SIA
TECHNOLOGY
Insights
Fall 2026
Volume 14, Number 2

AI for LP

Agentic platforms enhance retail security and operations

Page 20

Nuts and Bolts

Protection starts with secure fasteners

Page 32

All Aboard

Security at sea presents unique challenges

Page 50

Find the Power

Remote security requires careful energy planning

Page 62

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

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

SIA

Explore SIA's Training & Certification Programs

TECHNOLOGY
Insights

Fall 2026 Volume 14, Number 2

4

Advancing Beyond Video Surveillance
Proactive visual security is transforming monitoring centers
Wes Usie, CHeKT

12

Maintaining Security While Expanding Business
A growing portfolio needs a security standard that travels with it
Eric Hatty, Total Security Solutions

20

What Nobody Tells You About Deploying Agentic AI
How to set up for program success
Alexandria Hewko, Solink

26

From Analytics to Intelligence
GenAI is adding context and reasoning to video security
Matthew Cirnigliaro, IQSIGHT

32

Big Failures Start Small
Something as simple as a bolt can cause a costly cascade
Marcus Tonndorf, Hexlox

From Loss Prevention to Retail Visibility
How RFID, EAS and video analytics are reshaping store security
Joe Coll, Global Security Solutions
38

Taking AI to Sea
How rapid edge deployment is transforming maritime safety
Tom Larson, Velasea
50

Context Is Key in Alarm Response
Emerging technologies can turn information into intelligence
Peter Giacalone, 3Si
56

The Hidden Factor in Mobile Surveillance Reliability
Power design determines whether off-grid cameras will work when it matters most
Colin DePree, Mobile Pro Systems
62

The Most Valuable Asset You're Not Measuring
Monitoring contracts anchor a dealer's value and need a disciplined approach
Naomi Withers, Loyva
72

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.

Advancing Beyond Video Surveillance

Proactive visual security is transforming monitoring centers

Wes Usie (wusie@chekt.com) is the President and Founder of CHeKT (www.chekt.com).

For decades, video surveillance has been one of the cornerstones of electronic security. Yet, despite advances in camera technology, many systems continue to operate in much the same way they did years ago: recording events for later review rather than helping prevent incidents in real time. Today, that model is rapidly changing.

The security industry is undergoing a fundamental shift from reactive surveillance to proactive visual security, powered by artificial intelligence, cloud-based analytics, and real-time video verification. Increasingly, monitoring centers, security integrators, and end users are recognizing that simply collecting video footage is no longer enough. The future belongs to systems that can interpret activity, identify threats, and enable intervention before incidents escalate.

This evolution is creating new opportunities for monitoring centers while helping solve some of the industry's most persistent challenges.

> THE FUTURE BELONGS TO SYSTEMS THAT CAN INTERPRET ACTIVITY, IDENTIFY THREATS, AND ENABLE INTERVENTION BEFORE INCIDENTS ESCALATE.

REACTIVE SECURITY IS NO LONGER ENOUGH

Traditional security systems are reactive by design. Cameras record activity, alarms generate alerts, and operators respond when a signal is received. While this model has served the industry for decades, it has become increasingly strained by a growing number of alarms, staffing challenges, and customer expectations.

False alarms remain one of the most significant issues facing monitoring centers. Excessive false dispatches have overwhelmed law enforcement agencies in many jurisdictions, leading cities and municipalities to adopt alarm verification

> UNLIKE TRADITIONAL SURVEILLANCE SYSTEMS THAT SIMPLY RECORD ACTIVITY, VISUAL INTELLIGENCE PLATFORMS USE ARTIFICIAL INTELLIGENCE AND ANALYTICS TO CONTINUOUSLY EVALUATE WHAT THE CAMERA SEES.

requirements before dispatching officers. End users are also feeling the impact, with many facing costly fines and growing frustration over nuisance alarms.

At the same time, human monitoring has limitations. Studies have shown that operators monitoring multiple video feeds simultaneously can miss a substantial percentage of events. As camera counts continue to grow, expecting operators to manually identify every potential threat becomes increasingly unrealistic.

The result is a reactive security model that often suffers from alert fatigue, delayed response times, operational inefficiencies, and dissatisfied customers. In an environment where one missed event can have significant consequences, the industry needs a better, more reliable, and proactive approach

THE EMERGENCE OF VISUAL INTELLIGENCE

Proactive visual security represents the next stage in the evolution of video monitoring. Unlike traditional surveillance

systems that simply record activity, visual intelligence platforms use artificial intelligence and analytics to continuously evaluate what the camera sees. Rather than treating every motion event as a potential threat, these systems can distinguish between meaningful activity and environmental noise.

This allows monitoring centers to focus attention on verified events that require action rather than sorting through an endless stream of false positives. More importantly, visual intelligence transforms cameras from passive recording devices into active security assets capable of delivering actionable information in real time.

This shift is one reason industry analysts project continued growth in the commercial security market through the end of the decade. AI has become a primary area of investment for security technology providers, while predictive analytics and automated event verification are increasingly viewed as essential components of next-generation security solutions.

THE IMPACT ON MONITORING CENTERS

One of the most immediate advantages of visual intelligence for monitoring centers is alarm reduction. By leveraging AI-powered analytics and video verification, monitoring operators receive fewer nuisance alerts and spend more time focusing on legitimate security events. This creates a more efficient operation and improves operator effectiveness.

Proactive visual security also enhances response capabilities. Instead of receiving a simple alarm signal, operators gain access to visual context that helps determine whether a threat is real and what actions should be taken. This enables faster decision making and more accurate communication with customers, guards, and first responders.

Verified events also carry greater credibility with law enforcement and emergency responders, particularly in jurisdictions that prioritize verified alarms for dispatch. For monitoring providers competing in an increasingly crowded marketplace, these

capabilities create valuable service differentiation.

NEW MANAGED SERVICES OPPORTUNITIES

The rise of proactive visual security is also accelerating the industry's transition to recurring revenue-based service models. Cloud-based, camera-agnostic platforms allow monitoring providers and integrators to layer advanced intelligence onto existing camera infrastructure without requiring customers to replace hardware. This software-centric approach creates opportunities for ongoing managed services rather than one-time installation projects.

Instead of selling cameras alone, providers can offer continuous threat detection, video verification, remote guarding support, proactive intervention, and advanced analytics as subscription-based services. The result is a more predictable revenue stream and stronger long-term customer relationships.

For many integrators and monitoring companies, proactive visual security

represents a path toward higher-margin recurring monthly revenue while delivering greater value to customers.

EVOLVING CUSTOMER EXPECTATIONS

Customer expectations are also changing. Residential users increasingly expect security systems to

> CLOUD-BASED, CAMERA-AGNOSTIC PLATFORMS ALLOW MONITORING PROVIDERS AND INTEGRATORS TO LAYER ADVANCED INTELLIGENCE ONTO EXISTING CAMERA INFRASTRUCTURE WITHOUT REQUIRING CUSTOMERS TO REPLACE HARDWARE.

provide verified alerts, active deterrence, and intelligent filtering that reduces unnecessary notifications. Consumers have become accustomed to smart technology that can distinguish between meaningful activity and routine events. For example, a homeowner may receive dozens of motion notifications each week from passing cars, blowing branches, or neighborhood activity. Traditional systems often treat each event equally, but proactive visual security platforms can use AI to distinguish between, say, a delivery driver approaching the front door and genuinely suspicious activity, such as a person lingering near a vehicle or attempting to access a backyard, ensuring that only meaningful events generate alerts.

Commercial customers are taking an even broader view. Many organizations no longer see security solely as a cost center. Instead, they expect security investments to generate measurable business value. Take, for example, a large distribution center with hundreds of employees, dozens of loading docks, and continuous vehicle traffic. While cameras in this environment are deployed primarily for security, AI-powered visual intelligence can also help managers

identify operational inefficiencies, such as delivery bottlenecks, unauthorized access to restricted areas, safety compliance violations, or excessive dwell times at loading docks.

Visual intelligence platforms can offer operational insights, support compliance initiatives, improve situational awareness, and enhance overall organizational resilience. In many cases, the same cameras protecting a facility can also provide information that improves business operations. This expanded value proposition is helping security move beyond traditional loss prevention and into a more strategic role within organizations.

AI-POWERED VISUAL INTELLIGENCE CAN ALSO HELP MANAGERS IDENTIFY OPERATIONAL INEFFICIENCIES, SUCH AS DELIVERY BOTTLENECKS, UNAUTHORIZED ACCESS TO RESTRICTED AREAS, SAFETY COMPLIANCE VIOLATIONS, OR EXCESSIVE DWELL TIMES AT LOADING DOCKS.

THE FUTURE IS PROACTIVE

As the industry continues to evolve, one reality is becoming increasingly clear: Monitoring centers can no longer rely solely on reactive workflows designed for the analog era. The growing volume of alarms, rising customer expectations, staffing challenges, and demand for verified response are pushing the industry toward a more intelligent approach.

Proactive visual security addresses these challenges by combining AI-driven analytics, real-time verification, and actionable intelligence to help monitoring centers identify threats sooner, respond faster, and deliver greater value.

The future of security is no longer about watching video; it is about understanding what the video means and taking action before an incident becomes a crisis. That shift from surveillance to visual intelligence may prove to be one of the most significant transformations the monitoring industry has seen in decades. ◀

Maintaining Security While Expanding Business

A growing portfolio needs a security standard that travels with it

Eric Hatty (ehatty@tssbulletproof.com) is Chief Commercial Officer at Total Security Solutions (www.tssbulletproof.com).

Opening a new business location is a win that indicates your hard work is paying off. Yet, growth puts pressure on every system, and physical security is among the most vulnerable to variation.

New locations bring different contractors, different specifiers, and design teams working from different starting points. Add a construction deadline and a stretched budget, and security decisions can end up reflecting the pressures of the moment rather than your building's needs. Over time, what you are left with is a portfolio in which some locations were thoughtfully protected while others have gaps that nobody planned for.

The good news is that this is a solvable problem. One that requires treating security less like a separate line item for each individual project and

more like a standard that the organization carries forward.

NO TWO LOCATIONS ARE THE SAME

Consider a bank with branches in two communities, one rural and one urban. The rural branch may see a handful of customers on a slow afternoon, on a relatively calm street. The urban branch may serve hundreds of people a day, operate extended hours, and face more exposure to potential crime or disturbance. Both banks need protection. But the right configuration of ballistic barriers, transaction windows, and access points will vary.

> THE GOAL IS TO MAINTAIN CONSISTENCY IN THE PROCESS – ASKING THE SAME QUESTIONS EACH TIME – SO THAT SECURITY IS TAILORED TO EACH SITE.

Healthcare tells a similar story. A large hospital with a busy emergency department, multiple public entrances, and a behavioral health unit has different needs than a medical office with a single reception desk. Designing both facilities to the same specification would

> ONE OF THE MOST USEFUL THINGS A GROWING ORGANIZATION CAN DO IS ESTABLISH, IN ADVANCE, HOW IT WILL EVALUATE THE SECURITY REQUIREMENTS OF EVERY NEW FACILITY.

likely mean misallocating resources in one direction or the other.

Corporate real estate adds its own nuance. An organization's headquarters, where senior executives are present daily and public visibility is high, warrants a separate conversation from a regional satellite office with limited walk-in access and a lower exposure profile.

A new location should not be treated as a completely unique project, though. The goal is to maintain consistency in the process – asking the same questions each time – so that outcome is tailored to each site.

MAKING SECURITY DECISIONS UNDER PRESSURE

A new facility is nearing completion, and someone realizes the ballistic barrier specification has not been finalized. There is a deadline to meet, a tight budget, and a contractor waiting on answers.

In that moment, one of two things tends to happen.

In the first scenario, the team defaults to a higher level of protection than the

building's threat profile calls for. A newer, smaller office in a lower-exposure area ends up specified to the same standard as a long-established location with a very different footprint and history. Material and installation costs climb. Beyond immediate cost, it sets an expectation across the portfolio that is difficult to level-set later.

Alternatively, the specifications around protection are trimmed to fit the timeline. A reception area that regularly handles sensitive transactions or serves a high-volume, unpredictable public gets a standard glazing system instead of a rated ballistic barrier because there was not enough time to source and sequence the right solution. The facility opens, and the gap becomes part of the building.

Neither outcome reflects poor intentions, and both are understandable given the circumstances. Each scenario is avoidable when the security conversation starts earlier in the process, as part of the same planning discussion that is already underway about finishes, fixtures and building systems.

A CONSISTENT ASSESSMENT FRAMEWORK

One of the most useful things a growing organization can do is establish, in advance, how

it will evaluate the security requirements of every new facility. It can use a shared set of questions that travels from project to project, regardless of location, contractor or design team. For example:

- What threats are you planning for? Ballistic? Forced entry? Both?
- Are there access points that put staff in regular contact with people who may be in distress?
- Does the facility handle cash, controlled substances, or sensitive personal data?
- What does the surrounding environment look like, and has it changed in recent years?

Asking the questions consistently turns a one-time judgment call into an organizational standard. Leadership can stand behind, build on, and return to protection decisions as the portfolio expands.

Take a growing organization where senior executives split time across multiple offices. As threats to corporate leadership increase, the question of who occupies which space and how exposed they are becomes part of every new location decision. An assessment framework makes that

question standard practice, ensuring protection levels follow the people and the risk.

> SECURITY INSTALLATION THAT IS TREATED AS AN AFTERTHOUGHT TENDS TO BE DELIVERED LIKE ONE.

COORDINATED SPECIFICATION FOR A COHERENT PORTFOLIO

Once you have that clear picture of what you are protecting against, the next challenge is maintaining consistency across a portfolio that may involve multiple architects, contractors and design teams who are each working from their own starting points.

The organizations that navigate this well tend to share one approach. They work with a single architect or design engineer who develops and owns the ballistic glazing, framing and door specifications across all locations. Every new project starts from that shared framework. Site-specific conditions can shape how it gets applied while the baseline travels forward.

For a bank rolling out new branches, this typically begins with the teller line.

Ballistic fiberglass countertops, transaction windows, currency trays, and package passers are tested to established performance standards. From there, the framework extends naturally into private offices, flexible meeting areas, and any spaces that carry elevated risk.

Your team can start the foundational work from the first project.

SECURITY BELONGS IN THE BUILD SCHEDULE

Security installation that is treated as an afterthought tends to be delivered like one. When ballistic systems are added after a facility is already built and occupied, the process is more disruptive, and there is often a window of reduced security between opening day and the day the protection is in place.

Planning security installation alongside construction closes that gap. The timeline is clearer, and the facility is fully secure when it opens.

For organizations running multiple projects simultaneously, that coordination gives security providers the visibility to sequence fabrication and delivery across sites.

The real payoff, though, is consistency. Employees move from one location to the next knowing the same standard of protection is in place, even

if they do not see it. They are not wrestling with doors that are too heavy to open or straining to hear customers through a transaction window that was not specified for the space. Protection works because it was planned for the building.

GROWTH AND SECURITY MOVING TOGETHER

Research shows that 54% of workers do not fully trust their company's leadership or HR department to create a safe work environment. Growth gives organizations a chance to change that narrative.

When physical security is treated as a standard the organization carries forward, it is both a risk management decision and a cultural choice. Employees arrive at a new location on Day 1 knowing their safety was part of the plan. Leadership opens a new site with confidence that the care invested in every previous location is present in this one, too. That sense of confidence, felt on both sides, is what a thoughtful security program makes possible. ◀

WHEN PHYSICAL SECURITY IS TREATED AS A STANDARD THE ORGANIZATION CARRIES FORWARD, IT IS BOTH A RISK MANAGEMENT DECISION AND A CULTURAL CHOICE.

What Nobody Tells You About Deploying Agentic AI

How to set up for program success

Every business leader has heard some version of the same pitch in the past two years.

Artificial intelligence will transform your security or loss prevention program. It will surface incidents before they escalate, eliminate manual review, and give your team visibility that was never possible before.

In many respects, that pitch is accurate – as long as the right structure is in place.

WHAT AGENTIC AI ACTUALLY IS

Agentic AI is often lumped in with smart tools that can simply flag or explain what happened. The real difference is that agentic systems are able to intelligently interpret and act on what they find. It reasons through a signal, decides on the appropriate response, and executes a

Alexandria Hewko (ahewko@solinkcorp.com) is Senior Product Marketing Manager and GTM Strategist for Solink (www.solink.com).

workflow, whether that means restocking a bestseller before it sells out, rerouting staff to a checkout lane before a line builds, or notifying emergency response during a security event, all without a human having to intervene. It can also investigate further before confirming a decision or action.

But vendor conversations about agentic AI tend to focus on what the technology can do in a well-configured environment. What they rarely address is the condition of the environment most operators are starting from. Several factors must be considered.

> THE MOST VISIBLE REASON FOR FAILURE IS PHYSICAL INFRASTRUCTURE.

Hardware and Connectivity

The most visible reason for failure is physical infrastructure. Agentic AI depends on what its cameras and sensors can actually see. A system trained to detect a non-scan at self-checkout requires a camera positioned at the correct angle with sufficient resolution above the

> THE MORE DATA SOURCES AN AGENTIC SYSTEM CAN DRAW FROM, THE RICHER THE CONTEXT IT HAS FOR DECISION MAKING.

register. A perimeter agent that cannot distinguish a delivery driver from a threat actor in low light will not be able to protect anything.

Data Quality

Like any other intelligent system, agentic AI can only assess trends based on the data to which it has access. Retailers with unfinished or siloed data will still get a working program, just one that delivers a narrower and less accurate view than the technology is capable of.

Context Depth

Video-only solutions limit what an agentic system can become. Even the best video AI can only tell you what it sees within the frame, and a lot of the context that actually drives good decisions lives outside it. The more data sources an agentic system can draw from, the richer the context it has for decision making. A system with access to video, transaction records, access logs, scheduling data, and prior incident history can understand deeper trends and deliver more accurate and more relevant insights. Organizations that treat data availability as an afterthought are restricting what their AI investment can deliver.

Alignment on Outcomes

Before deployment, leaders need to define not just what the system will detect, but what the organization will do about it and why that insight or action matters to the business. For example, a behavioral detection solution that flags a potential shoplifter in real time has no value if the response is undefined. Will employees approach? Will the system build a case automatically? Will it feed a pattern analysis across locations? Those decisions about the intended action belong to humans, and AI agents can only act effectively once they have those guardrails. The same is true for measuring whether any of it is working. Defining how much impact the program is expected to make and how outcomes will actually be quantified is a human responsibility that no AI system can substitute for.

AGENTIC AI IS NOT JUST A SECURITY TOOL

The instinct to frame AI investments through a security and

> LIMITING AGENTIC AI TO THE SECURITY FUNCTION IS ONE OF THE MORE EXPENSIVE MISTAKES A MULTI-SITE OPERATOR CAN MAKE.

> AGENTIC AI SHOULD NOT REQUIRE A FULL TECHNOLOGY OVERHAUL TO PROVE ITS WORTH. THE BEST SOLUTIONS MEET OPERATORS WHERE THEY ARE TODAY AND BUILD FROM THERE.

loss prevention lens is understandable. That is where people naturally go when they think about security cameras, and the use cases are genuinely compelling. But limiting agentic AI to the security function is one of the more expensive mistakes a multi-site operator can make.

The same camera infrastructure and data integrations that power a refund fraud detection workflow can also serve a marketing team trying to understand how a promotional display is performing on the floor. The same behavioral pattern recognition that flags a break-in in progress can tell an operations leader whether staff are following best customer experience practices during peak hours. The same perimeter monitoring that protects a site after hours can give a human resources team data on whether opening and closing procedures are being executed consistently across locations.

Agentic AI is, at its core, a tool for turning physical world activity into structured, actionable intelligence. The security use case is well understood because it was first. But the underlying capability does not belong to any single department.

WHERE TO GO FROM HERE

AI adoption pressure is everywhere right now. But this is not the first time an industry has faced this exact pattern. Early e-commerce went through the same cycle with an initial rush

of hype, then years of unglamorous backend work that most companies quietly skipped, followed by a real payoff for the few who actually did it. Point-of-sale digitization repeated that same arc a decade later. What separated the winners was choosing a specific, high value problem to solve and delivering on it well.

Security professionals should start by addressing these questions:

- What tasks are being repeated manually that follow a consistent pattern?
- What is the one insight that could unlock growth for your business, if only you could find it?
- Where are processes slow because someone is waiting on data or input from another team?
- Where is information that exists in the business hard to access when it is actually needed?
- Where are decisions being delayed because the right context never surfaces in time?
- Where are teams duplicating effort because outputs from one function never reach the other?

The answers to these questions will point to where agentic AI creates real, defensible value for a business.

From there, leaders should prioritize vendors that can deliver meaningful results within the first 30 days using the infrastructure already in place. Agentic AI should not require a full technology overhaul to prove its worth. The best solutions meet operators where they are today and build from there. This technology is not reserved for enterprise programs with unlimited resources. It is an accessible tool, and the businesses that treat it that way are the ones that get the most out of it. ◀

From Analytics to Intelligence

GenAI is adding context and reasoning to video security

Matthew Cirnigliaro (matthew.cirnigliaro@iqsight.com) is the Head of Product Marketing – North America at IQSIGHT (https://www.iqsight.com).

Every security alert tells a story, but some tales only go as deep as the introduction.

Today, many security tools fail to deliver the context needed to empower teams to quickly understand the full story, slowing decision-making and response. When security operators are faced with multiple alarms, they need the narrative in order to move with speed and precision.

Current edge-based analytics excel at spotting objects, like a brandished weapon or a fence-hopper, but they lack the ability to explain the scene. The heavy lifting of interpreting the data and deciding what to do still falls entirely on operators.

But what if cameras did not just flag events, but actually understood them? By marrying edge-based video analytics with cloud-based large language models (LLMs), the industry is moving beyond simple detection into an era of true human-like interpretation. This technology can help users extract meaningful information from video footage, understand unfolding events,

and make faster, more informed decisions.

THE GenAI SHIFT

Generative artificial intelligence (GenAI) transcends basic object detection, interpreting complex environments to provide insights. With simple, user-defined prompts, GenAI-enabled video solutions can generate detailed descriptions of events or scenes, much like a human operator, without requiring training on specific objects or behaviors.

These solutions not only produce the descriptions but understand them as well, using the information to determine whether or not to send an alarm to a human operator. The human is brought into the loop only when events need attention.

> CURRENT EDGE-BASED ANALYTICS EXCEL AT SPOTTING OBJECTS, LIKE A BRANDISHED WEAPON OR A FENCE-HOPPER, BUT THEY LACK THE ABILITY TO EXPLAIN THE SCENE.

GenAI-enabled video solutions are highly customizable, making them adaptable to most industries. Prompts can be open-ended or specific, indicating what to monitor and giving context to any situation. Users can inquire whether or not there are any safety hazards present,

> GenAI-ENABLED VIDEO SOLUTIONS CAN GENERATE DETAILED DESCRIPTIONS OF EVENTS OR SCENES, MUCH LIKE A HUMAN OPERATOR, WITHOUT REQUIRING TRAINING ON SPECIFIC OBJECTS OR BEHAVIORS.

if an emergency vehicle has arrived on scene, or if a crowd has formed in an area.

Imagine automatically identifying blocked aisles in warehouses or retail stores, improper material handling at industrial sites, runway readiness at airports, vandalism, theft, or other safety and security issues. Timely alerts improve safety and efficiency by helping professionals address risks before they escalate. These solutions offer versatility across industries, for airports, schools and universities, factories, logistics centers, city traffic management, retail locations, and more. They provide insights to help users distinguish between critical events and routine activity, empowering security, safety and operations teams to work smarter.

One example is ATM vestibules being used as overnight shelters. For banks, this hinders their ability to provide customers with round-the-clock access to cash due

to concerns about safety, property damage and liability. While traditional motion-based video analytics struggle to detect a still person laying on the ground, GenAI-based solutions understand that an individual is present and can notify security personnel with a description of what is happening.

DIVERSITY OF USE CASES

The level of intelligence and understanding offered by GenAI can be used to provide context about behaviors that helps teams understand how to respond to incidents in a wide range of environments.

Smart Facilities

Traditional loitering detection alerts security teams to potential risks. A video solution that uses GenAI provides further insight into the situation. For example, it could inform an operator that a person stopped briefly to tie their shoe, is spraying graffiti on an external wall, is attempting to break into a vehicle in the parking lot, or appears to be injured or in distress.

Each of these events would prompt a different response from the personnel responsible for the security and safety of a building. The shoe-tying would likely result in no response or simple scene monitoring, while graffiti spraying or a vehicle break-in would prompt personnel to go to the location or contact local authorities. Similarly, the presence of an injured person would

> IMAGINE AUTOMATICALLY IDENTIFYING BLOCKED AISLES IN WAREHOUSES OR RETAIL STORES, IMPROPER MATERIAL HANDLING AT INDUSTRIAL SITES, RUNWAY READINESS AT AIRPORTS, VANDALISM, THEFT, OR OTHER SAFETY AND SECURITY ISSUES.

> ALERTS TO SPECIFIC EVENTS, ENHANCED AWARENESS OF BEHAVIORS, AND RECOMMENDED RESPONSE PROTOCOLS CAN HELP TO BETTER EQUIP AND NOTIFY PERSONNEL WHEN A POTENTIAL PROBLEM ARISES.

trigger those trained in emergency response to provide support. Solutions using GenAI help users quickly determine if something needs attention. Understanding context enables informed decisions and better responses.

Industrial Safety

Edge-based analytics can detect idle objects or people in an aisle. GenAI goes further to provide additional information, such as alerting to an injured person laying on the ground. Using a reference image for comparison, the system can also watch for improperly stored pallets or materials or cluttered aisles that pose a hazard. A layered approach enhances safety and situational awareness.

Enhanced Retail Support

Beyond loss prevention, GenAI video solutions can support operations and logistics management. It can notify personnel about empty shelves that require a restock, helping ensure

sales opportunities are not missed due to lack of product. By automatically recognizing exceptions to normal states, the solution can alert staff when displays need attention or high-demand items are running low.

Intelligent Transit

Smart cities can benefit from the ability of GenAI to interpret traffic conditions. While edge-based analytics detect slow or stopped vehicles, solutions using GenAI can determine whether the congestion is caused by weather, a roadside fire, or a major accident. Understanding the cause of the vehicle backup helps the traffic monitoring center dispatch the appropriate personnel to the scene.

A NEW STANDARD FOR VISUAL INTELLIGENCE

GenAI video solutions provide the context that is the first layer of an event response, helping to automate the decision as to whether or not action is required based on user-defined prompts. When intervention is needed, integration into workflows can trigger systems that

will suggest responses. Alerts to specific events, enhanced awareness of behaviors, and recommended response protocols can help to better equip and notify personnel when a potential problem arises. Users can quickly identify the best course of action, resulting in streamlined decision-making and increased efficiency.

For industry leaders, GenAI can serve as a strategic differentiator. By combining detection with real-time interpretation, it delivers visual intelligence that helps ensure human oversight is focused exactly where and when it is needed most. ◀

Big Failures Start Small

Something as simple as a bolt can cause a costly cascade

Security systems rarely fail all at once. Instead, they fail one small part at a time. Then the individual pieces take each other down.

In the engineering world, this is called cascading failure. One component makes others weak. The load from one failed part shifts to what is next to it, which was not designed to carry that load, so it fails, too. The chain keeps going until the whole system is down.

One classic example is the 2003 Northeast blackout. It started with a single generating plant tripping offline in Ohio. The load redistributed to neighbouring lines, which overloaded and failed in sequence. Fifty million people lost power. The estimated damage was around $6 billion. The trigger was tiny. The outcome definitely was not.

The security industry knows this pattern. We just don't always call it by its name.

Marcus Tonndorf (marcus@hexlox.com) is the Founder and CEO of Hexlox (www.hexlox.com).

THREE CASCADES, ONE LESSON

In January 2024, a door plug blew out of a Boeing 737-9 at 14,830 feet. The NTSB's final report found the cause: Four bolts were removed during factory rework and never reinstalled. No removal record was created, so no inspection caught it. The plug crept upward flight after flight until it finally let go. A multi-million-dollar aircraft, certified systems, trained crews, undone by four missing fasteners and a paperwork gap.

> THE WEAK POINT IS VERY SELDOM THE MOST EXPENSIVE EQUIPMENT. IT IS THE SMALL, BORING, OVERLOOKED PART THAT HOLDS THE EXPENSIVE DEVICE IN PLACE.

Rail networks tell the same story from the security side. In 2025, thieves cut 600 meters of copper cable near Lille, France, overnight. Eurostar services were cancelled or severely delayed. In a U.K. case, meanwhile, a thief made roughly £1,000 selling

stolen cable, while the cost to Network Rail was over £164,500 and more than 3,000 minutes of train delays. Rail systems are designed to fail safe. Cut one cable and trains stop across an entire route. The thief attacks the cheapest component. The operator pays for the whole network.

The pattern is very often the same. The weak point is very seldom the most expensive equipment. It is the small, boring, overlooked part that holds the expensive device in place.

IDENTIFYING THE WEAK LINK

Walk through any modern security installation and you'll see cameras, fences, sensors, card readers, perimeter lighting, cable trays, control cabinets. Now look at how each one is mounted.

Almost all of it is held by standard bolts. The tools to open them cost a few dollars and fit in a pocket. We spend heavily on encryption, analytics, redundancy and certification, and then attach the hardware with

fasteners that anyone can open in seconds.

That mismatch matters much more than it seems and looks. A camera that can be unbolted is not just a stolen camera; it is a blind spot. And that blind spot enables the next intrusion. The intrusion takes out cabling or power. Now the monitoring is down, the response is delayed, and an incident that should have been contained becomes an outage. The cascade did not start in the control room. It started with a bolt head.

Attackers understand this intuitively and they learn fast. Copper thieves do not defeat the signalling system, they unbolt and cut their way to the cable. Component thieves do not pick locks, they carry a hex/Allen key.

THINK IN LAYERS, DOWN TO THE FASTENER

The fix is not one product. It is a mindset.

> WE SPEND HEAVILY ON ENCRYPTION, ANALYTICS, REDUNDANCY AND CERTIFICATION, AND THEN ATTACH THE HARDWARE WITH FASTENERS THAT ANYONE CAN OPEN IN SECONDS.

> A CAMERA THAT CAN BE UNBOLTED IS NOT JUST A STOLEN CAMERA; IT IS A BLIND SPOT.

Cascading failures are prevented by breaking the chain at its first link, and the first link is usually mechanical. Three practical steps can help prevent this:

- *Map your fasteners.* Do a walk-through of any critical installation and ask one question at every device: What is required to remove this? If the answer is "a standard tool from any hardware store," you have found an entry point for a cascade.
- *Protect the mounting layer.* Tamper-resistant and keyed fastening systems exist for exactly this purpose. They turn a 3-second removal into a loud, slow, tool-intensive job. Most theft and tampering is opportunistic. Raising the cost of the first step ends most attempts before they start.

- *Verify, don't assume.* The Boeing case failed on process, not technology. If a fastener is safety or security-critical, its installation should be documented and inspected like any other control.

The economics here are unusual. A tamper-resistant fastener costs a few dollars. The cascading failure it prevents would cost thousands, sometimes millions. Very few security investments have that ratio. Most of the industry still ignores it, though, because a bolt is not a product demo. It is just a bolt – until it is not.

Security has always worked in layers. We have simply drawn the bottom layer in the wrong place. It is not the fence or the camera. It is the bolt that holds them. Small components decide large outcomes. The industry that internalizes this will stop more cascades than any single system upgrade ever could. ◀

> SMALL COMPONENTS DECIDE LARGE OUTCOMES.

From Loss Prevention to Retail Visibility

How RFID, EAS and video analytics are reshaping store security

Joe Coll (joe.coll@global-security-solutions.com) is Chief Commercial Officer at Global Security Solutions (www.global-security-solutions.com).

Retail loss prevention has always been measured by what it could stop. Did the alarm sound? Was the merchandise protected? Was the incident captured on video?

Those questions still matter. Retailers continue to face theft, organized retail crime, internal loss, operational errors and pressure to protect high value merchandise across stores, distribution centers and the supply chain. But the conversation around security investments is changing. More retail leaders are now asking a broader question: How can this investment do more?

A technology that once may have been evaluated only as a theft deterrent is now expected to support visibility, reporting, inventory accuracy,

traffic insight, operational efficiency, and better decision making. Cameras are no longer viewed only as tools for reviewing incidents after the fact. Radio frequency identification (RFID) is no longer seen only as an inventory solution. Electronic article surveillance (EAS) is no longer evaluated only by whether it alarms at the door.

The future of retail security is not simply about adding more technology. It is about understanding what each system can see, what it cannot see, and how the right combination of technologies can turn loss prevention into a broader source of retail visibility and business insight. When used well, these systems can go beyond traditional loss prevention use cases and inform decisions across operations, merchandising, inventory planning, and customer experience.

> A TECHNOLOGY THAT ONCE MAY HAVE BEEN EVALUATED ONLY AS A THEFT DETERRENT IS NOW EXPECTED TO SUPPORT VISIBILITY, REPORTING, INVENTORY ACCURACY, TRAFFIC INSIGHT, OPERATIONAL EFFICIENCY, AND BETTER DECISION MAKING.

> RETAIL SECURITY CONVERSATIONS ARE SHIFTING FROM ISOLATED EVENT DETECTION TO CONNECTED VISIBILITY.

NEW QUESTIONS TO ANSWER

Retail environments are complex. Merchandise moves from distribution centers to stores, from stockrooms to shelves, from fitting rooms to exits, and in some cases, through online order fulfillment workflows. At each point, retailers are trying to answer basic but difficult questions.

- Where is the product?
- Was it received?
- Was it placed on the floor?
- Was it moved to the correct location?
- Was it purchased, misplaced, stolen or returned?
- Did customer behavior or store traffic contribute to the outcome?

Traditional loss prevention systems can answer some of these questions, but rarely all of them. An EAS alarm may indicate that protected merchandise is leaving the store. A video system may show who was near a display. Inventory systems may indicate that units are missing. Point-of-sale data may show what was purchased. But when these systems operate separately, the picture is often incomplete.

That is why retail security conversations are shifting from isolated

event detection to connected visibility. The goal is not only to identify a loss event, but to better understand how products, people and processes move through the retail environment.

This shift is especially important as retailers look for stronger returns on their investments. Security systems are no longer expected to serve only one department or a single use case. A camera may support investigations, but it may also provide traffic patterns, dwell time, queue visibility and heat mapping. RFID may support inventory accuracy, but it may also help identify product movement, replenishment needs, and chain of custody gaps. EAS may continue to deter opportunistic theft while working alongside other systems that provide a deeper understanding of what happened before, during and after an incident.

In other words, the strongest retail security programs are moving from detection alone to context.

MAXIMIZING RFID CAPABILITIES

RFID is one of the clearest examples of a technology whose perceived value is still evolving.

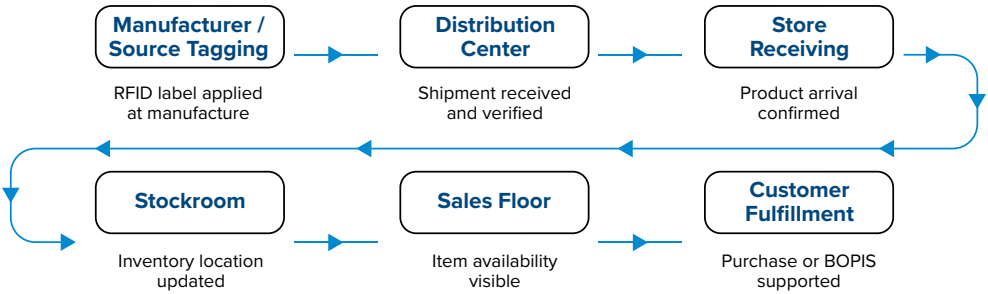
For years, many retailers associated RFID primarily with inventory counting. That use case remains

> WHEN RFID IS DESIGNED AROUND OPERATIONAL QUESTIONS, IT BECOMES MORE THAN A TAG OR READER. IT BECOMES A DATA SOURCE.

important. The ability to quickly identify items without line-of-sight scanning can improve inventory accuracy and reduce the labor required for manual counts. In today's omni-channel retail environment, that accuracy is no longer a nice-to-have. Customers expect reliable product availability across stores, e-commerce, and "buy online, pick up in store" workflows, and retailers need confidence that available inventory is where the system says it is. For many retailers, this visibility can begin before merchandise reaches the store through source tagging programs that apply RFID labels at the point of manufacture. But RFID's value extends beyond inventory accuracy alone.

Depending on the application, tag selection, reader placement, system design and supporting software, RFID can help teams across multiple departments gain visibility into item-level movement, pallet tracking, asset tracking, receiving, shipping, replenishment, and store-level workflows. In warehouse and distribution center environments, RFID can help identify when goods move through key transition points. In stores, it can help provide a more accurate picture of what is available, what has moved, and what may require attention.

RFID VISIBILITY ACROSS THE RETAIL JOURNEY



Some retailers underestimate these capabilities because they think of RFID as a narrow technology. Others may have experienced an early or limited deployment and assume that the technology itself is limited, when the issue may have been tied to reader placement, tag orientation, merchandise type, environmental factors, or system configuration.

This misunderstanding matters. If a retailer views RFID only as a basic inventory tool, they may miss opportunities to use it as part of a broader visibility strategy. On the other hand, if they view RFID as a complete replacement for every other retail security technology, they may create new gaps.

RFID can be powerful, but its value depends on design, deployment and integration. It is strongest when the use case is clearly defined. A retailer tracking apparel on the sales floor may have different requirements than a company tracking pallets in a warehouse, high-value electronics in a stockroom, or reusable assets moving between facilities. The question should not be, "Can RFID solve this?" Better questions are, "What information is needed, where is it needed, and what data will help teams act?"

When RFID is designed around operational questions, it becomes more than a tag or reader. It becomes a data source.

EAS IN A CHANGING ENVIRONMENT

As RFID adoption grows, some retailers are asking whether traditional EAS tagging is still necessary. That question is understandable, especially for organizations

> A LAYERED APPROACH ALLOWS RETAILERS TO MATCH THE TECHNOLOGY TO THE RISK, THE MERCHANDISE CATEGORY, AND THE OPERATIONAL GOAL.

evaluating budgets, labor demands, and overlapping technologies. But RFID and EAS do not serve the same purpose in every environment.

EAS has traditionally been one of retail's most visible theft deterrents. Tags, labels, pedestals and exit alarms create a clear signal that merchandise is protected. For opportunistic theft, that visibility still matters. A shopper who might otherwise take an unprotected item may think twice when a tag is attached or when pedestals are at the door.

The challenge is that today's theft environment is not limited to opportunistic theft. Organized retail crime, high-volume theft events, and repeat offenders have changed how many retailers think about deterrence. In some cases, offenders may be less concerned about alarms or visible security measures. That has led some to question whether EAS still provides value.

But EAS has not lost its place. It simply needs to be evaluated as one layer within a broader security and visibility strategy.

EAS can continue to support deterrence, alerting and merchandise protection. RFID can provide item-level data and movement visibility. Video analytics can add behavioral and environmental context. Store teams can use procedures, reporting and response protocols to bring those signals together. Each layer contributes something different.

The mistake is treating the decision as either-or. RFID does not automatically replace the need for physical deterrence. EAS does not provide the same depth of item-level data as RFID. Video does not identify every product movement on its own. A layered approach allows retailers to match the technology to the risk, the merchandise category, and the operational goal.

In practice, a high-risk apparel item may benefit from both visible protection and item-level visibility, while a lower-risk item may not require an EAS tag but can still benefit from RFID. A warehouse asset may require RFID tracking but not traditional EAS. A product that cannot be punctured may need a specialty tag to protect it. A high-traffic store may need video analytics to understand patterns around displays or exits. The right answer depends on the problem being solved.

That is where the value conversation is changing. Retailers are not only asking whether a security measure works. They are asking how it fits into a broader system of visibility, deterrence and response.

ADDING CONTEXT WITH VIDEO ANALYTICS

If RFID helps answer what moved and where it was detected, video analytics can help answer

> RETAILERS ARE LOOKING FOR DATA AND INSIGHTS FROM THEIR CAMERA INFRASTRUCTURE, INCLUDING TRAFFIC FLOW, HEAT MAPPING, DWELL TIME, QUEUE ACTIVITY, OCCUPANCY PATTERNS, AND UNUSUAL BEHAVIOR.

what was happening around it.

Modern video systems are expected to do more than record events. Retailers are looking for data and insights from their camera infrastructure, including traffic flow, heat mapping, dwell time, queue activity, occupancy patterns, and unusual behavior. This does not mean that every camera needs advanced analytics or that every use case requires artificial intelligence. It does mean that retailers are rethinking the role of video as a source of operational intelligence.

This shift is important because retail loss rarely happens in isolation. Product movement, employee activity, customer behavior, store layout, staffing levels and traffic patterns can all influence outcomes. A missing item may be the result of theft, misplacement, process failure, or inaccurate receiving. Video can provide context that other systems cannot.

Consider a retailer that knows a product moved from the stockroom to the sales floor but cannot explain why it is missing. Video may help identify

whether the item was placed in the wrong area, removed from a display, concealed, damaged, or taken through an exit. If a store has repeated loss around a category, video analytics may help show whether the issue is tied to display placement, blind spots, or staffing coverage. Beyond identifying a bad actor, video can also provide ongoing business insight, from traffic patterns and long queues to risk events such as slip, trip and fall prevention. In those situations, operational context may matter as much as the security event itself.

The strongest value comes when video analytics are not treated as a separate tool, but as part of the broader retail data picture. Video can validate events, add context to alerts and help teams understand the "why" behind the data.

THE FUTURE IS LAYERED VISIBILITY

Retailers do not need more disconnected systems. They need better answers.

That requires a practical understanding of the role each technology plays. RFID can provide item-level visibility. EAS can provide deterrence and exit alerting. Video analytics can provide behavioral and environmental context. Specialty tags can protect merchandise that does not fit traditional tagging methods. Warehouse and asset tracking technologies can extend visibility before products ever reach the sales floor.

Individually, each system has value. Together, they can help retailers move closer to a more complete picture of risk, movement and performance.

This does not mean that every retailer needs every technology everywhere. The most effective programs are built around specific questions:

- What products are most at risk?
- Where are the visibility gaps?
- What processes create uncertainty?
- What information is needed by operations and loss prevention teams in order to act more quickly?
- Which technologies can provide relevant information without creating unnecessary complexity?

These questions help retailers avoid the trap of buying technology based only on trends. RFID, AI, video analytics, and connected platforms are powerful tools, but their value depends on whether they are applied to the right problem.

A layered visibility strategy also helps retailers communicate value across departments. Loss prevention may care about shrink and theft. Operations may care about replenishment and labor efficiency. Merchandising may care about product availability. Supply chain teams may care about movement and receiving accuracy. Executives may care about return on investment.

When security technology supports more

LAYERED VISIBILITY

TECHNOLOGY LAYER	VISIBILITY QUESTION
RFID	What moved, where is it, and what needs attention?
EAS	Is protected merchandise leaving the store?
Video Analytics	What behavior or activity surrounded the event?
Specialty Tags	How can difficult-to-protect merchandise be secured?
Warehouse / Asset Tracking	Where are products or assets moving before they reach the sales floor?

than one of these priorities, the investment becomes easier to justify.

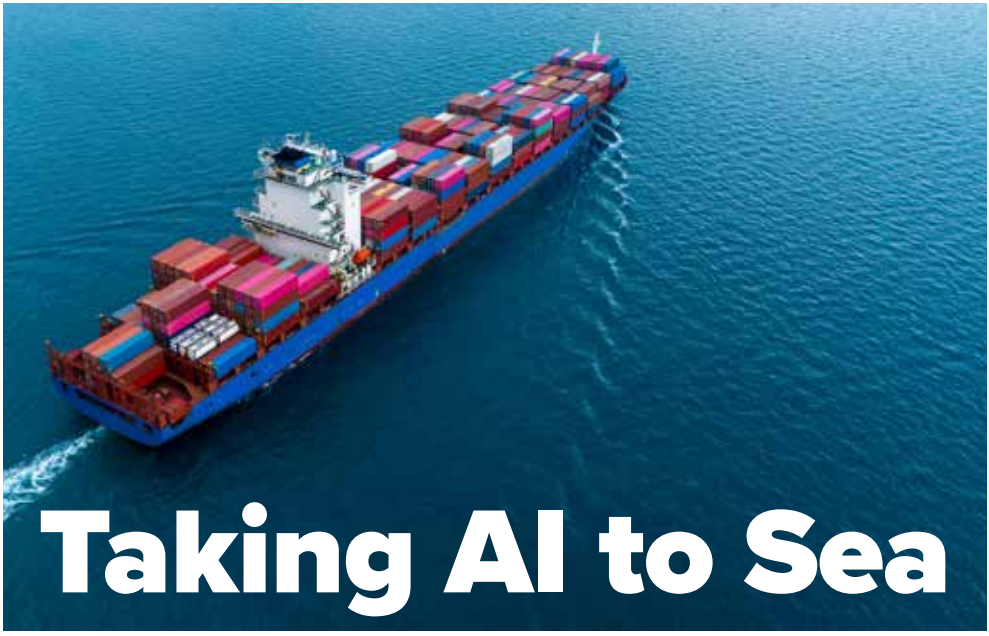
MOVING FORWARD

Retail security is entering a more connected phase. The focus is no longer only on whether a system can detect an event or protect an item. It is on whether the system can help retailers understand what is happening across stores, distribution centers, and the broader movement of merchandise.

This is where loss prevention and operational visibility are beginning to overlap. Retailers still need deterrence. They still need protection. They still need alerts and investigations. But they also need data that help them see patterns, correct issues, and make better decisions.

The future will be defined not by one technology replacing another, but by how well retailers align the right technologies with the right problems. RFID, EAS and video analytics each answer different questions. When those answers are connected, security investments can do more than prevent loss. They can help retailers see their operations more clearly.

And that is the real opportunity: Moving from loss prevention as a reactive function to retail visibility as a strategic advantage. ◀



Taking AI to Sea

How rapid edge deployment is transforming maritime safety

The maritime industry is undergoing a significant digital transformation as artificial intelligence becomes an increasingly important tool for improving operational safety, security, and efficiency. From offshore support vessels to commercial shipping fleets, operators are looking beyond traditional monitoring systems in favor of intelligent platforms capable of interpreting real-time data and providing actionable insights.

However, while AI software continues to evolve rapidly, one challenge remains constant: Deploying the right edge computing infrastructure quickly enough to keep development and implementation on schedule.

MEETING DEPLOYMENT TIMELINES

A U.S.-based developer of AI-powered maritime monitoring solutions recently faced this exact challenge while expanding its next-generation safety platform for offshore vessels.

The vision was ambitious. The platform would continuously analyze onboard video streams

Tom Larson (tom.larson@velasea.com) is President of Velasea (www.velasea.com).

while combining them with navigational and operational data to produce comprehensive, real-time understanding of vessel activity. Intended capabilities included bridge watch monitoring, voyage and collision awareness, dynamic positioning oversight, deck safety monitoring, personal protective equipment compliance, restricted area detection, and fire and machinery surveillance.

But before any of these capabilities could be validated in real-world conditions, the development team needed rugged edge computing hardware capable of operating reliably in demanding marine environments. And they needed it immediately.

> FOR ORGANIZATIONS WORKING UNDER AGGRESSIVE DEVELOPMENT SCHEDULES, HARDWARE AND INTEGRATION DELAYS CAN POSTPONE SOFTWARE INTEGRATION, CUSTOMER TRIALS, AND COMMERCIAL ROLLOUT.

Hardware procurement and integration often introduce weeks or even months of delay into AI deployments. For organizations working

> THIS MULTI-SOURCE APPROACH ENABLED THE PLATFORM TO INTERPRET EVENTS WITHIN THEIR OPERATIONAL CONTEXT RATHER THAN TREATING EVERY OBSERVATION AS AN ISOLATED INCIDENT.

under aggressive development schedules, those delays can postpone software integration, customer trials, and commercial rollout.

INFRASTRUCTURE AS AN ENABLER

Instead of allowing hardware logistics to dictate project timelines, the deployment strategy focused on minimizing friction from the outset.

Once suitable rugged edge infrastructure was deployed, development teams were able to begin validating AI workloads in operational environments. With infrastructure available early in the development cycle, engineers were able to spend their time refining AI models and validating operational workflows instead of troubleshooting hardware compatibility or waiting for equipment to arrive.

This approach illustrates an often-overlooked reality

of edge AI projects: The speed of infrastructure deployment can have a direct impact on the pace of software innovation.

ADDING CONTEXT TO DATA

With the hardware foundation in place, developers concentrated on the platform's distinguishing capability of combining multiple operational data sources into a unified situational awareness system.

Rather than relying solely on video analytics, the solution fused camera feeds with automatic identification system data, electronic charting data, and live vessel status data. This multi-source approach enabled the platform to interpret events within their operational context rather than treating every observation as an isolated incident.

For example, understanding whether a vessel is operating in dynamic positioning mode or is actively engaged in offshore work allows the

> BEYOND IDENTIFYING HAZARDS, THE SYSTEM CAN ALSO RECOGNIZE AND REPORT POSITIVE SAFETY BEHAVIORS, PROVIDING OPERATORS WITH A MORE BALANCED VIEW OF OPERATIONAL PERFORMANCE INSTEAD OF FOCUSING EXCLUSIVELY ON RULE VIOLATIONS.

> FOR APPLICATIONS SUCH AS COLLISION AWARENESS, BRIDGE WATCH MONITORING, AND DECK SAFETY, WHERE RAPID RESPONSE CAN MAKE A MEANINGFUL DIFFERENCE, EDGE COMPUTING BECOMES A PRACTICAL NECESSITY RATHER THAN SIMPLY AN ARCHITECTURAL PREFERENCE.

AI to determine which alerts are genuinely relevant. This approach can significantly reduce nuisance alarms while improving the relevance of safety notifications.

Beyond identifying hazards, the system can also recognize and report positive safety behaviors, providing operators with a more balanced view of operational performance instead of focusing exclusively on rule violations.

EDGE AI WHEN UNDERWAY

While cloud computing continues to play an important role in AI development and analytics, it is simply not practical to process many maritime workloads remotely. Offshore vessels may generate dozens of high-definition video streams alongside navigational and operational data, all of which would be expensive to transmit continuously over satellite connections. Even when connectivity is available, the latency introduced by cloud processing can delay the detection of time-sensitive safety events.

Processing data directly on the vessel addresses these challenges by enabling AI models to analyze video and sensor inputs in near real time while significantly reducing bandwidth consumption. For applications such as collision awareness, bridge watch monitoring, and deck safety, where rapid response can make a meaningful difference,

edge computing becomes a practical necessity rather than simply an architectural preference.

Decisions can be made with lower latency, bandwidth requirements are reduced, and mission-critical AI functions can continue operating even during periods of limited or intermittent connectivity. For offshore operators, for whom continuous awareness can directly influence safety and operational efficiency, these capabilities are increasingly valuable.

LOOKING AHEAD

The success of modern maritime AI initiatives depends on more than sophisticated algorithms. Equally important is the ability to deploy reliable computing infrastructure quickly enough to support rapid development, testing and operational rollout.

As organizations continue investing in intelligent vessel monitoring, the combination of robust edge computing, contextual data fusion, and streamlined deployment processes will play a central role in delivering safer, more efficient maritime operations.

In an industry where both time and reliability are critical, eliminating infrastructure bottlenecks may prove just as important as advancing the AI itself. ◀

Context Is Key in Alarm Response

Emerging technologies can turn information into intelligence

Peter Giacalone (info@3si.com) is Board Advisor at 3Si (www.3si.com).

More than a dozen years ago, during a discussion about alarm response and false alarm reduction, a law enforcement sergeant pointed to a memorial plaque honoring a deputy who had been killed responding to what was reported as a holdup alarm. His message was straightforward: Better information could have changed the manner and degree of the response, and perhaps the outcome.

When responding to an event, context matters. An alarm dispatch with no context is a relatively low priority. If the event is a verified crime in progress, however, typically the only incident with a higher priority is an officer in distress.

Police officers respond to regular alarm calls with limited information. What starts as a routine

dispatch with a mindset that most are false can turn out to be something far more serious. Later, everyone involved is left asking the same question: Would the outcome have been different if first responders had more information before they arrived?

For decades, that question has driven innovation across the security industry. It continues to drive it today.

While every incident is different, the lesson remains relevant. Security and public safety professionals make decisions based on the information available to them. When critical details are missing, those decisions become more difficult. When meaningful context is available, responders are better equipped to determine priorities and allocate proper resources.

> POLICE OFFICERS RESPOND TO REGULAR ALARM CALLS WITH LIMITED INFORMATION. WHAT STARTS AS A ROUTINE DISPATCH WITH A MINDSET THAT MOST ARE FALSE CAN TURN OUT TO BE SOMETHING FAR MORE SERIOUS.

The security industry has made tremendous progress over the past several decades. Video monitoring, video verification, analytics,

> WHEN MEANINGFUL CONTEXT IS AVAILABLE, RESPONDERS ARE BETTER EQUIPPED TO DETERMINE PRIORITIES AND ALLOCATE PROPER RESOURCES.

remote monitoring, and other technologies have dramatically improved the ability to detect, verify and assess events. Organizations today have access to more information than ever before.

Yet, despite these advances, many of the challenges surrounding response remain surprisingly familiar. The reason is simple: More information does not automatically produce better outcomes.

Many organizations already possess the information needed to improve response effectiveness. The challenge is getting that information to the people making decisions as soon as possible.

In many cases, valuable information remains trapped within individual systems. A monitoring center may have access to video. A dispatcher may receive an alarm notification. Each piece of information has value on its own, but greater operational impact is created when those insights combine to create a more complete understanding of what is happening.

Consider the difference between receiving a notification that an alarm has activated and receiving verified video that unauthorized activity is occurring inside a facility. The additional context changes how the situation is viewed and often influences how resources are deployed. This distinction becomes increasingly important as organizations seek to improve efficiency and effectiveness.

Security operations centers, monitoring centers, and public safety agencies all face the same challenge of determining which events deserve immediate attention and which do not. Better information helps make those decisions easier, and this is where the industry's focus has begun to evolve.

For years, conversations centered on detection. Could a system identify an event? Could it generate an alarm? Could it notify personnel when something occurred? Today, those capabilities are a given. The next challenge is helping people understand what

> MANY ORGANIZATIONS ALREADY POSSESS THE INFORMATION NEEDED TO IMPROVE RESPONSE EFFECTIVENESS. THE CHALLENGE IS GETTING THAT INFORMATION TO THE PEOPLE MAKING DECISIONS AS SOON AS POSSIBLE.

> THE OPPORTUNITY MOVING FORWARD IS NOT SIMPLY TO ADD MORE TECHNOLOGY. IT IS TO ENSURE THAT EXISTING TECHNOLOGIES WORK TOGETHER EFFECTIVELY.

an event means. This requires moving beyond notifications and toward actionable information. It requires providing context that helps decision makers assess a situation, determine its significance, and respond appropriately. Fortunately, the technologies necessary to support this shift are already available.

Video verification can help distinguish legitimate incidents from nuisance events. Remote monitoring can provide visibility into developing situations. Emerging situational awareness technologies, including AI-powered analytics that help identify patterns and highlight relevant activity, can contribute additional information about activity occurring within a protected environment. Collectively, these capabilities create a clearer picture of what is happening before responders arrive.

The opportunity moving forward is not simply to add more technology. It is to ensure that existing technologies work together effectively. For many organizations, the future of security will not be defined by the number of cameras installed, the quantity of data collected, or the sophistication of individual systems. Rather, it will be determined by how effectively information is shared, understood and acted upon.

This is particularly important for public safety. First responders routinely make decisions in real-time environments where circumstances can change quickly. The more context that is available before arrival, the better positioned they

are to make informed decisions that protect both themselves and the communities they serve.

The security industry has spent decades working toward more meaningful dispatches, fewer unnecessary responses, and better collaboration between private security and public safety. Significant progress has been made, and the tools available today would have been difficult to imagine just a generation ago. At the same time, though, the industry's work is not finished. Technology will continue to evolve. New capabilities will emerge. Additional sources of information will become available.

The organizations that benefit most from these advances will not necessarily be those that collect the most information. They will be those that do the best job of transforming information into understanding and delivering that understanding to the people who need it most.

Whether the goal is protecting people, reducing loss, improving officer safety, or increasing apprehensions, security, at its core, has always been about outcomes.

Better information supports better decisions.

And better decisions contribute to better outcomes. ◀

The Hidden Factor in Mobile Surveillance Reliability

Power design determines whether off-grid cameras will work when it matters most

Colin DePree (colin.depree@mobileprosystems.com) is the Vice President of Sales and Marketing for Mobile Pro Systems (www.mobileprosystems.com).

Mobile surveillance is one of the fastest-growing segments of the physical security industry. Analysts project that the market will nearly double by 2032, growing at roughly 10 percent annually, with trailer-mounted platforms accounting for approximately half of all deployments.

As construction sites, public venues, critical infrastructure, and municipalities adopt these platforms in record numbers, procurement conversations focus almost entirely on the most obvious factors: camera counts, resolution, analytics and coverage maps. Yet, even though these platforms earn their value precisely where the energy grid is inconsistent, unavailable or expensive to bring in, too little attention goes to the issue of power. When a mobile surveillance trailer loses power, coverage disappears with it. Such outages typically result from earlier decisions about power system design, expected load, and whether the design accounts for real world conditions.

> EVEN THOUGH THESE PLATFORMS EARN THEIR VALUE PRECISELY WHERE THE ENERGY GRID IS INCONSISTENT, UNAVAILABLE OR EXPENSIVE TO BRING IN, TOO LITTLE ATTENTION GOES TO THE ISSUE OF POWER.

THE POWER BUDGET: WHERE RELIABILITY BEGINS

Reliable off-grid deployments begin with a power budget that answers two questions: How much power, in watts, does the platform draw at any moment? And how many watt-hours does this total over a day, week and month?

Every device on a mobile surveillance platform – cameras, radios, analytics hardware, mast lighting, wireless backhaul, environmental controls – draws from the same finite energy pool. A disciplined power budget turns that reality into numbers that can be reasoned about. In practice, engineers build the budget device by device, capturing wattage and duty cycle, and the output is a daily energy requirement. That number, combined with the target runtime and climate, should drive decisions about how much solar generation is needed during the worst season, how large the battery bank must be to survive nights and storms, and whether a generator is an optional fuel saver or the reliability backbone.

Thermal management is often overlooked. In hot climates, cooling systems add continuous loads that are frequently underestimated. In cold environments, battery efficiency drops, reducing usable capacity. These factors are real and recurring.

THREE BUILDING BLOCKS, ONE SYSTEM

Beneath every mobile surveillance platform, the same three building blocks are at work.

Power consumption is the live, always-changing load, and each addition to the payload pushes the baseline draw higher.

Power generation is how energy enters the system, whether through solar arrays, generators or shore power when available.

Power storage bridges the gaps when generation drops, carrying the system through nighttime hours, multi-day storms, winter low-sun conditions, and temperature extremes that drive up thermal loads.

Reliability emerges when these three elements are sized and tuned together, then validated against the actual conditions under which the platforms will operate, not against an averaged weather model from an unusually good year. A basic single-camera trailer with limited networking might run comfortably within a modest solar and battery budget. A multi-camera platform with active analytics, lighting, and environmental

> HYBRID POWER SYSTEMS, WHICH COMBINE A GENERATOR, BATTERY STORAGE, AND SOLAR PANELS, ARE THE ARCHITECTURE THAT SERIOUS OFF-GRID APPLICATIONS TURN TO WHEN UPTIME TRULY MATTERS.

management can easily double or triple the demand.

THE LIMITS OF SOLAR-ONLY DESIGNS

Solar-only platforms have obvious appeal. They operate quietly, require no fuel, and reduce mechanical complexity. In the right circumstances, they perform well. Those circumstances usually involve a modest, tightly controlled power budget; brief, managed deployment windows; sites with good panel orientation and minimal shading; and missions that can tolerate occasional downtime.

The challenge is that solar production is inherently variable while surveillance missions are often mission critical. The sun sets every night, so stored energy must carry the system until morning. Storms and extended overcast conditions can

suppress production for days. Smoke, dust and pollution reduce output. When daily energy consumption approaches or exceeds what worst-season sunlight can reliably replace, the deployment is no longer operating on a solar solution; it is operating on an outage timer.

Field experience shows that solar-only failures rarely arrive all at once. Instead, several forces gradually erode the original design margin.

The environment is the first force. Mast shadows move across arrays throughout the day, nearby structures introduce partial shading, and panels that perform well in summer struggle as the sun sits lower in winter. Two trailers placed only a few blocks apart can produce very different outputs due to local shading or microclimatic differences.

Mission creep is the second force. Very few platforms remain in their original configuration for long. A deployment that began with a single camera and basic connectivity may gradually gain additional cameras, onboard analytics, upgraded radios, or brighter lighting. Each addition improves capability, but, collectively, raises the baseline energy demand. Unless someone revisits the power budget, the design slowly drifts away from its original assumptions. A practical audit should involve identifying every device added since the platform left the integrator and comparing that list to the configuration used to size the solar array and battery bank. The resulting gap frequently explains why a unit that once operated comfortably now struggles after storms.

System aging is the third force. Solar panels lose efficiency over time, with industry estimates typically around one-half percent per year. Combined with shading and load growth, that gradual decline can push a previously stable system into a state where it can no longer fully recover after periods of poor weather. From the field, none of this looks like a slow decline. A trailer appears fine until it suddenly goes offline, often at the exact moment

CAUSES OF FAILURE IN SOLAR-ONLY DESIGNS

- Environment
- Mission creep
- System aging

> FROM THE FIELD, NONE OF THIS LOOKS LIKE A SLOW DECLINE. A TRAILER APPEARS FINE UNTIL IT SUDDENLY GOES OFFLINE, OFTEN AT THE EXACT MOMENT OPERATORS NEED VISIBILITY THE MOST.

operators need visibility the most.

THE CONCEPT THAT SEPARATES ARCHITECTURES

One concept explains the practical difference between power architectures more clearly than almost anything else: Energy margin. This is the gap between the power a system needs and the power it can produce under difficult conditions. When that margin is large, the system absorbs storms, seasonal shifts, unexpected loads, and equipment aging without approaching failure. When the margin is small, minor disruptions compound until the system runs out of energy.

Solar-only systems often operate close to that boundary because their margin depends entirely on consistent sunlight. Hybrid systems address the problem differently by adding a controllable energy source. When solar production drops or load increases, generator runtime automatically expands to restore balance. Energy shortages do not typically cause outages; they simply cause longer generator cycles.

HYBRID ARCHITECTURES

Hybrid power systems, which combine a generator, battery storage, and solar panels, are the architecture that serious off-grid applications turn to when uptime truly matters. Telecommunications sites, remote infrastructure monitoring, and long-term surveillance deployments all lean on the same model because it delivers deterministic uptime.

Each component plays a distinct role. The generator

is the only element that can produce full power on demand rather than on the weather's schedule, making it the backbone during storms, short winter days, and periods of elevated load. Batteries are storage, not generation; they hold energy produced by the generator and solar array and release it gradually, allowing quiet overnight operation and smoothing fluctuations between generator cycles. Solar serves as the efficiency engine, reducing generator runtime, stretching fuel, and lowering operating costs without becoming a single point of failure.

Modern control systems manage this balance automatically around a simple priority structure: Maintain surveillance coverage, protect the health of the power system, and minimize fuel consumption. When battery levels fall below a defined threshold, or when temperatures threaten reliable operation, the controller starts the generator, charges the batteries through the efficient portion of their charge curve, and shuts down before wasting fuel on low-efficiency trickle charging. Telemetry surfaces battery state of charge, solar production, and generator runtime, enabling operations teams to identify shading, rising loads, or aging equipment

so they can schedule service before a site goes dark.

This architecture also changes the meaning of deployment autonomy, the length of time a platform can remain in the field without service. For solar-only designs, autonomy is ultimately limited by unpredictable weather and battery capacity. For hybrid designs, autonomy is primarily determined by fuel capacity and service schedules, variables that an organization can plan around.

QUESTIONS SECURITY LEADERS SHOULD ASK

Evaluating power design does not require running engineering simulations. A small set of questions can reveal whether the fundamentals have been addressed.

- What power budget was used for this configuration, and how was it built?
- Can the vendor show real or modeled production curves for the deployment latitude during winter and shoulder seasons, not just peak summer?
- How does the system behave when battery levels are low and solar production is low?
- What sheds first, and how is the operations team notified?
- Is the generator a primary reliability anchor or merely a backstop if the solar plan fails?
- How much has the payload changed since the original design, and how long do units actually stay in place?

> TREATING SOLAR-ONLY CONFIGURATIONS AS A DELIBERATE DESIGN CHOICE RATHER THAN A DEFAULT ALLOWS SECURITY TEAMS TO SHIFT FROM REACTING TO OUTAGES TO PLANNING FOR RELIABILITY.

These questions allow organizations to classify sites and platforms by risk. Low-risk cases combine constrained loads, short deployments, favorable sun, and tolerant missions. High-risk cases mix heavier payloads, long-term deployments, challenging climates, and locations where being

offline is simply not acceptable. Treating solar-only configurations as a deliberate design choice rather than a default allows security teams to shift from reacting to outages to planning for reliability.

POWER DESIGN ULTIMATELY DETERMINES UPTIME

A platform with a disciplined power budget and an appropriate energy architecture does more than reduce downtime. It creates operational trust. The confidence that, when an incident occurs, the system will be online, watching and recording. The video management system depends on the feed, the monitoring center depends on the connection, and the response team depends on the alert arriving when conditions change.

For leaders seeking to extend security beyond buildings and fixed camera networks, the goal is not simply to deploy a trailer with cameras. The goal is to extend the reach of the security program with a platform that remains visible, connected and operational in the moments that matter. Reliability is not an accident. It is the result of deliberate power design. ◀

The Most Valuable Asset You're Not Measuring

Monitoring contracts anchor a dealer's value and need a disciplined approach

Naomi Withers (naomi@loyva.io) is the Vice President of Strategy at Loyva (www.loyva.io).

Valuable assets held by alarm and monitoring companies typically have disciplined workflows built around them. Vehicles have maintenance schedules and depreciation tracking. Inventory gets counted and recorded. Employees get performance reviews and development planning. Yet there is one glaring exception.

Monitoring contracts are the most valuable and most under-managed asset class on a security dealer's balance sheet. Treating them as a filing problem rather than as a living, measurable, protectable asset is the single largest source of quiet value destruction in the industry.

Contracts sometimes are filed in a document management system. Sometimes they are put on a shared drive. Sometimes they are scanned into a customer record in the operating platform.

Occasionally, in the companies that have done the work, they get vaulted properly. But in almost no case does the industry apply the ongoing discipline that it applies to other assets of equal or lesser value.

This is not a technology gap. It is a framing gap. The industry inherited a paper-era mental model of what a contract is – a piece of documentation to be filed and referenced when needed. The reality is that a monitoring contract is a recurring revenue instrument that anchors the enterprise value of the business, secures lending relationships, and either accelerates or stalls an eventual sale. It deserves the same operational care as any other asset.

> THE REALITY IS THAT A MONITORING CONTRACT IS A RECURRING REVENUE INSTRUMENT THAT ANCHORS THE ENTERPRISE VALUE OF THE BUSINESS, SECURES LENDING RELATIONSHIPS, AND EITHER ACCELERATES OR STALLS AN EVENTUAL SALE.

THE ASSET CLASS HAS CHANGED

There is a technical point buried under the framing question that most dealers

> ANY DEALER WHO CANNOT PRODUCE, ON A GIVEN TUESDAY, A REASONABLY CURRENT VALUATION OF THEIR CONTRACT PORTFOLIO IS RUNNING THE BUSINESS PARTIALLY BLIND.

have not been asked to think about, and it matters more every year.

A signed piece of paper, a scanned PDF stored on a shared drive, and a UCC 9-105-compliant transferable electronic record are not the same asset. They may look similar on a desk, but they behave completely differently in front of a lender, a court, or an acquirer.

The federal Electronic Signatures in Global and National Commerce Act (ESIGN) and the Uniform Electronic Transactions Act (UETA), which has been adopted by every state except New York, established that electronic signatures carry the same legal weight as ink signatures for most purposes. This was a foundational shift. What most operators do not realize is that the deeper shift came with Section 105 of Article 9 of the Uniform Commercial Code, which defined the specific technical conditions under which an electronic record qualifies as a transferable electronic record, the

digital equivalent of a negotiable paper original. That distinction is what makes an electronic contract usable as collateral in a lending arrangement, transferable in an acquisition, and defensible in a dispute over ownership.

A scanned PDF of an executed contract is just a copy. A UCC 9-105 transferable record is the original. Most dealers do not know which one they are holding, because, on the surface, they appear the same.

Lenders, insurers and sophisticated acquirers, however, do know the difference.

MEASUREMENT IS THE MISSING DISCIPLINE

The framing shift only becomes real when it is measured, and measurement is where the industry has the furthest to travel.

Any dealer who cannot produce, on a given Tuesday, a reasonably current valuation of their contract portfolio is running the business partially blind. The number is not difficult to calculate in principle. The problem typically is that the underlying data is scattered across systems that were never designed to talk to each other, and the discipline of continuous

> THREE CONCRETE OUTCOMES EMERGE WHEN A DEALER TREATS THEIR CONTRACT PORTFOLIO AS AN ASSET CLASS RATHER THAN AS A FILING CATEGORY.

measurement was never built in.

The technology to do this, however, has become much easier. Integrations between operating platforms, contract vaults, and financial systems are no longer specialty projects. The barrier is no longer capability. The barrier is expectation.

WHAT CHANGES WHEN THE DISCIPLINE IS IN PLACE

Three concrete outcomes emerge when a dealer treats their contract portfolio as an asset class rather than as a filing category.

The first relates to lending. Lenders who finance the alarm industry have specialized underwriting frameworks that key off contract quality, contract portability, and the auditability of the collateral. Dealers with tightly measured,

vault-stored, standards-compliant portfolios receive faster terms and better rates. Dealers whose contracts live in three shared drives and a filing cabinet get slower diligence and thinner offers, if they get offers at all.

The second concerns mergers and acquisitions. Every experienced buyer in this industry has walked away from, or discounted, a deal because the contract portfolio could not be cleanly verified. Missing contracts, unclear assignability, questionable signature integrity, and undocumented modifications all compress multiples. The seller who can hand over a vault of transferable electronic records, tied to a live valuation tool, and demonstrate three years of clean measurement discipline, is running a fundamentally different sale process than one who cannot.

The third has to do with daily operations. Dealers who measure their portfolios continuously catch issues before they become big problems. They see revenue leakage as it happens rather than in an annual or one-time

> THE DEALERS WHO WILL COMMAND THE STRONGEST VALUATIONS, THE BEST LENDING TERMS, AND THE SMOOTHEST EXITS WILL BE THE ONES WHO STARTED MEASURING, PROTECTING, AND TENDING THEIR CONTRACT PORTFOLIOS YEARS BEFORE THEY NEEDED TO.

reconciliation. They know which sales branches are closing the loop and which are not.

None of these outcomes requires exotic technology. Rather, they demand the operational decision to treat contracts the way the industry treats every other asset that carries this much value.

CONCLUSION

The security industry has spent decades excelling at monitoring what happens inside a customer's home or business. It is time to be equally excellent at monitoring what happens with the contracts that anchor every subscriber, every dollar of recurring revenue, and every future exit.

The dealers who will command the strongest valuations, the best lending terms, and the smoothest exits will be the ones who started measuring, protecting, and tending their contract portfolios years before they needed to. The tools to do that work exist now. The discipline is what remains.

For any operator who is quietly recognizing the value leakage in their own business, the good news is that discipline can be built. It starts with a single decision: To stop treating contracts as mere documentation and to start treating them as the asset they have always been. ◀

Ready to improve how you manage security projects?

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

SPM
SECURITY**PROJECT**MANAGEMENT

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

Learn more at securityindustry.org/spm

CSPM®
Certified Security Project Manager

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

Learn more at securityindustry.org/cspm

Security Industry Association
securityindustry.org

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