



# TECHNOLOGY Insights

Fall 2024

Volume 12, Number 2



## The Artificial Intelligence Edition

8 experts examine applications, training, challenges and much more



### Active Listening

Emerging tech requires empathizing with clients



Page 22

### My AI Generation

Gen-AI is powerful, but caution is warranted



Page 44

### Watch Your Language

LLM platforms have both risk and potential



Page 58

# Protect

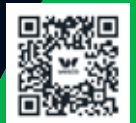
## *Your Partner in Security*

When it comes to protecting your people and property, you need a world-class partner. You can rely on Wesco's specialized teams and our integrator partners to support, consult, design and deliver customized solutions that solve your most important security challenges.

**We build, connect, power  
and protect the world.**



Wesco.com





# TECHNOLOGY Insights

Fall 2024

Volume 12, Number 2



## 2

### The Potential of Generative AI to Revolutionize Physical Security

Solutions are not just hype; they can reduce risk and improve productivity  
Jim Black, Microsoft



## 12

### Context is Key – For Both People and AI

Multimodal systems can make the leap from identifying to understanding  
Jonathan Wender, Ph.D., Polis Solutions



## 22

### Meeting the Full Spectrum of Customer Needs

Careful listening can solidify relationships and create opportunities  
Matt Powers, Wesco



## 30

### Considerations in AI Training and Deployment

Starting with the right implementation plan is vital to success  
Niru Satgunananthan, Johnson Controls



## 38

### The Future of Utilities Security

As attacks increase, AI-powered proactive solutions can help to keep the lights on  
Kurt Takahashi, Netwatch



## 44

### Gen-AI Mixes Promise with Pitfalls

When used wisely, the tool can be powerful, effective and time-saving  
Daniel Reichman, Ph.D., AI-RGUS



## 52

### A Solution for the Retail Theft Crisis

Facial recognition enhances security, loss prevention  
Dan Merkle, FaceFirst



## 58

### What AI Means for Physical Security

Managing risk is essential to leveraging this emerging technology  
Florian Matusek, Genetec

*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](http://www.securityindustry.org/techinsights). Questions, comments and article proposals may be submitted to the editor, Ron Hawkins, at [rhawkins@securityindustry.org](mailto:rhawkins@securityindustry.org).



# The Potential of Generative AI to Revolutionize Physical Security

Solutions are not just hype; they can reduce risk and improve productivity

ARTIFICIAL INTELLIGENCE (AI) IS DEFINED as the ability of a computer or other machine to perform tasks that are normally thought to require human intelligence. This description fits many of the automated security system features that have been on the market for many decades, so it is natural to wonder how AI suddenly became so newsworthy and a top agenda item in every security and related technology discussion.

A paradigm shift started a few years ago with the emergence of “Generative AI” (Gen-AI) systems that generate various forms of novel output, including text, code, graphics or audio (*Figure 1*). Examples of this type of system include generative pre-trained transformer (GPT) chatbots and text-to-image generators, which can be tailored to specific areas, tasks or personas. These most



Jim Black (jimblack@microsoft.com) is Senior Director, Security Architect for Microsoft's Cloud+AI Group ([www.microsoft.com](http://www.microsoft.com)).



recent advancements have signaled the dawn of a new era of potential.

### THE FUTURE IS NOW

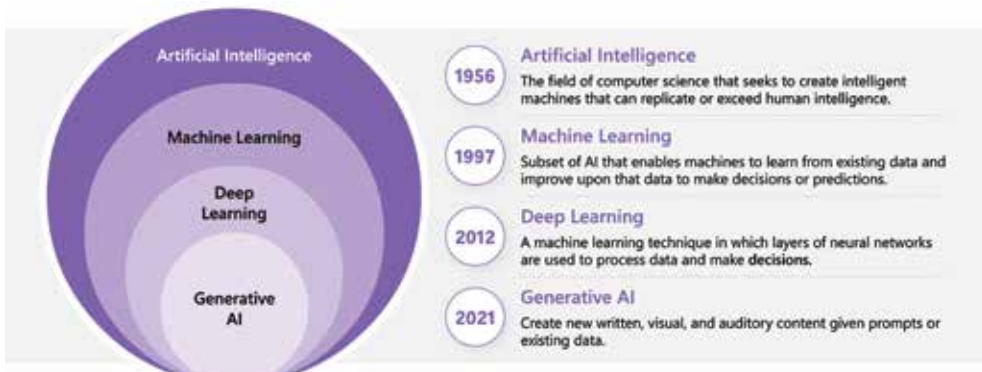
Gen-AI will revolutionize physical security in two foundational ways. The first is the manner in which users interact with systems, which will be transformed by more knowledgeable virtual assistants possessing a holistic understanding of the security program and the ability to learn continuously. Security system operators and managers will be able to leverage natural language queries into integrated technology systems and obtain results that historically took far more time and resources to produce. Officers who might ordinarily need to reference an exhaustive



**THE HIGHER RISKS ASSOCIATED WITH BLANKET ACCESS WILL BE MATERIALLY REDUCED WHEN SECURITY AND OPERATIONS WORK TOGETHER TO SEAMLESSLY ENABLE PERMISSIONS FOR ONLY THOSE LOCATIONS REQUIRING ACCESS TO PERFORM SPECIFIC TASKS.**

catalog of operating procedures, post orders, logs and site-specific documentation will be able to efficiently leverage a common tool via mobile or desktop device that quickly transforms typed or spoken prompts into actionable feedback. Benefits should be most visible for newer and less experienced staff, as well as during emergencies, when the performance of people is notoriously less consistent because of time pressures and stress.

Figure 1. Emergence of Generative AI





**BY IDENTIFYING AND ADDRESSING  
POTENTIAL SECURITY PROBLEMS  
BEFORE THEY OCCUR, ENTERPRISES  
WILL HAVE MORE POWER THAN  
EVER TO INFLUENCE USER  
BEHAVIOR AND ATTENTION TO  
SECURITY.**

Modern AI modules embedded into operational communication systems will enable real-time engagement with company employees, visitors and vendors. Tasks that might have traditionally required face-to-face interaction with onsite security will be addressed by a

straightforward tool that contains encyclopedic knowledge of the most current references securely in its dedicated model repository. Questions about security policy, work rules, access management, permissions, escorts and security systems can be quickly and consistently addressed in a way that will be easier for users to understand.

These tools can support onboarding and ongoing security awareness by addressing both common and complex queries on everyday issues that would have previously



required escalation or direct engagement with more experienced team members. Improved customer satisfaction will naturally result from the time, energy and cost savings associated with more efficient and effective interactions with security.

The second fundamental transformation will be tied to new capabilities that security systems and devices will have to perform tasks and identify issues that have eluded technology to date. Systems outfitted with enhanced reference models including current internal/external threats, risks, policies, procedures, system health, and other historical operations data will have the ability to identify emerging risks, trends, suspicious activity, security violations and other issues of potential concern that may not have been discovered until an attack or device/system failure had already occurred.

## **THE RISE OF COMPUTER VISION**

Whether referred to as video analytics, camera



cognition or computer vision, this tool will be able to achieve real-time processing of video data that can uncover complex security and safety issues. Individual devices will have embedded AI modules that can perform advanced analytics at the edge that previously demanded centralized, expensive and resource-intensive systems.

AI solutions based on machine learning modules will be applied to visual input from cameras both in

real time and on demand. Breakthrough experiences will include modules that learn to analyze video images based on current work rules, task-specific activities, and expected operations with historical context. Alerts can be triggered when variations from the established parameters are observed, giving onsite security timely and actionable intelligence they can use to assess the urgency of an incident and respond accordingly. Examples of situations in which this could be valuable include critical equipment being accessed without a valid work order, movement

of assets outside the secure path of travel within a facility, safety violations that historically have led to security incidents, identification and tracking of drone incursions, and the taking of pictures/video of critical assets without prior authorization.

Virtual video escorts will free up valuable officer resources by ensuring that security policies (e.g., two-person rule and persistent presence) are enforced. Systems will learn about the baseline attributes of each camera, including the approved field of view, areas of focus, and other settings.







AI modules will detect changes in these attributes and be able to identify if a camera has been knocked askew, critical areas are no longer in proper focus, home positions have been reset, or other settings have been altered. Subtle performance degradations that may indicate the need for service or replacement will also be spotted well in advance of outright failures, thereby eliminating more costly and impactful downtimes.

## ENHANCING ZERO TRUST

For both moderate and high-security applications, zero trust principles and least privileged access

will be further enhanced when AI-enabled security systems are integrated with operations and work authorization systems. Once systems are trained on facility attributes, access control zones, and asset location data, enterprises will be better equipped to proactively eliminate access over-provisioning in favor of a just-in-time model.

Granting most privileged permissions for longer than is necessary to complete work assignments and authorizing access to areas unrelated to specific tasks will no longer be a default posture. The higher risks associated with blanket access will be materially

reduced when security and operations work together to seamlessly enable permissions for only those locations requiring access to perform specific tasks. In addition, persistent access will be replaced by temporary permissions, whereby once a task is completed or the allocated time to complete work has expired, access will be automatically revoked.

### **SUPERCHARGED INVESTIGATIONS**

Investigation teams can look forward to using natural language query

features to produce more thorough and timely results. Machine learning modules will harness the power of AI to evaluate visual input from cameras and other sources. Classification, object detection and image analysis techniques will transform both the speed and quality of incident response and after-action reporting.

Natural language queries will facilitate exponentially easier searching for related prior incidents using targeted prompts. After a suspicious incident





involving a person on a green motorcycle at the facility entrance, for example, an investigator could query the video system for every other instance in which a person riding a green motorcycle was observed near the facility entrance. If circumstances warrant, customized alerting criteria could be created to alert security in real time whenever a person on a green motorcycle approaches the site.

Trends in the types of incidents and their root

causes will be more easily identified across sites and regions, yielding more actionable intelligence supported by historical data. For those who want to take a more proactive approach to identifying potential problems, AI-prompted near-miss analysis can help identify



**EDUCATION IS AN ESSENTIAL FIRST STEP IN TRANSFORMING ANY PHYSICAL SECURITY VISION INTO REALITY.**



**BUSINESS-RELEVANT AI CAN REALIZE A QUICK RETURN ON INVESTMENT, ESPECIALLY WHEN THE INTELLIGENCE IS APPLIED TO SUPPORT HIGH VALUE USE CASES, INCLUDING SECURITY.**

security issues and policy violations that did not lead directly to a security incident but could have, or flag actual incidents that, for whatever reason, may have gone unreported. By identifying and addressing potential security problems before they occur, enterprises will have more power than ever to influence user behavior and attention to security.

**RESPONSIBLE USE**

Threats to critical infrastructure continue to increase in sophistication, capability and frequency. Physical security stakeholders must thoughtfully consider how they will leverage emerging AI capabilities in a responsible way to modernize and transform physical security programs to address their most critical risks.

Implementing AI technology with clear and tangible links to the threats facing an organization eliminates any perception that the time and resources dedicated to such efforts are contributing to ineffective security theater. In addition to the obvious systems and technology implications, owners must also predict the impacts these innovative technologies will have on people and processes. Education is an essential first step in transforming any physical security vision into reality.

Responsible use will be best demonstrated by understanding AI systems well enough to choose the best solutions that work with existing systems,



improve security, fulfill due-care responsibilities, and keep promises to customers.

## EMBRACING OPPORTUNITIES

The physical security industry is now embarking on a remarkable journey to recognize the extraordinary potential that AI represents. Using AI in a responsible way has the potential to help solve our most pressing security challenges while transforming the way we work to be more productive, innovative and secure.

Business-relevant AI can realize a quick return on investment, especially when the intelligence is applied to support high value use cases, including security. For enterprises large and small, cost-benefit calculations must include both the direct and indirect costs of the AI system, as well as the savings associated with more efficient operations, reduced downtime, reduced numbers of incidents, and lower overall risks.

AI is also increasing excitement for work by



reducing the number of mundane tasks and creating efficiencies that help staff be more productive and creative in their roles. These opportunities are timely, as physical security must evolve rapidly to keep up with the pace of innovation, a distributed workforce, and shifting economic drivers. Physical security organizations innovating with AI amid these challenges are poised to emerge even stronger. ◀





# Context is Key – For Both People and AI

Multimodal systems can make the leap from identifying to understanding

A GROUP OF PEOPLE RUSHES INTO A STORE and coordinates to quickly steal a large amount of high-value merchandise.

A belligerent hotel guest confronts and threatens a front desk clerk working alone late at night.

A security officer at a large office park finds an intoxicated, mentally ill trespasser wandering around a parking garage.

A frantic parent comes to a shopping mall security office to report their young child is lost.

Whatever the differences among these varied security incidents, each of them at its core is a social interaction.

The intelligent deployment of security resources centers on understanding and anticipating



Jonathan Wender, Ph.D., (jonathan.wender@polis-solutions.com) is the President and CEO of Polis Solutions (www.polis-solutions.ai).

the complex human behaviors that lead to everything from retail theft to active assailant attacks. In fact, the entire security ecosystem can be seen as a vast network of social interactions. Better understanding and management of these interactions translates into more effective, efficient security.

Ideally, of course, security incidents should be prevented – or at least detected – before they become serious. Prevention and detection are also inherently social processes, because they require security organizations to have deep knowledge of



## UNDERSTANDING THESE BASELINE CONDITIONS AT SCALE IS ONE OF THE MOST IMPORTANT STEPS TOWARD THE ENHANCED DETECTION AND PREVENTION OF DANGEROUS ABERRATIONS.

how people behave and interact in ways that can lead to disorder, crime and violence.

Given the inherently social nature of security incidents and their prevention and resolution, the success of the security industry requires optimal leveraging of the exponentially growing amount of social data at its disposal. Artificial



“

**IT IS MORE IMPORTANT THAN EVER FOR THE PRIVATE SECTOR TO THINK STRATEGICALLY ABOUT HOW TO OPTIMIZE THE EFFICIENT USE OF SOCIAL DATA IN SECURITY ENVIRONMENTS WHERE LAW ENFORCEMENT RESOURCES ARE INCREASINGLY UNAVAILABLE.**

intelligence (AI) technology can transform the way security organizations analyze and use the massive amount of social data collected by video and audio devices, including fixed cameras, body-worn cameras, and mobile cameras deployed on

vehicles, phones, drones and other platforms.

At present, the ability of the security industry to analyze video-based social data is fairly basic. Most current video analytics technology is limited to the simple detection of people in a given location without a deeper understanding of what they are actually doing. At a more advanced level, there are newer computer vision technologies that can recognize emotions and facial expressions or identify individuals. However, despite their powerful capabilities, these tools are largely





incapable of analyzing the back-and-forth dynamics of human interactions and detecting essential social processes such as conflict, cooperation, de-escalation, violence, or the use of force. Given these limitations, the security industry is left in the operationally and financially untenable situation of collecting massive amounts of high-value video and audio social data that it cannot put to full use.

Video cameras are the security industry's single largest source of data about the myriad human interactions that occur before, during and after security incidents.

In addition to capturing anomalies and serious security events, video data also contain invaluable information about the normal conditions in which nothing goes wrong. Understanding these baseline conditions at scale is one of the most important steps toward the enhanced detection and prevention of dangerous aberrations.

Video surveillance networks around the world record thousands of petabytes of data every day. However, most of this data is never analyzed, let alone applied in ways that could optimize both operational success and commercial value. As the





**MULTIMODAL AI REFERS TO SYSTEMS THAT INTEGRATE COMPUTER VISION, NLP AND SPEECH PROCESSING TO CREATE ANALYTIC CAPABILITIES THAT APPROXIMATE WHAT HUMANS DO IN LIVE SOCIAL INTERACTIONS.**

security industry evolves to meet urgent challenges posed by mutually reinforcing factors, such as the steep rise in property crime and general public disorder and the parallel contraction of government policing services, it is more important than ever for the private sector to think strategically about how to optimize the efficient use of social data in security

environments where law enforcement resources are increasingly unavailable.

A recent article in these pages by Matt Powell stated that AI-driven video analytics are creating a “third wave” in surveillance innovation with the potential to “pay dividends as a force multiplier for end users and a moneymaker for integrators” (*SIA Technology Insights*, Spring 2024). Recent developments and emerging trends in multimodal AI and the related field of computational social science offer new opportunities for the security industry to







enhance its capabilities, efficiency and competitiveness by leveraging social data.

AI uses computer technology to approximate human abilities such as visual perception and language understanding. AI also enables the analysis of vast amounts of data that are too large and complicated for humans to manage without powerful computational resources. Computational social science refers to the use of computer tools like AI in conjunction with research on human behavior to address complex problems in areas ranging from

crime to public safety to healthcare to poverty. When the latest AI technology is combined with social science, the practical benefits can be huge.

The three kinds of AI most important for analyzing social interactions in security environments are computer vision, natural language processing (NLP), and speech processing. Computer vision uses AI to automatically identify patterns of behavior, movement and emotion. Computer vision tools can also detect various kinds of events such as violence or

a medical emergency. NLP uses AI to understand the content of speech – *what* people are saying – while speech processing uses AI to analyze the quality of speech – that is, *how* people are speaking to each other (tone, pitch, etc.). NLP and speech processing are especially important for the analysis of data collected by video devices like body-worn cameras and access control cameras that also have audio recording capability.

Multimodal AI refers to systems that integrate

computer vision, NLP and speech processing to create analytic capabilities that approximate what humans do in live social interactions. When people interact, they simultaneously analyze each other’s behavior, speech content (what is being said), and speech quality (how words are spoken). This is true for both face-to-face encounters and virtual interactions such as video meetings. For example, it is easy to identify which people in an online





meeting are actually listening and participating and which ones are “checked out” or doing other work.

People also intuitively understand the unique context of various interactions. Trying to get to a seat on a crowded airplane, checking out at the grocery store, or having a family dinner. This context provides us with the “metadata” we need to help make sense of all the other information we gather from observing people. Plainly said, other people’s behavior and

language only makes sense to us because we understand the context in which it is occurring.

Multimodal AI functions like a human observer and analyzes vast amounts of social data collected by surveillance systems. By integrating social data analytics with wider metadata, security organizations can radically enhance the efficiency and safety of their operations. This process of integration requires drawing on computational social science as well as domain expertise.



Simply having the latest multimodal AI technology is not enough to effectively analyze vast amounts of security-related social data. The analytics provider must also understand general principles of human behavior and how those principles function in each unique security environment. While AI will never replace human judgment as the heart of effective, ethical security, it can dramatically enhance the use of social data in beneficial ways that uphold the safety, welfare and dignity of all people.

Perhaps the most important feature of systems that combine multimodal AI, computational social science, and domain expertise is their capacity to understand the dynamics of entire social interactions, rather than just the isolated behavior of individuals. Multimodal AI can examine myriad interactions between members of the public, employees, security personnel and others to generate fine-grained understandings of what causes, prevents and



mitigates a wide range of security incidents. This kind of understanding not only helps to improve the efficient deployment of security personnel and technology, it can also inform best practices that can enhance safety and reduce liability.


Like any powerful new technology, multimodal AI has vast upside potential while also raising a host of complex legal, ethical and privacy questions. Answering these questions cannot be reduced to conference room abstractions, it can only be accomplished in the real-world context of disciplined, gradational testing, piloting and operational implementation.

The proverbial AI “cat” is out of the bag. The question is no longer whether it is possible to analyze the vast flow of social data collected by security video and audio networks, but, rather, how to do so in a transparent, rigorous manner that addresses the legitimate needs and concerns of diverse stakeholders.

The security industry can further this process

and ensure its success and integrity by asking the right, tough questions. How should security-related social data be structured, searched and analyzed? What should be the highest priorities for the analysis of security-related social data? How can accuracy be increased, error rates decreased, and biases mitigated? What are the legal, business and ethical implications of various data analysis strategies? What safeguards are necessary to ensure that social data analytics are ethical and defensible?

Finally, what are the risks of affirmatively foregoing the opportunity to analyze security-related social data as its powerful potential to improve public safety becomes increasingly evident? ◀



---

**WHILE AI WILL NEVER REPLACE HUMAN JUDGMENT AS THE HEART OF EFFECTIVE, ETHICAL SECURITY, IT CAN DRAMATICALLY ENHANCE THE USE OF SOCIAL DATA IN BENEFICIAL WAYS THAT UPHOLD THE SAFETY, WELFARE AND DIGNITY OF ALL PEOPLE.**





# Meeting the Full Spectrum of Customer Needs

Careful listening can solidify relationships and create opportunities

IT IS HARD TO OVERSTATE JUST HOW MUCH disruption the security industry has experienced over the past few years. Not too long ago, artificial intelligence (AI) was not even in the conversation. Now, it is a part of the top four megatrends from the Security Industry Association (SIA), and nearly half – 48 percent – of security solutions developers expect AI to have a strong impact on their strategy within the next five years.

But disruption is not just limited to AI. Network convergence, cameras as sensors, and the Internet of Things (IoT) are creating new opportunities for security professionals, as well as new challenges. Integrators need to learn new skillsets and stay on top of technology advancements, and they are facing new competition from players outside the traditional security industry.



Matt Powers (matt.powers@anixter.com) is Vice President, Technology & Support Services, for Wesco (www.wesco.com).

How should integrators respond? The temptation might be to double down on selling more technology, devices and solutions to customers. To be sure, that is never a bad thing. However, by taking a step back and incorporating design thinking into the sales process, security professionals can foster deeper customer relationships, sell more effective solutions and ultimately create greater revenue opportunities.

## **IMPLEMENTING DESIGN THINKING**

At its core, design thinking is a creative

“

**DISRUPTION IS NOT JUST LIMITED TO AI. NETWORK CONVERGENCE, CAMERAS AS SENSORS, AND THE INTERNET OF THINGS ARE CREATING NEW OPPORTUNITIES FOR SECURITY PROFESSIONALS, AS WELL AS NEW CHALLENGES.**

way of solving customer challenges by understanding their unique needs and perspectives. This holistic view often requires a paradigm shift. Rather than focusing on solving the immediate tactical challenge with technology, integrators seek to get to the heart of the larger business problem.



What does this mean? First, integrators need to invest time to understand each customer's unique situation. This generally has two steps.

### **1. Empathize**

This initial step is essential to the design thinking methodology. The goal is to gain a deep understanding of the customer's needs, goals and motivations. What internal or external factors are influencing their current situation? What challenges or pain points

are they facing? Who are the key stakeholders, and how might their perspectives differ? Clearly, this can take some time, but the information gained will set the stage for the rest of the process.

### **2. Define**

This is where the integrator and the customer will clearly frame the challenge that needs to be solved. Often, the initial problem is actually a symptom of an enterprise-wide issue – which is why the



“empathize” stage is so important. Also, in the process of defining the challenge, an integrator may uncover additional opportunities to help the customer. It is also vital to define and frame the challenge in the context of solving a broader business problem. Onboarding a new technology or tool is great, but keeping the bigger picture in mind ensures that the solution will not only meet the customer’s needs today, but also in the future.

With the challenge clearly defined, now it is time to move to the solution design phase, which integrators are well versed in. This phase also has two primary steps.

### 1. Ideate

This is the integrator’s bread and butter. This involves crafting bold, innovative ideas that meet the customer’s tactical needs *and* solve their overarching business challenge.

### 2. Prototype and test

Implementing the technology is not necessarily the end of the process. Experiment,



iterate and see what works and what can be enhanced. Ultimately, this will create more effective solutions and happier customers.

## THE PITFALLS OF LEADING WITH TECHNOLOGY

It can be tempting to skip the “Empathize” and “Define” steps and jump right to deploying a solution or technology. After all, if a customer says



**DESIGN THINKING IS A CREATIVE WAY OF SOLVING CUSTOMER CHALLENGES BY UNDERSTANDING THEIR UNIQUE NEEDS AND PERSPECTIVES.**





**SKIPPING THE “EMPATHIZE” AND  
“DEFINE” STEPS POTENTIALLY  
LEAVES THESE OPPORTUNITIES  
ON THE TABLE AND CREATES  
AN ENVIRONMENT WHERE  
THE INTEGRATOR-CUSTOMER  
RELATIONSHIP IS COMMODITIZED,  
INSTEAD OF SEEN AS A TRUE  
PARTNERSHIP.**

their surveillance cameras are not working, the easy solution is to provide them with new cameras, right? Not so fast. True, that approach might solve their immediate need, but it ignores the bigger picture. Plus, it could result

in leaving opportunities on the table.

In this example, simply selling new cameras might not get to the bottom of the underlying issue. Perhaps the customer’s network infrastructure is limiting their system’s performance. Maybe new cameras fix the immediate need, but if they do not play nice with other systems that are already in place, more headaches can result. Or maybe the existing solution was not developed with long-term needs in mind and will be obsolete in six to 12 months.





Case Study:

# Design Thinking in Action

A recent example of design thinking in action involved a large jewelry retailer. With more than 2,000 locations, the retailer faced many of same challenges that other retailers were contending with: Staff shortages were a constant struggle, and shrinkage was increasing. The simple fix would have been to upgrade or replace the traditional security system to help manage shrinkage and mitigate staffing issues.

However, during the “Empathy” phase, the integrator discovered that the retailer was challenged by several other issues that fell outside traditional security. Customer satisfaction was declining as shoppers grew frustrated with long checkout times, a lack of self-checkout options and a less personalized shopping experience.

Because the integrator took the time to understand the customer’s challenges, they were able to roll out a comprehensive solution that not only addressed the retailer’s security concerns, but also helped alleviate their other pain points as well.

- ▶ *Full-stack security solutions* allowed the retailer to deploy an advanced video intelligence system that reduced shrinkage and maximized the efficiency of the security team – even in the midst of staffing shortages.
- ▶ *Retail security expertise*

enabled the retailer to install modern, convenient self-checkout systems that satisfied shopper expectations without sacrificing security.

- ▶ *Pro A/V integration services* resulted in digital signage and displays that delighted shoppers and enhanced overall store profitability.
- ▶ *Networking solutions* ensured that all of these systems functioned effectively as part of a comprehensive ecosystem. And this enabled the retailer to be future-ready as their technology needs evolved. Leveraging a design thinking session with the customer allowed the integrator to capitalize on additional opportunities that they might have missed had they simply been focused on selling security products. Additionally, it deepened their relationship with the customer, and solidified their position as a valued partner.



“

**SECURITY PROFESSIONALS MAY NEED TO LEARN NEW SKILLSETS, OR BECOME FAMILIAR WITH A DIFFERENT SET OF STAKEHOLDERS, SUCH AS THE C-SUITE, OR THOSE IN OTHER DEPARTMENTS LIKE MARKETING OR FINANCE.**

Integrators might also miss out on additional business opportunities by going straight to the solution-selling stage. Understanding the customer's business needs can reveal opportunities

to create a bigger, more effective technology ecosystem within the organization. For example, perhaps a security camera could also be utilized by marketing or customer service to better understand their shoppers and provide an enhanced customer experience.

Skipping the “Empathize” and “Define” steps potentially leaves these opportunities on the table and creates an environment where the integrator-customer relationship is





commoditized, instead of developing into a true partnership.

### **ADOPTING THE DESIGN THINKING APPROACH**

Moving to a design thinking methodology often requires a shift in mindset, and it is not always easy. Security professionals may need to learn new skillsets, or become familiar with a different set of stakeholders, such as the C-suite, or those in

other departments like marketing or finance.

If an integrator is interested in adopting a design thinking mentality, they do not need to go it alone. Distribution partners can be a valuable extension of the integrator's team. The right distribution partner can connect integrators with suppliers and vendors that can meet all of their customers' needs and goals and create an ecosystem that produces both security and business benefits. ◀



# Considerations in AI Training and Deployment

Starting with the right implementation plan is vital to success

MORE BUSINESSES ARE STARTING TO DEPLOY artificial intelligence (AI), which means they need to understand new rules for using data properly and safely. When adding AI to their systems, especially in physical security, companies face not just technology challenges but also compliance demands that differ from state to state, industry to industry, and country to country.

An improper approach to AI deployment could put an organization's entire security program at risk. For large enterprise customers, this process can be a part of digital transformation. For end users, it is important to think about how to get ready for the big changes that come with AI.

There are many regulations related to AI around the world that companies need to follow, and they can get in trouble if they fail to do so. When companies want to use AI, they need to be



Niru Satgunananathan (niru.satgunananathan@jci.com) is ESS Business Development Manager & Consultant for Johnson Controls (www.johnsoncontrols.com).



careful about these rules, especially when they are handling personal information.

The first step in a deployment is understanding how AI works with current tools. Most likely, it will not provide a significant return on investment initially but, with a well designed implementation roadmap, it may enhance efficiency or improve how security operations are managed in the future.

AI requires a massive amount of data to build its learning models, which raises multiple issues.



## AN IMPROPER APPROACH TO AI DEPLOYMENT COULD PUT AN ORGANIZATION'S ENTIRE SECURITY PROGRAM AT RISK.

- *Ethical and privacy concerns:* Gathering large volumes of data often involves collecting personal information, posing significant privacy concerns.
- *Financial costs:* Acquiring high-quality, relevant data can be expensive. Costs are associated with purchasing





## LARGE DATASETS ARE NOT IMMUNE TO BIAS, WHICH CAN LEAD TO SKEWED AI OUTPUTS.

datasets, investing in data collection infrastructure, and partnering with data providers.

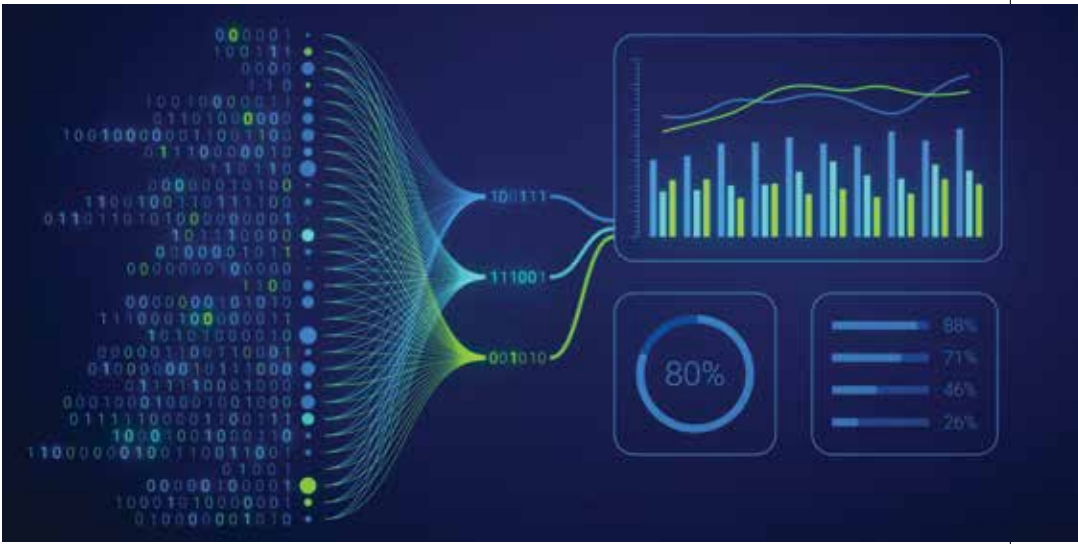
- *Data bias and quality issues:* Large datasets are not immune to bias, which can lead to skewed AI outputs. Ensuring diversity and representativeness in datasets requires additional efforts in

data curation and preprocessing.

- *Legal and regulatory constraints:* Data acquisition is heavily regulated, with laws varying by jurisdiction.

Addressing these challenges requires a balanced approach that considers the ethical implications of data collection, invests in data quality, and adheres to legal standards. Companies need to be transparent about their data practices and data protection. For example, processing access control event data





through a large language model (LLM) would involve collecting the behavior of employees when they enter and exit the facility. If this includes information about the CEO of the company, it could create risk if the data is acquired by bad actors. Banks, hospitals and critical infrastructure sites will face their own unique challenges.

To get a large amount of high-quality data for AI training, companies have a few options. They can gather data from their own activities and make their current data better with special techniques. They can work with others to buy data or use data that is freely available. They can ask people to share their data. Whatever alternative

is selected, making sure the data is clean and well organized is critical. Also, using existing AI models that have already “learned” some things can mean that less data will be required.

AI can significantly improve efficiency, predictive analytics and response times. However, the quality and maintenance of existing systems play a crucial role in determining the technology’s effectiveness. The planning and deployment of AI systems requires multiple factors to be considered.

- *Use of existing infrastructure:* It is often feasible to use existing systems as a foundation for implementing



**SYSTEMS WITH ISSUES LIKE FREQUENT FALSE ALARMS OR POORLY MAINTAINED SENSORS CAN GENERATE NOISY DATA, LEADING TO INACCURATE AI PREDICTIONS AND ANOMALY DETECTION.**

AI solutions.

Many AI tools and algorithms are designed to integrate with current infrastructure, processing and analyzing the collected data to provide insights, detect anomalies, or predict potential security breaches.

- *Data quality and maintenance:* The effectiveness of AI is heavily dependent on the quality of data. Systems with issues like frequent false alarms or poorly maintained sensors can generate noisy data, leading to inaccurate AI predictions and anomaly detection. If an organization has not sufficiently maintained its security system, this noise can significantly undermine the performance of AI





applications.

- **System compatibility:** Older systems may not be fully compatible with modern AI technologies, limiting the potential benefits or requiring substantial middleware development to facilitate integration.
- **Assessment and clean-up:** Before integrating AI, it is critical to conduct a thorough assessment of the current security system. Identifying and rectifying issues like false alarms, sensor malfunctions, or outdated software can improve the quality of data fed into AI systems.
- **Incremental modernization:** Completely overhauling the infrastructure may not be feasible, especially for large systems. An incremental approach – prioritizing upgrades that significantly affect



AI performance, such as improving sensor quality or updating to more compatible systems – can be a more manageable strategy.

- **Continuous monitoring and maintenance:** Ongoing maintenance of the physical security infrastructure and continuous monitoring of AI system performance are essential. This approach allows for timely adjustments and ensures that AI applications remain effective and reliable.
- **AI training and calibration:** Training



## ONGOING MAINTENANCE OF THE PHYSICAL SECURITY INFRASTRUCTURE AND CONTINUOUS MONITORING OF AI SYSTEM PERFORMANCE ARE ESSENTIAL.

AI models on the specific dataset of the organization, including data from faulty alarms, can help the system learn to identify and possibly ignore these anomalies over time. Continuous calibration based on real-world performance can further refine AI accuracy.

- *IT infrastructure complexity:* AI systems add layers of complexity to IT infrastructures, complicating data protection consistency across platforms.
- *Regulatory compliance:* The dynamic nature of AI challenges compliance with evolving regulations, necessitating constant vigilance.
- *Cybersecurity threats:* AI systems require the implementation of sophisticated, dynamic defenses to protect against





increasingly smart cyber threats.

- **Technical skill shortages:** The specialized knowledge required for AI data protection and the shortage of skilled professionals can impede effective strategy execution.
- **Budget constraints:** The ability to implement cutting-edge AI security solutions is often limited by the availability of funds, affecting the quality of deployed measures.
- **Data sprawl:** The rapid growth and dispersion of data generated by AI

systems challenge efforts to maintain control and visibility.

- **Ensuring reliability:** Updating AI systems with the latest security measures without compromising their reliability or performance poses a significant challenge.

While existing physical security systems can form the basis for AI integration, ensuring the quality and compatibility of these systems is crucial. Through careful assessment, incremental modernization and ongoing maintenance, AI can provide reliable, efficient enhancements to security operations. ◀



# The Future of Utilities Security

As attacks increase, AI-powered proactive solutions can help to keep the lights on

THE RECENT SURGE IN SECURITY INCIDENTS at electrical substations and utilities in the United States is alarming. Attacks have increased 71 percent over the past year and experts foresee this unfortunate trend continuing into 2025 and beyond. These events are not just statistics – they are real threats that pose significant risks to citizens, neighborhoods, vital industries and the national economy.

The growing number of attacks on utilities presents a multifaceted challenge for city administrations, public and private entities, and local communities. According to the Electricity Information Sharing and Analysis Center (E-ISAC), attacks of varying types, including gunfire,



Kurt Takahashi (ktakahashi@netwatchgroup.com) is the CEO of Netwatch (www.netwatchgroup.com).



sabotage, vandalism and security breaches, are increasing and have affected multiple regions of the country.

During a technical conference held by the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC), Eric Rollison, assistant director of the U.S. Energy Department's Office of Cybersecurity, emphasized the "heightened threat environment" in the industry. A NERC report

“

## THE FUTURE OF SECURITY SOLUTIONS IN THE UTILITY SECTOR CENTERS ON INTEGRATED AI TECHNOLOGY BECAUSE IT TRANSFORMS PREVIOUSLY PASSIVE SYSTEMS INTO PROACTIVE PLATFORMS.

also noted a significant increase in physical security incidents since 2020, with substantial outages reported in North Carolina, Washington and California. The motivations behind these





**WHILE TRADITIONAL SECURITY MEASURES LIKE FENCES, VIDEO SURVEILLANCE AND LIGHTING PROVIDE SOME LEVEL OF DETERRENCE, THEY TYPICALLY SERVE A REACTIVE ROLE AND FALL SHORT OF HELPING ORGANIZATIONS STAY AHEAD OF EVOLVING THREATS.**

attacks – from theft to ideological extremism – add complexity, complicating the efforts of law enforcement agencies, local governments and the energy sector to defeat them.

## **THE INDISPENSABILITY OF ELECTRICAL SUBSTATIONS**

Electrical substations and public utilities are critical to modern society, providing power to residences, offices, healthcare systems and various modes of transportation. A single attack on these vital facilities can trigger widespread disruptions, affecting daily life on a massive scale. For example, gunfire damage to two substations in Moore County, N.C., in December 2022 left 35,430 utility customers without power.





The financial repercussions of these incidents can be severe, as well. The potential impact is extensive, from immediate repair and restoration costs to longer-term consequences, such as revenue losses and operational downtime. Furthermore, following an incident, utilities may face surging insurance premiums, legal liabilities, reputational damage, and regulatory hurdles, which could entail penalties and the need for corrective measures to prevent future occurrences.

Protecting the vast U.S. electrical grid – which comprises more than

55,000 substations and extensive transmission lines – is no small feat. While traditional security measures like fences, video surveillance and lighting provide some level of deterrence, they typically serve a reactive role and fall short of helping organizations stay ahead of evolving threats. In addition, determined



**ARTIFICIAL INTELLIGENCE-DRIVEN VIDEO MONITORING SERVICES ARE GROWING IN DEMAND, AS THEY HAVE BEEN PROVEN TO ENABLE UTILITIES TO PREVENT THEFT AND ATTACKS BEFORE DAMAGE OCCURS.**



**WHILE THE CURRENT THREAT LANDSCAPE IS CHALLENGING, INNOVATIVE TECHNOLOGIES AND COLLABORATIVE EFFORTS LIKE PUBLIC-PRIVATE PARTNERSHIPS CAN ENHANCE SECURITY.**

perpetrators can bypass physical barriers like fences with relative ease, highlighting the limitations of relying solely on conventional security approaches.

**MODERN STRATEGIES FOR PROTECTION**

Emerging solutions, particularly proactive strategies and technologies, show promise. Artificial

intelligence (AI)-driven video monitoring services are growing in demand, as they have been proven to enable utilities to prevent theft and attacks before damage occurs. Rather than just recording incidents for later review, utilities can use existing camera deployments combined with video analytics to identify and counter threats in real time.

The future of security solutions in the utility sector centers on integrated AI technology because it transforms previously passive systems into proactive platforms. AI can allow video monitoring systems to identify unauthorized movements or actions automatically. For example, intelligent video monitoring combines real-time surveillance with immediate intervention. When a breach is detected, security personnel deliver live, customized voice commands informing the intruder that they have been identified and authorities will be dispatched if they do not leave. In cases where the intruder is noncompliant, operators contact local law







enforcement and other relevant parties to ensure a rapid and effective response. This solution is particularly beneficial at remote utility sites where traditional security approaches fall short.

## **A SECURE ENERGY FUTURE**

While the current threat landscape is challenging, innovative technologies and collaborative efforts like public-private partnerships can enhance security. Advanced technologies and services offer immediate intervention capabilities,

something not currently available with traditional security methods.

The urgent need for innovative, adaptive security strategies has never been greater. Through investments in technology, protective processes, and a commitment to enhancing security measures, the utilities industry can transform this sizable challenge into a stepping stone for stable, long-term growth. The clock is ticking and the risks are substantial, but a fortified and resilient energy future is within reach. ◀

# Generative AI Mixes Promise with Pitfalls

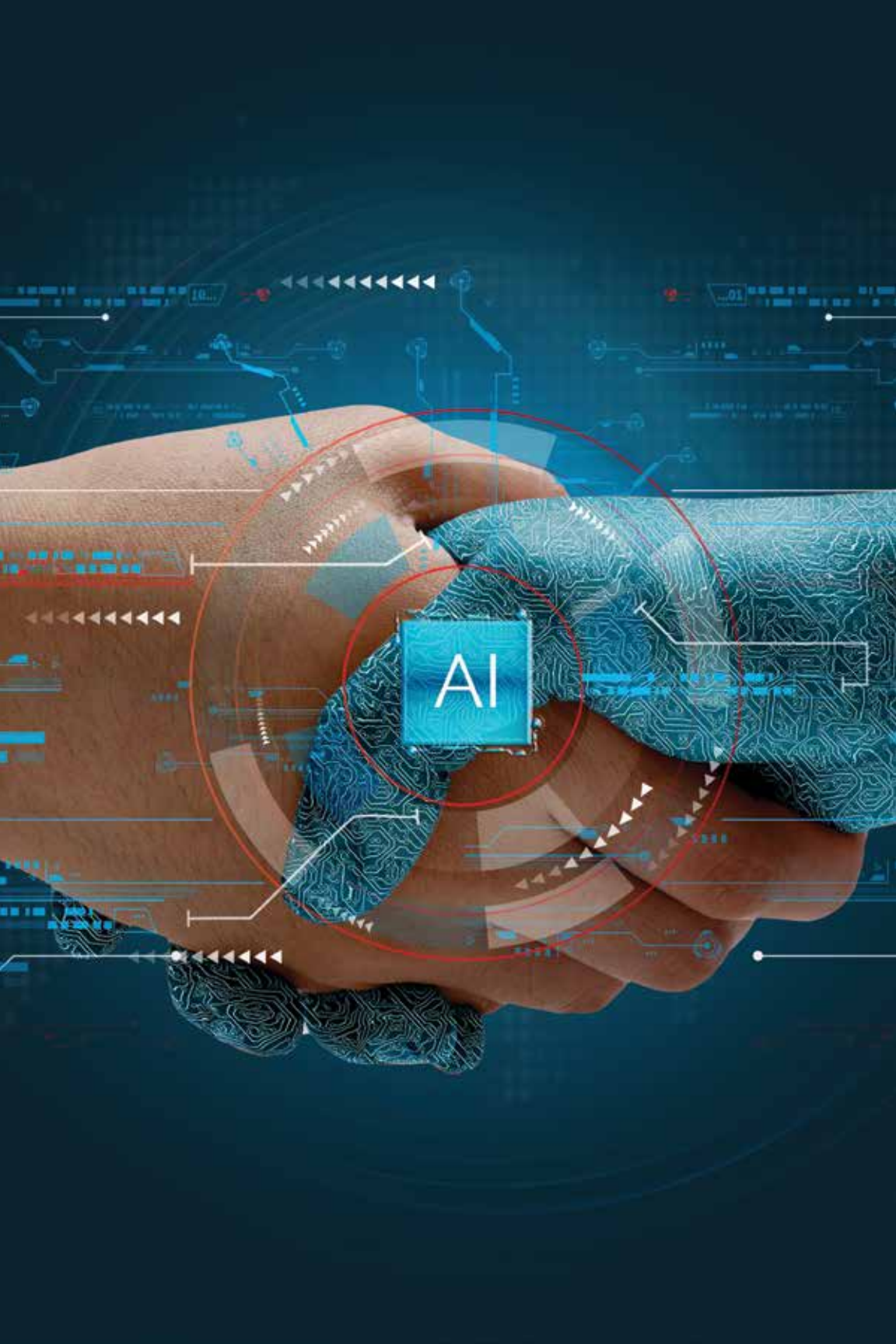
When used wisely, the tool can be powerful, effective and time-saving



Daniel Reichman, Ph.D., ([danielr@ai-rgus.com](mailto:danielr@ai-rgus.com)) is the CEO and Chief Scientist at Ai-RGUS ([www.ai-rgus.com](http://www.ai-rgus.com))

ARTIFICIAL INTELLIGENCE (AI) AND, MORE SPECIFICALLY, GENERATIVE AI (GEN-AI) is in the news on an almost daily basis. The technology captivated society's collective attention approximately 18 months ago with the release of ChatGPT, which garnered 100 million users in just two months, a feat that took social media giant Facebook two and a half years to accomplish.

Gen-AI creates new content automatically using AI (hence the modifier "generative"). The applicable uses range from jobs as simple as generating text and images to more complex tasks like creating music, videos and code. A Gen-AI model that can mimic human language, art, mannerisms and thought processes is a powerful



AI



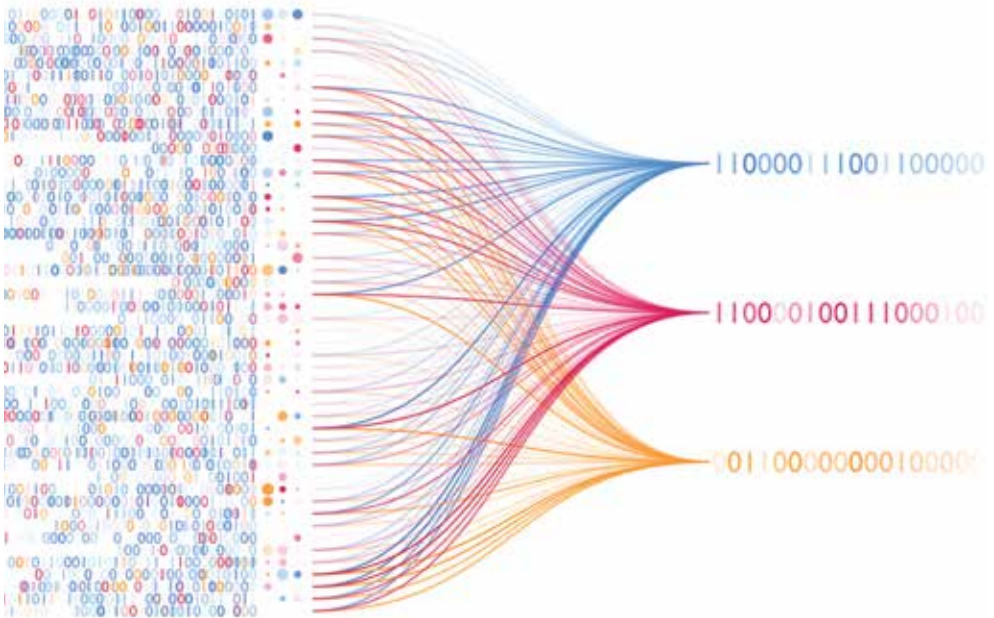
**WHEN NEW TECHNOLOGY SUCH AS THIS IS ROLLED OUT, IT IS AN EXCITING TIME FOR EXPERIMENTATION, AND WITH THAT COME BOTH SUCCESS STORIES AND TALES OF FAILURE.**

tool. Ultimately, this unleashes a new realm that can enable businesses to transform their work.

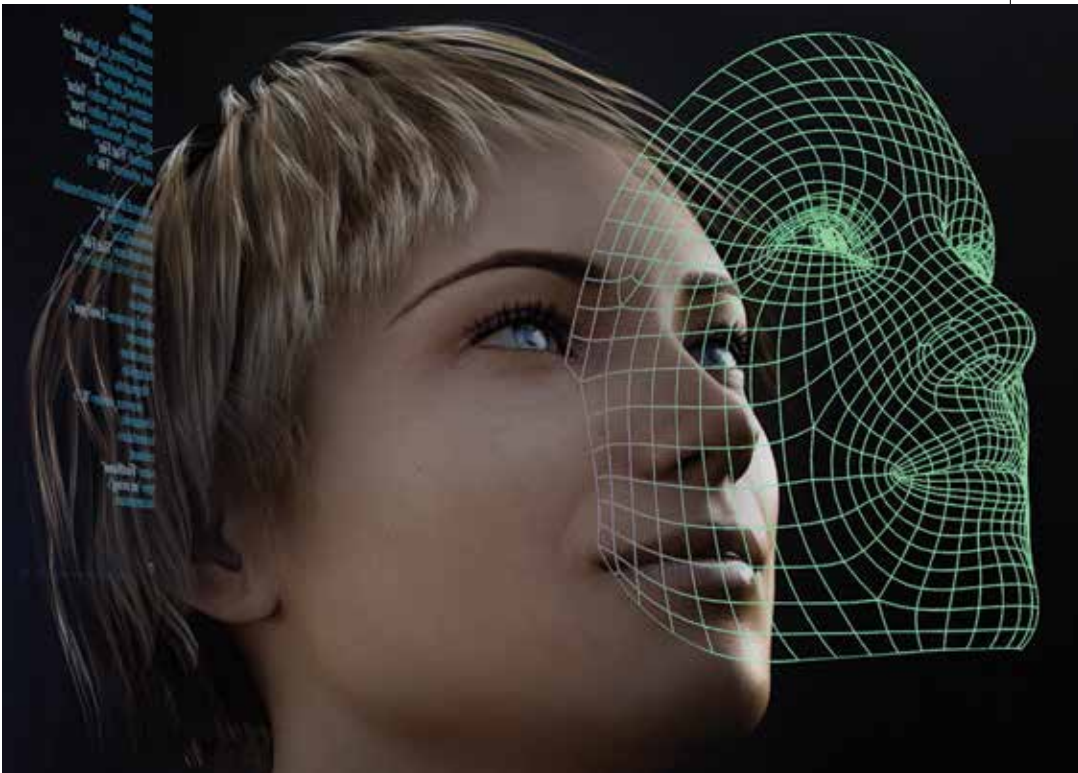
To build a Gen-AI system, the model needs to review enormous amounts of data. Thanks to the Internet, there is a seemingly infinite number of data sources (which is both a blessing and a curse). The AI must be fed this data so it can learn to

identify patterns in and structures of the source material. In this way, it learns both about language and the world around us (e.g., what is a correctly constructed sentence or image), as well as how to converse.

Gen-AI uses statistical methods to learn how to predict (or generate) a response to a prompt. For example, a user can ask a Gen-AI system to write creatively about a given topic. This would be an example of a large language model (LLM). A user could also use a diffusion model of Gen-AI to generate an image based on a piece of text.







Other models of Gen-AI can predict the word that comes next in a block of text or fill in a missing part of an image. Because it has reviewed a tremendous amount of data, it can use the information it has seen to answer questions with relevant content and correct-sounding prose and context.

When new technology such as this is rolled out, it is an exciting time for experimentation, and with that come both success stories and tales of failure. Laborious tasks that would

take employees hundreds of hours to complete can now be done in minutes – or even seconds. For example, people have used this tool as a way to get summaries of a topic that



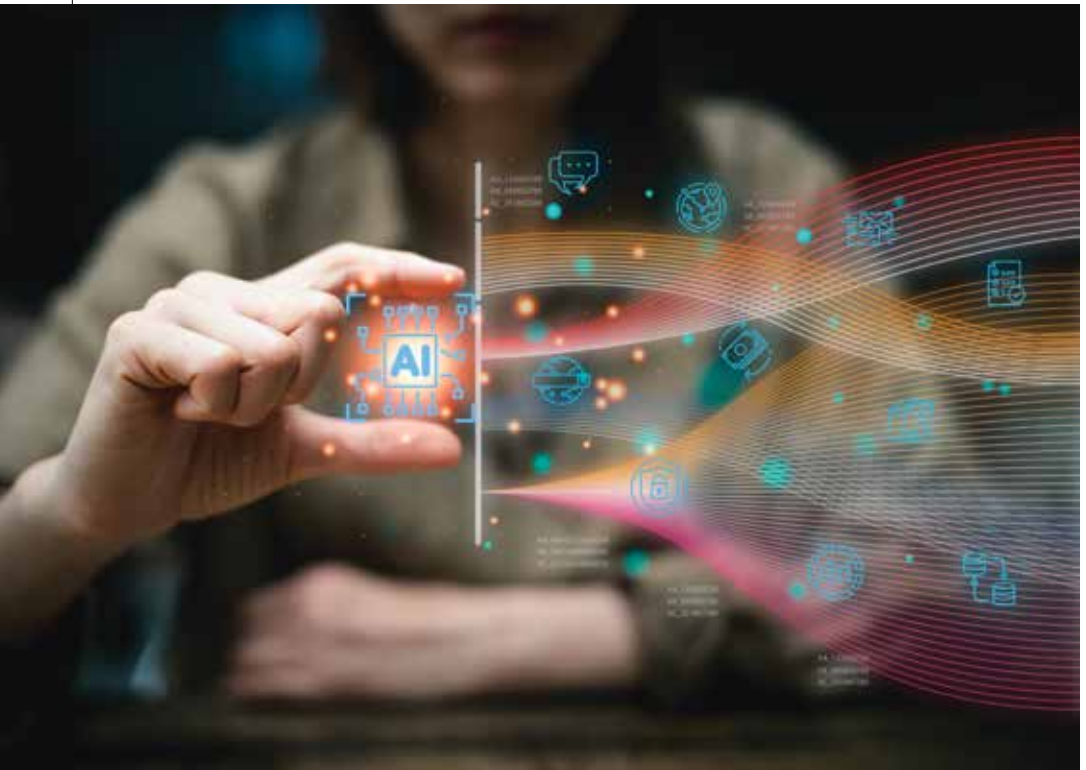
**THIS ISSUE IN AUTOMATIC CONTENT PRODUCTION IS REFERRED TO AS “HALLUCINATION,” AND AVOIDING OR MITIGATING IT IS AN ACTIVE TOPIC OF RESEARCH. TO SAY THE LEAST, IT IS HIGHLY ADVISABLE TO VERIFY THE CONTENT THAT GEN-AI PRODUCES BEFORE USING IT.**

would otherwise require extensive research. It can automatically generate documentation and how-to guides, and provide suggestions based on an explanation of a specific situation or project. It has the ability to generate photo-realistic images from just a short textual prompt.

The applications of Gen-AI include creating more engaging marketing campaigns, using predictive analytics to review video footage, and developing advanced

products based on the current research in a given field. It has spurred a wave of new companies that can customize and tailor the tool to fit specific use cases.

Some of the failures, meanwhile, stem from the way in which Gen-AI learns about the world. If the information it has seen on a topic is sparse, wrong or outdated, its knowledge will be limited, biased or corrupted. Another issue is that it learns how to complete sentences based on what is most likely, which, contrary to claims





of being “predictive,” can lead to unpredictable outcomes. One case that led to difficulty for its user was when the Gen-AI engine cited sources that were not real. The format and placement of the citations were correct because the Gen-AI system had seen many such examples, but the “sources” were entirely made up. This issue in automatic content production is referred to as “hallucination,” and avoiding or mitigating it is an active topic of research. To say the least, it is highly advisable to verify

the content that Gen-AI produces before using it.

Finally, an important aspect of utilizing Gen-AI models is the quality of the training material. As more people

“

**IF SOMEONE DOES NOT CHECK FOR ACCURACY AND UPLOADS TO THE INTERNET INCORRECT INFORMATION (THAT IS STATED AS FACT) FROM AN AI MODEL, THIS CAN LEAD TO GEN-AI SYSTEMS REGURGITATING INCORRECT INFORMATION REPEATEDLY.**

“

## THE MOST SUCCESSFUL WAY TO USE GEN-AI, TO DATE, IS AS A STARTING POINT AND NOT AS A FINAL PRODUCT.

and businesses publish AI-created content online, the pool of information can be polluted. If someone does not check for accuracy and uploads to the Internet incorrect information (that is stated as fact) from an AI model, this can lead to Gen-AI systems regurgitating incorrect information repeatedly. At some point,

this would evolve into a feedback loop of AI being trained on AI-generated material, further taking the “human” out of the process with each pass. With all of this in mind, the most successful way to use Gen-AI, to date, is as a starting point and not as a final product.

Notwithstanding these challenges, Gen-AI remains a powerful tool that has major potential to relieve people of repetitive and tedious work. One way that Gen-AI is being deployed in the security industry, for example,







is through video search and querying. To achieve useful results with video, like identifying a problem in real time or putting together a timeline of events after an incident, the video footage needs to be reviewed frame-by-frame. This is an immense undertaking for a human operator. Gen-AI opens the possibility of an interface in which a user can describe in plain English what content is of interest and then have AI produce the images that are related

to the query. This can save time, resources and money. In the future, a conversational engine will likely be a standard feature of user interfaces, allowing someone to retrieve specific information with ease. ◀

“

**GEN-AI REMAINS A POWERFUL TOOL THAT HAS MAJOR POTENTIAL TO RELIEVE PEOPLE OF REPETITIVE AND TEDIOUS WORK.**



# A Solution for the Retail Theft Crisis

Facial recognition enhances security, loss prevention



Dan Merkle (djm@facefirst.com) is Board Chairman and CEO at FaceFirst (www.facefirst.com).

**FACIAL RECOGNITION TECHNOLOGY** is not emerging.

*It's here.*

Millions of people already use artificial intelligence (AI)-driven facial recognition technology every day in the United States and around the world. Individuals from every demographic unlock their phones with their faces – instantly – multiple times per day. They use facial recognition for secure access to their financial accounts and to pass through airport security checkpoints quickly. Many retailers use face matching for both security and loss prevention.

In fact, new research reveals that senior retail executives cite facial recognition as a vital

anti-theft measure. The United Kingdom-based research firm Opinion Matters surveyed 300 senior retail leaders in the U.S. and the U.K. about their top business challenges and the most effective solutions. Respondents listed the current “theft crisis” among their top concerns.

“Facial recognition technology was said to be the most effective measure deployed to date among food retailers, followed by security guards,

“

## NEW RESEARCH REVEALS THAT SENIOR RETAIL EXECUTIVES CITE FACIAL RECOGNITION TECHNOLOGY AS A VITAL ANTI-THEFT MEASURE.

license plate recognition technology, and RFID tags, respectively,” according to *Progressive Grocer*.

At least 15 of the top 50 U.S. grocery stores now use facial recognition technology.

Violent organized retail crime (ORC) thieves and other criminals





## VIOLENT ORGANIZED RETAIL CRIME THIEVES AND OTHER CRIMINALS STOLE \$112.1 BILLION FROM RETAILERS IN 2022, ACCORDING TO THE NATIONAL RETAIL FEDERATION.

stole \$112.1 billion from retailers in 2022, according to the National Retail Federation. The public is understandably concerned about their safety in stores. Since 2022, criminals have killed more than 1,100 customers, employees and security personnel in U.S. retail settings, according to industry

publication *D&D Daily*. A similar dynamic is playing out on the international stage. In April, U.K. Prime Minister (at the time) Rishi Sunak announced a £55.5 million (\$70.5 million) facial recognition program to combat unprecedented retail theft and violence.

It should come as no surprise that retailers have turned to facial recognition in greater numbers, given the widespread adoption by consumers and government agencies. A majority of Americans surveyed by independent polling







firm Schoen Cooperman Research supported facial recognition's enhanced safety benefits and accuracy. Sixty-eight percent of respondents said the technology can make society safer.

In May 2023, the Transportation Security Administration (TSA) announced a \$128 million expansion of its passenger biometric checkpoints in U.S. airports. Then, in January 2024, TSA officials announced the facial recognition program would grow from nearly 60 airports to more than 400.

The public's embrace of the technology may be driven even more by its use at sports and entertainment venues. Major League Baseball has implemented facial recognition for ticketing and entry in some of its ballparks, with a planned expansion to more stadiums, and Universal



**THE PUBLIC'S EMBRACE OF THE TECHNOLOGY MAY BE DRIVEN EVEN MORE BY ITS USE AT SPORTS AND ENTERTAINMENT VENUES.**



**THERE REMAIN VOCAL OPPONENTS OF ALL FACIAL RECOGNITION USES, BUT IT IS IMPORTANT TO NOTE THAT RECENT EFFORTS TO RESTRICT THE TECHNOLOGY HAVE TENDED TO FAIL BECAUSE OF A LACK OF PUBLIC SUPPORT.**

has a new billion-dollar theme park opening in Orlando, Fla., next year that will use facial recognition for guest admissions, concessions and restaurants.

Retail and other commercial users of facial recognition

technology also have noted the state-driven trend toward expanded facial recognition use with guardrails for consumer privacy. Commercial use of facial recognition is legal in all 50 states, though the 2008 Illinois Biometric Information Protection Act severely restricts applications in that state. As of July 2024, 20 U.S. states have general data privacy laws that protect consumer privacy while permitting retailer use of facial recognition for life safety, security and loss prevention purposes. Of





course, there remain vocal opponents of all facial recognition uses, but it is important to note that recent efforts to restrict the technology have tended to fail because of a lack of public support.

Currently, there is no nationwide U.S. data privacy law, and no further action in Congress is expected on the proposed American Privacy Rights Act (APRA) until after the November 2024 elections. In May 2023, a Federal Trade Commission (FTC) policy statement reinforced facial recognition technology's continued expansion for retail use

cases. Seven months later, in December 2023, the FTC addressed the need for safeguards related to facial recognition technology use.

There remains an urgent need to take action against increasing threats and protect innocent retail employees and customers. To act fairly, retailers must identify the relatively few individuals responsible for the overwhelming majority of threats. Retailers and other commercial users are finding the most effective and accurate way to do this is by using AI-driven facial recognition technology with appropriate human oversight. ◀



U.S. Customs and Border Protection (CBP) has “processed more than 540 million travelers using biometric facial comparison technology” at U.S. air, land and sea ports of entry and “prevented more than 2,000 impostors from entering the United States,” according to the agency.



# What AI Means for Physical Security

Managing risk is essential to leveraging this emerging technology

**LARGE LANGUAGE MODELS (LLMs)** have recently taken the world by storm. Only months after OpenAI launched its artificial intelligence (AI) chatbot, ChatGPT, it amassed more than 100 million users. This makes it the fastest-growing consumer application in history.

And there is little wonder why. LLMs can do everything from answering questions and explaining complex topics to drafting full-length movie scripts and even writing code. Because of this, people everywhere are both excited and worried about the capabilities of this technology.

Although LLMs have recently become a hot topic, it is worth noting that the technology has been around for a long time. With advancements underway, however, LLMs and other AI tools are creating new opportunities to drive greater



Florian Matusek (fmatusek@genetec.com) is the Director of AI Strategy for Genetec (www.genetec.com).



automation across various tasks. Having a grounded understanding of AI limitations and potential risks is essential.

### **CLARIFYING THE TERMINOLOGY**

Artificial intelligence, machine learning, deep learning and other terms are often discussed, but what are the differences?

- **Artificial intelligence:** The concept of simulating human intelligence through machines. It refers to tools and processes that enable machines to learn from experience and adjust to new situations

without explicit programming. In a nutshell, machine learning and deep learning both fall into the category of artificial intelligence.

- **Machine learning:** AI that can automatically learn with little human involvement.
- **Deep learning:** A subset of machine learning that uses



**LLMS CAN DO EVERYTHING FROM ANSWERING QUESTIONS AND EXPLAINING COMPLEX TOPICS TO DRAFTING FULL-LENGTH MOVIE SCRIPTS AND EVEN WRITING CODE.**





## ONE OF THE BEST WAYS TO CAPITALIZE ON AI ADVANCES IN PHYSICAL SECURITY IS BY IMPLEMENTING AN OPEN SECURITY PLATFORM.

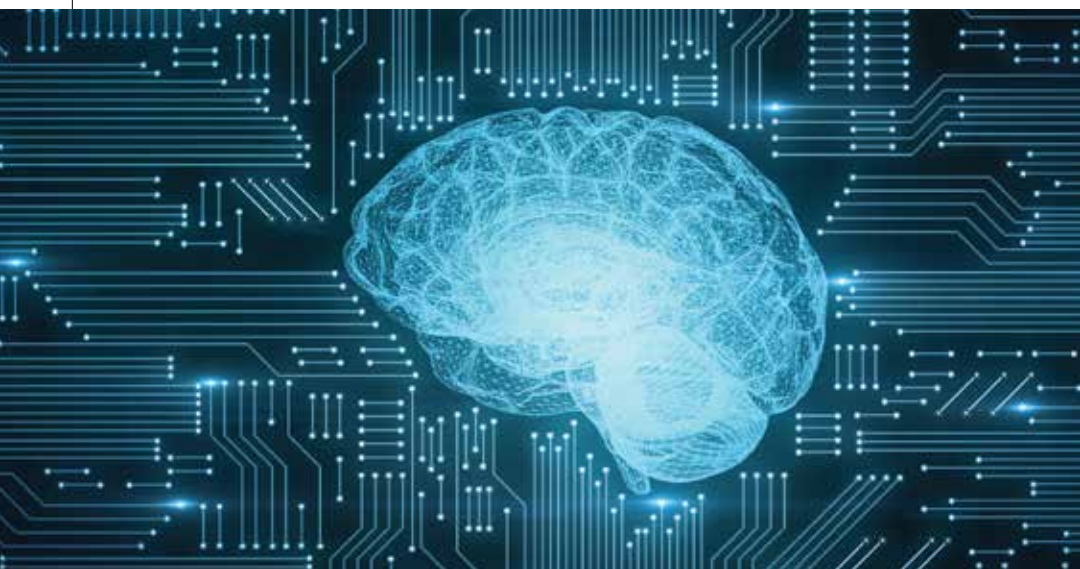
artificial neural networks that learn based on large amounts of data.

- **Natural language processing:** The process of using AI and machine learning to understand human language and automatically perform repetitive tasks such as spellcheck, translation and summarization.

- **Generative AI (Gen-AI):** Enables users to quickly generate content based on a variety of inputs, such as text and voice, resulting in outputs in the form of images, video and other types of data.
- **Large language model (LLM):** A type of Gen-AI that can perform natural language processing and is trained on vast amounts of data.

### **ARTIFICIAL INTELLIGENCE VS. INTELLIGENT AUTOMATION**

Automation is when tasks, whether easy or hard, are done without the





involvement of a person. Once a process is set up in a program, it can repeat itself whenever needed, always producing the same result.

Traditional automation requires a clear definition from the start. Every aspect, from input to output, must be carefully planned and outlined by a person. Once defined, the automated process can be triggered to operate as intended.

Intelligent automation (IA) allows machines to tackle simple or complex processes, without these processes needing to be explicitly defined. IA typically uses Gen-AI and natural language processing to suggest ways to analyze data or take

actions based on existing data and usage patterns.

## **RISKS OF LARGE LANGUAGE MODELS**

When weighing the risks of LLMs, it is important to consider that LLMs are trained to satisfy the user as their first priority. LLMs also use an unsupervised AI training method to feed off a large pool of random data from the Internet. This means the answers they give are not always accurate, truthful or bias-free. All of this can become dangerous in a security context.

This unsupervised AI method has opened the door to what are now called “hallucinations,” which occur when an AI model



## **KEY DIFFERENCES BETWEEN AI AND IA:**

- ▶ Artificial intelligence is a tool; intelligent automation is about outcomes
- ▶ Where AI is the means, IA is the ends
- ▶ AI is combined with other tools, such as automation, to achieve an outcome, which is IA



## AS AI EVOLVES, IT GREATLY EXPANDS THE RISK OF USING PERSONAL INFORMATION IN WAYS THAT CAN INTRUDE ON PRIVACY.

generates answers that seem plausible but are not factual or based on real-world data.

Using LLMs can also create serious privacy and confidentiality risks. The model can learn from data that contain confidential information about people and companies. And since every text prompt is used to train the next version, someone prompting the LLM about similar content might become privy to sensitive information through AI chatbot responses.

Then there are the malicious abuses of this AI technology. Consider how bad actors with little or no programming knowledge could ask an AI chatbot to write a script that exploits a known vulnerability or provide a list of ways to hack specific applications or protocols. One cannot help but wonder how these technologies could be exploited in ways that have not yet been anticipated.

### LEVERAGING AI IN PHYSICAL SECURITY

AI-enabled applications are advancing in new and exciting ways. They show great promise in helping organizations achieve specific outcomes that increase productivity, security and safety.

One of the best ways to capitalize on AI advances in physical security is by implementing an open security platform. Open architecture gives security professionals the freedom to explore AI applications that drive greater value across their operations. As AI solutions come to market, leaders can try out these applications, often for free, and select the ones that best fit







their objectives and environment.

As new opportunities emerge, so do new risks. That is why it is important to partner with organizations that prioritize data protection, privacy and the responsible use of AI. This will not only help enhance cyber resilience and foster greater trust in an organization, it is also part of being socially responsible.

Since AI algorithms can process large amounts of data quickly, AI is becoming an increasingly important tool for physical security solutions. But as AI

evolves, it greatly expands the risk of using personal information in ways that can intrude on privacy. The three pillars below can provide guidance when developing or evaluating AI solutions.

### ***Privacy and data governance***

Only use datasets that respect relevant data protection regulations. Wherever possible, ethically source, anonymize and securely store data used for training machine learning models. Treat datasets with the utmost care and keep data protection



## IN A PHYSICAL SECURITY CONTEXT, PRIORITIZING HUMAN-CENTRIC DECISION-MAKING IS CRITICAL.

and privacy top of mind. This includes sticking to strict authorization and authentication measures to ensure the wrong people do not get access to sensitive data and information across AI-driven applications.

### ***Trustworthiness and safety***

When developing and using AI models, always think about how to minimize bias. Ensure that AI models are rigorously tested and that accuracy is continuously

improved. Finally, make sure AI models are easily explainable. When AI algorithms deliver an outcome, one should be able to see exactly how it reached that conclusion.

### ***Humans in the loop***

AI models cannot make critical decisions on their own. A human should always have the final say. In a physical security context, prioritizing human-centric decision-making is critical. Machines simply cannot grasp the intricacies of real-life events like a security operator, so relying solely on statistical models is not an option. Systems should always drive insights to enhance human capacity for judgment.

AI models can inadvertently produce skewed decisions or results based on various biases. This can affect decisions and ultimately lead to discrimination. While AI has the power to revolutionize how work in the security industry and beyond is done and how decisions are made, it needs to be deployed responsibly. ◀





# Grow Your Expertise. Grow Your Career.

SIA's Programs for Security Professionals



**Security Project Management Training**

**The SICC: Cybersecurity for Physical Security Pros**

**Become a Certified Security Project Manager (CSPM)**

**GrantED: Identify and Obtain Grant Funding**

**SIAcademy: Online and Live Training**



Explore SIA's Training & Certification Programs





# SNG™

## SECURING NEW GROUND®

Oct. 8-9, 2024 | New York City

### The Business of Security

#### Featured Speakers:



**Rob Aarnes**  
President  
ADI Global Distribution



**Ann Fandozzi**  
CEO  
Convergint



**Dan Bresingham**  
CEO  
Everon



**Steve Jones**  
CEO  
Allied Universal



**Filip Kaliszan**  
CEO  
Verkada



**Sergio Castillejos**  
Vice President and  
General Manager  
Honeywell Commercial  
Security



**George Oliver**  
Chairman and CEO  
Johnson Controls



**Martin Huddart**  
Senior Vice President and  
Head of Physical Access  
Control Solutions  
HID



**Tara Dunning**  
Vice President of Global  
Security  
Wesco



Scan Here  
For More Info

[securingnewground.com](https://securingnewground.com)