SIA Insights TECHNOLOGY

Volume 7, Issue 1
Spring 2019

Welcome

Dear Reader,

With the Security Industry Association celebrating its 50th anniversary this year, we are reminded more than ever of how much security has evolved in the past few decades. From standalone devices that secured a door or videotaped an area to integrated systems to today's advanced solutions that leverage emerging connected technologies.

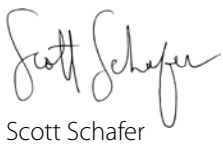
This edition of *SIA Technology Insights*, like those before it, examines this new world of security, where everything is online, machines are learning to perform tasks and threats can come from anywhere in the world.

With articles from experts in their respective fields about the potential for artificial intelligence to shape security, the critical role of cybersecurity, the elevated risk that comes with being a part of the Internet of Things and much more, our hope, as always, is that this publication will help security professionals better understand their technology options.

If you have any comments, questions or article proposals, please contact our editor, Ron Hawkins, at rhawkins@securityindustry.org. And, if you are currently reading a hard copy of *SIA Technology Insights*, remember that you can view and share all articles – past and present – by visiting www.securityindustry.org/techinsights.

Thank you for reading.

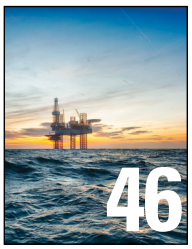
Sincerely,



Scott Schafer
Chairman, Board of Directors
Security Industry Association

Don Erickson
CEO
Security Industry Association

Table of Contents



Search the SIA Membership Directory

It is important to develop a comprehensive plan that includes layers of protection and utilizes the appropriate technology to *assist*, rather than *replace*, the humans who are responsible for physical security.

Artificial Intelligence, Real Security

AI has the potential to enhance multiple components of security systems

By John Carter
ReconaSense

When considering the challenges of ensuring life safety, improving physical security and increasing employee and contractor accountability, there are more options available than ever before. It is important to develop a comprehensive plan that includes layers of protection and utilizes the appropriate technology to *assist*, rather than *replace*, the humans who are responsible for physical security.

Before examining some of the new technologies and how they can be utilized, consider the progress that has been made to get here. Not too many years ago, the security industry was a collection of companies that produced proprietary, closed architecture systems that were not interoperable. Eventually, though, leading industry organizations agreed to unite and support open standards.

There is often resistance to new ideas and approaches for a variety of reasons – some fear change; some want to delay change until they can catch up; and some see change as an existential threat. Fortunately, the security industry accepted change and embraced open standards. That is what has enabled so many of the

advancements that are now available to improve life safety and security.

AI: The Myth, the Magic, and the Reality

It is important to clarify what AI is and how it affects physical security. While AI is one of the hottest trending topics, it seems to be often misunderstood or mistrusted. At a recent security conference, one industry technology executive stated that AI does not exist. In other words, he saw it as a myth.

Fortunately, he is incorrect. AI is not a myth. It simulates the human intelligence process in that it acquires information and learns. It identifies patterns and it reacts based on those patterns. One of the core components of this learning process is an artificial neural network (ANN). Similar to the human brain, an ANN works with thousands of sensors.

Human sensors are eyes, ears, nose, skin and tongue. They identify features of the environment – people, things, temperature, light or darkness, moisture, sounds and many other things. As those sensors activate, humans learn. Internal variables adjust, patterns are identified, and reactions are formulated. For example, the smell of smoke indicates fire, and the brain sends signals to the body to take appropriate action to escape danger.

A more sophisticated example would be how human behavior and, ultimately, a person's character is assessed. Over time, personality traits are identified and changes in behavior are observed. All of this information leads to the development of a trust or no-trust relationship.

When it comes to technology, the artificial neural network sensors are cameras, sensors, access control

equipment, Internet of Things (IoT) devices, big data, social media plug-ins and human input. As those sensors feed internal variables, the ANN learns and identifies patterns of risk, providing real-time situational awareness to human personnel.

> Reliable, secure and fast networks are fundamental to integrating security technology.

AI may seem like magic, but it is real. It can evaluate large amounts of data to identify threats that might otherwise go unnoticed. This fundamentally changes the game in physical security and will affect all traditional components of a layered solution.

Networks: The backbone of integrated security

Reliable, secure and fast networks are fundamental to integrating security technology. Over the past few years, there have been tremendous advancements in cybersecurity. The implementation of AI in this category has produced solutions that can identify a wide range of threats via anomalous event detection. This is particularly important when information is transported between facilities or across cloud-based solutions.

One of the fundamental decisions regarding networks is the choice of cloud or no cloud. There are many variables to consider when making this choice. Are you deploying at a single site, a campus or an entire enterprise? Will you need Internet

services or interaction with third-party systems or sites? What is the relationship of price versus vulnerability. What IT resources and support will you need? Will the system that you are selecting adhere to your IT policies and work with you as is or will it require specialized equipment and support?

Perimeter defense: Spotting threats at a distance

With the advent of AI-based approaches, perimeter defense solutions can be an integral part of a layered security system. Specialized sensors can be utilized in conjunction with other elements and monitored with software powered by AI to identify threats just outside the walls of an organization. Improvements in multi-axis sensor technology has made this layer more affordable.

Entrance control: Understanding people flow to identify risk

While turnstiles may not have changed dramatically in form, their use within a layered security solution can provide invaluable data to an AI-based solution. Anomalous traffic patterns or unusual access can be identified before individuals reach higher security areas. Randomized spot checks, controlled throughput and directed traffic flows can be initiated and managed via intelligent, risk-based solutions as threats are detected.

Access control: Mitigating risk in real time

No physical security devices have benefitted more from AI than physical access control systems. When integrated with an AI-based solution, an access control system can now

quickly react to threats and adjust permissions accordingly. Having the ability to identify anomalous events, insider threats, and hazardous situations and dynamically change permissions is a major breakthrough for the physical security world.

The use cases in this category are wide ranging. For example. when AI is applied to access control, it can identify unusual activity, such as off-hour and abnormal location access and combine it with other threat indicators to quickly identify insider threats. Risk-adaptive access is able to prevent people from entering an area where a traditionally "non-obvious" danger is located, and it can allow a first responder with the right credentials to access an otherwise restricted area when threatening conditions exist.

Having the ability to identify anomalous events, insider threats and hazardous situations and dynamically change permissions is a major breakthrough for the physical security world.

Video surveillance: The unblinking AI

Video has evolved tremendously with the migration from analog to digital and DVR to NVR, and with the adoption of ONVIF and cloud deployments. There is now a suite of video analytics available and some analytics even exist on the camera itself.

When used as a sensor for an ANN in an AI environment, video is a key component for providing real-time, situational awareness to the security operations center (SOC).

Traditionally, SOC operators have been presented with hundreds, possibly thousands, of camera feeds to monitor. Studies show that human attention spans are limited in their ability to effectively monitor video and identify potential threats. However, when video is part of an AI-based

solution, attention span is limitless. AI never gets bored or distracted. It can sift through the mundane and assist humans in identifying threats as they emerge.

Drones: Assessing risk from above

The use of drones is sparking interesting discussions about standards, public policy, safety and privacy. These conversations typically go down one of two paths. Some will look for systems that can use drones to assess threats. Others will look for systems that can detect drones, viewing the technology *as* a threat.

AI never gets bored or distracted. It can sift through the mundane and assist humans in identifying threats as they emerge.

In some security environments, drones provide tremendous assistance in threat assessment and verification. At critical infrastructure sites and across wide areas and difficult to reach locations, drones with video devices can help operators better understand developing situations. A drone can be quickly dispatched to evaluate anything from a pipeline leak to a lone worker who is non-responsive. Drones can also be sent into hazardous conditions, such as chemical spills, before humans enter, to assess the situation and gauge the danger level.

When added to an AI-based solution, drones can be automated, and the system can ensure that they work according to all public and private policies.

Robotics: Addressing risk on the ground

While drones can help *assess* a situation, advancements in robotics can help *address* it. Robotics options today can be overwhelming. Robots can ride motorcycles, drive vehicles, jump high, climb ropes and scale cliffs. This opens tremendous possibilities in the security environment. Robots can take action to rescue people from dangerous situations such as fires, explosions or accidents in locations that cannot be easily or safely reached by humans.

Software: Bringing the system together

Over the years, security software has evolved from single purpose systems to integrated systems. With standards, the evolution has continued to interoperable solutions. Physical security information management (PSIM) systems were an attempt to unify information into a common user interface.

Because of advancements in networking, data management, CPUs, GPUs and many other areas, today we see more than an evolution. Platforms have developed in interoperable environments fully utilizing the technological advancements that go well beyond the hopes of PSIM, moving the security industry into a new era.

It is an AI *revolution* in physical security. ■ **Back to TOC**

John Carter (jcarter@reconasense.com) is co-founder, president and chief technology officer of ReconaSense (www.reconasense.com).

Search the SIA Membership Directory

A place where a variety of systems and solutions come together, the GSOC exists to provide a common operational picture, mitigate threats, and promote enhanced communication during an incident.

At the Center of It All

Following a set of best practices can lead to a more effective GSOC

By Dan Gundry
Vistacom

There recently has been a renewed focus on the heart of an organization's security posture – the global security operations center (GSOC). Gone are the days when the GSOC was an afterthought on the road to securing a space. Today's GSOCs are innovative, comfortable, functional, mobile at times, and scalable. Enterprise organizations rely on their GSOC for business operations and, in times of emergency, a complete situational picture.

The goal of any GSOC is to monitor, assess, prevent and respond to a variety of threats and incidents. As technologies advance and trends develop, so do the strategies to meet this goal. Technology trends, such as data convergence, artificial intelligence (AI)/machine learning, and augmented reality are emerging as the future of GSOCs. These capabilities allow operators in command centers to achieve higher levels of security by promoting automation, awareness and rapid responses. A place where a variety of systems and solutions come together, the GSOC exists to provide a common operational picture, mitigate

threats, and promote enhanced communication during an incident.

Best practices for designing a GSOC must be taken into consideration to deliver the best possible results for security practitioners.

Consulting for Convergence

When a company decides to implement a GSOC or control room as part of its overall security plan, there are a number of ways the project can begin. Some know exactly what they want and the functionality they require, and they work directly with an integrator to accomplish their goals. Others, however, may need additional support in developing a vision for the safety of their facility. That is where consultants come in.

There are several ways in which a consultant can get involved in the GSOC development process. Often, the relationship begins with a comprehensive threat assessment of a facility that can reveal possible gaps in security. The next step in the process is evaluating the technology piece, which is where an integrator works side-by-side with a consulting firm to determine what is already in place, what is missing and what is needed.

A consultant may be tasked with creating a holistic approach for a security program. Many enterprise organizations are siloed, with IT, security and facility management each separate entities, and those silos must be broken down to create the kind of integrated environment that an effective security program requires. To do this, three elements must be addressed:

Policies and regulations

It is critical to develop policies and regulations to establish a consistent security program across the organization. These need to be well structured and clearly written.

People and procedures

Another important element is the people involved in the decision-making process. Answering questions

about the various roles that human resources, IT, security and management play in the process is crucial to the success of a security plan. A consulting firm can use this information to begin to craft standard operating procedures (SOPs) and an operational flow that will help the organization be most effective.

Technology

This is one of the most complicated elements. Typically, enterprise security systems are built on the foundation of IP networks, requiring software that interfaces with operations. Working with specialty integrators is important in this step because of the need for extensive knowledge of the various pieces of technology that must be in place to formulate a common operational picture.

Taking each of these elements as they relate to a company's organizational culture is critical to building a successful approach to security. Security can have a huge impact on an organization – and the effect can be negative if procedures are implemented in a haphazard manner with poor communication. That is where a consultant can come in and streamline the process.

> Many enterprise organizations are siloed, with IT, security and facility management each separate entities, and those silos must be broken down to create the kind of integrated environment that an effective security program requires.

Establishing procedures and communication is the first step toward delivering a GSOC that can meet the needs of an enterprise organization. This plays a major role in communicating to employees that they matter and are important to the company's overall goal of building an environment that is positive and forward-thinking and that places people at the heart of its business.

Incorporating Technology

After identifying what a GSOC will achieve, an enterprise, with the help of its partners, must identify the technology that will be included in the command center. These spaces combine multiple security components, such as video, audio, access control, intrusion detection, and more. Facilities are also starting to include additional pieces, such as risk and threat assessment, employee travel, executive protection, and social media monitoring.

Video walls

When it comes to building a mission-critical GSOC, there is a reason why large-scale overview video walls that display many incoming data points are dominant. Uniform and integrated visual elements are imperative to the success of the GSOC, as operators

and first responders require the most up-to-date and complete information regarding incoming security-related events. These visual displays must be able to aggregate a wide variety of devices and data into a single pane-of-glass view, and at the heart of this mission are the monitors and displays that project the most relevant and critical information. As part of the video wall selection process, customers must work with their consultant and specialty integrator to decide how information will be communicated, such as with peak communication over Ethernet as opposed to traditional matrix switching. This provides organizations with flexible, scalable and cost-effective video walls and desktop integration.

> Security can have a huge impact on an organization – and the effect can be negative if procedures are implemented in a haphazard manner with poor communication.

AI/analytics

Innovative security systems are continuously gathering information and funneling massive amounts of data into a GSOC for analysis and response. AI can make the detection and communication of anomalies easier and enable faster and more effective responses. Powered by computer vision and machine learning, solutions that employ AI technology can highlight

the 1-2 percent of video surveillance events that need attention from operators. These intelligent solutions can learn the difference between normal movement patterns and abnormal events in real time. This saves operators time and effort by only displaying the video that requires processing for increased situational awareness.

This type of technology is especially critical in GSOCs that manage a large number of video surveillance cameras at one time, a common issue that developed from an attempt to adjust to an evolving threat landscape. As risks have grown over the years, the traditional reaction has been to add more cameras. At some point, though, this starts to reduce efficiencies. The key is to apply a non-rules-based approach, where the analytics are not trained or told to look for any particular occurrence. Instead, by creating a statistical model of where pixels are at every moment in time, the technology can proactively identify an unusual movement or object and alert to a potential hazard. Operators in a GSOC can then facilitate the next level of action, if necessary.

Operator consoles

For maximum efficiency and situational awareness, the comfort of control room operators is crucial. If they are uncomfortable or distracted or in pain with a sore neck because of bad viewing angles, they can miss critical events or emergencies. One of the most significant elements contributing to control room comfort is a console. A console is not just a piece of furniture; it is the link between an operator and the technology he or she uses daily,

thereby making it exceptionally important that operators utilize ergonomically correct consoles.

Data incorporation

Almost all of the latest devices and applications are producing big data. The amount of information available to command centers will only increase, and as analytics improve, effective data aggregation must follow. New GSOCs will include dashboards that can make sense of a large amount of information and put it in a digestible format to drive streamlined decision-making.

Powered by computer vision and machine learning, solutions that employ AI technology can highlight the 1-2 percent of video surveillance events that need attention from operators.

Networking

The wall between cyber and physical security continues to crumble, as stakeholders realize the need for collaboration to protect the entire enterprise. Visualization platforms in command centers, such as video walls, will take advantage of the growing and valuable network architecture, resulting in less hardware, more redundancy and more reliability.

Improved communication

With decision makers spread out across buildings, campuses or even the world, GSOCs must include the ability to share real-time information about a situation with first responders and stakeholders, no matter where they may be, to enable them to make informed decisions and implement responses.

Bringing It All Together

Once best practices are established, a space is planned and technology is incorporated, it is time for the final piece of the puzzle: full integration. GSOC integrators and experts have a unique position in the industry to weigh in on the best possible configurations of furniture, hardware components and operator consoles. This can be a critical element, since line of sight issues must be addressed for operators to be able to make the best possible decisions for the security of the facility.

As more and more enterprise organizations realize the importance of having a well-designed, intelligent and integrated GSOC within their facilities, there will be a greater need for experts in the field to weigh in on best practices for building such infrastructure. Seeking out experts in this technology is vital to the success of a comprehensive security plan. ■ **Back to TOC**

Dan Gundry (dgundry@vistacominc.com) is the director of sales and marketing for Vistacom (www.vistacominc.com).

Search the SIA Membership Directory

When legacy security systems are upgraded and connected to one another, physically or operationally, companies are able to manage the security programs more efficiently and consistently across multiple facilities and geographies. The challenge is how to get there.

Making the (Up)Grade

When businesses combine, security enhancements are often necessary – and beneficial

By Kami Dukes
AMAG Technology

Three main drivers compel an organization to upgrade or connect legacy systems. Organizations make changes when they need to save money, reduce risk or comply with evolving regulations. Just one of these factors can have an impact on the organization as a whole, which is why the role of the security manager is ever-changing. Security technology is now playing a more critical and broader role in organizations than ever before. As a result, security managers are challenged to think creatively, engage with other departments and balance their existing technical infrastructures with today's cultural expectations of tighter, yet frictionless, security.

How Has Security Changed?

In the distant past, an organization's security personnel often reported to the facilities department. Occasionally, there were dedicated security teams, but they rarely interacted with other departments. Today, legal, finance, IT, cyber and human resources (HR) have a vested interest in security operations. Much of that interest is

driven by a need to meet compliance requirements and the role that each department has in the compliance process.

Some of the interest results from a better understanding of how security systems can affect departmental operations. An example of this is a physical identity and access management (PIAM) system. In large organizations, the onboarding and offboarding of employees, contractors and vendors can be extremely difficult. Many people are involved in approving building and secure area access, all in different departments at different locations, each with their own processes and requirements. No single individual has all the knowledge to ensure that the right people have the right access to secure areas at the right time and that they have the skills and/or certifications to prove it. Granting access often entails multiple emails and phone calls across the organization, so it can take days for a new employee to get an access card.

All of these manual, disjointed processes can bog down an organization in emails, reports and data entry. They also introduce risk to an organization because humans make mistakes. Today, a PIAM system can streamline operations, increase efficiency and manage identities seamlessly. Automating onboarding and offboarding and implementing a distributed model throughout the organization makes turnaround times faster and brings less risk. When a new employee is hired, the HR system acts as the authoritative data source, and the PIAM system initiates the approval workflows and automatically provisions the employee record into the access control system. What used

to take days now takes minutes.

As the economy has grown, we have seen an increase in merger and acquisition activity. Multinational companies are buying smaller companies and expanding into new markets. The security manager's job is now more complex than ever. Tasked with managing the entire security program, this person now must consolidate different types of security technologies, including multiple access control, video, audio, intrusion detection and incident management systems. Often these systems are standalone. They do not communicate with one another, much less with systems already in use at the parent company.

In recent years, this has been especially true in the health care industry, where large health care organizations have bought local hospitals. Similarly, in the data center industry, larger companies have bought smaller data storage facilities, and in the utility sector, there has been a trend toward consolidating utility plants. When legacy security systems are upgraded and connected

> Security managers are challenged to think creatively, engage with other departments and balance their existing technical infrastructures with today's cultural expectations of tighter, yet frictionless, security.

to one another, physically or operationally, companies are able to manage the security programs more efficiently and consistently across multiple facilities and geographies. The challenge is how to get there. How do security managers plan not only for tomorrow, but also for the next three, five or 15 years in a world of constant technology innovations?

Security teams are under pressure to streamline systems and adapt their policies to meet evolving industry regulations. The risk of non-compliance is too high, since it can negatively affect the bottom line and the reputation of the organization. In the health care industry, legacy systems may become an issue when complying with Joint Commission standards and Health Insurance Portability and Accountability Act (HIPAA) regulations. Data centers and financial institutions must report on security-related metrics related to Sarbanes-Oxley Act mandates. In the utilities sector, security managers may face greater scrutiny when under audit as a result of North American Electric Reliability Corporation (NERC) and critical infrastructure protection requirements. How can a security manager bring the entire security program into compliance while improving operational efficiencies? When security systems talk to one another across an organization, security teams can automatically produce the reports and assessments required when they are audited for compliance.

The reputation of a business is essential to its survival. In today's world of social networking and reliance on the Internet and instant communication, a business must be conscious of its reputation on

a continual basis and must be responsive to any crisis that may have an impact on its brand. The security manager is under greater pressure to protect employees, facilities and company assets. Having systems that are future-proofed with automated processes can help to mitigate crises and thereby help to protect reputation. Advanced reporting, for example, can help a security manager be proactive in preventing security incidents before they happen. And it can help to prepare for what could come after a critical incident, such as the inevitable investigations. Quickly and effortlessly proving that the company enforced compliant policies and protocols and did everything it could in a time of crisis is what will save the bottom line.

> How do security managers plan not only for tomorrow, but also for the next three, five or 15 years in a world of constant technology innovations?

How Should Upgrades Be Approached?

First, it is important to invest the time to fully understand the security ecosystem. How should the various systems work with one another? What departments have a vested interest in security operations, and how can the security ecosystem better help them? What are the relevant regulations and standards? A security director should take the

time to understand and maximize the performance of the current technology. Often, a technology has capabilities that are not fully understood. For example, how many people know what every single button and command in Microsoft Word does? Is it possible that, if a person took the time to learn more about Microsoft Word, he or she could learn some tricks that would lead to increased speed and productivity when using that software? Leveraging manufacturer information can be of great assistance in understanding an existing security system. No one knows the intricacies of a platform more than the developers themselves. Maybe there is a built-in visitor management system. Maybe intrusion capabilities exist that are all the company needs. Maybe the system does not require an upgrade. Maybe it can be integrated with other systems across the network.

There are tools designed to connect security systems to one another. Physical security information management (PSIM) software can provide a platform to integrate multiple unconnected security applications and devices and control them through one comprehensive user interface. But PSIM software can be expensive and sometimes difficult to deploy and maintain. Another alternative is command and control software, which is a more affordable platform that captures alarms from all systems in a single window.

Unified and connected systems can save a substantial amount of money on alarm response. Before embarking on a new system design, a security director should take the time to study the hard and soft costs of the

current alarm management program. What manual processes are followed when responding to an alarm? What processes are followed in the aftermath of an alarm? If any of the processes involve opening and sharing multiple spreadsheets or programs or, worse, three-ring binders, time and money are being wasted. Policies and procedures should be automated. The same can be said for implementing identity and access management systems that will streamline processes, save money and ease compliance.

Having systems that are future-proofed with automated processes can help to mitigate crises and thereby help to protect reputation.

Security integrators and consultants can help to assess an organization's security program and design solutions to solve issues with legacy systems and unconnected networks. There can be an upfront cost for this work, but these experts can identify areas for improved efficiency. In addition, they can help to ensure that the system meets industry requirements and is future-proof.

Machine learning and artificial intelligence (AI) are growing trends in security technology. It may be worth the time and investment to upgrade older systems to new technologies that apply data analytics to alarms and events, identifying which types of events are more important than others. What if a system could look beyond the alarm and distinguish behavioral anomalies in employees? Pairing this sort of technology with an insider threat program can be highly effective and can enable a more effective allocation of resources. Manufacturers, integrators and consultants can help with the necessary research.

Lastly, outsourcing elements of a security program in a managed service model can be a cost-effective way of managing capital expenses and ensuring that a program will not soon be obsolete.

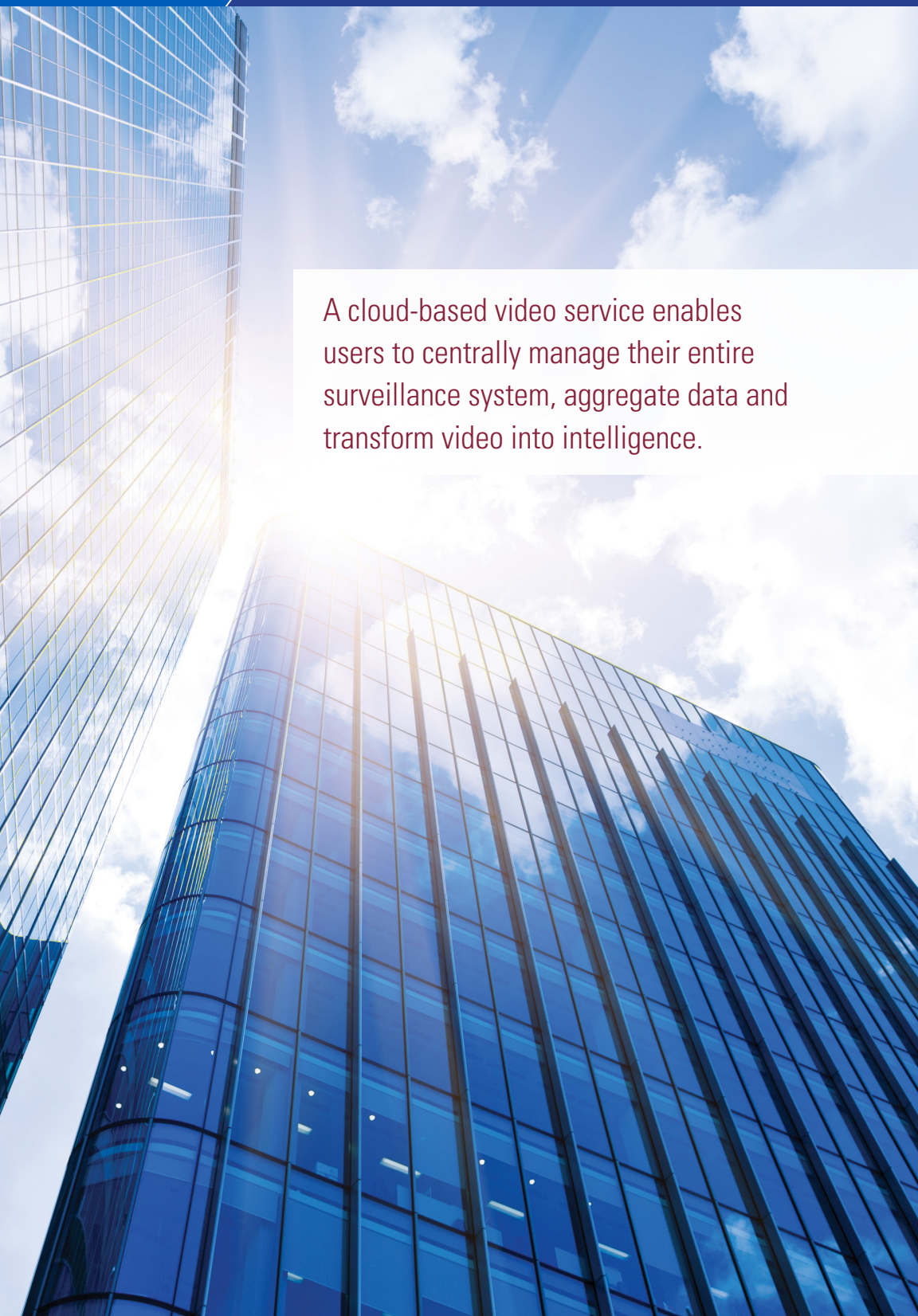
Conclusion

A risk assessment will provide an understanding of an organization's security ecosystem and whether or not it is sufficient to address current and future needs. It will help to identify both the obvious and hidden costs that are required to manage the current program. Before upgrading a legacy system, the critical issues must be diagnosed, and once a new system is deployed, the results should be measured. This process can not only enhance security, but also improve overall business operations. ■

Back to TOC

Kami Dukes (kami.dukes@amag.com) is director of business development at AMAG Technology (www.amag.com).

Search the SIA Membership Directory



A cloud-based video service enables users to centrally manage their entire surveillance system, aggregate data and transform video into intelligence.

No Dark Cloud, Only Silver Lining

Cloud solutions provide multiple advantages over on-premises storage

By Andreas Pettersson
Arcules

We have been talking about the cloud for a while, but the rate of adoption within the security industry has lagged significantly behind other sectors. That is starting to change as the cloud becomes a more viable option for mid-market, distributed and enterprise companies seeking to harness real-time information gathering and evaluation, gain valuable and actionable business intelligence, and increase storage and computing capabilities.

According to Gartner, more than $1.3 trillion in IT spending will be directly or indirectly affected by the shift to the cloud by 2022, with key enterprise IT markets devoting 28 percent of spending to cloud services that year, up from 19 percent in 2018. Gartner also predicts that the worldwide public cloud services market will grow 17.3 percent in 2019 to $206.2 billion, up from $175.8 billion in 2018, highlighting the growth that the cloud is seeing across sectors.

Cloud-based security solutions provide a new approach to detecting and mitigating threats, and applying

the cloud to video takes this one step further. Integrated, intelligent video cloud surveillance solutions are emerging as a go-to tool for organizations seeking to revolutionize the way video and Internet of Things (IoT) sensor data is collected and aggregated to provide insights for both proactive security and business efficiency. But these solutions are not without critics, as this shift requires forward-thinking stakeholders to move beyond the traditional, hardware-focused way of thinking.

The security industry has long relied on on-premises security solutions, often resulting in hardware-based deployments and vast data centers.

> Through 2020, public cloud infrastructure workloads will experience at least 60 percent fewer security incidents than traditional data centers.

For many organizations, the disruption caused by cloud-based technology is significant. Change like this does not happen overnight. It requires high levels of market awareness and education, as well as an evolution in the understanding and acceptance of the cloud. However, as other markets have discovered, the significant benefits of a cloud-based solution – especially in the realm of video data – far outweigh the perceived challenges.

Benefits of the Cloud, Simplified

Cloud-based technologies provide many benefits, including centralized management of solutions, the

ability to monitor and assess risk in geographically dispersed locations, enhanced security, scalability, and flexibility of storage options.

Proactive updates

In traditional on-premises video surveillance solutions, manual updates to hardware and firmware are a time-consuming and complex process. Cloud-based options provide a more proactive approach to protecting video data in order to maximize uptime and identify potential system failures. Gone are the days when someone had to manually check each and every video camera; now, time and money can be saved through automatic updates.

Increased security

As more people do business "in the cloud," there has been an uptick in concern about cloud security. However, cloud services offer significant security advantages as a result of regular maintenance and updates, as well as automatic patches when vulnerabilities are discovered, all of which allows the companies using these services to focus on higher-value, customer-centric projects. Through 2020, public cloud infrastructure workloads will experience at least 60 percent fewer security incidents than traditional data centers, according to Gartner, highlighting the need for a shift to the cloud in many of today's markets. Alternatively, in many legacy video monitoring systems, any open ports could be subject to exploitation if firewalls are not properly maintained.

Scalability and cost

Growth-centric mid-market and enterprise organizations with plans to expand geographically must consider the scalability of their technology infrastructure. Cloud architecture is built to scale with processing and storage needs in mind, empowering organizations to scale up (or down) without the limitations of traditional software and hardware. On-premises video surveillance can present a management and cost challenge for a growing business. As needs change and the business grows, there are hardware and storage purchase requirements in addition to camera investments that must be made. Harnessing the power

of the cloud for video storage and management reduces the cost for both capital investment and management.

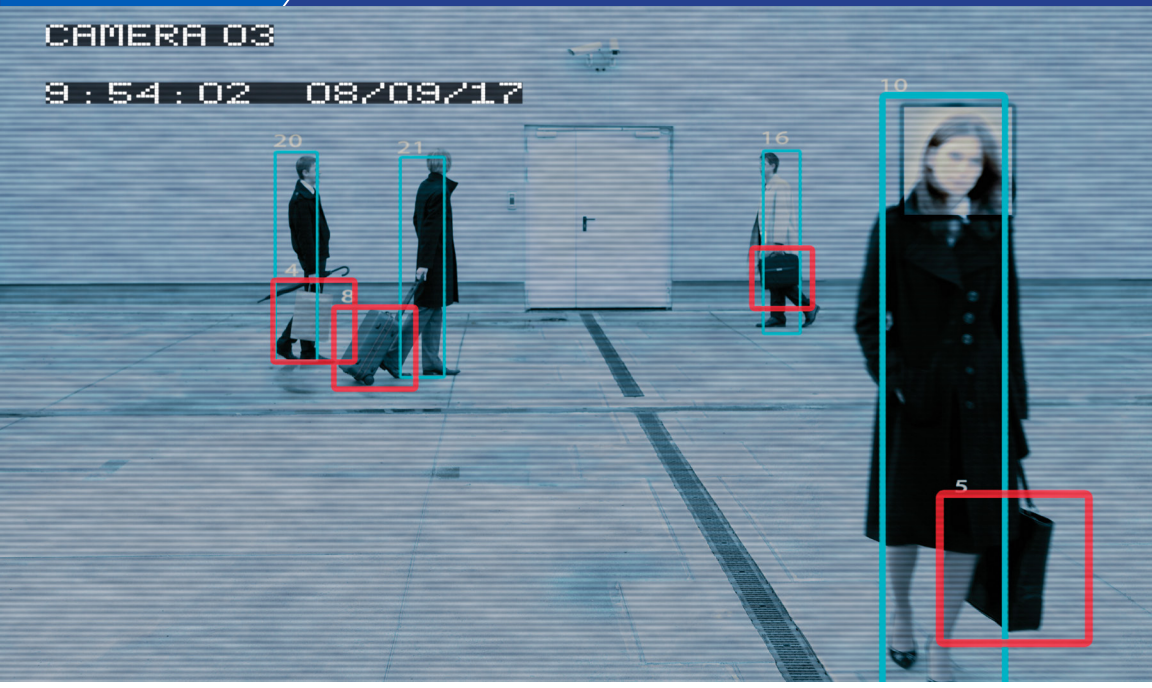
Storage advantages

Memoori recently reported that the world market for video surveillance products in 2018 was $17.57 billion and that this will grow to $32.64 billion by 2023. This will mean significant growth in storage needs as well. According to IHS Markit, the global enterprise and IP storage market is projected to expand at a compound annual growth rate of around 24 percent between 2016 and 2021. However, on-premises storage solutions lack scalability and may require frequent capital investments, depending on a company's needs. Cloud-based solutions reduce those investments.

On-premises storage solutions lack scalability and may require frequent capital investments, depending on a company's needs. Cloud-based solutions reduce those investments.

Centralized management

A cloud-based video service enables users to centrally manage their entire surveillance system, aggregate data and transform video into intelligence. It also combines the visualization of all geographic locations into one global view, giving organizations a comprehensive picture of devices and their status at any given time, which provides an overall picture of system health. A cloud-based solution also has the potential to direct alarm notifications to a single platform that brings together the corresponding video to enhance and streamline footage for investigations.



Bolstering Security with Video-Based AI

To achieve the full potential of cloud-based video, artificial intelligence (AI) and machine learning technologies are being incorporated to enhance video service offerings. By leveraging these offerings, companies can utilize video data in ways they never imagined, helping them make better informed decisions that can transform how they respond to security alerts. As more video data is added, the machine learning models become better adjusted to what is considered "normal" and what might be an anomaly for an organization.

For example, a smart, cloud-based video solution does not just alert a security guard to an intruder; it triggers other IoT sensors to lock down the building and call the police. This technology can notify operators if a person appearing on a video feed might be in a restricted access area. Instead of only functioning as a source of forensic evidence after an incident has occurred, an integrated cloud-based video solution becomes a source of proactive intelligence that can enable personnel to respond immediately to events. Cloud-based services can also leverage AI and machine learning to improve video camera capabilities, a function that is not available with traditional on-premises solutions.

Additional functionalities are being developed every day, including crowd density monitoring and suspicious behavior identification. These tools allow security personnel to observe in real time what they could once only see in retrospect. With intelligent

technology, video shifts from being static to being dynamic in nature, and intelligent analytics can make it useful not only for security, but also for business operations.

Adding Real-Time Business Intelligence

For years, business owners used video cameras as an investigative tool and nothing more. Now, though, AI algorithms are working with video and IoT sensor data to provide companies with business insights that can improve operations.

Cloud functionality adds significant value, as well. Most of the unstructured video data that is collected becomes structured once it is pushed into an integrated video cloud service. In the cloud, video data can be combined with IoT sensor data, such as information from access control and building management tools. As a result of all of these data sources being aggregated in the cloud, businesses are able to identify patterns, investigate anomalies and optimize for efficiency, all from a single platform, no matter the geographic location.

For example, in a hotel, the solution enables management to monitor guest movement, which could assist properties with addressing security concerns and optimizing workflows. A number of markets, in addition to retail and hospitality, are poised to gain significant benefits from the adoption of cloud-based video services, including professional services, distributed environments, enterprise locations and more.

A Valuable Solution into the Future

Integrated video cloud surveillance allows customers the ability to use a

single, unified platform to monitor an entire network of devices and cameras across multiple locations, keeping simplicity, reliability and IT security in mind. Integrated video cloud surveillance is a valuable resource for organizations looking to scale while minimizing operating expenses.

While the security industry is still learning about the possibilities that the cloud brings to the table, it is important to note the many advantages it presents to customers who look to manufacturers, integrators and software providers to present a viable, secure and easy-to-use option for managing video and other IoT sensors. Before this technology is implemented, however, the industry must first clearly understand the business and security value that it provides. ■

Back to TOC

> Instead of only functioning as a source of forensic evidence after an incident has occurred, an integrated cloud-based video solution becomes a source of proactive intelligence that can enable personnel to respond immediately to events.

Andreas Pettersson (andreas@arcules.com) is the CEO of Arcules (www.arcules.com).

Search the SIA Membership Directory

By securing, managing and auditing the use of physical assets, a business can reduce downtime and use resources more efficiently.

In the First Place You Look

A key and asset management system can provide ROI by mitigating loss and theft

By Danny Garrido
Traka USA

How do you determine the return on investment (ROI) that comes from securing your company's keys and assets? As a professional in the security industry, you start to realize just how many companies struggle to answer that question. It goes well beyond lost keys and devices.

Modern security and building systems can be highly intelligent ecosystems that do much more than just preventative maintenance by monitoring, tracking and controlling access to keys and assets. These systems create more streamlined operations for a business, which then create opportunities for continuous ROI.

However, there is a difference between knowing what your current methods are costing you and understanding where and how they are affecting your bottom line. This article will examine how features of intelligent key and asset management can improve operational efficiency and accountability and create financial return.

Operational Efficiency

What do your day-to-day operations look like? Do your employees meet up every morning to check in or receive their keys from a supervisor? Are they starting the day by waiting patiently in line to check out their laptops, scanners or keys to pooled vehicles?

Some organizations use a peg board filled with keys, some an endless set of paper or plastic tags, and some even still have the classic ring of keys hanging from a supervisor's belt. Using these methods to manage keys and assets is a massive drain on operational efficiency in three key areas:

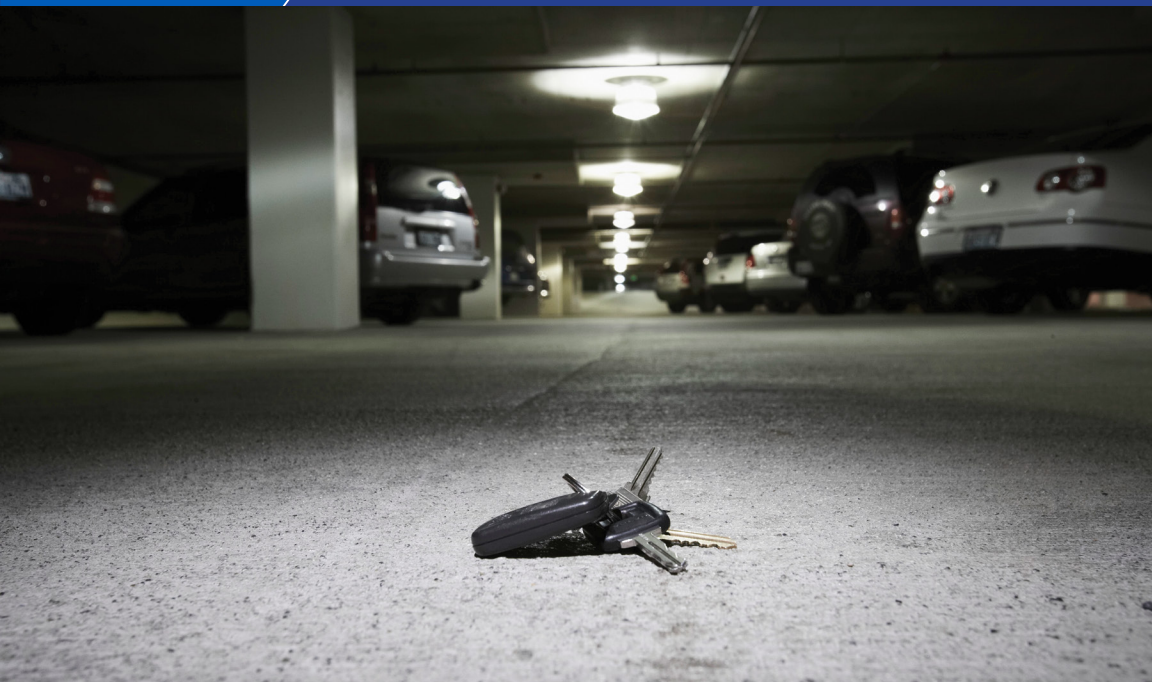
- Use of time
- Risk mitigation
- Operational expenses

Resolving those problems creates an opportunity to save time, proactively manage risk and reduce operational overhead. By securing, managing and auditing the use of physical assets, a business can reduce downtime and use resources more efficiently.

Use of Time

The larger an organization, the longer that manual methods of tracking keys and assets can take. For example, consider the real example of a large university with multiple buildings and more than 10,000 staff members. With 800 employees needing keys at any given time and multiple key sets for each building, this university did not have time for a key shop or supervisor to manually administer keys. They were already experiencing delays from contractors on weekends, who, of course, charged for the time they spent waiting to receive keys.

What was the result? An overall lack of supervision. Keys would go



home with employees or get lost in drawers. When a vehicle was needed by groundskeepers, they often wasted up to 45 minutes looking for the keys, sometimes coming up empty handed. Management had no method of knowing who had what keys or assets at any given time.

The administrative cost of overseeing all of this manually, or with a system that does not function as it should, is massive. When combined with time lost to locating keys and assets – such as scanners, radios and vehicles – this can easily add up to thousands of dollars in lost productivity each year.

Improper asset management can lead to loss in productivity, loss of sensitive data or even loss of life, so it is critical to have the right tools configured for a business's unique needs.

One method that works well for larger organizations, like the university mentioned above, is decentralizing the location of critical keys and assets. Instead of having everything picked up in one location, for example, an organization can automate the distribution of keys and assets where they are going to be used. This limits the amount of time that is spent running back and forth to get ready for shift startup, while freeing up management's time to focus on other tasks.

Again, consider the university example. If 10 minutes of wasted time is saved every day for each of 800

employees, that equals more than 133 hours saved every day. If those employees work five days a week, 50 weeks of the year, then more than 33,000 hours are saved annually.

Risk mitigation

Risk comes in many forms. A key or an asset, for example, could fall into the wrong hands, compromising the safety of employees, the privacy of client information and more. These can be catastrophic losses on many levels, but the right security system and process control can mitigate the threat.

Stolen keys are as much of a danger as lost keys. When an employee leaves on bad terms, a company needs to ensure that that person no longer has access to any sensitive areas or assets. If an ex-employee refuses to return a key, it forces the company into a costly rekeying. When one company redid the roof of its building, workers found hundreds of keys that disgruntled employees had thrown onto the roof after being terminated.

Some of the better software solutions are rich in features that define limited access parameters and provide total visibility over item access, both critical factors in risk mitigation. Several of these systems have the option to limit an employee's area of access to their working hours, or to have an alert go out if an important asset or key has not been returned by day's end. Another benefit of these solutions is that it is much easier to adjust permissions electronically than to do so physically.

This does not just apply to facility keys, either. These permissions can cover virtually any sensitive asset, like heavy machinery, R&D equipment, data racks or firearms. Improper asset management can lead to loss of productivity, loss of sensitive data or even loss of life, so it is critical to have the right tools configured for a business's unique needs. Through an intelligent key and asset management system, a business can automate and enforce safety protocols consistently, effectively and with measurable results.

Operational expenses

When considering an access control or human resources system that integrates with key and asset management, a business should think about the ways in which it can simplify administrative overhead. Can the system automate the check-in and check-out of keys and assets so that a manager does not have to do it? Can it automate the addition or removal of employees and security access seamlessly in real time? These functionalities free up administrative resources, allowing personnel to focus on revenue-generating tasks, translating time saved into money earned.

> When employees know they are accountable for how they treat company property, they tend to be more careful, which extends the life of the assets.

Take a moment to consider all of the expenses of manual operations:

- Loss of management's time to supervision
- Loss of employees' time at start-up
- Loss of employees' time "looking" for something
- Higher overhead costs
- Rekeying and other lost key costs
- Lost or damaged device replacement
- Loss of time because of uncharged devices

It can reach a point where many companies do not even know how much they are spending on these expenses each year.

One retailer had a giant cardboard box full of price scanners. Between staff misplacing scanners, using them roughly and not tracking their use, the retailer did not know how much money it was losing to asset replacement each year. It was just "the way it has always been done."

"We don't know what works and what is broken," the retailer said. "We don't even know how much we're spending on them each year. We just write it into the cost of doing business."

A large benefit of a fully integrated key and asset management system is that it can remove any doubt about how much is being spent on operations. By having that transparency and visibility, business operations become more efficient and produce more value at lower cost.

The Benefits of Accountability

A key part of everything mentioned above is accountability. That is especially the case when it comes to reducing inventory. When operations

lack traceability, the result can be that employees are more careless with company assets and equipment. To cite an example from another retailer, one employee hid a new price scanner above the ceiling tile in the bathroom, just to ensure that no one else had access to it.

It is even more common to see employees monopolize a "favorite" company vehicle, or for new vehicles to suddenly accumulate high mileage while older vehicles go unused. As with keys, it is tedious to do manual logging to track a vehicle's status, fuel level, mileage and discrepancies. Such records are also likely to have errors and incomplete data, as people often skip processes for convenience.

With an integrated key and asset management system, there is no guessing about where items are at any time. If the system tracks user access, then it provides a clear trail to follow if an asset is damaged or missing. When employees know they are accountable for how they treat company property, they tend to be more careful, which extends the life of the assets.

Solutions are also available that allow for the monitoring of the condition of assets, such as the operational status of vehicles. If a staff member notices that a vehicle is faulty, there are integrations that can immediately alert management to lock out that vehicle's use until the situation is resolved.

In short, more accountability creates better staff behavior, which produces a positive impact on a business's annual inventory budget.

Options for Fully Integrated Systems

The ROI of a fully integrated security system is about more than creating

peace of mind; it is a modernization of operations. When in the market for a security system, a business should not only focus on immediate pain points and needs. Instead, the long-term potential of the system as a holistic solution should be considered. The goal should be an all-encompassing security strategy, not just an access control or camera system.

In your industry, which devices do you regularly oversee? What sensitive information do those devices manage? What areas do you need to control access to and why, and can you extend that reach? How do those factors affect your administration, employee efficiency, risk mitigation, external threats and inventory accuracy and cost? The answers are different for everyone.

The goal should be an all-encompassing security strategy, not just an access control or camera system.

No matter which industry you are in, gaining full visibility of your keys and assets through a fully integrated security ecosystem can increase your uptime and productivity while reducing costs and risk for your business.

Some options that can achieve this include:

- Smart keys and locks, intelligent and integrated key cabinets, and lockers that can automate and regulate the check-in and check-out of any asset and, if applicable, keep assets charged
- Setting access permissions to limit key and asset access by user, shift hours and equipment managed
- Tracking the use of keys and assets with 24/7 audit trails to create accountability for staff, while improving safety and reducing the need for rekeying
- Custom notifications and alerts to inform management of faulty vehicles, restricted access and other issues
- Detailed software reporting to oversee operations remotely and gain a high-level view of the performance of the key and asset inventory
- A fully integrated and proven system that can scale if needed and that lives seamlessly in a business's existing security strategy.

These solutions can help extend the reach of existing security systems to crucial offline assets and areas. Chances are, there are multiple avenues to achieving maximum ROI through the security system, so do your due diligence to assess your operations and determine where you can improve. As with any other investment of this type, ensure that the organization implementing the system has a proven and reliable track record and will be around to provide support for many years to come. ■ **Back to TOC**

Danny Garrido (danny.garrido@assaabloy.com) is president of Traka USA (www.traka.com).

Search the SIA Membership Directory

It is critical for organizations in hazardous areas to select security cameras that are made to withstand the harshest environments while remaining able to collect critical information.

Hazard Counting

Hardened video cameras can secure even the most dangerous of sites

By Jumbi Edulbehram
Oncam

Video surveillance technology is a key component of security plans for enterprise organizations. And nowhere is this more true than at oil and gas production sites, critical infrastructure facilities, and manufacturing locations that are considered "hazardous environments." Here, protection, safety and security go hand-in-hand with operations management, and video technology is at the heart of these plans.

These locations can often become targets for vandalism, theft and even terrorist attacks, and a comprehensive security plan that incorporates emerging technology solutions can protect employees, assets and the surrounding communities. The video surveillance technology being developed to meet the needs of these sectors balances providing innovation

with robust functionality and enhanced security in order to protect day-to-day operations.

Technology Innovations and Advancements

Technology advancements in this space include artificial intelligence

(AI)/machine learning, connected devices and the Internet of Things (IoT), cybersecurity and video analytics. Each one of these innovations relies heavily on video, and in hazardous environments, the robustness of the equipment and the resilience of the infrastructure is critical.

Machine learning and AI-enabled devices

Software manufacturers are looking toward AI/machine learning to propel advanced analytics in an effort to deliver more situational awareness to operators.

Seamless integration ensures that events that require more investigation can be pinpointed easily within the system, and that multiple camera angles, access control information and alerts can be immediately called up to formulate an overall picture of what is happening.

While video and data analytic capabilities have been around for quite some time, some would argue they were rudimentary in comparison to software that uses AI and machine learning to make applications such as facial recognition much more accurate and to create new ways to detect anomalies in an environment. In addition, AI/machine learning will increasingly be used to make sense of the large amounts of data that are being

generated by intelligent sensors and by analyzing the growing amount of video.

In hazardous environments, this use of technology becomes vital, especially in locales such as remote oil and gas production sites, where it is difficult, if not impossible, to provide adequate on-site coverage for safety and security. Software that utilizes AI-centric technology can "learn" the normal perimeter of a site down to a pixel change in a video and, when anomalies occur, can send alerts to an operator.

Rise of connected devices

IoT and connected devices have been a major trend in the industry for several years. This is expanding to include environments that must meet stringent regulatory standards, as cybersecurity efforts are bolstered and sensors are integrated into the network. The collection and analysis of data will give rise to a plethora of applications, such as intelligent management of facilities, an increased ability to detect anomalies, and the performance of predictive maintenance. Organizations can benefit by having additional intelligence for situational awareness and emergency management, as well as opportunities to provide advanced asset performance management.

Connectivity also means integration – between video surveillance technology, access control, fire and intrusion alarms, and more. Seamless integration ensures that events that require more investigation can be pinpointed easily within the system, and that multiple camera angles, access control information and

alerts can be immediately called up to formulate an overall picture of what is happening.

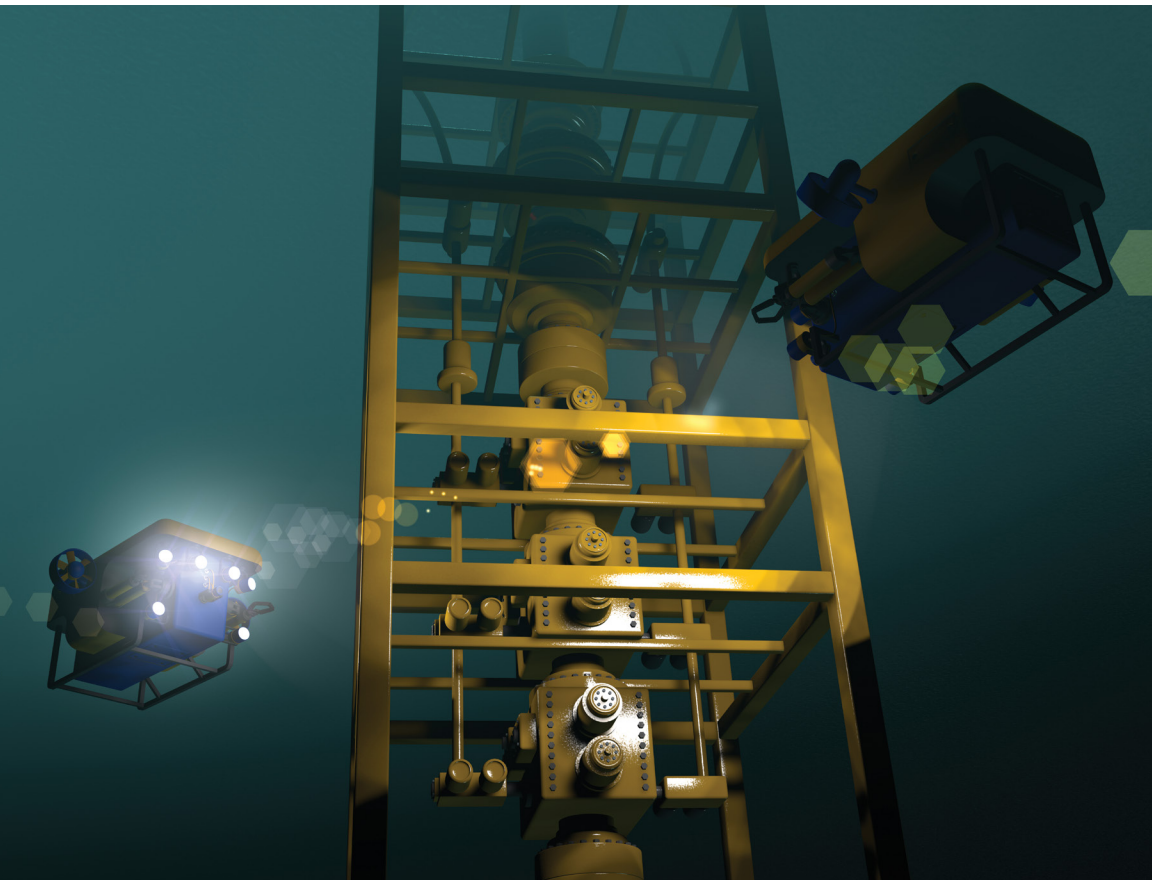
Increased focus on cybersecurity

Cyber attacks have become, and will continue to be, a major threat to critical infrastructure sites and other enterprise-level organizations. It goes without saying that as devices are increasingly connected to a network, the risk of breaches goes up, which is why the shift over the last few years has been around strengthening the security of networked devices. All network-connected devices, such as DVRs/NVRs, servers, video cameras, access control equipment, intrusion alarms and smart sensors, are vulnerable, leading manufacturers to build additional cybersecurity into their products. What is also emerging is that integrators and end users are starting to factor cybersecurity into their buying criteria.

Review of video can reveal sources of shrinkage and ensure proper handling and control of goods across the facility.

Increasing use of video

Video is the cornerstone of security, providing both real-time and forensic coverage for emerging



threats and incidents. The use of video will continue to grow for traditional applications in new markets, such as manufacturing and logistics, as well as for use in newer applications that are not necessarily related to security. In some industries, such as oil and gas, there is a trend toward extending video coverage to monitor operations in extremely harsh and hazardous environments, so surveillance manufacturers will have to develop appropriately certified equipment to meet this demand. Manufacturing facilities such as food processing plants are also increasing their use of video for training and compliance purposes to prevent incidents such as food recalls.

Robust Protection in Hazardous Environments

It is critical for organizations in hazardous areas to select security cameras that are made to withstand the harshest environments while remaining able to collect critical information. Video solutions that use hardened protective enclosures and provide exceptional video quality make the safekeeping of these critical sites possible.

Strategic placement of panoramic surveillance cameras is key to maximizing coverage and enhancing situational awareness. Panoramic IP cameras are now available with ATEX, IEC and IECEx-certified enclosures for locations where combustible fuel

materials are in close proximity and explosions may occur. (See the sidebar for more of these standards and where to look for them.) Combined with additional ratings such as IP69K/IK10, these enclosures are rated for resistance to high-pressure water jets, dust and vandalism, greatly enhancing the surveillance of critical infrastructure.

Another important consideration in selecting video surveillance equipment for hazardous environments is ease of integration. "Open" platforms can deliver the flexibility and scalability that organizations need in order to utilize existing systems and implement new ones as needs change. Incorporating solutions that allow for the flexibility to scale, as well as the means to achieve business intelligence and increase situational awareness, can aid security personnel in establishing a comprehensive security plan that maximizes return on investment.

Open platform solutions also enable relatively easy integration between disparate systems, incorporating not only video data capture, but also data from third-party systems, such as access control, industrial controls, motion detection sensors, leak detection sensors, thermography and license plate recognition. The ability to combine data from multiple sources enables full situational awareness.

Additionally, specialized 180 and 360-degree surveillance technology has emerged as an important element in a comprehensive security plan, delivering wide-angle views of large, open areas. Panoramic coverage offers security operators and facility managers the ability to see a large area with no blind spots and also

Certifications for Hazardous Environment Protection

When customers with facilities in hazardous environments seek out products, there are multiple certifications available to ensure the utmost in protection for video surveillance equipment. These include:

IECEx: The International Electrotechnical Commission (IEC) has identified the IECEx voluntary certification scheme as its system to facilitate the acceptance of equipment for use in explosive environments in many countries around the world. The system is based on zones that define the probability of ignitable hazardous material being present in the atmosphere, such as gas and dust.

ATEX: National deviations of the IECEx standard are used throughout the world, with ATEX a requirement in the European Union. The ATEX certification describes what equipment and work is allowed in an area with an explosive atmosphere, and its qualifications are similar to those of the IECEx certification. The ATEX mark certifies a camera for use in non-mining, explosion-prone environments, with an ambient temperature between -20°C and +55°C.

NSF Certification: NSF International Standard 169 – Special Purpose Food Equipment and Devices serves as the benchmark by which all commercial foodservice equipment products are measured. Certification signifies to customers, specifiers and health departments that the products have been reviewed and certified by an independent third-party organization to the industry's leading standards and that they meet all applicable North American regulatory sanitation requirements.

NEMA: The National Electrical Manufacturers Association (NEMA) develops product standards for the North American market equivalent to the ingress protection (IP) ratings for various grades of electrical enclosures typically used in industrial applications. Each is rated to protect against personnel access to hazardous parts, and additional type-dependent designated environmental conditions.

IP69K and IP68: The IP rating system is an internationally recognized scale that relates to proven protection against environmental factors such as liquids and solids. IP69K is the highest IP protection rating available against water and dust ingress and is widely used to test products that need to withstand sanitary washdowns. IP68 certifies protection against submersion in water.

IK10 and IK10+: The impact protection (IK) rating signifies the degree of protection provided by an enclosure against external mechanical impacts. In other words, this rating determines the camera's level of impact and vandalism protection.

allows operators to zoom in on areas of interest in live as well as playback mode. A single 360-degree camera can replace multiple narrow field-of-view cameras, resulting in a more expansive, cost-effective solution for critical infrastructure and hazardous sites.

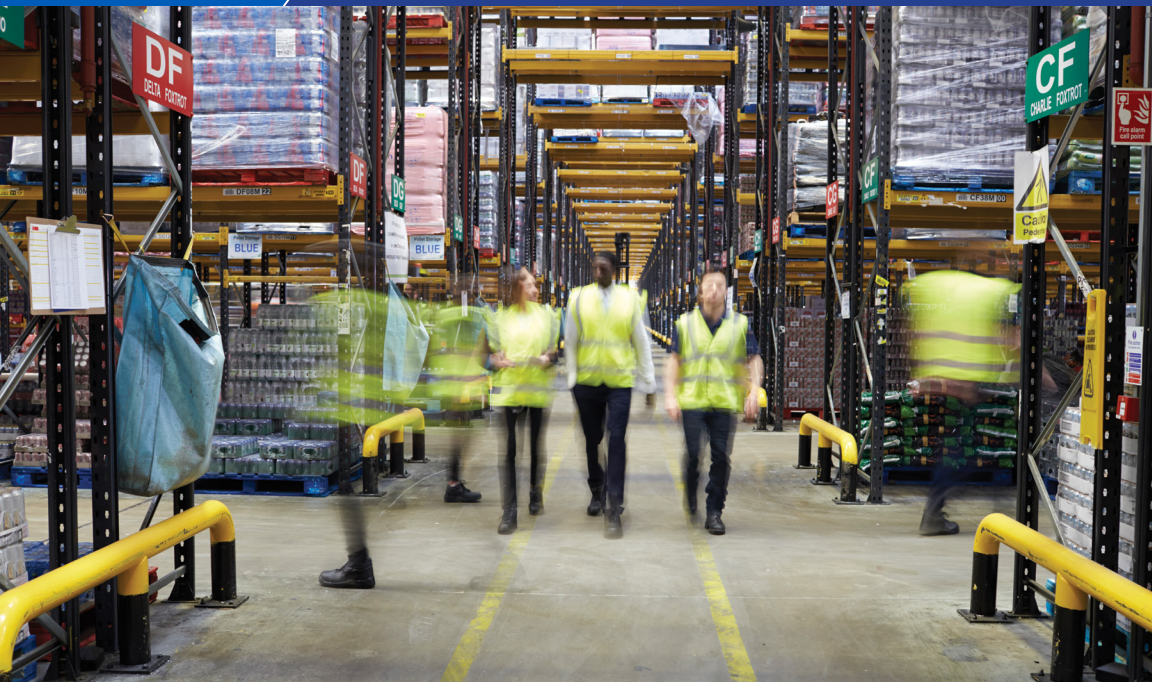
The advanced level of situational awareness provided by wide-angle surveillance cameras enables management to pinpoint instances in which policies are breached and to identify areas that can be improved.

Manufacturing and Logistics Protection

There is another area where hazards exist in the workplace and video surveillance is required to adhere to stringent regulations: manufacturing and logistics. With many moving parts and challenges to consider, manufacturing, logistics and even transportation services must turn to advanced security solutions that enhance safety, compliance and business operations.

One of the biggest challenges for companies that operate industrial facilities – factories, warehouses, loading bays, etc. – is the fact that activity is not confined to one location; the supply chain is extensive and complex. As goods are transferred between facilities, each individual location creates an additional area of exposure and risk.

A key requirement is tracking products and processes throughout the entire supply chain, which requires extensive use of video. This coverage can be made more robust with the use of 180 and 360-degree video technology. Deploying high-resolution,



wide-angle surveillance cameras in facilities, vehicles, handling spaces, docks, and entrances and exits can ensure extensive coverage for live monitoring and, if necessary, incident review.

These surveillance tools can also be useful for business operations, as a bustling supply chain and expansive facilities raises the risk of shrinkage. Review of video can reveal sources of shrinkage and ensure proper handling and control of goods across the facility. Another major concern is compliance with appropriate health and safety procedures. With many people and assets moving in a variety of directions on foot and in vehicles, it can be challenging to guarantee comprehensive compliance.

The advanced level of situational awareness provided by wide-angle surveillance cameras enables management to pinpoint instances in which policies are breached and to identify areas that can be improved. Additionally, when it comes to liability, recorded video allows for easy verification of the cause of an incident.

Protecting critical infrastructure and hazardous environments is of paramount importance to the health and well-being of society. Video surveillance systems are vital to ensuring safety and security in these areas, so it is essential for organizations to make sure their systems meet or exceed quality standards and regulatory requirements. ■ **Back to TOC**

Jumbi Edulbehram (jedulbehram@oncamgrandeye.com) is regional president – Americas at Oncam (www.oncamgrandeye.com).

Search the SIA Membership Directory

Security practitioners and systems integrators need to work together to move forward and embrace new technologies that help them collaborate and deploy technologies efficiently and quickly.

The More You Know

New technologies can improve information sharing and efficiency

By Brandon Wimer
System Surveyor

One of the biggest headaches for a security practitioner typically is finding the most up-to-date version of an organization's security system floor plan or "as-built drawing." Is it in an old PDF on a computer used by someone who has since left? Is it in the file cabinet gathering dust? Is there a system of record with locations of device assets in the first place?

Why is this a problem? The issue is that when a stakeholder or executive needs to see the plan, it is not easy to show a current visual map. It also makes designing, planning and moves/adds/changes inefficient for an already under-resourced team, and it makes budgeting for the year ahead difficult or inaccurate.

Why are we still in this state in 2019? There are a few factors at play here that are addressable. First, most security practitioners and facilities managers need to work with not one but several integrators to address the needs of multiple geographically dispersed sites. Integrators are essential to the planning, purchase, installation and maintenance of security

technologies, but it is easy to get out of sync with them and realize that they hold the key to the castle, since they have the most recent as-builts. Second, security managers say that they have information in many places, including Visio, spreadsheets and siloed project documents, and are frustrated that it is not all in one place. Having to locate and gather all of this information creates inconsistencies and inefficiencies.

This article addresses opportunities to improve the process for the security practitioner and integrator partner alike. It puts the technology manager in a better position to rapidly meet the organization's demands, maintain a high-quality system, and effectively budget for the future.

In most cases, the information flow between security technology managers and their integrator and vendor partners leaves much to be desired.

Improve Collaboration with Integrator Partners

Systems integrators are a vital partner when designing, procuring, installing and maintaining security and IoT assets. However, in most cases, the information flow between security technology managers and their integrator and vendor partners leaves much to be desired. It all starts with the site survey. This is where you walk the site with your integrator and talk about precisely what you need. The question is: Did they record this information accurately and completely? Nine out of 10 integrators still do this by using a paper floor plan and drawing in the needs and taking some pictures. Unfortunately for the

customer, they miss a lot of information this way and often come back several times with an inaccurate proposal. Moreover, once they do get it right, it is not easy to share a CAD plan or detailed engineering document. That is when you lose a bit of control.

What if you could communicate more effectively and visualize the planning process? What if all of the information could be captured in one place? These capabilities are critical because the use of paper, spreadsheets and cameras is inadequate to meet the demands of internal customers.

Security practitioners and systems integrators need to work together to move forward and embrace new technologies that help them collaborate and deploy technologies efficiently and quickly. As an example, at the University of Nevada, Las Vegas, students working with the police's IT department have not only mapped all of the surveillance cameras on campus using a digital design tool, they have made it possible to capture site surveys when areas need new video surveillance cameras, making it easier to collaborate with integrators and vendors to rapidly meet the institution's demands.

Embracing Technology to Gather Information

Both security managers and integrators say they are using multiple tools to gather information – sometimes five or six to address all of the system needs. While paper floor plans and traditional information gathering approaches are familiar and comfortable, they are causing hours of inefficiency. Today's mobile tablets, integrated cameras and apps can be game changers for gathering details more effectively in one place.

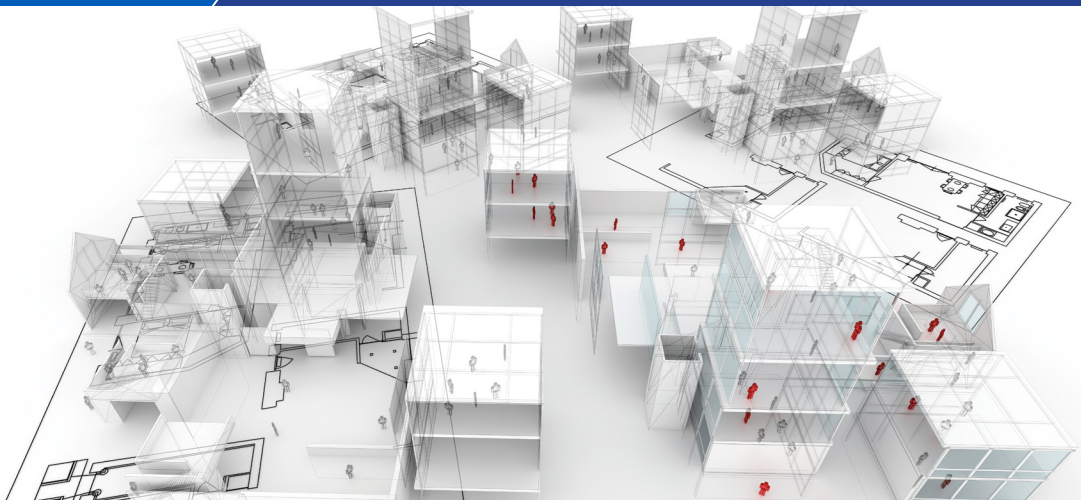
Along with the development of industry-specific apps, the proliferation of cloud-based security-as-a-service

makes it easier for security practitioners and their technology managers to securely share information with their team of integrators. Uploading and sharing documents, photos, data, and spreadsheets through the cloud makes it easier for integrators to quickly and accurately collect details for every project. Security professionals and integrators can now bring all of the information together in one place, making the collaboration process more efficient.

> While paper floor plans and traditional information gathering approaches are familiar and comfortable, they are causing hours of inefficiency. Today's mobile tablets, integrated cameras and apps can be game changers for gathering details more effectively in one place.

Establishing Consistency

Electronic security systems are part of the massive proliferation of Internet of Things (IoT) technologies. They are IP-based devices that need to be implemented, maintained and managed to end-of-life. From a security practitioner's standpoint, the technological changes are all coming fast and furiously, even as they have to find ways to do more with fewer resources. One area of opportunity is to improve



the management of security and IoT. Several facilities managers at large, multi-site enterprises have said that every location has a different way of sharing information. This represents another opportunity to standardize information sharing so that when a new hire comes on, that person can be brought up to speed quickly.

Take, for example, a financial institution that acquired more than 50 branches in a year's time. The security director needed to implement the standard security framework to ensure branch compliance, conduct the budgeting for new technology, and plan for the implementation with various integrators and vendors covering different geographic areas. This type of situation requires consistency and access to plans to understand precisely what security assets are in place and how they can be managed.

From a security practitioner's standpoint, the technological changes are all coming fast and furiously, even as they have to find ways to do more with fewer resources.

Improving Control over System Delivery

It is time for the industry to embrace better ways to manage critical security systems and other IoT assets. The good news is that it is a win-win-win situation for security managers, integrators and vendors. If each of the key players in the ecosystem more effectively shares information, designs systems accurately and transparently (and securely), and collaborates on digital plans, there is much to gain for everyone involved. Most importantly, this allows security practitioners to most efficiently and effectively do what they do best: keep people and property safe and sound. ■ **Back to TOC**

Brandon Wimer (bwimer@systemsurveyor.com) is the digital marketing manager for System Surveyor (www.systemsurveyor.com).

IoT device manufacturers and platform service providers have a responsibility to make sure their devices can be patched remotely so they are resilient to attacks.

Mitigating Risks from A to Z-Wave

A wireless standard delivers interoperability but could create vulnerability

By Pamela Gupta
OutSecure

Zigbee and Z-Wave are wireless standards that enable home and building automation devices to communicate with each other without using Wi-Fi or Bluetooth. Z-Wave is lower power than Wi-Fi and has a longer range than Bluetooth. This article will examine the complexities and vulnerabilities introduced by the Internet of Things (IoT) in physical spaces.

In any product development life cycle, it is more cost effective to perform threat modeling and security testing early in the development cycle, but with IoT, that issue gets magnified.

Z-Wave is a wireless networking technology designed for home automation. It transmits data in small chunks and uses minimal power. There are more than 50 million Z-Wave devices worldwide, and more than

200 companies manufacture Z-Wave compatible hardware.

The Z-Wave Alliance and certification process ensures that devices from different manufacturers can interoperate and that they work correctly in a mixed-vendor

environment. These devices include, for example, electronic door locks, HVAC systems, lamp dimmers, swimming pool pumps, and garage door openers.

Z-Wave uses radio frequency communication in a mesh network to monitor, control and read the status of devices. Each of the devices can relay data packets through the network, obviating the need for a router. Home automation systems can be controlled either via a remote control or through an online connection. For Internet connectivity, a gateway needs to be installed that can be configured to control the home automation network via Wi-Fi or, for some products, an Ethernet wired connection.

Z-Wave protocol has the following layers:

- Physical Layer – The physical layer specifications for radio communications
- Data Layer – Where MAC address is stored and encryption occurs, if enabled
- Transport Layer – Responsible for packet transmission and retransmission; devices with limited power supply, such as door locks, are often designed to reduce power consumption by entering a sleep mode and periodically checking for incoming data; this layer wakes up the device when necessary
- Network Layer – Z-Wave uses mesh networking that enables any node to communicate directly with another node or through relays; there can be 232 devices and one controller device on a network; this layer contains a unique 32-bit ID for the home controller and an 8-bit node ID for each accessory,

which is assigned when a new device is paired with the system

- Application Layer – This layer parses network packets to decode the Z-Wave command payloads which define functionality for the devices, such as door locks and thermostats; each command class can contain multiple commands that can be actions or data collection (i.e., lock the door or get information if it is in a locked state)

For transmission to occur between a device and the central controller of the home, both must share a network key that allows for communication. When a new device is paired via Z-Wave, a specific syncing protocol is executed in order to share this network key with the device. First, a "preamble" packet is sent between the receiver and transmitter, containing a specific series of bits, the home ID and node ID of the device to pair.

> In any product development life cycle, it is more cost effective to perform threat modeling and security testing early in the development cycle, but with IoT, that issue gets magnified.

Critical Security Issue in Wireless Door Locks

Behrang Fouladi and Sahand Ghanoun, in their presentation at Black Hat 2013 titled *Honey, I'm Home! – Hacking Z-Wave Home Automation Systems*, explained the security implications of a particular lock that used Z-Wave.

They found that the first time the lock was paired with a controller, the devices exchanged encryption keys using

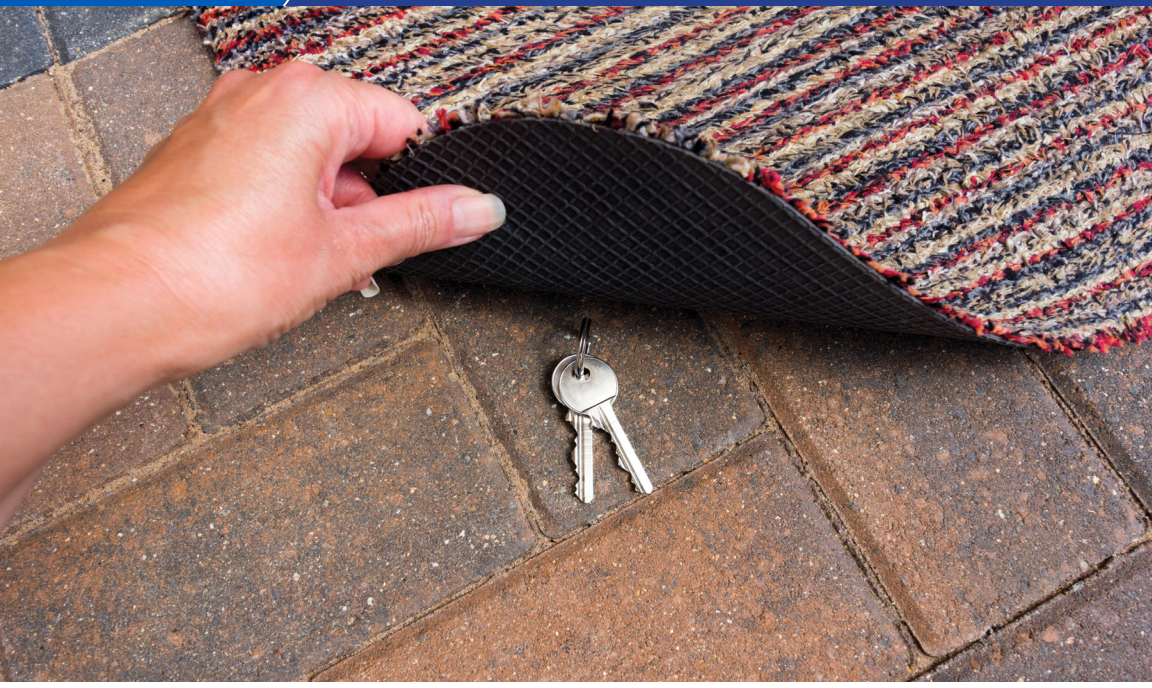
custom key establishment protocols AES-OFB and AES-CBCMAC, and a 64-bit nonce value, a random value that can only be used once, as well as a 128-bit random number key to encrypt transmission of the network key. The keys were generated using a hardware-based pseudorandom number generator on the Z-Wave chip and encrypted using a hard-coded temporary default key of all zeroes in the chips's firmware.

"The word 'custom' in cryptography rings off alarms," Fouladi said in the Black Hat presentation. They went further, even without documentation, to crack the key establishment protocol and carry out attacks. The protocol begins with the controller sending an initialization packet to the device, which responds with a ready packet. The controller replies with a nonce value and the lock returns it to confirm that communication has successfully been initialized. Next, the controller generates a random network key and temporary encryption key, and sends it with the actual network key to the device. The device then constructs a secure packet using this information to prove that it has properly decrypted the securely transferred network key.

> This illustrates how a simple design flaw can have major repercussions on multiple levels – for the owner of the device, the device manufacturer, implementers of firmware and radio protocols.

Now, both the controller and the device have the same network key and can use it for further communication when the homeowner wants to lock or unlock the front door.

The team also described a severe vulnerability: "Key Reset Attack," which



takes advantage of the fact that the pairing protocol can be run multiple times for a single device. Using the home ID of the controller, which is easily retrieved from any intercepted packet, the team could pretend to be the controller and run the key establishment protocol with the door lock again.

The security issue here is that once the lock has paired with a controller, it should check its current key and load the existing key from its electrically erasable, programmable, read-only memory. The lack of this basic validation step is what allows the door lock to be compromised and not perform its basic function. Another important result is that, once the lock has been compromised, events such as "door open" will be rejected by the controller, since it will now only accept packets from the new pairing and will therefore reject the valid payload, worsening the situation since no warnings will be issued that the door is open or unlocked.

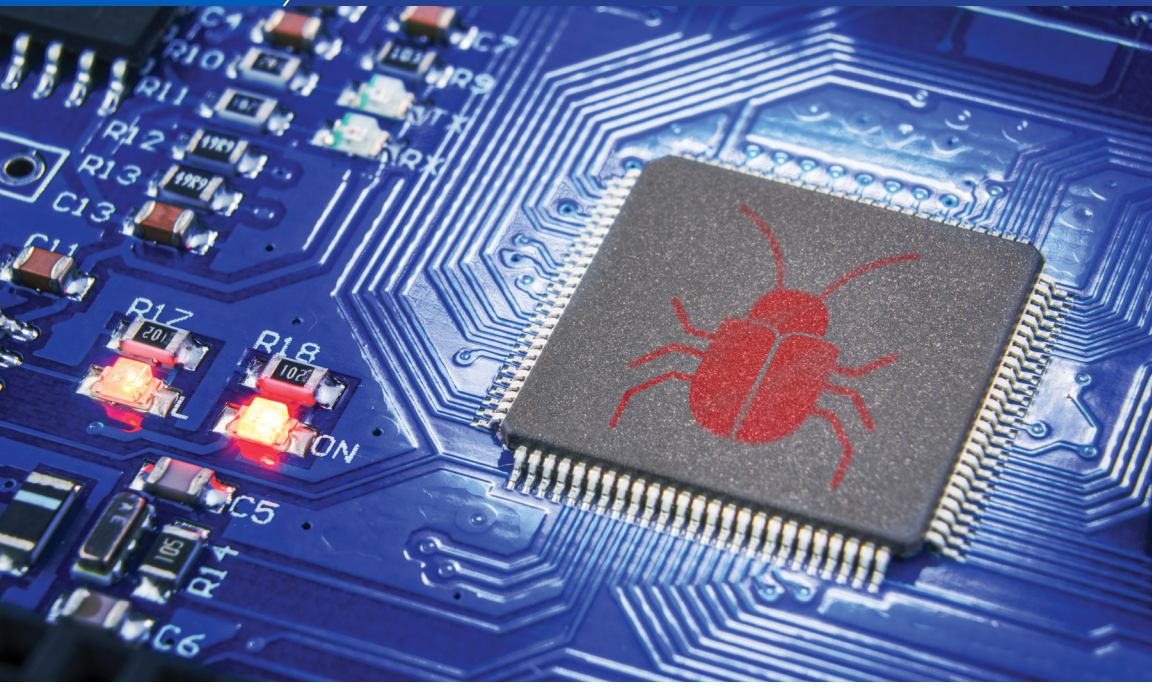
> Tens of millions of smart home devices are, as a result, vulnerable to hacks that could lead to break-ins or a digital haunting.

This illustrates how a simple design flaw can have major repercussions on multiple levels – for the owner of the device, the device manufacturer, implementers of firmware and radio protocols.

Even though the owners of Z-Wave responded quickly to Fouladi and Ghanoun to validate their findings and remediate the vulnerability, the issue of applying firmware updates still stands. Managers of physical facilities and homes do not normally have a process that involves checking for firmware updates and applying them to their door locks and controllers. What's more, the 6-year-old flaw lies in software that has been shipped to more than 100 million home automation and security installations. Doorbells, bulbs and house alarms are among the countless products from 2,400 different vendors that contain the flawed code. Tens of millions of smart home devices are, as a result, vulnerable to hacks that could lead to break-ins or a digital haunting.

> Manufacturers must ensure that their engineers and architects fully understand the threat model of their products and that the proposed architecture is fully assessed and inspected by an independent, qualified third party.

In 2018, a white hat hacking group found a vulnerability in an underlying standard used by a Z-Wave lock in the communications between the lock and the paired device that



controls the system. The flaw meant that communications could be intercepted and manipulated to make it easy for someone in the local area to steal keys and unlock the door.

So the problem continues and is not going to be eliminated any time soon.

Moving Forward

IoT device manufacturers and platform service providers have a responsibility to make sure their devices can be patched remotely so they are resilient to attacks. In June 2017, we saw the first state attorney general action, in New York, against a wireless security company for failing to implement adequate security in IoT devices.

Manufacturers must ensure that their engineers and architects fully understand the threat model of their products and that the proposed architecture is fully assessed and inspected by an independent, qualified third party. A clearly defined process should exist for communicating and reporting security vulnerabilities that are discovered outside the company, such as by security researchers. There are a range of upcoming applicable regulations globally that include sanctions for non-compliance, which could have serious financial and reputational implications for corporations and staff. ■ **Back to TOC**

Pamela Gupta (pamela.gupta@outsecure.com) is president of OutSecure (www.outsecure.com).

Search the SIA Membership Directory

The reactive approach to dealing with IoT security must be transformed into proactive engineering practices aimed at locking down and securing IoT capabilities from the beginning.

Online and Under Attack

Cybersecurity must be built in to protect connected security products

By Brian Russell and Leo Dorrendorf
VDOO

The December 2018 McAfee Labs Threat Report identified 45,000 new Internet of Things (IoT) malware variants in the third quarter of 2018. The number of attacks will continue to increase as more products are "IoT-enabled," opening new communication pathways but also exposing vulnerabilities. Yet Gartner's chief of research has said that, in 2019, most IoT security budgets will go toward fault remediation, recalls and safety failures. The reactive approach to dealing with IoT security must be transformed into proactive engineering practices aimed at locking down and securing IoT capabilities from the beginning. Security product manufacturers must understand the types of threats their products are exposed to when connected to the Internet. Having this knowledge allows proper decision making regarding where to spend limited budget resources.

A look at the cybersecurity threat landscape shows a trend toward new attack methods. For example, automated malware is beginning to target IoT products to mine cryptocurrencies. The goal here is to collect as many vulnerable devices as possible and use them all for a single purpose. Volume is critical, so attack scripts are constantly searching for newly connected products that have known vulnerabilities. Ransomware attacks also introduce new concerns

for security product manufacturers. If automated attack scripts can compromise a product and use it for malicious purposes, these same scripts can also be used to shut down product services and render them useless without payment of a ransom.

What this means to security product manufacturers and consumers is that, as soon as a product is connected to the Internet, it is exposed to a torrent of attacks. There is no time to properly configure the security of a product if it is shipped with a known weakness. It will simply be compromised from the start.

Establish Product Cybersecurity Goals

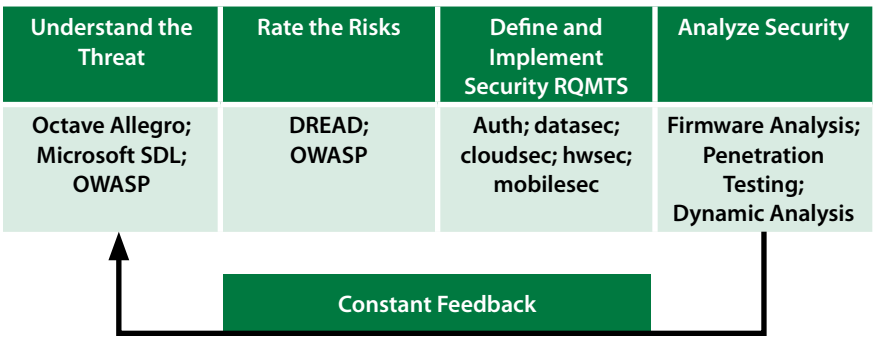
The starting point for any cybersecurity program is to establish goals. These goals are defined by examining the impact areas associated with a security breach. A breach might result in a diminished reputation, financial loss, productivity loss, negative safety consequences, or fines and legal penalties. For example, a critical set of cybersecurity goals might include:

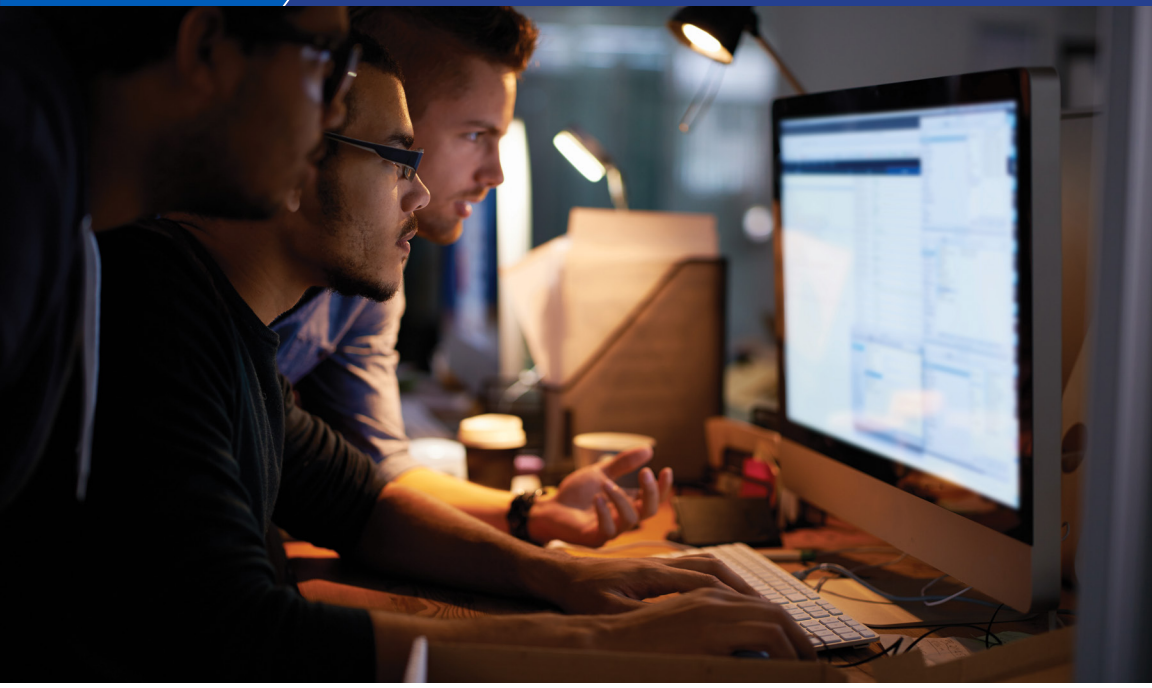
- Maintain product availability – Guard against ransoming, denial of service and misconfigurations that render a product, service or feature unusable
- Protect sensitive data – Guard customer and stakeholder data from compromise, whether it resides in the cloud, in a mobile application or on a device
- Protect privacy – Guard against eavesdropping on customers through video, audio or even data hijacking
- Protect from automated attacks – Apply basic cybersecurity hygiene to safeguard products from being hijacked into botnets

Accomplishing these goals requires a methodical cybersecurity development program. This program should provide product management staff with the knowledge needed to understand the unique threats to the product line and to be able to translate that knowledge into actionable product requirements.

Understand the Threats

Product managers should understand the specific threats to their product line. Not all threats are applicable to all products. For example,





the threat that an attacker might tap into a video feed to surreptitiously monitor their victim may be limited to surveillance (audio/video) equipment. It is a good practice to document threats based on a set of criteria. One threat profile methodology known as Octave Allegro from Carnegie Mellon supports building a threat profile by defining the actor that would exploit the threat, how that actor would attack, the motive for doing so, and the resulting effects.

A key step in understanding threats is gaining a better understanding of the specific types of attacks that might be executed. Table 1 provides a sampling of attack types that are used on the Internet to gain access to IoT products.

Once the members of a security team understand the types of attacks that a product might face when connected to the Internet, they should document the threats in a consistent manner that can be communicated to the product development team. The process of understanding product-unique threats is known as "threat modeling." Although this process can seem complex, there are tools that can help security analysts. The Open Web Application Security Project (OWASP) provides a free

> What this means to security product manufacturers and consumers is that, as soon as a product is connected to the Internet, it is exposed to a torrent of attacks.

Table 1. Sample Attack Types Used to Gain Access to IoT Products

Attack Type	Description
Credential extraction	Obtain credentials which can be used to communicate to the device while impersonating a legitimate user, or which can be used to communicate with other hosts while impersonating the device
Data collection	Extract private, sensitive, restricted or otherwise valuable data from the target device
Denial of service	Evade detection of pirate tools and avoid other defenses; usually done by variations of techniques in other categories that have the added benefit of subverting a particular defense or mitigation
Device hijacking	Subvert the device's resources for the attacker's purpose; this includes the device's network connectivity, computation capabilities and physical capabilities, if any
Lateral movement	Access, control and gather information from remote systems on a network, possibly including execution of remote access tools; movement across a network from one system to another may be necessary to achieve an attacker's goals
Malicious code execution	Execute a code which is not an original code of the device but is maliciously plugged into it for execution; this code is intended to either take advantage of a device function or just harm it
Malicious login	Gain control of the device in the form of an interactive login session
Malicious update	Gain control of the device in the form of an update which modifies the device's behavior to suit the attacker
Privilege escalation	Obtain a higher level of permissions on a system or network; adversaries enter a system with unprivileged access, taking advantage of system weaknesses to obtain local administrator or root level privileges
Reconnaissance	Gain knowledge about the system and the internal network so the attackers can orient themselves to what they have gained control of and to the benefits the operating system can provide to their objectives
Remote exploitation	Exploit a software weakness to make the device execute code provided by the attacker over the network
Traffic interception	Passively intercept network traffic from a device via a man-in-the-middle attack or by eavesdropping on unencrypted communication
Traffic manipulation	Actively modify data sent and received between the device and other hosts by intercepting, modifying, replaying or otherwise manipulating network traffic

threat modeling tool known as Threat Dragon that allows users to diagram systems and generate threats and mitigations. Microsoft also provides a threat modeling application that can be downloaded at no charge. With this, users can create templates that can be reused for new product versions. These templates can define standard information flows, types of threats, components, and attribute values associated with the components of a product.

Rate and Prioritize Threats

The mere existence of a threat does not mean that action must be taken to mitigate it. A risk analysis process is an essential component of a cybersecurity program. Product teams should be able to evaluate each individual threat to determine a risk score. The risk score is based on the likelihood of the threat being realized and the impact of the threat. A standard calculation for risk score is:

> Risk calculations provide quantitative information that can help managers decide whether to mitigate a risk, defer it, or even accept it.

risk=likelihood*impact

OWASP again provides useful information that can be used to better understand all that goes into determining the likelihood of an event occurring. It offers tips on understanding and evaluating the skill level and motivations of an attacker, as

well as ways to quantify the impact of an event.

Microsoft also provides a well-known methodology for calculating risk known as DREAD:

- Damage – What amount of damage (physical, monetary, reputational) would occur?
- Reproducibility – Can the attack be reproduced easily?
- Exploitability – How difficult is it to execute the attack?
- Affected users – How many customers or stakeholders will be affected?
- Discoverability – Is the threat well known? Can anyone discover it?

Prioritization of risks is a business process. Risk calculations provide quantitative information that can help managers decide whether to mitigate a risk, defer it, or even accept it.

Define and Implement Security Requirements

Once a product team has prioritized the risks and defined the mitigations that will be required to combat the most pressing threats, it can begin to identify security requirements to be added to the backlog. Security requirements and controls are available from a variety of industry organizations, including:

- The Security Industry Association (SIA), specifically its IoT, Cloud and Mobility Subcommittee, which is in the process of defining recommended cybersecurity controls for connected security products
- The Cloud Security Alliance (CSA), whose "Future Proofing the Connected World" paper recommends a set of controls for secure product development
- The European Union Agency for Network and Information Security (ENISA), which has published recommendations for minimum baseline security requirements for connected systems

Product teams can review documentation from these organizations, then map applicable controls to the mitigations identified in their risk analysis. Although each security product is unique, certain security controls should be considered for every type of connected product. Table 2 provides a set of best practice security guidelines that product manufacturers should consider implementing.

Test Product Security

One of the most important aspects of any cybersecurity program is testing. Comprehensive testing of connected devices allows the program team to identify design flaws, gaps in requirements coverage or handling, and flaws in code. There are several types of security testing that a product team should conduct. Ideally, testing should be continuous. Test tools that look for non-adherence to coding standards and typical software development flaws should be incorporated in the continuous integration (CI) environment and run upon each check-in. These tools will alert the team and will even halt code

Table 2. Best Practice Security Guidelines

Objective	Description
Secure the boot process	Enforce device policies that: • Verify the firmware signature prior to booting • Restrict standard users from making modifications to boot process options • Reset the product if the boot process fails
Enable a secure onboarding process	The bootstrap process allows the user to bring the product into an operational state; products should: • Provision unique default passwords for each device • Incorporate hardware-based security for cryptographic key storage • Optionally partner with a cloud service provider to enable zero-touch provisioning
Develop good authentication practices	Authentication weaknesses represent a common attack vector; products should: • Require strong (complex) passwords • Require that default passwords be changed upon first use • Ideally use certificates instead of passwords for authentication • Incorporate multi-factor authentication for cloud services
Manage privileges	Once an attacker gains access to a device, limit his ability to cause more damage by: • Disabling the root account and requiring sudo access for all elevated privileges, • Limiting the privileges associated with any particular account
Enable secure pairing	Many options exist when implementing pairing mechanisms; be sure to: • Use security-enabled pairing mechanisms for all device-to-device interactions
Use good cryptographic practices	The selection of cryptographic libraries and protocols underpins the security of a product; make sure to: • Use Transport Layer Security (TLS) 1.2 or above for all interfaces to the cloud • Enable Secure Shell (SSH) for remote access • Only use standards-based cryptographic algorithms and protocols
Enable logging	Many IoT products are shipped with limited audit and logging features; provide this basic security service to users by: • Defining security-relevant events and logging them to an access-controlled file • Logging security-relevant events to a remote server
Secure hardware	Firmware extraction can allow attackers to identify zero-day vulnerabilities in a product and open test ports can sometimes provide direct command line access; make sure to: • Disable test ports (JTAG, UART, USB) • Implement tamper resistance techniques, if needed

integration upon detection of certain issues.

An equally important type of testing involves analysis of a product's firmware. Firmware analysis allows an evaluator to perform a binary analysis on the code that runs the product. Analysis tools extract and analyze the file system to identify known malicious files. They can also run static analysis to quickly identify product vulnerabilities. This includes performing an analysis on third-party code. Firmware analysis can also prove useful from a license management perspective, as it can often provide a report detailing the third-party libraries that have been implemented and their licensing requirements.

> Comprehensive testing of connected devices allows the program team to identify design flaws, gaps in requirements coverage or handling, and flaws in code.

Firmware analysis tools should be integrated into the CI environment just like other automated testing tools. This allows them to be run automatically on new versions of firmware so they can report on issues requiring remediation. New innovations in firmware analysis even report back on design flaws in a product and map back to groups of requirements from standards and best practices published by industry organizations such as SIA, ENISA, CSA, the IoT Security Foundation and others. ■ **Back to TOC**

Brian Russell (brussell@vdoo.com) is a security adviser at VDOO (www.vdoo.com) and Leo Dorrendorf (leo@vdoo.com) is a senior security architect at VDOO.

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.

securityindustry.org/techinsights

Security Industry Association
8405 Colesville Road, Suite 500
Silver Spring, MD 20910
301.804.4700