

Top 10 List

Key questions to evaluate drone detection systems

Page 6

SOC It to Me

The benefits of intelligent security operations centers

Page 16

Back to School

Meeting security challenges on campus

Page 24

SIA
Insights
TECHNOLOGY

Volume 7, Issue 2
Fall 2019



Welcome

Dear Reader,

This edition of *SIA Technology Insights* begins and ends by looking at an emerging trend in the security industry – the use, for both good and ill, of drones and robotics.

The first article uses 10 questions to examine drone detection systems and their role in mitigating the threat posed by unmanned aerial systems being operated by unintentional airspace violators as well as bad actors. And the last explains how robots are being integrated more and more into security operations, serving as a force multiplier for human guards.

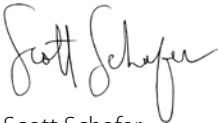
This is a technology area in which the Security Industry Association has taken a special interest by creating a Drones and Robotics Working Group, which has produced whitepapers, podcasts and other resources that are available on the SIA website.

In between those two articles are features on building an intelligent security operations center, linking physical and digital access control, moving security services to the cloud, and more.

If you have any comments, questions or article proposals, please contact the 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 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



Observe and Report..... 6

Identifying and locating drones and their pilots can mitigate threats

By Linda Ziemba, AeroDefense



All in One Security 16

An intelligent security operations center can enhance situational awareness and effectiveness

By Alan Stoddard, Verint Situational Intelligence Solutions



Higher Security for Higher Education 24

Securing college campuses requires strategy, collaboration and integration

By Rich Reidy, Siemens Industry Inc.

All Access 32

A comprehensive approach is needed to provide physical and digital access control

By Mark Duato, ASSA ABLOY Door Security Solutions



Moving to the Cloud..... 40

Off-premises solutions can provide multiple advantages to integrators

By Martin Renkis, Johnson Controls



Robot Evolution..... 50

New technologies are enhancing the security teamwork between man and machine

By Travis Deyle, Cobalt Robotics





Given that it is illegal for non-federal entities to use kinetic countermeasures against a drone, the next line of defense is detection. And, as with any security threat, the earlier the warning, the better.

Observe and Report

Identifying and locating drones and their pilots can mitigate threats

By Linda Ziemba
AeroDefense

Consumer-grade unmanned aerial systems (UAS), also known as drones, promise to enhance lives and operations in significant ways. As with many new technologies, though, safety and privacy concerns abound.

Inexpensive and widely available, drones flown by clueless or careless pilots can create public safety hazards. Criminals or activists can spy on and record video of sensitive sites. They can even drop rogue access points on rooftops over corporate data centers or fly over corporate campuses to gather information from employees' mobile devices.

And drone-borne terror attacks could threaten sites in the United States. This is not paranoia. Look at the short amount of time it took for airplanes to be weaponized. Less than 10 years after the Wright brothers' first



flight, a person flying a plane dropped a brick onto someone's head.

It seems obvious that a person should have the right to defend against criminal or terroristic drone uses, but the reality is that very few legal remedies are available. In fact, because of the curious complexities of several

laws, defenders against drones may find themselves in more legal trouble than the offending drone pilots.

Given that it is illegal for non-federal entities to use kinetic countermeasures against a drone, the next line of defense is detection. And, as with any security threat, the earlier the warning, the better. Early detection of drone threats in the airspace provides more time to respond effectively. Luckily, there are many drone detection systems on the market today, but they all work differently, and each has its strengths. The following 10 questions should be considered when evaluating drone detection systems.

1. What Is a Drone Detection System?

A drone detection system typically consists of two key components:

- Sensors that detect drones in the airspace, which may include both physical sensors and the computers required to process the data that is collected
- A user interface that displays drone detection data hosted on a local server or in the cloud.

2. What Are the Different Types of Drone Detection Sensors?

The Federal Aviation Administration (FAA) divides four commonly used sensor types into primary and secondary categories.

Primary Sensors

Primary sensors are able to detect drones with high enough accuracy and low enough false alarm rates to operate as standalone solutions. That is, they do not require data from other

sensor types in order to validate their detections. The two types of primary sensors are:

- Radar
- Radio Frequency

Secondary Sensors

Secondary sensors need additional data from other sensor types in order to accurately detect drone threats with a low false alarm rate. These additional sensor types can be used to enhance the accuracy of – or provide more detail about – drone threats, but they cannot be used as a standalone system. Examples of secondary sensors include:

- Acoustic
- Camera/Infrared

3. How Do Drone Detection Sensors Work?

Radar

A radar system consists of two components, a transmitter and a receiver. The transmitter sends a radio signal in a particular direction, and the receiver detects the echoes off any objects in the path of the signal.

Radio Frequency (RF)

An RF system detects the signals transmitted between the drone and the controller. As a result, if a drone and controller are within range of the sensors, it can even track them before a drone takes flight – which provides very early warning. This also makes RF detection unique because, unlike other systems, it can detect the controller, which means it can identify the location of the pilot.

Acoustic

Acoustic sensors listen for noises in the environment, and the data

provided by the sensor helps confirm whether or not a drone is in the area.

Camera/Infrared

Some camera systems can detect movement but require a complementary system to confirm that the movement is a drone and not, say, a bird or a piece of trash blowing in the wind. Other camera systems are used to gather visual evidence, but data from another sensor is needed to tell the camera which way to point.

People often ask if an RF system

can detect a drone that is flying autonomously on a pre-programmed path. Typically, the answer is yes, because even in this situation, the drone sends a periodic signal to “check in” with its controller to make sure there are no updated instructions.

4. What Are the Pros and Cons of the Different Sensors?

Each type of sensor has its own advantages and disadvantages. See the chart below.

SENSOR TYPE	Pros	Cons
Primary Sensors		
Radar	Very long range Provides altitude	Detects anything that moves, therefore has a high false positive rate in a busy urban environment Cannot detect until a drone is in flight Cannot detect a controller Actively transmits a signal, which may not be appropriate for all environments
Radio Frequency	Only solution that can detect both drone and controller Does not require line of sight Can detect a drone and controller as soon as they are turned on and connected (before flight)	System must be configured to filter out ambient RF signals Location accuracy may vary depending on the environment Performance degrades in heavy RF environments
Secondary Sensors		
Acoustic	Does not require line of sight	Must be combined with another detection method High false positive rate in noisy urban environments Very short range Cannot detect a controller
Camera/Infrared	Easily captures visual evidence	Requires line of sight Must be combined with another detection method to guide camera angle

5. Should Redundancy Be a Concern?

It is important to consider the impact on a drone detection system if a sensor fails, whether by sabotage or component failure.

A camera-based or acoustic system would simply be “blind” or “deaf” in the failed sensor area.

Depending on the configuration of a radar-based system, the system would be either somewhat degraded in a distributed model or totally down in a centralized model.

Some RF systems require multiple sensors: one to detect and three to locate. If the “detector” goes down, the system may still operate for some drones, but much more slowly. If a “locator” sensor goes down, the location accuracy degrades.

For RF systems that use a single detector/locator sensor type, consider a minimum of four sensors to provide for redundancy in system deployment. Three sensors provide the most accurate location information so, if one is down in a four-sensor deployment, location information can still be provided.

6. How Many Sensors Are Needed to Protect a Facility?

It varies a lot. And there are many considerations, including:

- **Facility Size:** How large is the site? Larger sites require more sensors, not just on the perimeter, but potentially in other areas, too.
- **RF Environment:** Some sensors simply do not work in extremely busy RF environments. For sensors that do work in such areas, detection range is reduced, along with drone flight range, so more sensors will be required.
- **Topography:** Are there any hills, cliffs or large buildings in the area? Do the structures or traffic change regularly? Buildings, metal structures and hills all affect drone and controller detection and location accuracy. Sensors that require line-of-sight will be defeated. Drone signal distortions caused by environmental elements render some RF-based systems inoperable. Other RF systems continue to function with somewhat degraded location accuracy.

It seems obvious that a person should have the right to defend against criminal or terroristic drone uses, but the reality is that very few legal remedies are available.

7. What Is the Range of a Drone Detection System?

This is one of the most misunderstood questions. The reason is, most detection range statistics are based on ideal conditions: a clear, sunny day in a flat, open area with no

major obstacles, like buildings, hills or other moving objects, or signal transmissions, like Wi-Fi networks, cell phones, metal detectors or dashcams.

So if a facility is located in the desert, a vendor's statistics can probably be taken at face value. But if not, the vendor should be asked whether they have deployed in an area similar to where the facility is located. Ask them about the detection range in those specific areas. And even then, understand that every environment is unique, so range estimates will be a guide, not a definitive answer.

8. How Do RF Drone Detection Systems Locate a Drone or Controller?

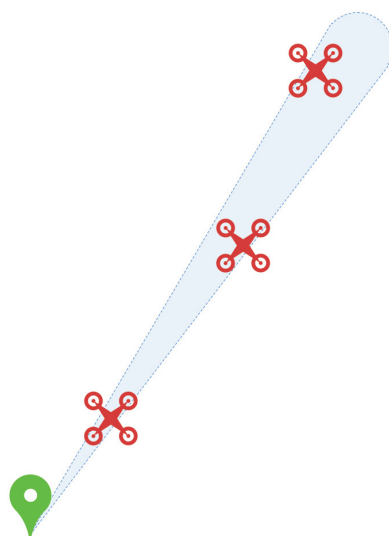
First, it is important to establish that there are RF-based drone detection systems on the market that extract the GPS coordinates of a drone and controller from the signals they send. There is just one problem with this: it is illegal. It requires the system to demodulate and decode the signal, which violates federal wiretapping laws.

With legal systems that use the physical characteristics of a signal to identify location, there are two key methods: triangulation and trilateration.

Triangulation

In triangulation, the sensor uses the angle of the signal to determine the approximate line of approach. Typically, it is accurate to within +/- 5

degrees, so it is best represented by a cone.



Sensor

Figure 1: The triangulation method provides the angle of approach, not the distance.

The triangulation method, however, cannot tell how far away a drone or controller is from the sensor. The drone could be anywhere along the angle of approach.

The intersection of three cones is required to locate a drone or controller.

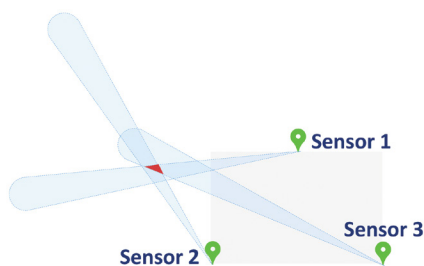


Figure 2: The area where the three cones overlap represents the location of the device.

Trilateration

In trilateration, the sensor uses the power level of the signal to calculate the distance of the signal from the sensor. A drone or controller could be anywhere at that distance, so this is best represented by a circle.

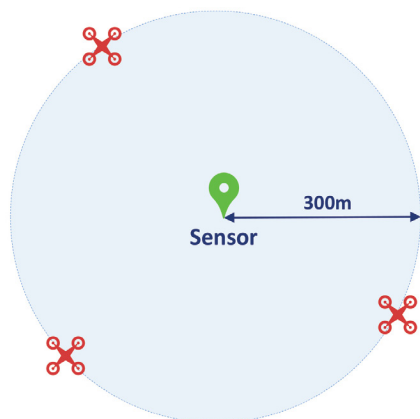


Figure 3: The trilateration method provides distance, but not the angle of approach.

The intersection of three circles is required to locate a drone or controller.

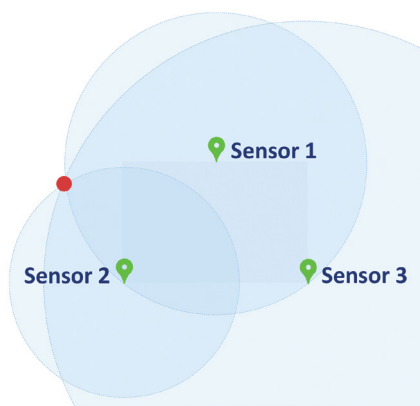


Figure 4: The area where the three circles overlap represents the location of the device.

Pros and Cons of Triangulation

Triangulation provides early warning of the approach path, even if only one sensor is initially detecting, so security personnel immediately know in which direction they need to go. However, because one sensor cannot provide distance information, this can result in a high false positive rate, as a drone may be too far away to be a threat.

RF signals can reflect off of many surfaces, including buildings

The best option to stop a drone from flying is to find the controller. If the controller can be found, so can the pilot.

and vehicles, and this can diminish location accuracy. In the case of a reflection that results in no overlapping cones, it can prevent the system from locating at all. While this may affect drone location accuracy, the greatest impact is to controller location accuracy.

Pros and Cons of Trilateration

Trilateration allows for the setting of a distance threshold for alerts, which can reduce the false alarm rate. However, the system will require data from more than one sensor before security personnel can know where to respond.

RF Location Method	Pros	Cons
Triangulation	Provides early warning of the approach path	When only one sensor is used, may result in a high false positive rate if drones detected are too far away to be a threat Signal reflections off objects like buildings or vehicles degrade location accuracy (and sometimes the ability to locate at all)
Trilateration	Can be configured to only alert to drones within a certain distance of a facility to reduce false alarms Able to locate even if signals are reflected off buildings or vehicles	Does not provide early warning of the approach path

Because signal reflections have very little impact on signal power levels, a system that uses trilateration will be able to detect drones and controllers even in busy urban environments.

9. How Should Desired Outcomes Be Defined?

Goals and response tactics drive the type of drone detection system that is right for a given organization and situation.

Drone vs. Pilot

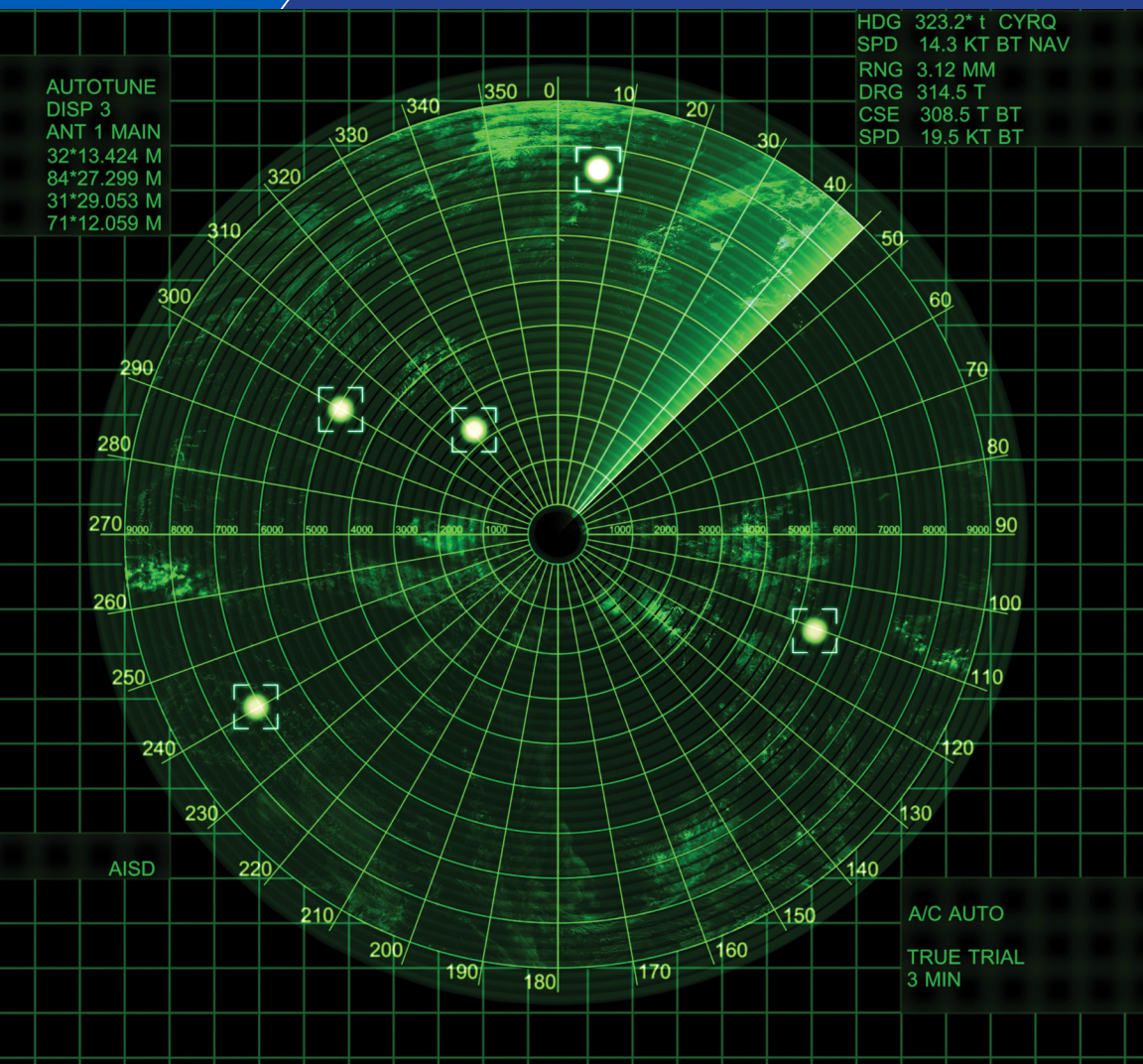
The system may be called drone detection, but the reality is, not much can be done about the drone. Outside of the military and federal government, mitigation is illegal. And even if mitigation were lawful, would an insurance company provide liability

coverage if an organization's security personnel caused a drone to fall from the sky and injure a person or damage property? Maybe not. So the best option to stop a drone from flying is to find the controller.

If the controller can be found, so can the pilot. If the pilot is just a careless or clueless operator, security personnel can ask him or her to land the drone. In the case of a bad actor, local law enforcement can make an arrest.

Accuracy vs. Reliability

Drone detection requests for proposal (RFPs) often contain a lot of technical questions. They ask for details on range, location accuracy, and time to detect, which is not surprising. Organizations are under pressure to use more data to justify decisions.



What's more, hard data feels much easier to compare than lists of features and capabilities.

But what will provide the best outcome? A system that has a long range and provides high location accuracy, but has a high false positive rate, so security tends to ignore the alerts? Or one that provides a good approximate location with a low false alarm rate, so security personnel take

detection notifications seriously? It is something to think about.

Lots of Arrests vs. No Drones in the Airspace

How will the success of the drone detection program be measured? What is the goal? Often, when organizations start to plan, their goal is to get the bad guys. Lots of warnings or arrests equals success. But when a drone detection

system is deployed, and security staff is empowered to respond quickly and effectively, something else often happens.

The drone threat is reduced as drone operators learn to stay away from facilities where security comes after them. At the end of the day, the best outcome is to eliminate the drone threat altogether.

10. Will Regulations Change to Allow More Active Countermeasures?

Drone technology moves quickly. Regulatory changes do not. Most security personnel regard taking a

“wait-and-see” approach as not being a responsible option.

Situational awareness of drones in the airspace provides actionable knowledge of a security risk. Pilot

detection and location information gives a security team a chance to prevent an incident from occurring, and that is an effective form of mitigation. ■ [Back to TOC](#)

Linda Ziemba (linda.ziemba@aerodefense.tech) is founding CEO of AeroDefense (www.aerodefense.tech).



Combining video management, video analytics and artificial intelligence provides new levels of insight – and automation – to improve safety and provide peace of mind to security leaders.



All in One Security

An intelligent security operations center can enhance situational awareness and effectiveness

By Alan Stoddard
Verint Situational Intelligence Solutions

The threat landscape is changing rapidly, becoming more sophisticated and complex with each incident. Those responsible for keeping people, property and assets safe need a comprehensive and cohesive approach to security.

To protect what matters most, organizations of all sizes and industries must take a multi-dimensional look at their security demands and build a holistic plan that delivers the actionable intelligence needed for critical decision-making. The reality is that today's complex and modern threats cannot be addressed using yesterday's solutions – it is time to evolve and embrace the movement toward the intelligent security operations center.

While physical security is always a top priority for security leaders, it is no



longer the only concern. Cybersecurity threats are on the rise, with forecasts estimating that IT attacks will cost organizations \$6 trillion by 2021. This increases the need for a converged security approach in which video

surveillance, physical security and cybersecurity solutions are combined to meet an organization's needs.

No More Silos

Physical security systems such as access control, intrusion detection, fire detection and suppression, perimeter security and others have traditionally operated separately from logical systems like identity management. So separate, in some cases, that they have been managed by a different department. But now, with the growth of cyber threats and the impact of these risks on physical security assets, the industry is moving toward converged security initiatives.

With the growth of cyber threats and the impact of these risks on physical security assets, the industry is moving toward converged security initiatives.

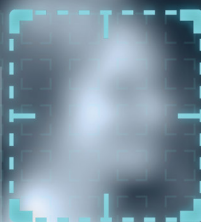
An integrated, holistic response enables comprehensive management of security. Typical security systems, however, operate in silos. Video and business analytics can be part of these deployments, but without a common metadata layer, intelligence cannot be added across the spectrum of the security infrastructure. Therefore, the

operator must coordinate data from multiple subsystems and then collaborate with other stakeholders as needed – a tedious and time-consuming manual process. Combining

video management, video analytics and artificial intelligence (AI), though, provides new levels of insight – and automation – to improve safety and



ID : 462578624

FEMALE
BLOND HAIR
CAUCASIAN
RELAXED
BAG

BIOMETRIC IDENTIFICATION : ON - OBJECTS DETECTION : ON - BEHAVIOR ANALYSIS : ON

provide peace of mind to security leaders.

The Essential Video Management System

A critical part of any holistic security strategy is video surveillance. Security managers and operators rely on a multitude of solutions and systems to ensure comprehensive protection of people and property, but video is – or should be – at the heart of the approach. Video can transform security operations by enabling intelligent, data-driven management and response, while also offering business value by increasing operational efficiencies and reducing costs. Video enhances decision-making, facilitates real-time monitoring, provides greater situational awareness, and helps personnel respond faster and more efficiently to incidents and threats.

With forensic investigation a critical component of security strategies, video becomes a central part of ensuring efficient operations. Data gleaned from video management platforms provide enhanced situational awareness and can assist in keeping people and property safe. But the sheer volume of data results in a burdensome process that consists of manually identifying anomalies and risks. However, the introduction of data-driven search and video analysis empowers operators to streamline their work and improve their performance.

Imagine what video could help a business achieve if security personnel could look beyond how it is currently used? Imagine if they could enhance that video with dynamic geographic mapping information, sophisticated event management and investigation engines, and extensive bi-directional

integrations. All of that and more is becoming a reality as technology evolves. Leveraging the power of video in a security operations center can help a team achieve higher levels of safety and greater influence in developing an overall security strategy.

Introducing the Intelligent Security Operations Center

Interest in the intelligent security operations center (ISOC) is growing as organizations seek to adopt a more proactive approach to physical and IT security. The ISOC concept addresses this need by aggregating multiple systems into a single interface and applying an analytic layer that produces actionable intelligence. The ISOC incorporates AI and deep learning to provide data about what is happening across an enterprise's domains and demonstrate how it affects the business as a whole. Over time, the system can even identify

patterns in the data to provide early warning of threats.

By collecting intelligence from digital sensors and systems such as video surveillance cameras, open-source Web intelligence, building management systems, crowdsourcing, weather sensors, mobile devices, and more, operators can identify potential anomalies and more efficiently manage and respond to situations. A centralized approach allows information to be shared easily with employees, external agencies, citizens and first responders, which is especially valuable in the event of a safety incident when rapid response is paramount. With a single enterprise-wide view across disparate systems and technologies, organizations experience new levels of situational awareness, reduced operational costs, and increased employee safety.

The ISOC approach empowers enterprises to be more efficient,





effective and proactive. Keeping people and property safe is a complex challenge. Those wishing to do harm are constantly evolving their tactics. Because of this, it is more critical than ever for security leaders to implement coherent and cohesive security plans.

Why is the ISOC such an important concept to grasp?

Quite simply, it can help leaders deal with vast amounts of data. Data is all around us, in the words transmitted via voice or text, in the geolocation information sent by smartphones,

tablets and other mobile devices, and in the videos and images that people share. It is also in the background, unbeknownst to many end users, in the layers of metadata cataloging every

interaction throughout the day. In its native form, raw data is not very useful. But introduce the right analysis and the value of the data grows exponentially, often revealing key insights, reducing errors, transforming businesses, and even saving lives.

Powered by machine learning

algorithms and multiple detection engines, the ISOC uses extensive data analysis that can be a tremendous resource to organizations by providing early detection of

The introduction of data-driven search and video analysis empowers operators to streamline their work and improve their performance.

suspicious activity. By aggregating data from multiple systems into a single interface, the ISOC enables security operators to assess threats across all domains of an enterprise. Additionally,

it can continuously monitor and investigate the dark web, leveraging cyber threat intelligence to identify attacks in the making and gauge their potential impact on the organization, thus taking a converged approach to risk management.

With the many moving parts involved in an organization's security operations, the benefits that an ISOC can deliver are immense. The ISOC methodology gives businesses the ability to access a solution that can act as a virtual analyst and automate processes, boosting effectiveness and helping to better leverage existing resources. By applying the same practices an investigator would, only faster, the system can automatically collect and analyze leads across an enterprise's infrastructure, simplifying the responsibilities of security operators. This frees up time and resources to focus on more critical tasks.

ISOCs in Retail Environments

Big-box retailers are at a high risk for various security threats. In 2018, the National Retail Federation estimated that theft, error, shoplifting and fraud cost the industry more than \$46 billion. With millions of dollars in inventory stored across multiple facilities, even the largest and most successful retailers in the world are likely to be targets for fraud, theft, vandalism and even violent crime. These threats put the safety of customers and employees in jeopardy while negatively affecting the overall business and its bottom line.

In these high-traffic environments, it is imperative for management and security teams to obtain clear situational awareness and real-time information. This information, which can be extracted from advanced video systems and other intelligent security solutions, can help to not only improve safety in and around the stores, but also enhance operational efficiencies



and the customer experience.

One of the largest retailers in the world chose to implement a solution that drives effective protection at its many locations across the United States. With initiatives in place to reduce crime, the company decided to leverage various strategies, such as the strategic positioning of employees, the use of visible security cameras in high-theft areas, the implementation of data analytics to detect fraud, and the hiring of private security guards and off-duty police officers to mitigate risk. Additionally, the retailer uses scan avoidance detection technology to strengthen loss prevention efforts in self-checkout lanes.

The company also takes advantage of a collaborative and scalable solution at its corporate office. The system manages data from sources such as license plate recognition, facial recognition, access control, and analytics platforms to provide a comprehensive, single-pane-of-glass ISOC.

Retailers will always have to contend with bad actors and attacks on their businesses, which further demonstrates the need for best-in-breed security solutions that combine video surveillance, physical security and cybersecurity to deliver a holistic solution that provides the actionable insights necessary to identify potential

threats and rapidly respond to incidents. By improving situational intelligence, streamlining data collection and analysis, and decreasing response times, these solutions can enable retailers to face today's biggest

threats while also evolving to meet the demands of the future.

As the security risk and technology landscapes continue to evolve, so will the way organizations

protect personnel and property. Threats, from both the cyber and physical worlds, are changing rapidly, and with various systems becoming more and more interconnected, enterprises need solutions that scale to address shifting demands.

Meeting this challenge demands a more collaborative approach than ever before. Organizations must align their cyber, IT and physical security teams to comprehensively improve risk management and ensure that vulnerabilities can be identified before an incident causes harm. The video-based ISOC stands at the core of this effort, streamlining the process for enterprises and allowing them to achieve their business goals while maintaining security. ■ **Back to TOC**

Alan Stoddard (alan.stoddard@verint.com) is vice president and general manager of Verint Situational Intelligence Solutions (cis.verint.com/product/situational-intelligence).



Ensuring a reasonable level of security for all students, staff and faculty means creating and implementing the right security strategies, as well as integrating the right technologies.

Higher Security for Higher Education

Securing college campuses requires strategy, collaboration and integration

By Rich Reidy
Siemens Industry Inc.

On April 30, 2019, two students were killed and four others were injured in a shooting at the University of North Carolina at Charlotte. On May 7, a Savannah State University student was injured in a residence hall shooting. And while mass shootings rightfully demand the nation's attention, the majority of campus violence is unrelated to gunfire. In 2016, there were 28,400 reported criminal incidents (including burglary, vehicle theft, sexual assault, and hate crimes) on college campuses in the United States, a number that reflects a 32 percent increase since 2001. In other words, the risks to students has never been more apparent.

The Impact of Campus Violence

Incidents of violence have a profound impact on students'



academic performance and mental health. One study found that violence is associated with significant decreases in grade point average, which often makes students more likely to leave an institution. Exposure to violence also negatively affects mental health,

leading to anxiety, depression, even suicide. Faculty and staff are also likely to experience these effects. In addition, an institution could suffer damage to its reputation and ability to attract students and premier faculty.

Educators, administrators, and campus security strive to minimize exposure to danger while maintaining an open, comfortable, welcoming place for students to learn. As incidents continue to occur and risks continue to evolve, a broad understanding of security is more important than ever.

The Benefits of Practice

Creating safe and secure campuses starts with effective emergency plans

Securing campuses is not just about having an emergency plan. It is also about practicing that plan, running drills, and studying the research so that, in the event of an emergency, everyone can react appropriately.

and processes. What happens when there is a fire alarm? A problem in a lab? An active shooter? If the dorms or academic buildings must be evacuated, where is the rally point and how is accountability addressed?

Administrators and security staff must know exactly what to do in each of these situations and many others. And the time to learn these processes is not during an emergency.

The National Fire Protection Association (NFPA) fully understands the implications here, and thus has developed a new provisional standard, NFPA 3000 (PS). This standard is designed to identify minimum program elements needed to organize, manage and sustain active shooter/





hostile event response (ASHER) programs to reduce risks and effects on schools and other organizations.

Securing campuses is not just about having an emergency plan, though. It is also about practicing that plan, running drills, and studying the research so that, in the event of an emergency, everyone can react appropriately.

Creating an Ideal Campus Environment

Colleges and universities are, at their core, about learning and research, so creating a campus environment that enables the educational mission of the school is central to success. Ideal learning and researching environments are those where all students, faculty and staff feel safe and secure. And while it is a more challenging responsibility than ever, it can be achieved when everyone is working together.

In addition to having a well-designed and well-practiced emergency plan, campuses must strategically align security into all

daily operations and take a proactive approach to emergency management. Ensuring a reasonable level of security for all students, staff and faculty means creating and implementing the right security strategies, as well as integrating the right technologies.

In the event of an emergency, situational awareness is paramount. Knowing what is going on in and around the campus enables personnel to identify, process, understand and respond to the information at any given time. The steps below outline how forward-thinking campuses are creating safe and secure environments that remain a welcoming place for students, faculty and staff.

1. Define the Organization's Security Objectives

While universities may share many of the same security concerns and objectives, each campus is unique with respect to location, buildings, students, community and access to capital, and all of these factors will influence an institution's specific objectives.

An effective approach to campus security will depend on the security

mission and objectives in order to determine the strategies, processes, technologies and equipment that will be used. Be sure to consider how these strategies will affect the campus population and surrounding community while creating an environment that cares about the security and safety of its occupants. Success here may mean starting with the most critical areas first and designing a program that is in line with both budget and staff resources.

2. Secure the Perimeter of the Campus

Keep intruders out and regulate access to campus facilities by securing the perimeter. Most organizations

By integrating individual security systems to function as one unified solution, administrators and campus security improve their situational awareness.

rely on a combination of security technologies, natural and artificial barriers, and other fortifications like window film. Remember that campus facilities extend beyond residence halls and academic spaces and include green spaces, athletic fields, and other gathering spots.

3. Control Access to Campus Buildings and Secure Areas

Access control is an ideal way to balance the need for an open and welcoming campus with the responsibility to protect the people within. The system should include a range of technologies that control





building entry and egress while also hardening the building perimeters.

Look for solutions that will help control entry to the campus and other secure areas and generate an alarm if a door is propped open or there is unauthorized access. In addition, an access control system should create a record of who enters and leaves buildings or areas, as well as integrate with video surveillance solutions to verify incidents, enable more effective responses, and provide necessary information for forensic review.

4. Install Intelligent Video Systems that Perform Analytics and Provide Alerts

Video surveillance technologies are not new to security operations, but the latest solutions offer smart cameras that provide high-quality, searchable digital video. And these intelligent cameras do far more than capture video; they can analyze the scene and recognize people and objects that are

out of place or inconsistent with typical campus activities.

For example, when the campus perimeter is properly configured with an intelligent video solution with license plate recognition, the system will recognize when a vehicle has driven around campus multiple times over the course of a day and flag the incident for additional investigation. Gone are the days of assigning a person to watch security camera feeds. These new systems automatically detect motion and begin recording, which helps activate emergency plans and simplify follow-up investigations.

5. Integrate Technologies to Increase Efficiency and Enhance Situational Awareness

Many campuses rely on a variety of disparate systems to monitor and manage access control, video surveillance, and other building systems, and most of these systems

require a high level of human interaction. This disconnectedness increases the risk of human error, delays response times, and impedes the ability to respond quickly and effectively to an emergency.

By integrating individual security systems to function as one unified solution, administrators and campus security improve their situational awareness. Adding other solutions, such as shot detection devices, makes the integrated system even more robust and supportive of effective emergency plans.

6. Deploy a Mass Notification System

Another vital component to emergency plans is communication. Research shows that people are more likely to take a warning seriously if they receive it more than once and from multiple sources. Thus, administrators must be able to get the right messages to the right people at the right time so emergency responders can move to the scene, so faculty, staff and students

know where to go and what to do, and so parents and the public stay informed, and misinformation and panic is contained.

The right mass notification system will quickly, reliably and accurately get emergency and routine communications sent to and received by the right people, no matter where they are or what they are doing. These solutions, when properly implemented and configured, can also support colleges' and universities' efforts to comply with the NFPA 3000 provisional standard.

7. Perform Maintenance and Install Updates to Security Systems

Security systems function day and night, 365 days a year, and they require scheduled maintenance, as defined by the manufacturer and regulatory agencies. A gap in maintenance could put the entire system at risk.

Proactive, preventive maintenance, including software and firmware updates where appropriate, helps





ensure that access control, intrusion detection, video surveillance, and

other security systems are fully functional and available around the clock to secure the campus, students and staff, and valuable university assets.

As important as it is to maintain any equipment, system or technology in a building, it is especially critical to ensure that the components that protect building occupants are kept fully operational.

As important as it is to maintain any equipment, system or technology in a building, it is especially critical to ensure that the components that protect building occupants are kept fully operational.

secure and monitor complex campus environments, and control access to

facilities, all while maintaining an open and welcoming environment.

A layered approach to campus security, which includes emergency planning and practice, physical security measures, and intelligent

technologies, is required to enable campus security officers to achieve their ultimate goal: a safe, secure learning environment for students, faculty and staff. ■ **Back to TOC**

Facing Complex Security Challenges

Colleges and universities face a range of security challenges today. Personnel must anticipate threats,

Rich Reidy (richard.reidy@siemens.com) is security segment head for Siemens Industry Inc. (usa.siemens.com/perfect-places-highered).



It is vital for security and IT professionals to not only stay abreast of technological changes, both in physical components and cybersecurity, but also to work together from the earliest planning phases through project implementation and maintenance.

All Access

A comprehensive approach is needed to provide physical and digital access control

By Mark Duato
ASSA ABLOY Door Security Solutions

Controlling access no longer simply means deploying a secure lock and tightly controlled keys. It is not that traditional mechanical locks and high security keys are not still an effective form of security – they have been an important element of good security planning for many years and will most certainly remain critical components of a sound access control strategy – but the rapidly changing nature of threats in today’s world, coupled with the blistering pace of technological advancement, means traditional solutions have evolved significantly, as well.

Technological change and emerging security threats are not unrelated. As new devices and capabilities become available, bad actors find new ways to exploit weaknesses, and the perpetual



counterbalance will assuredly go on. The industry, as a whole, needs to continue to break down operational silos and view various elements of enterprise security as part of a unified, harmonious strategy.

With the accelerating growth of electronic access control solutions,

including wireless technologies and biometric elements of identity management, enterprise security practice and data management are fully entwined.

What has traditionally been thought of as physical security, such as perimeter deterrents and door locking systems, often depend on network infrastructure to effectively carry

out their purposes. Physical security and cybersecurity objectives must, therefore, be viewed cohesively and addressed comprehensively to deliver an optimal return on investment.

This means, for example, that the traditional locksmith or security professional can no longer think only about mechanical locks and keys, and

The industry, as a whole, needs to continue to break down operational silos and view various elements of enterprise security as part of a unified, harmonious strategy.

similarly, the IT professional can no longer think only about the network infrastructure; both must be able to understand the priorities and needs

of the other so that their respective remits work seamlessly together. Minimum skillsets are evolving quickly across the services spectrum. Certainly, not every security specialist needs

to know how to program, deploy or repair a mechanical or electrified access control opening, but a high degree of collaboration must exist between the physical and digital infrastructure domains to execute effective security policies.

The more closely security professionals work with other facility





stakeholders, the more detailed and effective the layers of security become. A comprehensive, layered security plan is about hardening potential weaknesses and implementing deterrence factors at every point of risk in the system in an intelligent way. That means physical, logistical and virtual perimeter barriers must be analyzed, identified as effective or problematic, and measured for risk and/or investment. This ensures to the greatest degree possible that people, intellectual property and related assets are prioritized and safeguarded.

It is vital to bring all these stakeholders together early and often on any project, even if it is a year or two before breaking ground on a new site or many months prior to putting a construction or retrofit aftermarket project out to bid. Doing so encourages comprehensive, systemwide thinking

from the beginning. The result is a much smoother process when designing and implementing solutions and working with partners for comprehensive security management and access control. It also allows for optimizing resources by shifting to more value-oriented operational systems.

By addressing the relationship between physical and digital security early in the planning phase, risk mitigation objectives and contingency investments can be identified before weaknesses are exploited. These solutions then need to remain vested and top of mind after the infrastructure is deployed. This type of proactive, integrated, comprehensive approach results in a multi-layered formula where obstacles – both physical and digital – stand between potential bad actors and the people, data and assets in an enterprise.

Fence Line to Frontline

The confluence of physical and network security features is important for all commercial enterprises, but particularly in environments representing critical infrastructure – communications, power and utility, transportation and traffic control, water resources such as dams, and other sites that are vital to public safety or the economy.

Secure fence lines and perimeter gate control are crucial deterrents but are often expensive and difficult to deploy. The technology must be able to withstand possibly harsh outdoor conditions. Padlocks and mechanical or electromechanical locks can utilize “intelligent” physical keys electronically programmed with access control rights without the expense of the traditional network infrastructure that is typically required to actively communicate

access control transactions. Intelligent keys cannot be hacked since they are not actively connected to a security network, making them a cost-effective step forward in protecting layered critical infrastructure sites, and for that matter, any type of offline secure opening.

The Critical Link Between Cybersecurity and Physical Security

Whether through RFID cards, mobile credentials or biometrics, access control systems increasingly, if not exclusively, rely on data passing from a credential to a reader to a controller on a network. And, as with all networks, an access control system can be hacked and its data stolen.

When access control data is compromised, an unauthorized person can use it to gain access to a network or facility, just as if he or she



had stolen a password or physical key. Beyond that, hackers can use access control data to break deeper into Wi-Fi networks and steal other types of secure data. These events happen far too often at major finance, retail and telecommunications firms, where stolen identities and credentials allow hackers to install malware that, for example, can unlock phones.

Situations like these are precisely why physical security and cybersecurity

objectives must be aligned. As a result, the ubiquitous Wiegand protocol, the standard of access control communication infrastructure for decades, is being phased out, and security industry professionals would be wise to support and hasten this process because of the protocol's vulnerabilities.

The Wiegand protocol, for example, is plain-text code, so once the signal between the reader and the controller is hacked, it is relatively simple to copy the code and gain access to a particular credential. This was demonstrated at a 2007 conference by a hacker who installed a PIC chip in a reader and showed how easily he could steal access control data and manipulate the system to gather and capture data about other authorized users. The hacker even tricked the system into locking out everyone but

him, despite the other users having authorized credentials.

Fortunately, the security industry has awakened to these threats, and the cross-collaborative Open Supervised Device Protocol (OSDP) is now available in many devices for access

control solutions. This protocol involves two-way communication between the reader and the controller, and the wiring system is far more sophisticated than that found in Wiegand

Hackers will not become less capable over time, so security professionals must implement defenses that will keep enterprises at least one step ahead.

communication structures.

For security professionals involved in new construction projects, using OSDP should be a no-brainer. When tackling a retrofit project or legacy infrastructure, however, the investment in changing from Wiegand to OSDP can present some obstacles, which is why IT and network professionals need to work closely and collaboratively with security professionals. All parties can understand the value of improving access control security and are vested in getting greater stakeholder buy-in early in the process. Over time, the security enterprise is stronger, and costs of ownership will decrease dramatically.

The upfront cost of security installation can be further lessened by leveraging cloud-based data storage, as well as Wi-Fi and/or Power over Ethernet (PoE) infrastructure at the

access control opening, which can remove many of the limitations of traditional systems.

Ultimately, the cost of data breaches can far exceed that of installing updated access control systems, and the idea of “doing things how they have always been done” is no longer an acceptable approach to enterprise security. It is incumbent on security professionals to have a unified view of the system and point out where weaknesses lie so that new layers, from encryption to smart locks and beyond, can be implemented to stay ahead of evolving threats while lowering the total cost of ownership in the long term.

The Value of Data

The need for comprehensive security and a multi-layered approach is just as important within the facility itself, as exemplified by the deployment of access control solutions at server cabinets and network closets. Actively controlling traffic to and through server cabinets, which house the most sensitive data infrastructure, is vital. Once again, there is a confluence of physical and digital security at play: maintaining the physical integrity of network assets prevents unauthorized

users from damaging or tampering with the infrastructure that stores data, and thus, the data itself. Of course, like any other card reader or access control component, the physical system using intelligent locks and keys must be grounded in encrypted, secure data.

In addition to protecting an organization's proprietary data, servers also contain identity data for staff and/or customers. With breaches becoming a near daily occurrence, it should go without saying that data must be safeguarded to the highest degree possible.

As seen with the Wiegand codes being easily hacked, it is not just hardware that needs to be robust when preventing identity theft. It is also imperative to use sophisticated encryption to prevent unauthorized users from accessing networks, just as deadbolts and locks are utilized to

keep people out of restricted spaces. Hackers will not become less capable over time, so security professionals must implement defenses that will keep enterprises at least one step ahead. Doing so requires not just vigilance to watch for

new threats, but also an openness to continual education and solution updates as more robust options become available.

It is no longer possible to view enterprise security functions in isolation, and indeed, it is no longer desirable since security encompasses everything from perimeter fences to encrypted identities.



The Future of Security

Both threats and technology are constantly evolving. It is no longer possible to view enterprise security functions in isolation, and indeed, it is no longer desirable since security encompasses everything from perimeter fences to encrypted identities. Innovations such as high-security physical keys, which can be programmed and managed through the cloud, are breaking down the barriers between physical security and cybersecurity. As the technology evolves, though, so too will the threats to the way openings are secured.

It is vital for security and IT professionals to not only stay abreast of technological changes, both in physical components and cybersecurity, but also to work together from the earliest planning phases through project implementation and maintenance. This can ensure that enterprises have a multi-faceted, multi-layered system of

security measures in place.

From a remote perimeter to the closets containing data servers, access control systems play a key role in securing enterprises. Intelligent keys, the OSDP standard, cabinet locks – these are just a sampling of the access control technologies available to create as many barriers as possible to unauthorized entry or access, whether physical or digital, onsite or virtual. And by working in tandem from the very beginning of a project, security and IT professionals can implement solutions that secure an enterprise while lowering the total cost of ownership over time. Physical assets and data are no longer separated, so the approaches to securing them cannot be separated either. ■ **Back to TOC**

Mark Duato (mark.duato@assaabloy.com) is executive vice president of aftermarket solutions at ASSA ABLOY Door Security Solutions (www.assaabloydss.com).



While preparing an integration business to provide cloud services for video, access control and other solutions can be a challenging and uncomfortable transformation, it is one that will ultimately prepare integrators for the future.



Moving to the Cloud

Off-premises solutions can provide multiple advantages to integrators

By Martin Renkis
Johnson Controls

When systems integrators embrace cloud technology, they enable a long-term solution that allows a transitional approach with many options available to customers. While preparing an integration business to provide cloud services for video, access control and other solutions can be a challenging and uncomfortable transformation, it is one that will ultimately prepare integrators for the future. Moving services to the cloud does require a totally different financial model and sales process. While profit margins are compressed and upfront payouts for installing hardware are much smaller, security businesses will benefit from incremental and predictable income from recurring monthly revenue (RMR) that is generated from system



management, maintenance and monitoring.

The real story here is that it is not *if* an integrator moves to the cloud, but *when*. End users are asking for the cloud, with many CEOs, CIOs and CSOs

insisting on moving all their “iron” off premises, relying on hosted, off-site cloud solutions for secure and easy upkeep and maintenance. Systems integrators need to be able to deliver the value proposition expected of the cloud – reliability, expandability, and the move to operating expense versus capital expense. With the cloud, integrators can offer services that can be maintained on a grand scale, even with thousands of cameras around the world, ensuring the solution is running reliably. Installations are also simpler, utilizing one portal for all systems, services and user management, yielding a unified platform for video and access control.

Long term, leveraging cloud solutions means a healthier revenue stream and additional options for future profitability. There is also inherent, enhanced cybersecurity and compliance embedded in cloud

platforms. It is easy to add or offload services, as well as provide remote maintenance and management through a single interface or mobile device. Together, these help to create a better user experience and a stickier customer.

Moving to cloud management and storage starts with a deep dive into the functionality of the platform. Education and research come next, homing in on what customers are looking for and what the cloud offers to meet their physical security needs or challenges. When posed to cloud providers, these five questions should provide guidance in the quest to decide what is best for an integrator.

It is not *if* an integrator moves to the cloud, but *when*.

and research come next, homing in on what customers are looking for

1. How Does the Platform Positively Affect My Business Growth?

Look for a platform that is not entirely tied to technology, but instead helps to build a managed services





business through efficiency and scalability. It should be ready for the ongoing digital transformation and the future of security contracting – everything “as-a-service.” Leveraging a single user interface and reporting structure for all customers helps an integrator scale the offering so that devices can be added as needed, boosting RMR.

Storage is critical and is tied to many parameters, including bandwidth, how video is stored and used, and if there are regulations to meet for archiving. These parameters can vary drastically from job to job, so an integrator needs flexibility from a cloud provider. For example, customers should have the ability to record and store at the edge and upload video as needed at the resolution required. They should also be able to record and store either on motion or 24/7. Dynamic, on-demand services to store and manage all solutions are what is needed.

2. What Capabilities Will Provide Better Service to Customers?

Capabilities that an integrator should be able to leverage from a cloud platform include the ability to obtain status updates in real time to address issues when or before they happen, thus avoiding possible compromise of security solutions. An integrator should be able to see the entire surveillance system on a map and click on any camera or gateway to see details and troubleshoot immediately. A robust cloud platform will enable an integrator to add, edit and delete users, remotely upgrade systems, track and report on bandwidth utilization, view live video and recorded playback, uploads and cloud storage, and more from a single dashboard. The cloud platform should be able to provide health reports and other system and process documentation. Finally, e-commerce and billing management and reporting to track revenue per camera per

customer should also be part of the solution.

Ease of maintenance and labor savings, as well as built-in security and updates, are also keys to effectively utilizing the cloud. When the cloud can be used to manage a client's services and even reboot field devices or take locks offline, that saves time, labor and costs. Even across an enterprise with thousands of cameras, integrators can manage users, cameras, gateways and services from one web browser and track bandwidth and provide customers with network and cloud storage utilization reports. Monitoring the status of all systems in an intuitive map mode allows integrators to jump to any device for instant, on-the-fly troubleshooting.

3. Is the Platform Robust and Open?

It is a simple question, but it is essential to the decision-making

process. The cloud platform should run on an open and modern architecture to deliver fast, scalable and secure services globally, and it should cover video, access control, artificial intelligence, cybersecurity and unified legacy products. It is important to clarify that having a cloud-based service does not mean that all video must be stored in the cloud. In fact, the best cloud platforms allow users to share video securely and to store video in cameras, via gateways, in the cloud, or in a hybrid combination. This gives integrators the ability to custom-design their managed services for all their customers, from small and mid-sized businesses to large enterprise accounts. Some cloud platforms require the use of specific cameras, but the beauty of cloud services is the ability to use existing devices with a gateway product or new hardware,





which addresses problems related to the transition of legacy equipment.

4. In Terms of Cybersecurity, How Are Customers Protected?

The cloud is one of the most secure platforms, but not all cloud services are created equal. The cloud provider's experience in handling a variety of vertical markets comes into play. Architecture is also paramount, and one that is design-built from the ground up as a secure, multi-tenant platform for capture, transport, storage, management, analysis and distribution of a variety of video sources over different networks makes the most sense. With a cloud infrastructure, there is more overall reliability in the configuration. It is almost like a mini network operations center, where if one camera goes out, the remainder stay online. With NVRs

Ease of maintenance and labor savings, as well as built-in security and updates, are also keys to effectively utilizing the cloud.

and DVRs, it is the opposite; the entire solution networked together can suffer a failure, knocking out all cameras and components.

Uptime and reliability are paramount, and the cloud provider should have documentation of these performance factors. Video surveillance is network intensive and can interrupt

critical data collection such as point-of-sale, so select a platform that handles bandwidth management and controls network utilization, as

well as one with integrated failover that buffers video when a network disconnects and then sends data automatically when connectivity is restored. Recording services should optimize video for different connection speeds and deliver storage bandwidth control. Another nice perk is the availability of secure third-party app

There Is More to Cameras than Megapixels

By Peter Ainsworth
Johnson Controls

For systems integrators, it is not enough to sell megapixels alone. Sure, the number is important, but ultimately end users want to know the value proposition and how the camera will help solve security, safety or other challenges at the protected premises. Users want to be able to target specific areas with technology that resolves issues or addresses risk. They are most often looking for a solution that can be handled as an operating expense, versus a large capital expense that may take months or even years to budget for.

The good news is that with the higher resolutions, image quality and clarity provided by megapixel cameras come a wealth of other benefits and capabilities that translate into a lower total cost of ownership, heightened business intelligence and other valuable services that systems integrators can provide to customers.

Evolution in Action

The state of megapixel and high-definition camera research and development has evolved to higher resolutions, superior imaging and the ability to apply the latest compression codecs for more efficient bandwidth use in transmission and storage as well as cloud computing. Higher definition is great, of course, but what it affords in new implementations is what really matters to security integrators and users – and there is no shortage of exciting and trending features

that installers can leverage to target customers' applications.

First, a clarification: Resolution and image quality are actually very different. A high-resolution product can still result in a poor picture if the end-to-end solution does not have the right compression, cabling, monitors, servers, transmission, PC graphics cards, and so on. Even with a 12MP camera, the image quality at the other end could translate down to a nearly useless 1MP if the entire ecosystem has not been carefully planned.

The benefits of improved resolution have been widespread, with significant impact on the systems integration channel. While high-quality imagery has become the norm, integrators want to know what value-added features they can provide to differentiate their offerings and bring even greater value to the end user, making them a happier and perhaps stickier client.

Technology Benefits and Impact

Megapixel technology provides higher resolution for viewing greater detail, covers an expansive area and helps more fully define objects. These advancements can be effectively deployed with live images, where one high-resolution camera can cover the same visual area of two or three lower resolution cameras. For cameras in applications such as sports stadiums or arenas, surveillance can pick out individuals at greater distances with exceptional clarity.

Installations seeking a combination of high resolution and high

performance at a competitive price point are making the jump to 4K cameras, which have dropped in price like other units on the market. The increased amount of pixels per foot with 4K cameras improves image detail, which can be especially useful in areas such as loading docks, transportation hubs and distribution centers, and airport terminals. With additional processing power a key part of the equation, built-in infrared illuminators can produce clear images at an effective distance in subpar lighting conditions.

Real Bandwidth Reduction

Integrators now have technology available that reduces network bandwidth and video storage requirements. Intelligent bitrate control mechanisms adjust the compression configurations during live streaming, minimizing bandwidth and storage requirements for H.264 and H.265 video streams. This embedded technology continuously monitors and optimizes system streaming parameters to match the level of activity within the camera's field of view, offsetting the added video storage required when streaming at 4K resolution. Users enjoy cost savings by both reducing the load on their network and lowering the amount of storage required.

Customers with scenes that feature times of no movement or areas within the image that remain static stand to gain the most from this technology. For example, a car parking facility

or building entrance may have low motion activity for extended periods. These conditions let users dramatically reduce the amount of bandwidth and storage needed while still allowing them to record and/or view a high-quality video stream.

Resolution and image quality are actually very different.

At the Edge Gains Speed

With greater processing power, camera analytics are moving to the edge. Cameras can now process complex analytics, including motion detection, line crossing, loitering, audio classification and other activities. New technology that enables "trickle storage" has made its way to edge-based video for guaranteed assurance of recording. With this capability, a camera automatically detects short-term network interruptions and starts recording video to an onboard SD memory card, followed by a seamless video transfer of the recording to a hard drive or VMS once the network connection is reestablished.

Numbers are great, but think first about what is to be accomplished, as well as what the challenges are, and then marry the appropriate megapixel camera to the specification. Become a problem solver, which is easy to do with the wide range of camera features and capabilities now available.

Peter Ainsworth (peter.1.ainsworth@jci.com) is general manager, video products, at Johnson Controls (www.johnsoncontrols.com).

access to recorded video on demand from any location and any connected device.

Leading cloud providers create their own secure software, helping deliver services that achieve higher levels of security, privacy and compliance. Encryption, redundancy, two-factor authentication, backups and software updates are automatic. Best of all, the cloud regularly adds features, which enables integrators to pass along a continuing array of new services to customers.

5. Are There Ways to Create Recurring Revenue?

It is important to select the most versatile, flexible and scalable platform available. When a platform is versatile, a cloud solution can be used where

it makes the most sense to move complex and costly infrastructure off premises. Unlimited storage options provide simple and cost-effective cloud and hybrid video storage and allow for the selection of days, motion event counts, bookmarks, and quality settings for each camera and the scheduling of video uploads during off-peak times. There should be flexibility for cloud recording in a simple-to-use interface, with the ability to select all cameras or any single camera, enter the number of days to record (from one day to a year or more), record only when motion is detected, and specify video resolution. With a flexible cloud platform, an integrator can turn recording on and off as necessary and can create a custom upload schedule to send video to the cloud in the evening or at other





non-prime times to save bandwidth.

In the case of a large boutique bank, for example, the customer stores video in the camera and the cloud. The integrator managing these devices can view recorded video and can ascertain the current camera status: how many people have been logging in and viewing, how much data has been used, and whether a camera has been tampered with or hacked. With the ability to manage thousands of locations from one interface, the integrator is in control of the levels of management provided and can easily add or customize services, providing for a stickier customer.

The amount of RMR from cloud services can vary dramatically. If the camera is sending video to the cloud

24 hours a day at 4K resolution at 5 Mbps, the RMR can be around \$100 per month, but if it is recording motion activity only, the RMR may be less than \$10 per month. Bandwidth is one of the limitations in the growth of cloud recording, but it also provides a lot of variables and scenarios. Some customers only record on motion or dial

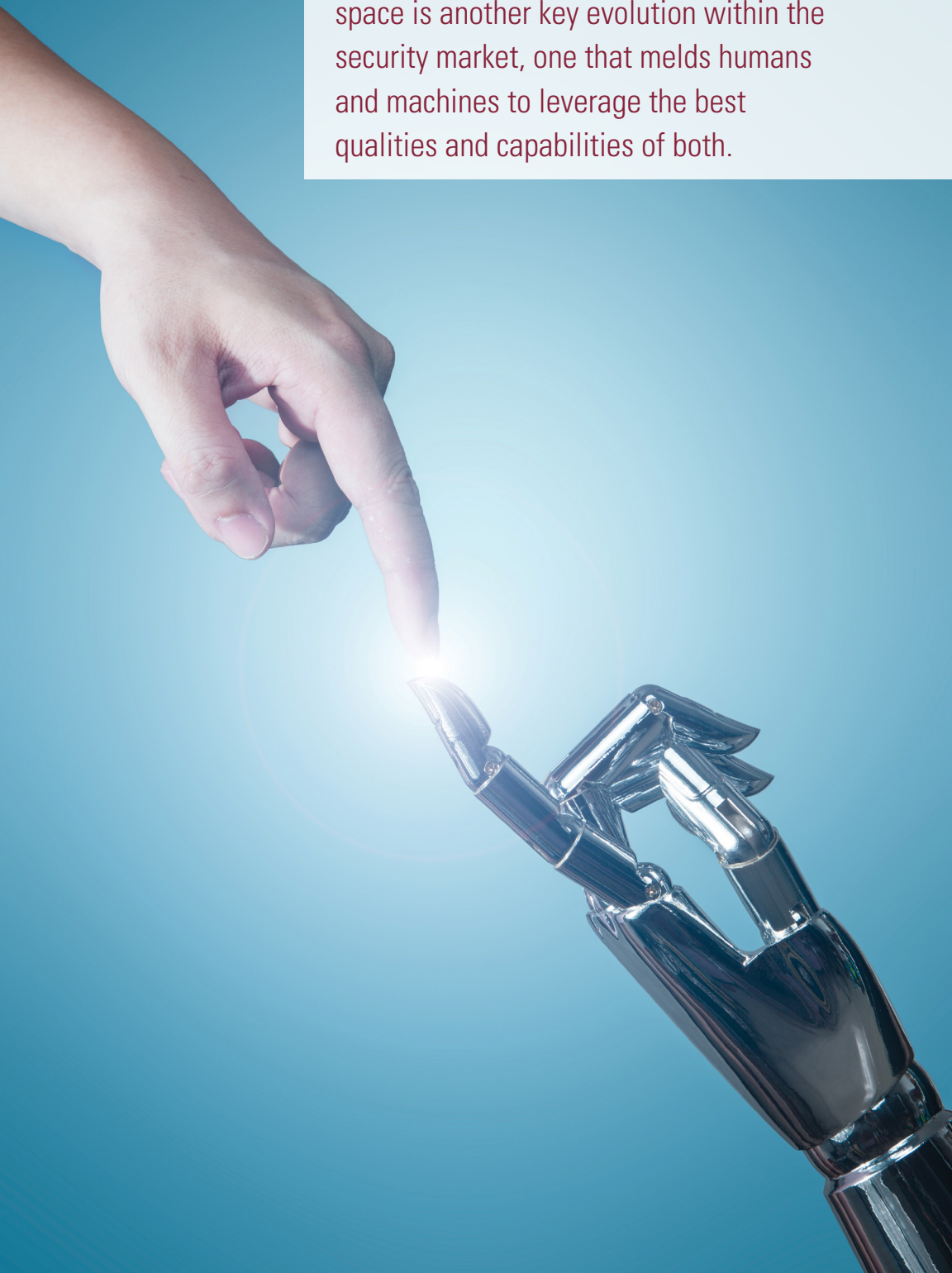
down to one or two frames per second to save bandwidth. Again, it is all dependent on a project's parameters, and

integrators should have the flexibility to address every customer and vertical market. ■ **Back to TOC**

It is important to select the most versatile, flexible and scalable platform available.

Martin Renkis (martin.renkis@jci.com) is the general manager of cloud solutions, global security products, for Johnson Controls (www.johnsoncontrols.com).

The introduction of robots to the security space is another key evolution within the security market, one that melds humans and machines to leverage the best qualities and capabilities of both.



Robot Evolution

New technologies are enhancing the security teamwork between man and machine

By Travis Deyle
Cobalt Robotics

In many industries, the introduction of machine learning, computer vision and robotics is changing the paradigm of security and facility management. Robots are more than a compilation of sensors and computation. They offer both innovation and adaptability, and they are, quite literally, computers that can reach out and touch the world. They are designed to move around human spaces safely and in a way that avoids being intimidating or scary, thus easing cultural acceptance. As the use of security robots increases, costs will decrease and capabilities will improve.

As a result of new integrations, robots have evolved considerably in just a few years. Robots can, for example, detect open doors, unauthorized people and water leaks, and they can investigate



suspicious events and sounds. They easily integrate with existing security solutions such as access control; they enable security personnel or facility executives to add remote coverage; and they can augment existing manned guard operations. With continuing advances in technology

and integrations with other legacy systems, it is predicted that, within five to 10 years, security robots will be a commonly used tool for security professionals.

Already, corporate security directors have found that robots can address several pain points.

For example, robots enable a single person to oversee multiple areas at once. Rather than a company stationing guards to occupy every floor in a corporate facility, robots with telepresence features, as in remote two-way audio and video chat capabilities, can allow an individual to monitor and respond to events across a large area in real time.

In addition, security professionals are using robots to identify safety risks and liabilities, including unauthorized

guests or environmental hazards. A robot can detect people who are breaking and entering into a facility, and the robot and a remote specialist can monitor the event and escort the intruder out of the building, without putting anyone in harm's way.

Similarly, robots can interact with visitors and employees and can be a useful tool for

emergency response situations, such as by instructing building occupants to vacate the premises during a fire alarm and then ensuring that the floor is clear.

Security robots are quickly becoming an extension of smart buildings and smart organizations. Robotic systems can build models of what is normal, flag anomalies, and then act to detect, prevent and

Corporate security directors have found that robots can address several pain points.





respond to events in real-time. Through complex machine learning algorithms, robots will continue to improve over time. For example, they can regularly and rapidly perform many learning tasks as a part of customer onboarding, including

modifying patrols based on past encounters and time of day; learning to differentiate between real

people and posters on a wall; and building maps of thermal signatures to search for anomalies.

Robots speak to the changing nature of physical security in the modern enterprise. Historically, physical security largely consisted of “guns, gates and guards.” More recently, security has been heavily focused on

Robots speak to the changing nature of physical security in the modern enterprise.

people and assets. But there is another change afoot at the strategic level, where security practitioners more and more concern themselves with matters such as risk compliance, business continuity, and accountability. In short,

physical security is increasingly resembling a cyber system because of the adoption of technology. This is a shift in which

security can become more rigorous, consistent, accountable and responsive across an organization. As a byproduct of this change, physical security will be elevated within the modern organization, where it can enable business operations to function at maximum capacity, reduce downtime risk for shared services, augment

human services, and improve overall employee health and happiness.

The introduction of robots to the security space is another key evolution within the security market, one that melds humans and machines to leverage the best qualities and capabilities of both. As

with most new technologies, it will take some time for people to realize the full potential of security robots, including the specific problems they are best at solving. The industry needs to remain honest and realistic about the capabilities and limitations of

the technology, while maintaining a level of technical expertise to deliver immediate value and long-term vision.

For security practitioners, security robots present a unique opportunity to enhance security programs by leveraging machine learning technology that will continue

to improve and provide additional functionality and value. ■ **Back to TOC**

The industry needs to remain honest and realistic about the capabilities and limitations of the technology, while maintaining a level of technical expertise to deliver immediate value and long-term vision.

Travis Deyle (travis@cobaltrobotics.com) is the founder and CEO of Cobalt Robotics (www.cobaltrobotics.com).



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.



www.securityindustry.org

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

