

FOR GOVERNMENT FACILITIES AND CIVILIAN ORGANIZATIONS ALIKE, ESTABLISHING AN EFFECTIVE PHYSICAL ACCESS CONTROL SYSTEM (PACS) is a top priority. Given the sensitive nature of the resources and information contained within many U.S. government facilities, though, designing a PACS that complies with the latest updates to Federal Information Processing Standards (FIPS) 201-3 is of vital importance.

THE IMPORTANCE OF FICAM-APPROVED TECHNOLOGY

Nearly all applications that deal with financial, privacy, safety or defense deploy some form of identity authorization systems at their entry points. In the government space, the Federal

Identity, Credential and Access Management (FICAM) architecture establishes standards that determine the allowed activities of legitimate users and mediate every attempt by a user to access a resource in the system.

The latest revisions to FIPS 201 lay the foundation for PACS to incorporate recent advances in both biometric recognition technology and derived credentials to ensure that new and existing FICAM deployments can take advantage of these developments. This third revision to the standard—FIPS 201-3—makes the best PKI-based high assurance access control and biometric identity technology available to federal government facilities by codification.

> THE LATEST REVISIONS TO FIPS 201 LAY THE FOUNDATION FOR PACS TO INCORPORATE RECENT ADVANCES IN BOTH BIOMETRIC RECOGNITION TECHNOLOGY AND DERIVED CREDENTIALS.

IMPORTANT CHANGES INCLUDED IN FIPS 201-3

Published in January 2022, revision 3 of FIPS 201 introduces several important changes to FICAM's common set of

> THE ELEVATION OF FACIAL RECOGNITION TECHNOLOGY FOR IDENTITY VERIFICATION MEANS THAT THE MOST ADVANCED CONTACTLESS BIOMETRICS TECHNOLOGIES ARE NOW SUPPORTED FOR SYSTEMS THAT USE COMMON ACCESS CARDS, PIV, AND TRANSPORTATION WORKER IDENTIFICATION CREDENTIALS.

standards, best practices, and implementation guidance for federal agencies. Included among them is the elevation of face biometrics to be equivalent to fingerprint biometrics for the highest assurance level, in addition to a further definition of derived personal identity verification (PIV) credentials and their appropriate use cases.

PIV credentials, as defined by FIPS 201, are secure and reliable forms of identity credentials issued by the federal government to its employees and contractors. Their purpose is to authenticate both the identity of the person and the authenticity of their credential for access to federally controlled facilities, information systems, and applications. As part of an industry-wide push to adapt to touchless technology in the aftermath of COVID-19, the elevation of facial recognition technology for identity verification means that the most advanced contactless biometrics technologies are now supported for systems that use common access cards (CAC), PIV, and transportation worker identification credentials (TWIC).

Another significant change involves the use of derived credentials, including the potential for PIV-derived credentials to be loaded onto phones for logical, physical and mobile access control for CAC, PIV and TWIC-based security solutions. As the use of

these methods of identity authentication continues, so will the relevance of FIPS 201 in an increasingly digital world.

FIPS 201-3 specifically allows the use of the face image from the PIV applet on the PIV card to be used. However, this image is typically small, low quality, and lacks special data elements – such as infrared and 3D – that make modern face biometrics work.

The combination of the approval of face biometrics for high assurance levels and face biometrics with infrared and 3D elements being categorized as derived credentials results in the potential for a fully FIPS 201 FICAM-compliant system that performs to the same level as the latest face biometrics technologies.

To streamline access control for government facilities, integrators should prioritize integrating both hardware and software that incorporate the latest updates to FIPS 201 and are designed for frictionless access. ◀

> “
>
> ANOTHER SIGNIFICANT CHANGE INVOLVES THE USE OF DERIVED CREDENTIALS, INCLUDING THE POTENTIAL FOR PIV-DERIVED CREDENTIALS TO BE LOADED ONTO PHONES FOR LOGICAL, PHYSICAL AND MOBILE ACCESS CONTROL FOR CAC, PIV AND TWIC-BASED SECURITY SOLUTIONS.

Boosting the Return on Security Investment

Thermal cameras can enhance both situational awareness and operational efficiency

SINCE THE DAYS OF ANALOG VIDEO, COMPANIES USING BOTH VISIBLE AND THERMAL SENSORS to improve situational awareness at their facilities have focused primarily on surveillance. By leveraging sensors positioned at areas of interest, a single person could monitor multiple sites. Today, the concept has not changed, but the technology has evolved, and sensors have become more intelligent.

Now, sensors can not only enhance surveillance, they can also improve internal operations for specific, condition-based maintenance applications as well. Facilities are able to leverage a variety of fixed sensors to improve overall awareness, from surveillance to asset management, condition monitoring, and beyond.

Matt Strautman (matt.strautman@teledyne.com) is the director of global business development for Teledyne FLIR (www.flir.com).

SENSORS FOR SECURITY

BECAUSE PEOPLE AND VEHICLES CANNOT HIDE FROM THE HEAT THEY PRODUCE, INTEGRATING THERMAL CAMERAS INTO EXISTING SECURITY SYSTEMS IS A GREAT WAY TO EXPAND SITUATIONAL AWARENESS.

Perimeter protection and general outdoor surveillance is a great application to highlight the advanced functionality of sensor technology. When laying out a design for exterior cameras, integrators are often faced with multiple challenges that range from inadequate lighting to lack of infrastructure to unexpected environmental conditions. Traditionally, a customer would have to settle for what a visible camera could see from available vantage points. Today, however, they can layer technologies to better understand what is happening around a property.

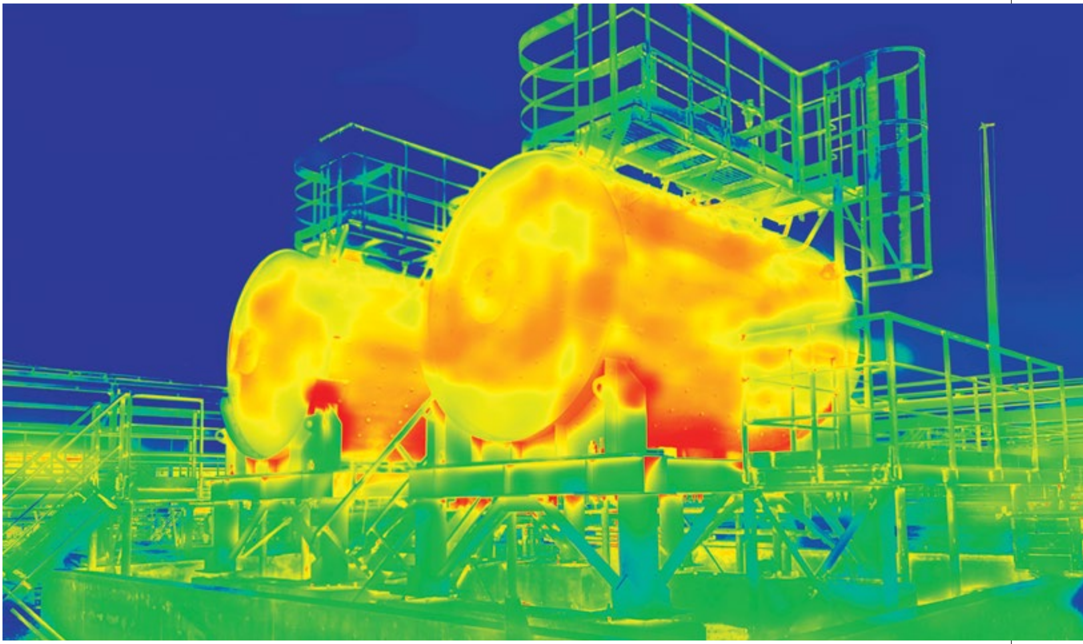
Unlike visible cameras, thermal cameras measure minute variations in

temperature. Because people and vehicles cannot hide from the heat they produce, integrating thermal cameras into existing security systems is a great way to expand situational awareness.

For even more coverage, pairing a ground-based radar with a pan-tilt-zoom camera enables the radar to communicate with the PTZ when an object of interest is detected. The camera can then automatically slew to and track the object. Coupled with onboard analytics for security applications, these devices can act as a first line of defense that is able to identify a human up to a half-mile away in stable conditions. For long fence lines and wide area monitoring, this capability delivers better coverage and more consistent performance using fewer cameras.

SENSORS FOR MAINTENANCE

Looking beyond security, many organizations are exploring ways to use fixed sensors to improve operational efficiencies. The application will vary by industry, but, in a general sense, customers are looking to fixed radiometric cameras to analyze temperature data. For example, many industries are adopting this technology to provide early fire detection for bulk storage materials and during lithium-ion battery production. If a camera senses a sudden rise in temperature, it can immediately alert an operator. Customers are also using these sensors to analyze temperature patterns



as a way to address potential mechanical/electrical failures, improve manufacturing processes, and prevent general maintenance issues from negatively affecting uptime.

SINGLE-PANE-OF-GLASS STRATEGY

Bringing both threat intelligence (external and internal) and log/sensor data (internal) applications together under a single architecture represents the "single-pane-of-glass" strategy, which makes it possible for security and operations professionals to access everything in one place. Many organizations recognize the unique capabilities of these kinds of systems to strengthen the collection and management of data, which allows teams to instantly collaborate and decide on the best course of action for high-priority alerts.

> PAIRING A GROUND-BASED RADAR WITH A PAN-TILT-ZOOM CAMERA ENABLES THE RADAR TO COMMUNICATE WITH THE PTZ WHEN AN OBJECT OF INTEREST IS DETECTED. THE CAMERA CAN THEN AUTOMATICALLY SLEW TO AND TRACK THE OBJECT.

CUSTOMERS ARE ALSO USING THESE SENSORS TO ANALYZE TEMPERATURE PATTERNS AS A WAY TO ADDRESS POTENTIAL MECHANICAL/ ELECTRICAL FAILURES, IMPROVE MANUFACTURING PROCESSES, AND PREVENT GENERAL MAINTENANCE ISSUES FROM NEGATIVELY AFFECTING UPTIME.

Because thermal and visible sensors are already a trusted technology in security and condition-based maintenance applications, they have proven to be an integral part of this shift to seamless data management. As more organizations successfully merge the systems into one, the value of and need for these sensors will only grow.

It should come as no surprise that the same technology that provides security personnel with situational awareness around the clock is also useful for non-security purposes. The key opportunity for integrators is the potential integration of operations and security applications. Bringing these systems together under a single unified alarm system not only saves end users money, it also creates multiple business opportunities across functions. ◀

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