TECHNOLOGY Insights

Spring 2022

Volume 10, Number 1

Security in 3D

LiDAR and other sensors allow the creation of rich, video game-like digital maps

Page 4

I Saw the Light

Agro-businesses can benefit from illumination solutions

Page 14

The Ears Have It

Audio solutions provide essential information

Page 34

Virtual Screening

Millimeter wave scanners aren't just for airports anymore

Page 68

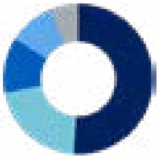
DISCOVER THE VALUE OF SIA MEMBERSHIP

Who We Are

The Security Industry Association (SIA) (securityindustry.org) is the leading trade association for global security solution providers, with more than 1,100 innovative member companies representing thousands of security leaders and experts who shape the future of the security industry.

1,200+

Member companies representing thousands of security professionals



Membership Breakdown

- ■ manufacturers, 53%
- ■ service providers, 18%
- ■ integrators/dealers, 15%
- ■ distributors, 5%
- ■ other, 9%

97%

SIA Members would recommend SIA to an industry colleague, according to the SIA Member Satisfaction Survey

How SIA Helps You

Advocacy

Standards

Research

Networking

Professional Development

Join SIA Today!

Learn how to maximize your membership! Help your business succeed and thrive in the global security industry! Visit us online at securityindustry.org.

For more information, contact Kevin Murphy, Director of Membership:
email: kmurphy@securityindustry.org or phone: 301-804-4716

securityindustry.org/join

Industry Partner

iSC

Security Industry Association
securityindustry.org

SIA

TECHNOLOGY Insights

Spring 2022

Volume 10, Number 1

Security in 3D

LiDAR and other sensors allow the creation of rich, video game-like digital maps

Martin Vojtek (martin.vojtek@tacticaware.com) is the CEO of TACTICAWARE, part of Hexagon Geosystems (3dsurveillance.hexagon.com).

DIGITAL TWIN, LIDAR, SENSOR FUSION, MIXED REALITY AND GAMIFICATION – these are all terms that are more familiar to the IT, autonomous vehicle and gaming industries. But a 3D surveillance control system (3DSCS) brings these cutting-edge technologies to the usually conservative security industry by delivering real-time 3D data and superior intruder detection in an intuitive way.

A 3DSCS works with rich 3D maps (models) that users are able to move around in just like in a video game. Add to this the elimination of the sometimes difficult search for the exact location of alarm events on a 2D map and the true power of the technology becomes compelling.

Accurate 3D models of large areas can quickly and easily be created for the 3DSCS using aerial photos captured by a drone. Inexpensive commercial drones can perform automatic flight missions over an area of interest using Google Maps for reference. Through photogrammetry

techniques, a 3D model is then built from the photos.

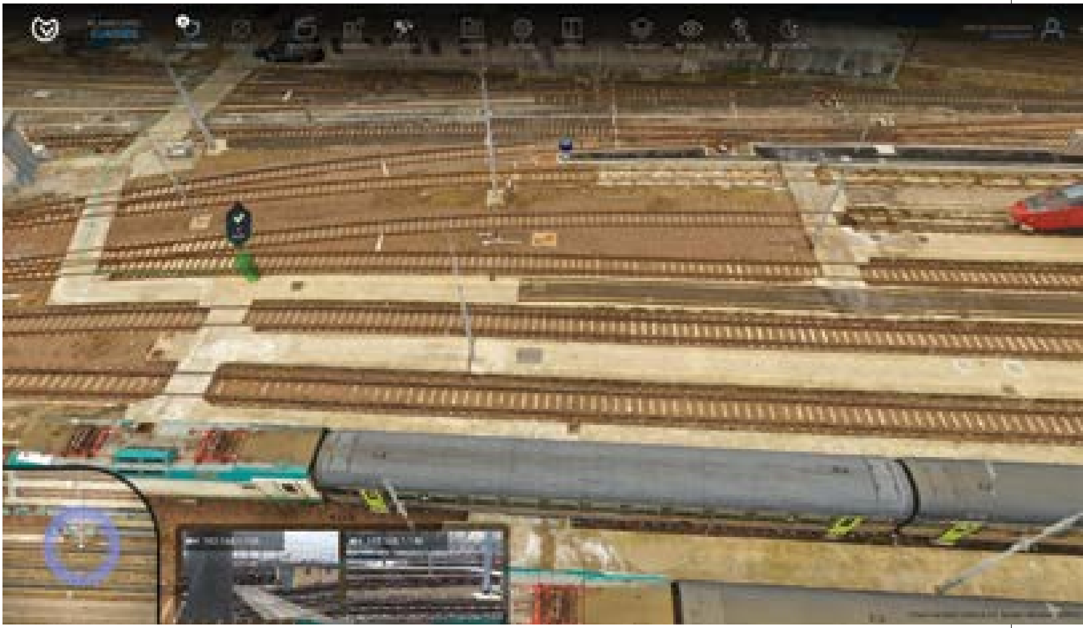
Flight missions usually take 15 minutes to one hour, and the automated generation of a 3D model of a site takes from two to three hours. The result is a full-color 3D map of the area that is a digital twin of the actual environment to be protected. 3D models of various objects, such as trees, bushes, streetlamps, fences, etc., can be added to further enhance the map. If the 3DSCS user is using a 3D engine, as in computer gaming, it is possible to further enrich the viewing experience with shadows and other visualization effects.

THE KEY TO THE ENTIRE PROCESS IS THAT THE 3D MODELS ARE TRUE TO SCALE, SO WHATEVER IS MEASURED WITHIN THE MAP CORRESPONDS TO REALITY.

The key to the entire process is that the 3D models are true to scale, so whatever is measured within the map corresponds to reality. This highlights the essence of why a 3DSCS is based on 3D maps. It is not simply because they are visually attractive, but because the map serves as an internal universal coordinating system. Each point within the map has its own spatially correct X, Y, Z position relative to the center of the grid upon which the entire map rests. This allows for coordinated interaction between all components of a security system, i.e., detectors, cameras, 3D zones and even intruders. It also eliminates the complex manual setting up of presets for rotating cameras to enable coordinated interaction with a detector. The 3DSCS knows exactly where an intruder is located based on LiDAR detection and knows which pan-tilt-zoom (PTZ) cameras should be directed toward the alarm event.

A 3DSCS also provides a powerful tool for security system design through the use of advanced virtual planning in the digital twin environment. It is very easy to insert a virtual rotating camera into the 3D map and then perform tests for coverage.

Security camera coverage can be presented as a green light source so



A 3D map of a rail yard, including an authorized railway employee (green object)

that camera blind spots can be understood by projecting both green light and shadows. This gives the user instant information on how well a given area is covered by cameras and whether they may need to add more cameras or change locations. LiDAR detectors can also be added to the 3D map and validated in the same way.

Since the entire system is three-dimensional, the detection method is also volumetric. In order to better understand exactly where an alarm event is occurring in 3D space, detectors are needed that provide this information. This is why a 3DSCS uses LiDAR detection technology, which is also found in self-driving cars.

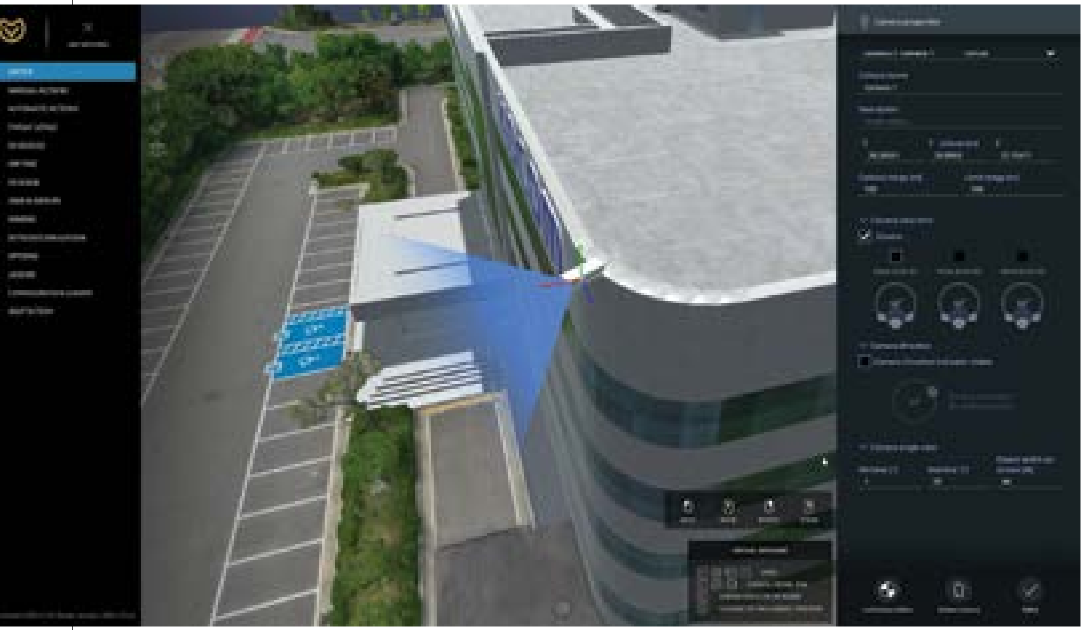
LiDAR detectors send beams of invisible laser light into space. The reflected laser pulse is returned to the detector, and the time-of-flight of each pulse is measured to calculate the range of the object from the detector, up to a distance of 250 meters with an accuracy of 2 centimeters. These LiDAR detectors usually rotate 360 degrees and fire their eye-safe lasers with a horizontal resolution of 0.1 degree. This means 3,600 beams per rotation, up to 20 times per second. They, therefore, make millions of

> IF THE DESIGNER IS SATISFIED WITH THE VIRTUAL PLACEMENT OF BOTH THE CAMERAS AND DETECTORS, THE ENTIRE DESIGN CAN BE VALIDATED BY INSERTING A VIRTUAL INTRUDER. THIS PART IS NOT UNLIKE A COMPUTER GAME, BUT IT IS A VERY POWERFUL TOOL.

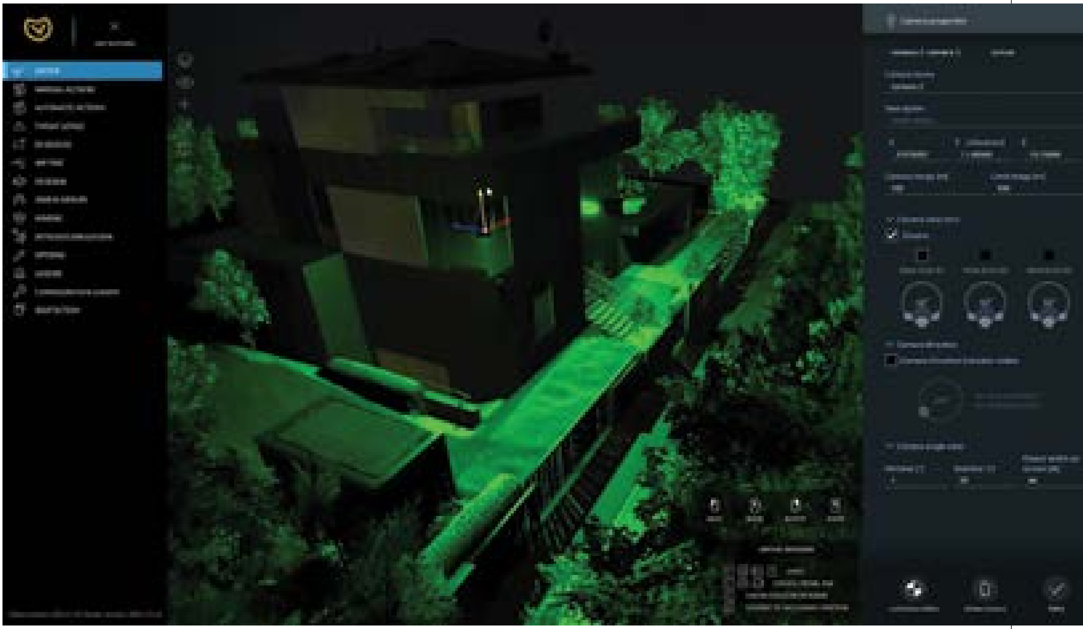
measurements per second, creating a “cloud” of points that the 3DSCS uses to detect static and moving objects.

There are several types of LiDARs on the market. The most common are spinning “puck” and/or solid-state LiDARs. However, more sophisticated sensor fusion models have, in recent years, been introduced which combine LiDAR with dual panoramic RGB cameras and thermal imaging. A mature 3DSCS should support all commonly available LiDARs.

So which LiDAR to choose? How many will be needed? How high and where should they be placed? These are standard design questions that can be easily answered by using the virtual planning tool described above. Just as with a security camera, a user can drag and drop the selected LiDAR and insert it into the 3D scene. Once the technical specifications are understood (range, field of view, etc.) a 3DSCS



Virtually planning security camera system design within the 3D map



Security camera coverage and blind spots depicted in the 3DSCS using a green light source and shadows

can immediately display a snapshot showing the coverage of the laser beams. This makes it very easy to determine if the detector “sees” the area to be protected. Adjustments are easily made in the virtual environment prior to actual installation.

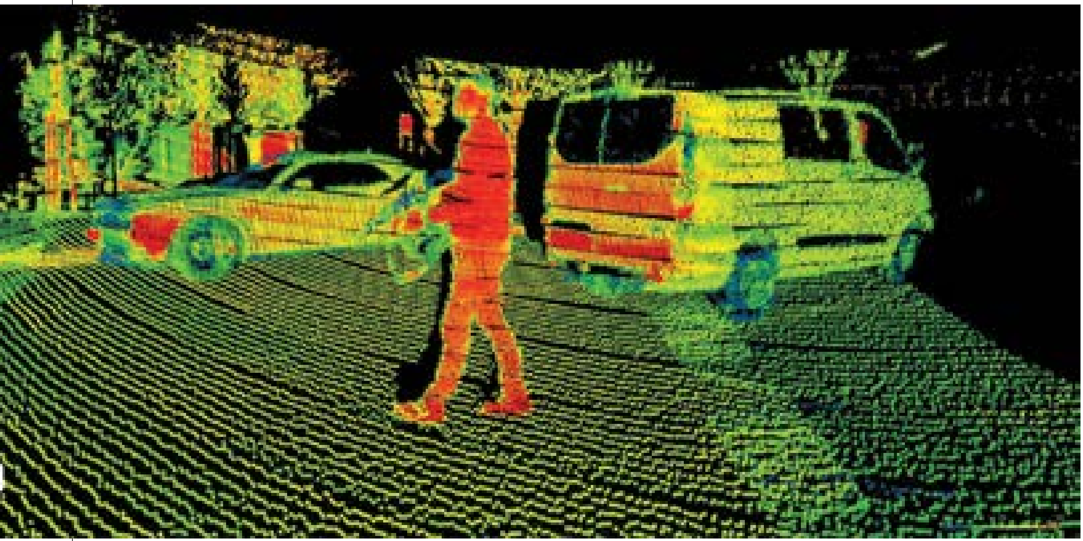
If the designer is satisfied with the virtual placement of both the cameras and detectors, the entire design can be validated by inserting a virtual intruder. This part is not unlike a computer game, but it is a very powerful tool. On the body of this virtual intruder, laser beam “hits” are displayed and it is possible to see whether or not there will be sufficient detection in a given area, even if the intruder is attempting to evade detection by crawling around in critical places, such as in front of building entrances. The location and type of LiDARs can be adjusted as needed to achieve the desired quality of detection.

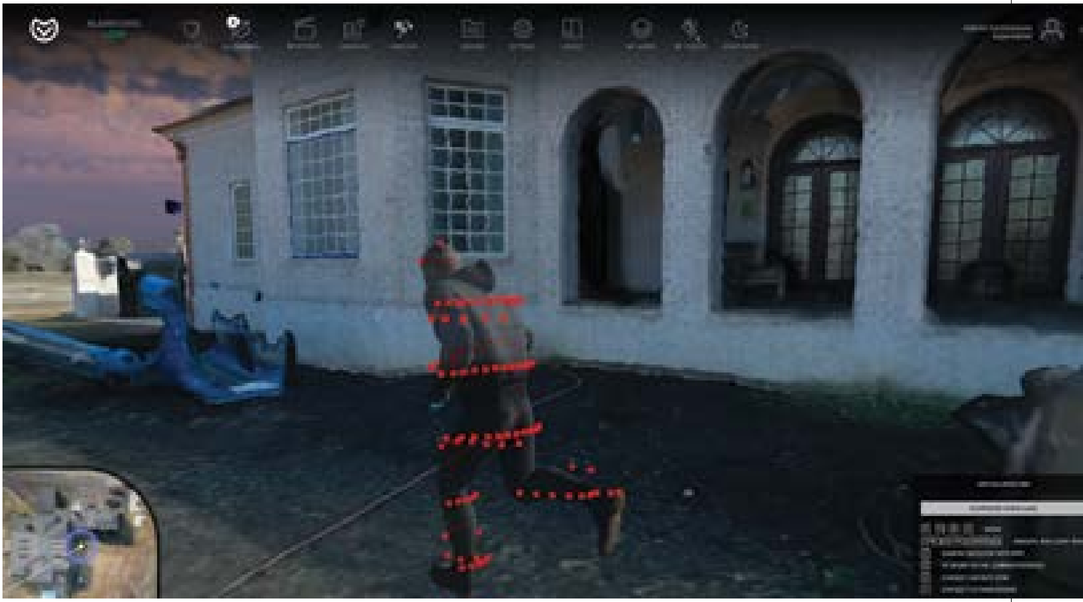
Another advantage of a 3DSCS is the design of the detection zones themselves. By clicking on the map, 3D zones of different shapes, sizes and alarm parameters can be created in seconds. An alarm event will only occur if a moving intruder enters this zone. And how does the system detect what is a moving object? The LiDAR creates point clouds and monitors the entire scene precisely – both static points and moving points. A 3DSCS can group these moving points into objects (known as "bounding boxes") using a clustering method. The user can then define the minimum and maximum size of objects of interest. For example, objects smaller than 70 centimeters, such as cats and rabbits, or objects larger than 6 meters, such as a passing train, can be ignored. In addition to detection zones, a 3DSCS can be equipped with other types of zones, including pre-alarm zones, loitering detection zones, delayed zones, entry zones, and zones that monitor the safe distance between objects of different classes.

The system is designed so that it manages everything itself. The operator is more of a spectator and supervisor. The moment an intruder enters a detection zone, an alarm is triggered. The operator can observe all intruders on a monitor in real time and can see their positions, their sizes, their movement speed, and the trajectories of their movements. If the overall security system is equipped with PTZ cameras, these automatically slew to view the intruders.

The system stores all breach information, including camera footage, in a forensic archive. A 3DSCS can also control downstream devices,

Raw LiDAR data of a human and vehicles





LiDAR detector locations being tested for effectiveness within the 3D map by moving a virtual intruder through the scene

such as sirens, lights, barriers and gates. Video management systems (VMS), physical security information management (PSIM) systems, and other supporting software can instantly be made aware of the alarm. Importanly, a 3DSCS can be added to an existing security system, so there is no need to rip and replace.

The system can be set up so that, when an outdoor zone is breached, an alarm occurs and the threat level is raised. In this case, the operator/security guard immediately handles the situation according to normal procedures. If three or more intruders enter the zone, the system can automatically raise the threat level even higher and automatic actions can be intiated, such as closing entrances, locking sites containing operators, calling the police, and switching on lights and sirens.

> THE SYSTEM IS DESIGNED SO THAT IT MANAGES EVERYTHING ITSELF. THE OPERATOR IS MORE OF A SPECTATOR AND SUPERVISOR.

The highest threat level can be automatically triggered by a larger detected object in a certain zone or an object moving at a higher speed. This may be a vehicle that has entered the guarded area. If the automated actions are set up appropriately, the premises can be protected very effectively.

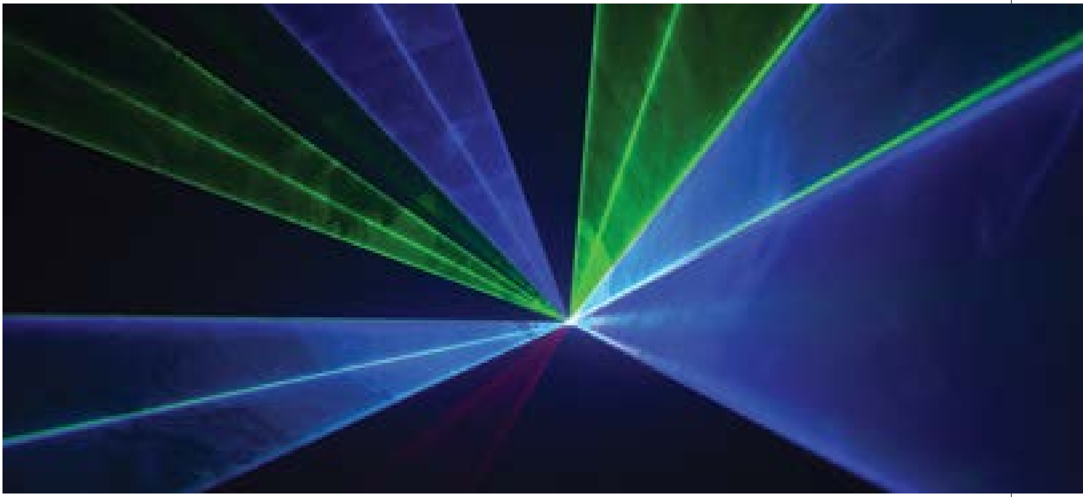
What about false alarms? Outdoor detection systems can be susceptible to being triggered by animals and swaying vegetation. A 3DSCS can combat this in several ways, the simplest being to put the tree or shrub in question in an exclusion zone so that any movement in this area is ignored.

LIDAR DETECTION IS RESISTANT TO RAIN AND SNOW, IT DOES NOT MIND HIGH OR LOW TEMPERATURES, AND THE TIME OF DAY OR NIGHT DOES NOT AFFECT DETECTION.

Alarm handling is performed by the operator by clicking on the dialog box. The system may require a comment on the alarm event, or it can be set to automatically clear alarms after a certain period of time. This is particularly advantageous for unmanned premises. The alarm is recorded but does not hang in the system for hours or days. The system can also "age" objects. This is a practical aid in cases in which a new object, such as a car being parked, enters the guarded area. This will, of course, trigger an alarm. But the system can recognize that the object has stopped moving and, after a user-defined time, it can place it in the scene and not react to it anymore – that is, until it moves again. These are typical functionalities for the residential segment, where there is no full-time operator.

Further, a 3DSCS is ideal for residential security because it can intelligently create perimeter and volume detections. For example, it can secure the area around swimming pools, including a virtual path from the house to the pool, and seal off the rest of the location. Or, conversely, it can deactivate everything during the day and leave only the pool protected to detect children who might fall in.

LiDAR detection is resistant to rain and snow, it does not mind high or low temperatures, and the time of day or night does not affect detection. Unlike conventional 2D security cameras, it can perform detections in total darkness.



The only thing that limits the range of LiDAR detection is very dense fog. But even this does not disable the whole system, which operates with infrared barriers. A LiDAR system is both the source of the light and the receiver of its reflection. In dense fog, this visibility may be reduced, but the system informs the operator about it and the detections continue, albeit with a shorter range. The system also actively monitors for deliberate obscuration of the LiDAR, with the threshold at which it is unacceptable set by the user. Once this level is reached, a sabotage alarm is issued.

Rotating cameras can be connected to the system and their rotation can be intelligently controlled. Communication with the cameras is via ONVIF protocol, so there is no need to alter an existing VMS. A 3DSCS also includes its own media server, so camera recordings can be stored directly in the system. Both LiDAR points and camera recordings belonging to a given alarm event can be played back in the archive. The standard is that the camera stream goes to both the VMS and the 3DSCS.

3D surveillance control systems are currently being deployed worldwide to protect residences as well as critical infrastructure. In coming years, they will play an increasingly larger and more important role in the evolution of physical security. ◀

Illumination for Safety, Security … and Crop Growth

The right lighting systems can serve multiple purposes in the agricultural sector

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

POTENTIAL VULNERABILITIES IN THE UNITED STATES' CRITICAL INFRASTRUCTURE have come under increasing scrutiny in the two decades since 9/11. When most people think of "critical infrastructure facilities," transportation, telecommunications and municipal utilities usually come to mind first. The food and agriculture sector, though, represents one of the most important resources for public health and welfare.

Generating roughly one-fifth of the nation's economic activity, 2.1 million farms, 930,000 restaurants, and 200,000 registered food manufacturing, processing and storage facilities make up the U.S. food and agriculture sector. They form the backbone of the nation’s $1 trillion food and fiber business, with nearly $60 billion in annual exports, according to the Cybersecurity and Infrastructure Security Agency. A terrorist attack on this vital industry – whether contamination of crops and livestock or sabotage of facilities critical to agricultural resources – would result in substantial health, social and economic repercussions.

ADDRESSING THE ISSUE

For this reason, the U.S. government enacted the Agricultural Bioterrorism Protection Act of 2002, which was designed to equip stakeholders at every point along the “farm-to-table” food chain to prepare for, prevent and respond to bioterrorism and other public health emergencies that could threaten the nation’s agriculture.

Before 2002, many farms and food processing/packing plants across the country lacked the resources to invest in

> THE FOOD AND AGRICULTURE SECTOR NEEDS POWERFUL TOOLS TO PROTECT ASSETS AND CONTROL CONDITIONS. EXTERNAL ILLUMINATORS OFFER EXACTLY THIS DUAL USE.

“

ILLUMINATORS ENABLE THE MOST COMPETITIVE SURVEILLANCE SOLUTIONS TO OPERATE RELIABLY, DAY OR NIGHT, REGARDLESS OF ADVERSE OR UNPREDICTABLE ENVIRONMENTAL CONDITIONS.

adequate security and safety preparedness measures, according to the Rand Corporation. This left many enterprise facilities vulnerable to coordinated attacks and small and mid-size facilities completely unprotected.

In the years since, many food supply and agricultural facilities have implemented long-term, end-to-end safety measures, such as robust perimeter intrusion detection systems (PIDS), the best of which are outfitted with high-definition surveillance cameras, industry-leading white light or infrared (IR) illuminators, artificial intelligence (AI)-enabled video analytics and command-and-control video management systems (VMS). Though their purpose was singularly focused in the beginning – robust safety and security – today, those technologies are proving themselves to be valuable in additional ways.

EXPANDING THE POSSIBILITIES OF SECURITY TECHNOLOGY

If agroterrorism was the biggest threat to the U.S. food and agriculture sector in 2002, the globe's changing climate, uncontrollable natural phenomena and everchanging security risks are the biggest threats today. This shift has irrevocably redefined the importance of long-term, end-to-end protective measures.

To the benefit of agricultural facilities, many best-in-class security devices – namely external illuminators – can be easily repurposed to address the food and agriculture sector's ever-changing, multi-faceted dangers. Illuminators enable the most competitive surveillance solutions to operate reliably, day or night, regardless of adverse or unpredictable environmental conditions. In addition, they are easily repurposed as heat-controlled, artificial illumination for farmers growing sensitive crops, which require both round-the-clock security and customizable lighting conditions.

THE IMPORTANCE OF ILLUMINATION TO PIDS SECURITY

In the age of advanced video analytics, clear images are critical to achieving results. Without proper illumination, most traditional video surveillance systems yield dark, grainy images at best. These low-quality images significantly hinder intrusion detection, intruder identification and incident prevention, rendering a PIDS essentially useless after the sun goes down.

Built-In vs. External

Cameras with built-in LEDs do not necessarily solve the problem. Integrated LEDs that encircle a camera lens have a range of only about 150 feet and can typically cover only a 30-degree field of view, even though a standard camera's field of view is often 90 degrees. This creates "hot spots" in the middle of a camera's view at night, which can cause a total "whiteout" of the rest of the image. LEDs are also known to

cause heat buildup, which degrade LED distances over time.

External illuminators, however, minimize heat accumulation, extend illumination ranges (as much as 900 feet or more) and offer users several size, light and range options in order to meet individual deployment needs.

Visible vs. Invisible

External illuminators are also configurable as white-light or IR devices, both of which offer their own benefits.

White light illuminators, which operate at a much lower cost than fluorescent and incandescent bulbs, are durable and insensitive to vibration, and they are extremely long-lasting. They also enable 24/7 color image capture, which is invaluable to certain object detection analytics, and can double as a floodlight-like deterrent to potential bad actors.

> “
>
> IN AN AGE WHERE THREATS TO FOOD AND AGRICULTURE FACILITIES COME IN ALL SHAPES AND SIZES, EXTERNAL ILLUMINATORS ARE A VERSATILE AND POWERFUL TOOL THAT CAN ENHANCE PIDS EFFECTIVENESS.

IR illuminators, meanwhile, are detectable only by black-and-white or true day/night cameras, making any camera placement enhanced with IR an invisible, covert form of surveillance. They also offer significantly longer range than visible light, enabling video monitoring of much larger areas.

In an age where threats to food and agriculture facilities come in all shapes and sizes, external illuminators are a versatile and powerful tool that can enhance PIDS effectiveness.

THE VERSATILITY OF ILLUMINATION

The same external illuminators used by security personnel to bolster a PIDS can also be used by farmers to support crop growth.

As every agronomist knows, in order to grow crops efficiently and sustainably, farmers must account for multiple conditions, including:

- Temperature
- Soil type and fertility
- Precipitation
- Crop history
- Elevation
- Light intensity

Calibrating and controlling each of these variables is vital in agriculture. Because so many areas are now subject to unstable and inconsistent conditions resulting from changes in climate patterns, artificial illumination has become even more important.

For sensitive crops, such as cannabis, which require specific conditions to grow correctly, white-light artificial illumination is an attractive choice, both for security measures and the maintenance of optimal growing conditions.

But if a facility requires round-the-clock, in-and-out door surveillance and is growing a crop that is extremely light sensitive, an IR illuminator fits the bill perfectly. The same goes for crops that require precise temperature control.

Pigment optimization is another area where environmental control is important. When different variables affect the expression of different genes – such as the color a plant develops or the size something grows into – control over lighting is indispensable.

> BECAUSE SO MANY AREAS ARE NOW SUBJECT TO UNSTABLE AND INCONSISTENT CONDITIONS RESULTING FROM CHANGES IN CLIMATE PATTERNS, ARTIFICIAL ILLUMINATION HAS BECOME EVEN MORE IMPORTANT.

In conditions where the heat from visible light hinders crop development, advanced external illuminators give farmers flexibility and customizability.

CONCLUSION

Now more than ever, the food and agriculture sector needs powerful tools to protect assets and control conditions. External illuminators offer exactly this dual use. When it comes to security, lighting is critically important to the performance of video surveillance. Both white light and IR illuminators allow systems integrators to precisely control the lighting for PIDS. These same illuminators enable security systems to be integrated into existing agronomic workflows – and even be repurposed to optimize them – wherever there is a need. ◀

Pandemic Changes in Building Access Are Here to Stay

Multi-tenant dwellings continue to move toward mobile access and touchless sensors

Norbert Artur (norbert.artur@aiphone.com) is the Director of Sales – Canada for Aiphone (www.aiphone.com).

SECURITY IN MULTI-TENANT BUILDINGS AND CONDOMINIUM COMPLEXES has been evolving for many years. Property managers continuously look for ways to ensure the safety and security of individual living spaces, as well as common and shared areas, and the events of the past two years increased the already existing demand for comprehensive and efficient access control systems.

With more people working from home, many permanently, there has been more activity in neighborhoods, increased deliveries, and a greater need for tenants to protect their work and personal assets.

Going beyond basic security, many homeowners associations are searching for solutions to ensure resident health and safety through systems that are as streamlined and contactless as possible.

> THE EVENTS OF THE PAST TWO YEARS INCREASED THE ALREADY EXISTING DEMAND FOR COMPREHENSIVE AND EFFICIENT ACCESS CONTROL SYSTEMS.

MANAGING ACCESS WITH MOBILE DEVICES

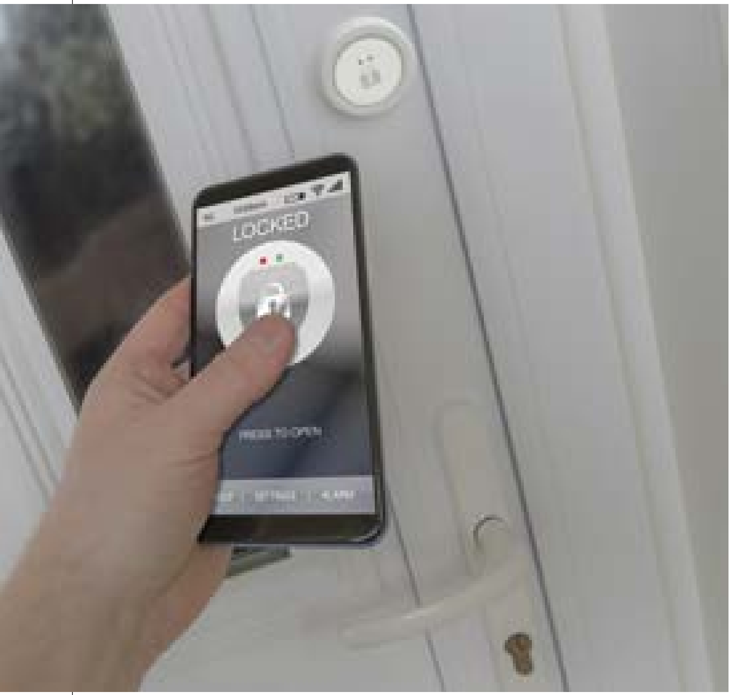
One of the biggest trends in the multi-tenant market is using mobile devices to manage access. Pre-pandemic, flexibility and ease-of-use were top of mind for everyone, and residents of multi-tenant facilities were finding value in taking their building security into their own hands. This functionality proved to be especially convenient when Covid restrictions reduced the number of onsite staff.

With a mobile app, tenants have flexibility in managing access to condominium complexes, private living spaces, and shared common areas. For larger condos and mixed-use buildings, this addresses a major pain point, offering a security

WITH A MOBILE APP, TENANTS HAVE FLEXIBILITY IN MANAGING ACCESS TO CONDOMINIUM COMPLEXES, PRIVATE LIVING SPACES, AND SHARED COMMON AREAS.

solution for both tenants and facility staff.

Application-based access control is also an ideal solution for managing access in high-end luxury apartments where there are pools, gyms and other amenities. Residents can use their mobile device to gain access to the building lobby and elevators, as well as their own living spaces.



Another benefit of mobile management is the ability to provide a seamless process for deliveries. If a multi-tenant building has a separate room for mail deliveries, a tenant can use their mobile device to confirm identity and grant the mail or delivery person entry into the building lobby and then into the mailroom. The same applies for any grocery, food or dry-cleaning deliveries, adding an extra level of safety during a time when the use of delivery services has increased.

While mobile-based access control offers many advantages, it is not without challenges. Older people, for example, may be less familiar with using smartphone-based applications or might misunderstand how the technology works. As such, it is best to start the conversation soon, as it is only a matter of time before outdated technologies are phased out. Mobile solutions continue to grow in popularity with residents, and soon everyone will be managing access from their smartphones.

UTILIZING VIDEO AND AUDIO

Audio communication for multi-tenant complexes used to consist of a simple telephone or intercom system. However, tenant expectations now include a full-service system, one that combines audio communication and visual verification. It is no longer sufficient just to hear a person through an intercom before pressing a button to enable entry. Tenants and building managers want the ability to visually confirm – ideally through their smartphones – that the person requesting access is who they say they are.

ENHANCED SECURITY AND TOUCHLESS ENTRY

The pandemic boosted interest in contactless and touchless solutions, including mobile credentials, sensors and biometrics. A touchless sensor can be integrated with an access control system to detect motion within a preset range and be activated with a simple hand gesture. In a residential facility where key cards are not used, a sensor can enable access to a lobby or shared common space. An individual would simply approach the sensor field to trigger a signal to communicate to the front desk. This hands-off approach is increasingly popular, and it can also facilitate the delivery of packages, groceries, or food, especially in situations in which a person has their hands full.

Condo buildings and other multi-tenant facilities are searching for comprehensive security and safety solutions that provide peace of mind and ease of use. Whether enabling entry or communicating with a delivery driver, security remains as important as ever. At the same time, efficiency and hygiene have become bigger concerns during the pandemic, which has resulted in the development of valuable new functionalities. ◀

> “ IT IS NO LONGER SUFFICIENT JUST TO HEAR A PERSON THROUGH AN INTERCOM BEFORE PRESSING A BUTTON TO ENABLE ENTRY.

The Still Essential 90-Year-Old Technology

Radar can do what visual security solutions, alone, cannot

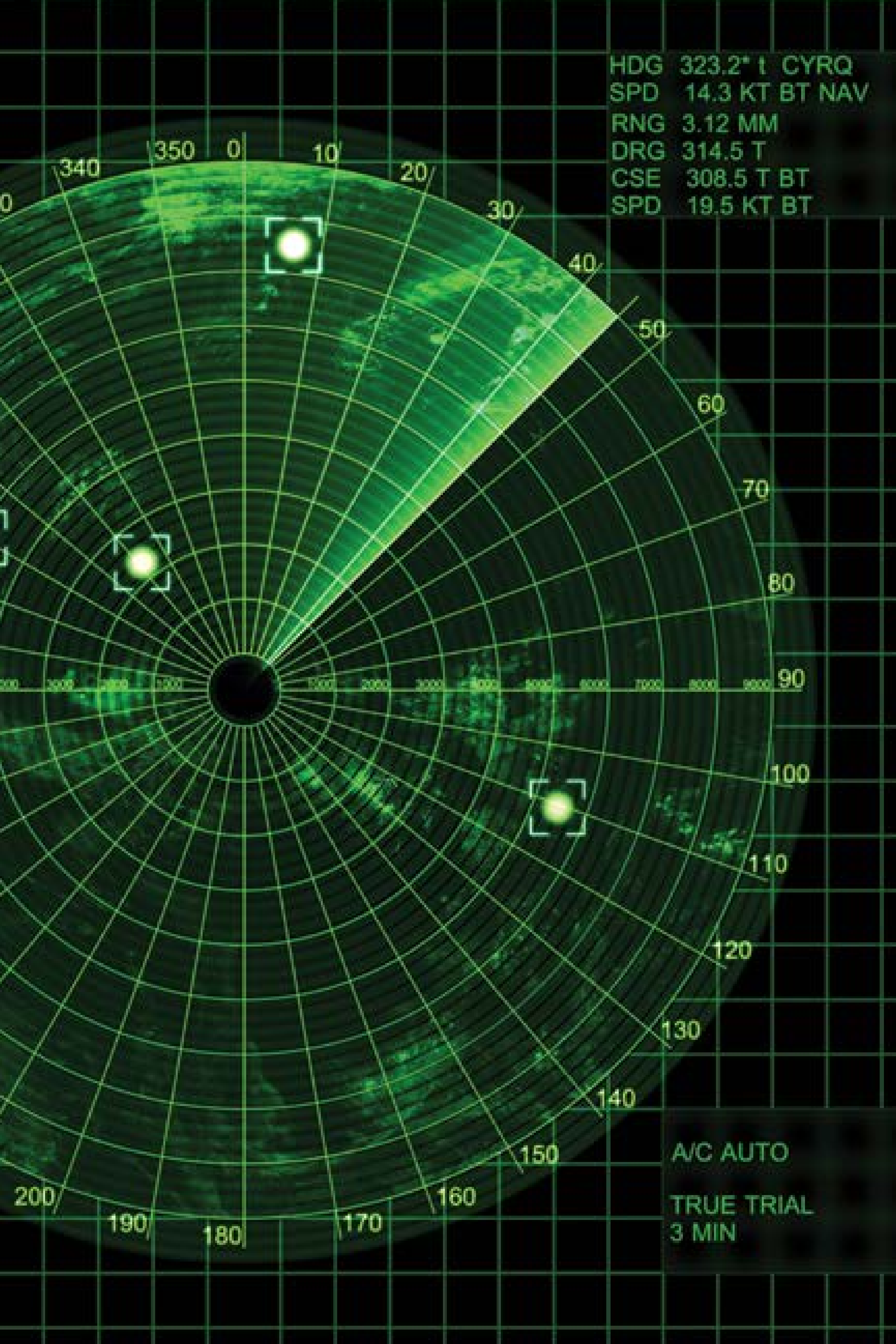
SINCE 1934, WHEN RADIO DETECTION AND RANGING WAS INTRODUCED to the U.S. military, radar has added value to numerous applications across a wide range of industries. Utilizing microwaves to determine the range, angle and velocity of objects, radar's dynamic ability to map human and vehicle movement and deliver early warnings of intruder activity has made it indispensable to military and commercial perimeter security efforts alike.

In the 1930s, radar revolutionized ground, air and ship-based warfare. Today, radar has drastically improved the protection of airports, utilities, data centers, and many other sites.

Kai Moncino (kai.moncino@teledyneflir.com) is Director of Global Business Development, Security, at Teledyne FLIR (www.flir.com).

THE BENEFITS OF RADAR

Many modern perimeter intrusion detection systems (PIDS) rely heavily on camera-based solutions to monitor areas of importance. In ideal conditions, these solutions are effective, especially


HDG 323.2° t CYRQ
SPD 14.3 KT BT NAV
RNG 3.12 MM
DRG 314.5 T
CSE 308.5 T BT
SPD 19.5 KT BT
340
350
0
10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170
180
190
200
A/C AUTO
TRUE TRIAL
3 MIN

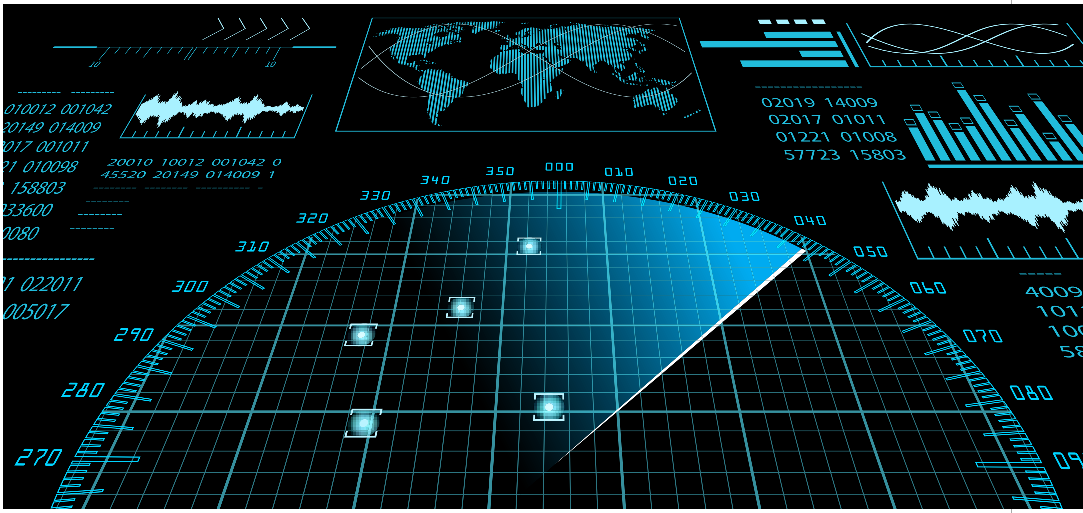
> BECAUSE RADAR SYSTEMS CAN SCAN EXCEPTIONALLY LARGE AREAS GIVEN THEIR WIDE FIELD OF VIEW AND LONG-RANGE DETECTION, THEY PROVIDE TRUE WIDE-AREA PROTECTION AND SITUATIONAL AWARENESS WELL BEYOND THE FENCE LINE.

with the advent of artificial intelligence (AI)-enabled video analytics to detect intruders. However, problems arise for these devices in adverse environmental and imaging conditions, poor visibility, areas with obstructions, and hours of darkness.

Radar directly addresses these challenges by offering security personnel the ability to detect intruders 24/7, even in harsh weather and low or no-light scenarios. When ground-based radar is integrated into PIDS systems outfitted with visible and/or thermal cameras, security personnel can maximize detection coverage, receive early warnings of threats, and gain game-changing intelligence in a turnkey, end-to-end security solution.

THE POWER OF LAYERING PIDS SENSORS

A trusted strategy when strengthening a PIDS involves layering multiple



sensor technologies to maximize the strengths of each sensor while compensating for the limitations of any one technology. When securing large open areas, pan-tilt-zoom (PTZ) multi-sensor (thermal/visible) cameras paired with radar can provide immense benefits to security teams.

Radar can scan a 360-degree area as often as four times per second at ranges of up to several miles. If radar integrated with sophisticated management software detects an object of interest, it will commence two processes: It will, one, relay the precise GPS location of the intruder to central command and display it on a dynamic map, delivering real-time insights, and, two, initiate slew-to-cue functionality for integrated PTZ cameras in order to visually verify the location of the alarm, which allows security operators to dispatch a response with high confidence that the threat is real. Using PTZ cameras with both thermal and visible imagers allows security operators to assess threats that the

> “
>
> A TRUSTED STRATEGY WHEN STRENGTHENING A PIDS INVOLVES LAYERING MULTIPLE SENSOR TECHNOLOGIES TO MAXIMIZE THE STRENGTHS OF EACH SENSOR WHILE COMPENSATING FOR THE LIMITATIONS OF ANY ONE TECHNOLOGY.

RADAR CAN SCAN A 360-DEGREE AREA AS OFTEN AS FOUR TIMES PER SECOND AT RANGES OF UP TO SEVERAL MILES.

radar detects in any lighting conditions and in inclement weather.

This layering of intrusion detection sensors enables system-wide redundancy, which reduces the risk of costly false alarms. It also enables target tracking prioritization by integrating PTZ camera software with logic, such as “follow closest” or “follow furthest,” taking the operator out of the equation and allowing personnel to focus their time on response efforts.

A layered, multi-sensor PIDS ensures that security personnel in a remote command center always have eyes on the target, regardless of conditions, improving overall threat assessment and accelerating real-time response.

OPTIMAL APPLICATIONS FOR RADAR

Though there are many different models of radar devices, purpose-built and specialized to address individual needs,

the following three applications effectively capture the range, reliability and versatility benefits that radar offers.

Wide-Area Monitoring

Because radar systems can scan exceptionally large areas given their wide field of view and long-range detection, they provide true wide-area protection and situational awareness well beyond the fence line. In scenarios where multiple cameras would need to be installed to cover a 360-degree field of view, integrating a single security radar system alongside strategically installed thermal and visible cameras delivers the same coverage with an extended detection range, while using fewer devices.

24/7 Surveillance

Because no two security environments are the same, a one-size-fits-all PIDS configuration does not exist. Add in ever-changing environmental conditions and often unpredictable visibility limitations and designing a PIDS with consistency and reliability in mind is a challenge. Because radar systems transmit high-frequency electromagnetic signals to a location and measure the radiation of the reflections to detect foreign objects, they are unaffected by many of the challenges that limit visual camera performance.

C-UAS Systems

The above benefits are especially important when security personnel are designing a PIDS to address novel airborne threats, such as unmanned

aerial systems (UAS). When integrating effector tools, such as jammers and spoofers, into a PIDS outfitted with thermal sensors and radar, an already powerful system transforms into a C-UAS solution. Built to detect, identify, locate, track, and mitigate both ground-based and aerial threats, these solutions rely on radar to detect incoming UAS, PTZ and multi-sensor systems to verify detection alerts, and effectors to neutralize the threat.

OPTIMAL VERTICALS FOR RADAR

The following verticals are examples of sites where radar provides critical added value for perimeter protection.

Airports

For large airports with perimeters spanning several miles, security managers can deploy radar and experience the combined benefits of robust detection range and wide-area coverage. For airports too large for the human or even digital eye to surveil, or where there is 24/7 activity, radar delivers a strategic advantage in its ability to monitor the perimeter and tarmac around-the-clock.

Utilities

As reported by the electricity non-profit organization CIGRE, 88 percent of substations experience at least one break-in every year. For electric utilities, whose rural substations often have no full-time security staff onsite, early intrusion detection is critical for crime prevention. Radar can detect intruders long before they reach the fence line, allowing a remote security officer to quickly assess alarms, verify threats by reviewing video footage, and dispatch

LIMITED C-UAS OPTIONS

Outside of government and military users, UAS countermeasures that go beyond simple identification – such as jamming and spoofing – are generally illegal in the United States.

police before the situation escalates and equipment is damaged or stolen.

Data Centers

According to the "2020 State of the Data Center Report" from Data Center World, 50 percent of respondents said their biggest security concern was "outside human threats." Typically, for large enterprise data center locations, multiple data centers are built within a single perimeter in a remote environment. Integrating radar into a PIDS ensures that all critical areas are monitored so that no threat goes unnoticed.

CONCLUSION

With reliable performance in all weather and lighting conditions, simultaneous tracking of multiple targets, and precise geolocation capability, radar adds a critical layer of intrusion detection to any PIDS. When paired with PTZ cameras, radar can activate alarms and guide the cameras for streamlined target tracking, visual verification of threats, and faster reaction times. ◀

> USING PTZ CAMERAS WITH BOTH THERMAL AND VISIBLE IMAGERS ALLOWS SECURITY OPERATORS TO ASSESS THREATS THAT THE RADAR DETECTS IN ANY LIGHTING CONDITIONS AND IN INCLEMENT WEATHER.

RICHARD BRENT, LOUROE ELECTRONICS

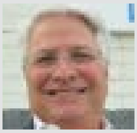
Using Audio for Alarm Verification

The ability to hear, as well as see, increases situational awareness and reduces false alarms

ALARM-BASED SECURITY SYSTEMS HAVE A LONG HISTORY. The first systems proliferated after World War I, when an increase in property crime created a need for homeowners and businesses in the United States to find creative ways to protect their property. Around the same time, insurance companies began offering premium discounts to alarm subscribers, which drove popular demand.

One of the first approaches to residential security was a group of night watchmen called "door shakers" who were paid to shake subscribers' doors each night to ensure they were locked. More advanced systems installed around the same time fixed electromagnetic contacts onto doors and windows, which were connected to a battery and bell and monitored by a central station that sent a guard to the residence when an alarm was triggered.

Today's system designs are not very different. Using the same concept of electromagnetic contacts, modern systems, for residential and



Richard Brent (rbrent@louroe.com) is the CEO of Louroe Electronics (www.louroe.com).

commercial customers alike, leverage technologies such as video monitoring, intruder alarms, and access control to alert emergency responders of possible intruders. Though security technology has evolved over time, one shortcoming has not gone away: false alarms.

THE PROBLEM OF FALSE ALARMS

The following statistics illustrate this shortcoming:

- Historically, more than 98 percent of alarm calls in the United States are false alarms, according to the International Association of Chiefs of Police (IACP).
- False alarms are most often caused by faulty equipment, human error, or inconsistent power supply, as well as pets, rodents, and insects, according to a study from the Cleveland County, Okla., Sheriff's Office.
- False alarms cost U.S. police departments an estimated $1.8 billion and 64,000 person-hours annually, according to research from the Center for

> THE QUALITY THAT DIFFERENTIATES AN ADVANCED SECURITY SYSTEM FROM AN INADEQUATE ONE IS THE ABILITY TO DISCERN BETWEEN FALSE AND TRUE ALARMS.

Problem-Oriented Policing and *Security Sales & Integration*, respectively.

The reason for this sizable expense is that, typically, two patrol cars are dispatched to the scene of an alarm call, as all alarms are treated as high-priority events. These responses not only cost police departments, they also can generate fines that companies and residents must pay.

A solution that can mitigate false alarms will not only save first responders time and security system users money, it will also redirect resources to the alarm events that actually require attention.

THE IMPORTANCE OF ALARM VERIFICATION

Though it may sound strange at first, the solution to false alarms is not the elimination of false positives. A false alarm trigger is the result of a highly sensitive security sensor doing its job, which is to detect any and every abnormality. The quality that differentiates an advanced security system

from an inadequate one is the ability to discern between false and true alarms. The question is not how to prevent the causes of false alarms, but rather how to verify whether alarm activations signify a real breach.

Verifying alarm events using a second-source verification device before first responders are notified reduces the probability of false alarms drastically, preventing fines and saving resources. Any true alarm labeled as "verified" is also elevated to a higher priority level, increasing the likelihood of a timely and effective response.

A verified alarm event is defined as "an electronic security system event in which a trained central station operator, utilizing a standardized protocol, has determined the presence of human(s) and the high probability that a criminal offense is in progress," according to the IACP.

> A SOLUTION THAT CAN MITIGATE FALSE ALARMS WILL NOT ONLY SAVE FIRST RESPONDERS TIME AND SECURITY SYSTEM USERS MONEY, IT WILL ALSO REDIRECT RESOURCES TO THE ALARM EVENTS THAT ACTUALLY REQUIRE ATTENTION.

For decades, video surveillance devices have been the primary choice for security monitoring and incident verification, but video feeds are only able to tell part of the story.

“IT IS ONE THING TO WATCH AN ALARM EVENT UNFOLD; IT IS QUITE ANOTHER TO HEAR THE WORDS A PERPETRATOR SPEAKS WHILE CARRYING OUT A CRIME.

A PROVEN SOLUTION

The problem with video-only security systems comes down to the limited scope of the alarm data they provide. It is one thing to watch an alarm event unfold; it is quite another to hear the words a perpetrator speaks while carrying out a crime. Significant evidence is collected when an audio component of a security system is engaged. Industry-leading audio monitoring technology, which is specially designed to act as a force multiplier when integrated into a security system, takes safety and security to the next level.

Incorporating audio monitoring technology into a security system helps first responders confirm whether an alarm event is true, reducing false alarms and ensuring police only respond to actual threats, saving alarm users thousands of dollars in fines. These devices also enable first responders to arrive on scene with significantly more information.

Upon receipt of an alarm from an audio system, monitors can listen to both live and recorded audio feeds, which allows them to better determine what happened and why. This also provides additional information regarding the event’s location and threat level, ensuring that first responders are able to deploy the best-informed mitigation efforts possible.

ADDITIONAL BENEFITS OF INCORPORATING AUDIO

Situational Awareness

Audio provides greater situational awareness for alarm events, capturing sounds – such as breaking glass, distressed voices, verbal directives, etc. – that give security managers a deeper, more robust view of an incident.

In the case of a school shooting, for example, a surveillance system with both video and audio capture would reveal where a suspect fled and the names or directives that were spoken while the event unfolded, all information that is critical to police response.

Real-Time Communication

Audio enables real-time, two-way communication, allowing remote operators to issue verbal warnings to the unauthorized personnel on the premises and dissuade them against unlawful activity.

> “AUDIO ENABLES REAL-TIME, TWO-WAY COMMUNICATION, ALLOWING REMOTE OPERATORS TO ISSUE VERBAL WARNINGS TO THE UNAUTHORIZED PERSONNEL ON THE PREMISES AND DISSUADE THEM AGAINST UNLAWFUL ACTIVITY.

Audio deployed in retail environments, for example, aids security officers in preventing employee theft, shoplifting, and organized retail crime, as posted audio security serves as a major deterrent. It can also be used as a training tool to coach employees on proper protocol and customer service.

Robust Threat Detection

Audio analytics enable threat detection by recognizing sounds such as gunshots then immediately notifying police, thus shortening response times, which can make the difference between stopping a crime in progress and arriving after the suspects have fled.

BEST PRACTICES

When integrating audio into existing surveillance systems, it is vital that systems integrators and end users consider the following factors:

- **Define Audio Needs** – First, assess the location's specific needs to ensure that the best possible audio technology is selected, whether it is used for incident detection, alarm verification, two-way communication, mass notification, etc.
- **Understand Federal and State Regulations** – After installing microphones, post clear and visible signage at all points of entry that communicate that audio and video surveillance is taking place on the premises.

- **Determine Line Level or Mic Level** – When integrating audio devices into security surveillance systems, confirm that the microphone's output level matches the camera's input level.
- **Consider Microphone Locations** – When deciding where to install an audio device, consider entryways, reception areas, point-of-sale terminals, stairwells, and parking lots – all spaces where people gather often and, thus, where audio is most effective.
- **Select the Right Form Factor and Features** – Once an installation location has been selected, evaluate whether a ceiling is standard height or high/vaulted. This will determine whether a standard microphone is needed or the deployment will require a device featuring a drop-down microphone cable.
- **Define Power and Audio Playback Source** – Because output microphones require power sources, consider using an audio base station, which powers audio devices and provides playback features to interface with other devices, such as cameras, video management systems (VMS), etc.
- **Integrate with VMS** – Ensure the VMS supports the type of audio functionality, such as bi-directional audio, that will be installed. Then tailor the audio settings within the VMS interface.
- **Test the Solution** – Once everything is set up, evaluate the audio pickup and make adjustments where needed.

At the end of the day, it is always better to design a surveillance system that is able to both see and hear events as they unfold. For complete situational awareness, business optimization, false alarm minimization, and robust remote security, audio offers a highly effective solution. ◀

BEST PRACTICES SUMMARY

1. Define Audio Needs
2. Understand Federal and State Regulations
3. Determine Line Level or Mic Level
4. Consider Microphone Locations
5. Select the Right Form Factor and Features
6. Define Power and Audio Playback Source
7. Integrate with VMS
8. Test the Solution

Cybersecurity Outlook for 2022

Four trends to drive the protection of online systems

DURING THE PAST YEAR, IT HAS BEEN COMMONPLACE FOR ORGANIZATIONS across the globe to face increasing cyber threats. No business is immune. In fact, Gartner reports that, by 2025, 70 percent of CEOs will mandate a culture of organizational resilience to combat threats from cybercrime, as well as severe weather events, civil unrest, and political instability.

It is no surprise why more organizations are prioritizing cybersecurity. The ever-growing network of connected devices, many with insufficient security measures, has opened the door to a wide variety of potential risks. Multiple events have demonstrated that every business segment can face a threat, and more sophisticated hackers and attacks are emerging daily.

Cybersecurity risks also expand as teleworking and online video conferencing adds vulnerabilities that can be exploited. Of course, technology providers continue to keep a laser focus on keeping cyber threats at bay to ensure a secure user experience, but it is an ongoing challenge, and everyone must be vigilant. Here are four considerations and priorities likely to drive cybersecurity in the coming year.

Tom Reilly (t.reilly@commendusa.com) is the President of Commend Americas (www.commendusa.com).

SECURE DATA TRANSMISSION AND COMMUNICATIONS

Significant product development efforts have gone into leveraging the advantages of cloud services and networking technologies. Disruptive innovations like the cloud carry considerable potential and offer substantial benefits for customers, like user convenience and higher levels of accessibility. At the same time, though, cloud services must be secure, and this is made possible by a growing set of tools and features that maintain the utmost cybersecurity protection.

These developments have spurred new, security-focused product development processes centered around Dev(Sec) Ops. This process ensures that services and systems within cloud architecture are constantly monitored for performance and availability, using fully automated tests and latest-generation artificial intelligence (AI) technologies. This "monitoring" allows engineers to take proactive action against possible problems.

> FOR END USERS, THE TERM 'SECURITY' NO LONGER JUST MEANS PROTECTING ACCESS TO A BUILDING; IT ALSO INVOLVES SECURING CORPORATE NETWORKS AND SENSITIVE DATA.

SECURING THE IOT

Another area where the security of connectivity and networking comes to the forefront is the effective integration of individual devices into Internet of Things (IoT) environments. This will enable devices like next-generation intercom stations and modules to interact intelligently with other devices in the same IoT domain. These interactions will make possible new methods of automation

> THE EVER-GROWING NETWORK OF CONNECTED DEVICES, MANY WITH INSUFFICIENT SECURITY MEASURES, HAS OPENED THE DOOR TO A WIDE VARIETY OF POTENTIAL RISKS.

in applications from building management to smart cities by integrating seamlessly with barrier gates, information terminals, security equipment, and the like to allow for situation-specific control and communication. To enable all of this, it is essential to elevate device hardening and cybersecurity efforts.

ARTIFICIAL INTELLIGENCE

AI and machine learning algorithms, controls, and tools have opened another avenue for further improvement of solutions. For example, voice assistant solutions will rely heavily on AI technology to answer common user questions. AI and machine learning also serve as the basis for future developments in voice recognition as a means of authentication and distinguishing between regular and distress calls. As far as cybersecurity is concerned, intelligent methods will be highly valuable in detecting irregular or suspicious system access or behavior anomalies automatically.

MULTI-FACTOR AUTHENTICATION

In the days of rapidly expanding cloud environments and growing AI-driven cyberattack arsenals, logins alone will no longer suffice. Authentication factors to complement the user's login credentials include push-based authentication via mobile phone, security tokens for randomly generated passcodes, device certificates, QR codes, biometric scans, and more. As a result, multi-factor authentication finds

its way into an intercom, security device, and unified communication system. As the technology progresses, product development efforts will continue to find new ways to keep data and communications under lock and key.

LOOKING AHEAD

For end users, the term “security” no longer just means protecting access to a building; it also involves securing corporate networks and sensitive data. Businesses are much more focused on evolving IT and cyber threats, a growing paradigm that challenges leaders to stay one step ahead of risk trends to ensure business continuity.

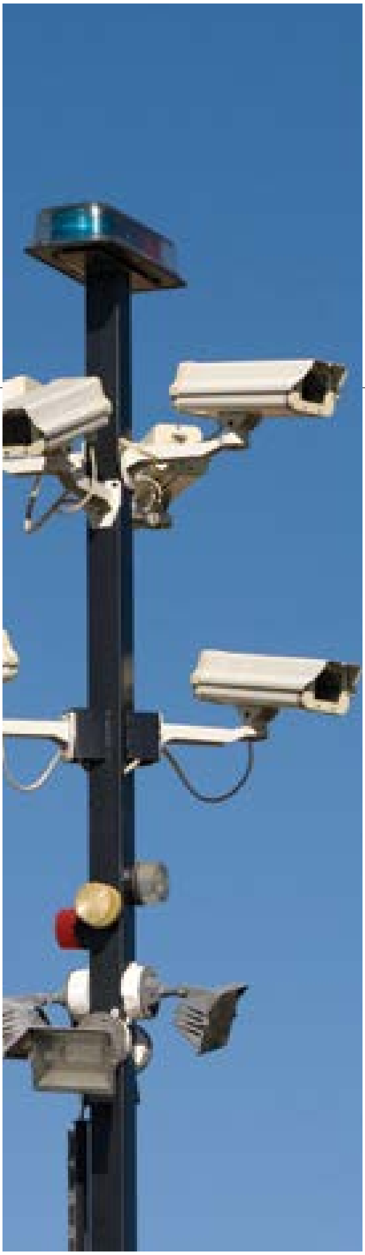
An ongoing dialogue between enterprise security teams, product vendors, and integration partners is necessary to gain more extensive knowledge of how best to mitigate cyber threats.

> CYBERSECURITY RISKS ALSO EXPAND AS TELEWORKING AND ONLINE VIDEO CONFERENCING ADDS VULNERABILITIES THAT CAN BE EXPLOITED.

Stakeholders must continue to communicate to assist each other in identifying vulnerabilities more proactively and addressing them before a breach can occur. ◀

The Unique Benefits of CCTV Towers

Overt security has its advantages



RETAILERS HAVE HAD CAMERAS, BOTH INSIDE AND OUTSIDE THEIR STORES, since the VCR made it economical. Traditionally, the cameras have been hidden in corners, mounted on light poles, or attached to the sides of buildings. But that is changing. Now when visiting retailers, customers might actually notice the cameras because they are not subtly installed on the roof. Instead, they are mounted to an imposing mobile trailer or tower.

CCTV trailers and towers are the newest security trend sweeping across multiple industries, including retail, construction, law enforcement, critical infrastructure, and more. These towers are stationed outdoors and can include wheels and a hitch for easy mobility, as well as solar panels, batteries, flashing lights, and other features. When deployed, they can measure more than 20-feet high, so they are hard to miss. Why are CCTV towers making such an impact? And how are they different from a typical pole-mounted or building-mounted camera?

Mobile security towers provide several benefits over traditional security cameras, and even over guards. First, they can help prevent problems, not just record them. Second, they can increase safety on the property for both employees and customers. Third, they can send autonomous, mobile alerts around the clock. And fourth, they are easy to install since they do not require hardwired

David Studdert (dstuddert@lvt.com) is the Chief Business Development Officer of LiveView Technologies (www.lvt.com).

communication or power lines. Instead, they can be deployed quickly wherever there is a problem.

MOBILE SECURITY TOWERS PROVIDE SEVERAL BENEFITS OVER TRADITIONAL SECURITY CAMERAS, AND EVEN OVER GUARDS.

DETERRENCE-BASED SECURITY

The biggest advantage to CCTV towers is that they help prevent crimes, instead of just recording them as they happen, by employing deterrence-based measures.

These mobile surveillance units are imposing. If they are deployed in a parking lot, they will often take up an entire stall, and they have a massive mast that extends several dozen feet into the air. Furthermore, most have a head unit with multiple cameras. Obviously, each tower will look and function differently depending on which company manufactured it. Some will have strobe and flood lights whereas others will not. Some even have an attached speaker that allows remote personnel to audibly interact with people onsite. Each company adds different features to fit their clients' needs. However, no matter what features the towers may or may not have, they all share one characteristic – they are extremely overt.

And overt security works. Mike Lamb spent his career in retail security. He worked for more than four decades as the head of asset protection and loss prevention for multiple Fortune 500 companies, including The Home Depot, Walmart, and the Kroger Company.

AT A GLANCE: CRIME REDUCTION

One national retail chain deployed CCTV towers to their parking lots and saw a reduction of as much as 70 percent in parking lot incidents. Another retailer had a 62 percent reduction in high-risk crimes and a 69 percent reduction in grab-and-go thefts because of CCTV towers.

"Traditionally, asset protection is playing a game of catch-up," Lamb said. "Countermeasures are only implemented after an incident has happened." But by deploying CCTV towers, Lamb found a way to get ahead of criminals.

Lamb deployed towers to retail parking lots across the country. "The benefit of these towers is that the bad guys see it, get it, and fear it – then leave," he said. "Criminals are always looking for the easy target, the low-hanging fruit, and these towers take that option away from them. … A strategy focused on prevention is much more effective than one focused on reactive measures."

INCREASING SAFETY

The deterrence factor does not just scare away criminals, it also makes customers and employees feel safer. Instead of seeing the units and fearing them, as criminals do, they see them and are comforted knowing that someone is watching, and that criminals are less likely to strike when under surveillance.

Another national retailer with CCTV security trailers said, "Customers intuitively know that this (area next to the unit) is a good place to park. In

fact, a young lady parked underneath it and we asked why. She pointed at the unit and said, 'Because of this. I know nobody is going to mess with my car if I park here and, if they do, you guys will have video of it.'"

CCTV towers are unique in their ability to scare bad actors away from the property and improve the site for customers. One retailer said, "Having something that can monitor the parking lot and keep our employees and customers safe is a win-win."

Furthermore, retailers have found that the steps they take in the parking lot have impacts elsewhere.

"By effectively mitigating crimes occurring in the parking lot, there's a residual benefit to any criminal activity that was occurring inside the store," Lamb said. "If you can prevent the bad guys from entering the parking lot, they will not enter the store. Deterrence-based security enhances your brand

> THE BIGGEST ADVANTAGE TO CCTV TOWERS IS THAT THEY HELP PREVENT CRIMES, INSTEAD OF JUST RECORDING THEM AS THEY HAPPEN, BY EMPLOYING DETERRENCE-BASED MEASURES.

for honest customers because it creates a safer environment and increases positive interactions with your brand.”

“THE BENEFIT OF THESE TOWERS IS THAT THE BAD GUYS SEE IT, GET IT, AND FEAR IT – THEN LEAVE.”

AUTONOMOUS, MOBILE ALERTS

The third difference between traditional security cameras and CCTV towers is autonomous alerts. Traditional cameras rely on guards identifying threats from the feed while onsite in a backroom. This system inherently has some problems. First, guards are human and will never be perfect. They will miss things if they are late or call in sick, if they accidentally fall asleep or are distracted by their phones or a coworker. Even under the best of circumstances, human attentiveness when watching security video wanes quickly.

In addition, having a guard in a backroom is a waste of resources. Retailers have found that human guards are one of the best deterrents for theft and other crimes, even more than CCTV towers. So why pay a guard to monitor the feed when

they can be better utilized elsewhere?

CCTV towers can augment and, in some cases, replace guards because they use artificial intelligence (AI) to trigger alerts. An end user can designate an area they want the camera to watch and specify when to watch it, what to look for, and what the response should be if one is needed.

When an alert is triggered, the user can log in to the feed remotely and see what is happening – whether it is just a vehicle driving through or a crime in progress. It gives the user the chance to intervene with features on the unit (like lights and speakers) or to call security or local law enforcement. Either way, the end user can better direct their efforts because of the CCTV tower. In this instance, a guard is replaced because the tower tells the user when there is an issue, rather than a human middleman relaying the message.

Autonomous alerts can also help augment the abilities of guards on patrol by pointing them to the right place. “Even at their best, guards are only effective at one place, at one time,” Lamb noted. “However, with the tower helping watch, the guards can know when and where to direct their efforts.”

In short, autonomous alerts from CCTV towers help leverage guards and security budgets while

MANAGING ALERT FATIGUE

CCTV tower clients can set an area around the front of a store with an active watch from 9 p.m. to 6 a.m. and can direct that only human and vehicle intrusions into the designated area will trigger an alert. This specificity helps to avoid alert fatigue.

“A STRATEGY FOCUSED ON PREVENTION IS MUCH MORE EFFECTIVE THAN ONE FOCUSED ON REACTIVE MEASURES.

increasing situational awareness. They identify when there is a threat and when human attention is required. They watch 24/7 and they never take a day off.

RAPID DEPLOYMENT

CCTV towers have a huge advantage over traditional surveillance cameras because they are quick to install. In fact, some CCTV trailers can be deployed in as little as 30 minutes. This opens the door to quick responses by asset protection teams instead of having to wait weeks or months for installation.

Most CCTV towers rely on a combination of solar power, batteries and backup generators. Furthermore, while some connect to Wi-Fi, others use cellular connectivity. These features ensure that the towers are completely mobile and require no construction. Cameras mounted on a pole or on the building do not enjoy this advantage.

The mobility of the units allows additional freedom. If a unit is deployed to the front of the store but a problem develops at, say, the fuel center, relocating the tower is easy. Interestingly, retailers who use CCTV trailers will move them around on the property but tend to leave the units on location. They avoid moving them offsite because of parking lot liability.

“Not only do the towers increase safety on the property, but they also help mitigate risk for the retailer,” Lamb said.

CONCLUSION

CCTV cameras are everywhere, especially in retail. Traditional cameras on poles or the side of a building capture video but are a passive form of security. As retail crimes continue to grow, passive security measures will not be enough. While there is no silver bullet solution, retailers are taking every step they can to protect their customers and employees, their assets, and their properties.

Unlike traditional cameras, CCTV towers are very overt and intentionally so. Overt solutions still capture the same video feeds, but criminals see them, understand them, and fear them much more readily. Furthermore, the deterrence-based solution does not scare away customers or employees, but actually helps them feel safer.

While other cameras may use AI analytics, CCTV towers can put the analytics into action, not only through autonomous alerts but also by providing the physical tools the user needs to act on those alerts remotely. Instead of just watching something happen, a client can use the lights and speakers to respond and prevent wrongdoing.

Lastly, the towers are quick to deploy. While other solutions can take weeks or months to get a plan approved, a construction team onsite, and the lines run, CCTV towers do not need hardwired communication or power lines. Instead, they use solar, cellular connectivity, and other mobile technologies to help retailers solve problems quickly.

All of these advantages make CCTV towers the next big thing in enterprise security. ◀

Integrating Technologies, Security and Privacy

Hospital security systems must do more than lock doors and record video

HEALTH CARE FACILITIES ARE FACED WITH A CONSIDERABLE NUMBER OF CHALLENGES. The responsibility to balance security with a welcoming and therapeutic environment demands a unique approach that involves security leaders, the IT department and the C-suite. Paramount to this idea is executing a multilayered strategy that includes creative security solutions, staff safety training, and the capacity to gain comprehensive situational awareness of the facility. It is also essential that the systems that keep a health care facility safe and functional integrate into a comprehensive streamlined infrastructure.

3 MAJOR SECURITY CHALLENGES IN HEALTH CARE

Hospitals around the globe face the challenge of meeting the needs of a wide variety of people,

David Sullivan (kayla@compassintegrated.com) is the President of ACRE Americas (www.acre-co.com).

> PHYSICAL SECURITY SYSTEMS MUST ACCOUNT FOR THE NEED TO PROTECT PATIENT CONFIDENTIALITY AT EVERY TURN.

from protecting patients (and their confidential information) to ensuring the well-being of staff and physicians to providing a safe environment for visitors. The sheer number of people entering and exiting health care facilities makes securing them difficult, and a perceived lack of security can be detrimental and set a negative tone for a patient's visit. Unfortunately, the challenges do not end here.

Protecting Patients and Privacy

Strict privacy laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), are important considerations when deploying and financing security solutions in the health care sector. Health care providers must balance the demand for privacy with ensuring high levels of security. Network safety threats disproportionately affect health care institutions and patient data, so a focus on boosting cybersecurity is vital. Additionally, robust security solutions that

combine access control and video surveillance are critical, as these systems are valuable in streamlining the investigation process.

Compliance with Regulations and Standards

Physical security systems must account for the need to protect patient confidentiality at every turn. Role-based access control that ensures the right people have access to controlled areas, patient files, and data goes a long way toward achieving this. Additionally, having a system that allows security officials to manage access and rules quickly and efficiently through an easy-to-use interface is key to ensuring that proper procedures are followed.

> “ HEALTH CARE PROVIDERS MUST BALANCE THE DEMAND FOR PRIVACY WITH ENSURING HIGH LEVELS OF SECURITY.

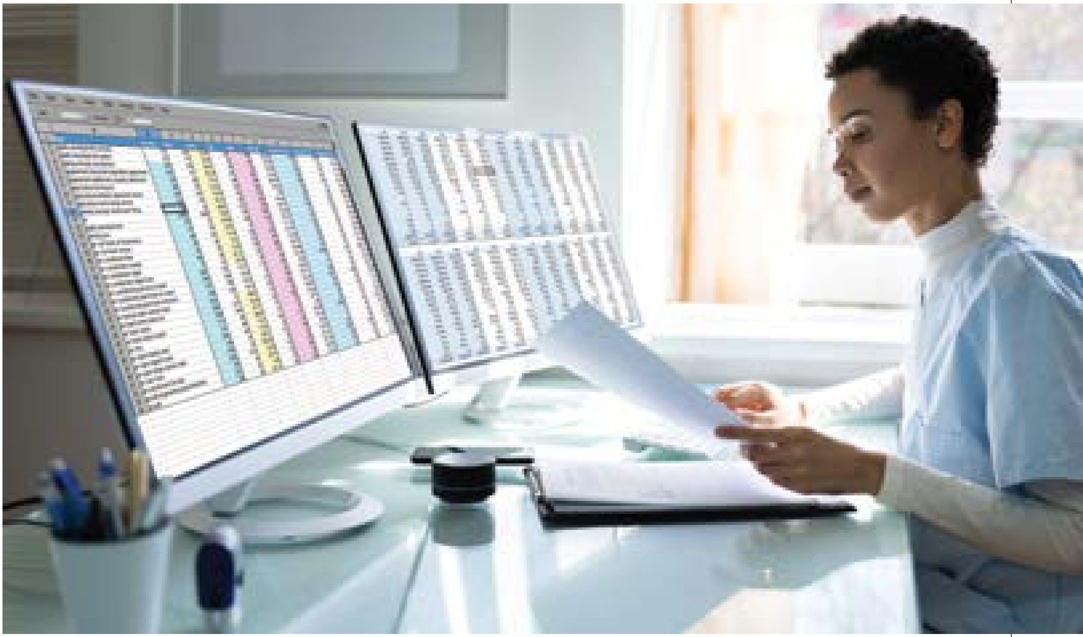
Database Maintenance

Enterprise facilities with multiple sites and sometimes thousands of employees entering and exiting during the day can be cumbersome to manage, especially when dealing with data input and output that grants and restricts access. Human resources and security leaders must work together to ensure that the right people are granted the proper access levels. Otherwise, the health care facility might open itself up to liability.

7 HEALTH CARE SECURITY ESSENTIALS

Various systems and solutions can be implemented to mitigate risk and manage some of the challenges that health care facilities face. Numerous sectors of a hospital have complex needs for role-based access control. For instance, ease of access to managed entrances is critical to medical crash units, and the ability to implement a zonal access control lockdown could be life-saving during an infectious disease outbreak. Susceptible areas such as blood banks and pharmaceutical storage also require controlled access.

Hospitals need a system that will permit them to carry out access rules while dealing with immense volumes of traffic. A conventional key-based system is not designed to keep up with the demands of such a dynamic



atmosphere. This is where cloud-based access control and open API architecture come in. A modern security management system can integrate a facility's digital video, alarm management, and access control technologies into a single, streamlined solution. The benefits to this approach include scalability, flexibility and the ability to serve multiple sites. This flexibility can demonstrate itself in various ways. For example, if a staff member is let go, access can be automatically revoked when an HR manager updates the individual's employment status from "active" to "inactive."

Managing Data

Hospitals can have hundreds, if not thousands, of employees who need varying levels of access based on their positions. Custom, configurable data management systems that integrate with human resources, personnel management and IT can help streamline

> HUMAN RESOURCES AND SECURITY LEADERS MUST WORK TOGETHER TO ENSURE THAT THE RIGHT PEOPLE ARE GRANTED THE PROPER ACCESS LEVELS. OTHERWISE, THE HEALTH CARE FACILITY MIGHT OPEN ITSELF UP TO LIABILITY.

IT IS CRITICAL TO PROTECT CONTROLLED SUBSTANCES, AS WELL AS MEDICAL FILES, WITH ELECTRONIC ACCESS-CONTROLLED CABINET LOCKS TO PROVIDE HOSPITALS AND ADMINISTRATORS WITH AUDIT TRAILS IN CASE OF A BREACH.

and automate business workflows between systems. Not only does this assist security administrators in ensuring that the correct people have the correct access, but it also decreases systems administrators' workloads by eliminating data entry errors that could result in threats to patients, staff and visitors.

The demand for integration will continue to propel innovation in access control, not only for security systems, but also for human resources, software tools, and event management programs. Active facilities and aligned stakeholders demand the capability to grant automatic permissions in order to save time and energy on manual input and make changing authorizations efficient and straightforward.

Mobility

Having a mobile application to grant access, freeze access, or change permissions instantaneously is essential in health care. Security teams need to stay on the move throughout a facility, and mobile applications allow them to control systems remotely.

Lockdown Functionality

An essential feature within today's health care market is lockdown capability. Manufacturers are being driven to provide solutions that make it effortless for security directors to manage access quickly and efficiently in an emergency. The ability to lock down portions of a hospital or even an entire facility is critical to ensuring the continuity of operations.

One area where this is particularly vital is in nursing homes, which need to be able to lock down a facility to prevent patients from leaving while maintaining a welcoming environment. Access control systems can enable caregivers to allow visitors in and out with the press of a button, while keeping the doors tightly managed to prevent patient elopement.

Video Surveillance and Access Control Integration

The integration of access control and video surveillance plays a crucial role in the ability of administrators to make swift, impactful decisions during an emergency.

Choosing an access control system that is flexible and has an open API architecture allows for greater integration. The combination of video and access control expands situational awareness, allowing security personnel to better assess potential threats. For example, access control systems

7 HEALTH CARE SECURITY ESSENTIALS

- Managing Data
- Mobility
- Lockdown Functionality
- Video Surveillance and Access Control Integration
- Restricted Access and Pharmaceutical Protection
- Protecting Patient Privacy
- Multi-Layer Techniques

can generate alerts, such as an invalid badge being scanned or a door being forced open. Coupling such alerts with video allows the operator to make decisions based on what is occurring even before security arrives on scene, thus enabling a quick and decisive response.

Restricted Access and Pharmaceutical Protection

Sensitive materials, such as narcotics, need added security, along with stringent access restrictions based on differing roles. It is critical to protect controlled substances, as well as medical files, with electronic access-controlled cabinet locks to provide administrators with audit trails in case of a breach.

Protecting Patient Privacy

In the United States, HIPAA sets national standards to secure the confidentiality and integrity of protected health information that an entity creates, receives, maintains or transmits. Internationally, similar privacy rules exist, including the European Union's General Data Protection Regulation (GDPR) and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

In some facilities, iris or fingerprint scanners are used to safeguard essential

data from would-be bad actors. This way, only authorized users have access to the information. Furthermore, IT departments are working closely with security leaders to guarantee that networks and access points are as secure as possible to protect against ransomware threats. Video masking, which refers to hiding or anonymizing a portion of a video feed (that is, blurring it), allows health care facilities to record video in sensitive areas while protecting an individual's identity. This lets security officials gather critical video data while also respecting the right to privacy.

Multi-Layer Techniques

Administrators can achieve higher levels of security and interoperability by integrating systems through a centralized platform, like a security management system. Taking different technologies, such as access control, intrusion, video, alarms, infant protection systems, and emergency towers, and integrating them to formulate a single operational system is a highly effective way to protect a facility. Bringing all of these solutions together should be a primary goal when designing security infrastructure. ◀

Putting Video in a ‘Container’

Containerization technology can provide end users with an integrated and future-proof C2 platform

John Rezzonico (jrezzonico@edge360.com) is the CEO of Edge360 (www.edge360.com).

VIDEO MANAGEMENT SYSTEMS (VMS) WILL ALWAYS BE NECESSARY for mission-critical organizations because they are the foundational application that security systems are built upon. Therefore, VMS architecture should promote interoperability, scalability and reliability.

Historically, one of the biggest challenges in video surveillance deployments has been ensuring the ability to scale a system as the need arises. While security as a service (SaaS) and cloud offerings have allowed stakeholders to do this more efficiently, what often get overlooked are the command and control aspects, such as integration with access control and intrusion detection, that cannot be migrated because of proprietary architecture.

And that is only one of the problems. Delivering a command-and-control platform that produces solid video is another. The only way to get the footage required has long been to buy everything from one manufacturer. But this locks the user in and inhibits their ability to prepare for the future.

What is needed is a solution designed to fit a modern enterprise's needs, one that is built on current IT policies and that enables end users to scale on top of a containerized architecture.

WHAT IS CONTAINERIZATION?

As those with IT backgrounds may know, containerization is essentially the virtualization of an application or operating system. The solution enables an end user to deploy resources as needed across the enterprise without making significant configuration changes on the backend.

Containers eliminate much of the friction typically associated with moving applications from testing through to production, but applications packaged as containers can also run anywhere. All the dependencies associated with any application are included within the containerized application. This makes a containerized application highly portable across virtual machines or bare metal servers running in a local data center or on a public cloud.

> "THE CONTAINERIZED APPROACH PROVIDES END USERS WITH THE TECHNOLOGY THEY NEED – NOT THE TECHNOLOGY THEY ARE BEING TALKED INTO BECAUSE IT FITS WITHIN THE STANDARD TECHNOLOGY OR BRAND FOOTPRINT.

> ONE OF THE BIGGEST CHALLENGES IN VIDEO SURVEILLANCE DEPLOYMENTS HAS BEEN ENSURING THE ABILITY TO SCALE A SYSTEM AS THE NEED ARISES.

To break it down for the uninitiated, containerization is like going to a department store and buying a large dining room set that comes in a small flat box. But rather than having to combine numerous parts to complete the assembly, the work has already been done for you. In effect, the furniture in that box is already configured and ready for you to sit down and start eating.

Containerization provides an application-specific container where the environment is controlled. The container is already configured when an application is built, instead of being installed on a traditional server. Everything needed from an application standpoint is in that container, and it is packed up and compressed. To deploy the container, one pushes it forward and expands it. When the container expands, it installs everything it needs – all the application and database dependencies, along with the application needs within the expanded container.

FUTURE-PROOFING THE VIDEO ENVIRONMENT

Command and control solutions depend on emerging technologies. To provide security for a large footprint, end users must anticipate that new technologies will be introduced regularly. Today, many solutions do not allow the use of third-party add-ons or technology.

The containerized approach, though, provides end users with the technology they need – not the technology they are

being talked into because it fits within the standard technology or brand footprint. This means they can access a foundational video product that works seamlessly with other technologies. A global deployment allows users to log on anywhere and have complete access – based on permissions – as well as the ability to manage the solution. It is a way to scale across one single, global cluster.

Deploying a containerized solution also dramatically cuts down on not only hardware resources, but also travel expenditures, by dramatically reducing the engineering required to manage the system remotely during all phases – deployment, production, patching and upgrades.

While security stands to benefit from the development of this technology, it is a significant change of mindset to move away from traditional VMS solutions. But end users should look ahead and consider how their current technology investments will support their efforts down the road. The future is right around the corner, and now is the time to build a solid video foundation. ◀

> “
> CONTAINERIZATION IS ESSENTIALLY THE VIRTUALIZATION OF AN APPLICATION OR OPERATING SYSTEM.

Leveraging AI for People Screening

Millimeter wave technology and deep learning can produce effective and automated virtual searches

Christoph Baur (christoph.baur@rsa.rohde-schwarz.com) is the Director of Software Imaging Products at Rohde & Schwarz (www.rohde-schwarz.com).

DESPITE ADVANCEMENTS IN SECURITY TECHNOLOGIES ACROSS NEARLY EVERY INDUSTRY, options for screening people have largely remained the same for more than a decade.

People screening for loss prevention, data center security, high-value manufacturing, event security and other use cases generally relies upon low-tech and personnel-intensive measures like physical searches, pat-downs and metal detection systems. Some imaging systems that screen people use ionizing radiation or low-resolution terahertz imaging, which present health risks, lack sufficient resolution to detect items of interest, and sacrifice personal privacy. The performance challenges and staffing requirements of these legacy screening technologies have consistently undercut the business case for making investments to procure and operate.

However, the risks and costs of inadequate people screening are higher than ever. New threats and new security challenges require new high-performance tools that meet the expectations and operational needs of a wide range of applications. Combining high-resolution imaging technology with artificial intelligence (AI) and deep learning, emerging solutions are finally available to support high-fidelity people screening in security applications in a manner never before possible.

> AUTOMATED DETECTION ALGORITHMS DEVELOPED USING AI AND DEEP LEARNING METHODOLOGIES MAKE IT POSSIBLE TO DETECT APPLICATION-SPECIFIC ITEMS OF INTEREST.

High-performance people screening systems using millimeter wave imaging technology has historically been used primarily in aviation security operations, where regulators, like the Transportation Security Administration (TSA), have well established detection, operational and functional requirements.

Outside of aviation security, use cases like event screening, asset protection and loss prevention have challenging requirements and urgent needs for tailored high-performance screening solutions. Ultra-high definition millimeter wave imaging systems

are now available that can detect a wide range of threats and materials of interest to meet very specific security screening needs.

Security operations in many use cases and applications naturally present a variety of detection challenges based on the mission and desired security outcome. Whether screening for mass casualty threats like weapons and explosives, detecting high-value items to prevent theft, or finding small data-bearing devices or manufacturing prototypes to protect intellectual property, security decision makers have had limited technology options. With some vendors presenting extraordinary performance claims, it is important to understand the fundamentals of various detection technologies' capabilities, as well as their limits.

Similarly, for security equipment manufacturers, it is essential to consider the varying requirements of these environments to ensure that products can be adapted to address specific security applications.

With collaborative and focused industry segment input, high-resolution millimeter wave imaging technology has proven that it can be adapted to meet specific mission needs and concepts of operation. Moreover, automated detection algorithms developed using AI and deep learning methodologies make it possible to detect application-specific items of interest.

High-performance millimeter wave technology utilizes automated detection

software and algorithms to identify targeted threats, contraband and high-value items. Moreover, it eliminates the need for screeners to review raw images and ensures that the privacy of people being screened is protected. If the algorithms identify an item of interest concealed on a person, the security officer is presented with a representative human image, or an avatar, that identifies the location where the item was detected. The underlying raw image data analyzed by the algorithm is immediately deleted and overwritten as soon as the detection result is determined, typically less than three seconds.

In addition to addressing privacy concerns, automated detection algorithms reduce the burden on security operators and eliminate the time and challenge of relying on humans to perform image analysis and interpretation.

> “
>
> THE RISKS AND COSTS OF INADEQUATE PEOPLE SCREENING ARE HIGHER THAN EVER.

The combination of high-resolution image scanning and powerful automated detection algorithms gives operators new tools to tackle challenging applications like those in asset protection and loss prevention. It enables the ability to not only detect large concealed threats, such as guns and explosive devices, but also very small and thin objects like pharmaceuticals, USB sticks, and SD cards.

IMPROVING SECURITY EFFECTIVENESS AND OPERATIONAL EFFICIENCY

Previously, detection performance was limited to the ability of the human eye to spot anomalies and threats. The emergence of automated detection algorithms addressed some of the challenges screeners faced. However, with the higher detection provided by these algorithms came higher alarm rates, which affected security efficiency. Recent developments in AI and deep learning have enabled more effective targeted algorithms to be developed.

> “ WITH DEEP LEARNING, INTELLIGENCE INCREASES OVER TIME AND CAN CREATE NEW CAPABILITIES AND CONTINUOUS IMPROVEMENTS.

Regardless of the security application, effective detection algorithm software demands a high probability of detection and a low false or nuisance alarm rate. If the false alarm rate is too high, security operators may be required to conduct intrusive pat-downs, reducing the efficiency of the screening process and contributing to lengthy security wait times. New algorithms combined with high-resolution imaging systems support faster and more accurate screening in a variety of use cases.

DEVELOPING FULLY AUTOMATIC DETECTION ALGORITHMS

The development of automated detection algorithms typically relies on defining certain features of images, such as reflection, absorption, and edge effects of various materials when scanned by a millimeter wave imaging system.

Using these features, it is possible to establish parameters and size or detection thresholds for items of interest. For example, to train an algorithm to detect a gun in an image, one might begin by defining a feature or image refinement

that enhances metallic objects, then configure the detection parameters so that, if more than a certain quantity of metal is present in an image, then the system triggers an alarm. If a user has an eight-color system versus 256 colors, the blended resolution is 32 times less, and, thus, the object to be detected must be significantly larger in size.

For gun detection databases to assess an image, one might consider creating a millimeter wave image library of all known firearms and then manually label them to define the detection features of the algorithm. While this seems like a straightforward approach, it can quickly become ineffective as new or unconventional firearms, such as 3D-printed “ghost guns,” are being developed all the time. Considering all the different types and shapes of dangerous objects, maintaining such an image database would present a daunting challenge.

The challenges of people screening in applications like loss prevention and asset protection are just as difficult, as security operators are tasked with detecting targets from secret prototype materials to high-value manufactured parts made of glass or plastics to packages of pharmaceuticals and expensive cosmetics.

Machine learning has been used to develop enhanced and specialized algorithms that do not need massive image libraries. This, along with other techniques, is helping to advance people screening technology.

FROM MACHINE LEARNING TO DEEP LEARNING

Machine learning has been widely used in computer security applications when one is asked to select images containing stoplights or bridges before gaining access to a system. Newer deep learning techniques are opening up many more possibilities.

Deep learning relies on a system of deep neural networks. Every node in the network is essentially a mathematical model of a neuron, similar to what is found in the human brain or central nervous system. Much like the development of the human brain, with deep learning, intelligence increases over time and can create new capabilities and continuous improvements.

To better understand the concept of an active deep learning system, one can think of a voice-controlled smart speaker in a house and the speech recognition software that learns the different voices giving it commands. Initially, the system might struggle to understand the various people that live in the home as it learns different pronunciations and accents. Over time, though, as the system continues to receive data – that is, the commands from various voices – its deep learning capabilities allow it to improve the computations in its nodes – even to the point that it can identify the voices of specific individuals. So, the next time you are at the store, your digital assistant can let you know who keeps adding chocolate bars to the shopping list.

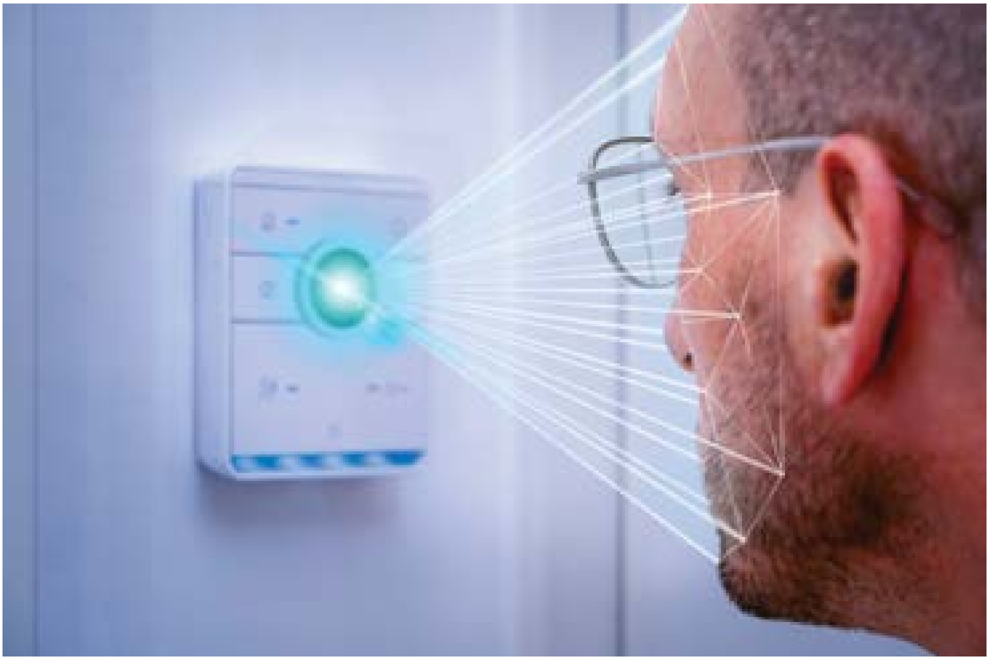
These deep learning techniques can be developed with hundreds of layers and millions of parameters. To accomplish computations of these magnitudes just a few years ago required extremely powerful and expensive computer systems and hours of computation time. Today, these complex tasks can be performed much faster and more economically.

CONCLUSION

Combining deep learning techniques with imaging capabilities, coupled with databases of images of items of interest, means that rapid development of bespoke detection algorithms can be realized for very specific use cases and detection challenges. These range from screening people in various clothing types to enabling screening to be conducted in an environment where people are wearing face masks. Specific and optimized detection algorithms can be developed for narcotics and other contraband in border control applications or to enable the detection of data-bearing devices in data centers.

Choosing the right technology for people screening involves developing a detailed problem statement and defining the desired security outcome. Then security professionals can add effective people screening to their operations and leverage high-performance technology to address specific security challenges. ◀

> “ REGARDLESS OF THE SECURITY APPLICATION, EFFECTIVE DETECTION ALGORITHM SOFTWARE DEMANDS A HIGH PROBABILITY OF DETECTION AND A LOW FALSE OR NUISANCE ALARM RATE.



Using Technology to Bring Employees Back Safely

Touchless access control and other solutions enhance security *and* health

Tina D'Agostin (tina@alcatraz.ai) is the CEO of Alcatraz AI (www.alcatraz.ai).

WILL WE EVER RETURN TO THE OFFICE FOR GOOD? The rise of the Omicron variant and the pandemic's rapid resurgence has forced companies to postpone office return dates. However, many companies will soon welcome people back, and they will need to address people's safety concerns in the process.

A Gartner survey of global HR leaders found that more than three-quarters are hesitant to come back to the office because of health and safety concerns. That is why organizations must adapt to new workspace requirements, ensuring compliance with Covid-19 guidelines and leveraging technology to ensure safety. Access control applications, including touchless authentication, mobile credentials, and distancing analytics, can help businesses create a secure and healthy working environment for all employees.

Simply put, companies can leverage digital tools and novel technologies to create a safe back-to-work strategy as employees return to the workplace in 2022. Here's how.

TOUCHLESS TECHNOLOGY FOR HYGIENIC ACCESS CONTROL

Key card access controls are ubiquitous in workplaces, securing facilities and employees with little friction or complication. However, the pandemic presents an opportunity to enhance these technologies by adopting touchless authentication to further reduce both friction and the risk of virus transmission.

High-touch contact points across the workspace, from employee workstations to conference rooms, can benefit from touchless authentication,

> A GARTNER SURVEY OF GLOBAL HR LEADERS FOUND THAT MORE THAN THREE-QUARTERS ARE HESITANT TO COME BACK TO THE OFFICE BECAUSE OF HEALTH AND SAFETY CONCERNS.

RELYING ON MULTI-SENSOR TECHNOLOGY, TOUCHLESS AUTHENTICATION SOLUTIONS CAN VERIFY ACCESS CREDENTIALS IN REAL TIME WITHOUT THE USER ENTERING A CODE, SWIPING A CARD OR TOUCHING A SENSOR.

which decreases cross-contamination by reducing contact with humans and objects. When coupled with enhanced cleaning regimens at these touchpoints, companies can best adhere to Centers for Disease Control and Prevention (CDC) guidelines and shifting employee expectations.

Relying on multi-sensor technology, touchless authentication solutions can verify access credentials in real time without the user entering a code, swiping a card or touching a sensor. In addition, these technologies can easily check employees' temperatures, denying entry to anyone showing a potential fever. Similarly, they can help companies detect if people are not wearing face masks where required.

For these reasons, developing touchless openings is a more hygienic and viable access control solution for many workplaces.

FACE CREDENTIALS COMBINE SAFETY AND PRODUCTIVITY

Contactless face credentials provide employees with quick and smooth access to the workplace while preventing fraudulent entries. Face authentication control systems will automatically allow access to the authorized person while notifying security of any unauthorized entry attempts. This eliminates the risk of a stolen or lost

ID being used to access a workspace, or multiple people accessing it with the same card.

What's more, companies can instantly issue secure face credentials to staff members, and these credentials can also be used to activate printers or create a frictionless environment at office cafeterias and vending facilities.

At the same time, touchless face authentication can be integrated into time management systems to improve workspace efficiency. This way, when employees and temporary staff (e.g., cleaners and contractors) pass through a biometric security checkpoint, the timesheet will automatically mark their attendance.

DISTANCING ANALYTICS HELP MAINTAIN COMPLIANCE

Physical distancing can help slow and prevent the spread of coronavirus. Several technologies can encourage and enforce physical distancing, including:

- Video surveillance
- Occupancy management analytics

- Remote and/or scheduled locking and unlocking of spaces

When deployed effectively, these technologies encourage social distancing throughout an organization, helping companies maintain health and safety protocols and compliance measures and creating hygienic working conditions for all employees.

> SECURITY CAMERAS EQUIPPED WITH SOCIAL DISTANCING FEATURES CAN HELP ENSURE OCCUPANCY MANAGEMENT, SOCIAL DISTANCING, AND FACE COVERING COMPLIANCE.

For example, security cameras equipped with social distancing features can help ensure occupancy management, social distancing, and face covering compliance. With these tools, businesses can track the number of people entering and exiting a space, automatically restricting access when a predefined occupancy limit is reached.

EMPLOYEE SAFETY IS THE FIRST PRIORITY

The Omicron variant may have slowed the return to work, but offices will not be empty forever. As companies consider when and how to bring employees back to the office, safety must continue to be the top priority. Protocols alone cannot keep people safe from Covid-19, but the right tools can help employers address employee concerns before offices are reopened.

Modern technologies, such as touchless authentication, mobile credentials, and distancing analytics, can help organizations provide a safe working environment, allowing their people to thrive in the office once again. ◀

Verified. Bench Tested. Proven. Compliant. Trusted.

VERIFIED OSDP™ VERIFIED

When you need interoperable, high-security access control solutions, ask for products that bear the OSDP Verified mark.

OSDP Verified means these products have been tested by the Security Industry Association as conforming to one or more profiles of the OSDP standard. For you, that means peace of mind knowing these solutions can communicate securely and seamlessly.

To learn more about OSDP and find a guide to OSDP Verified products,

visit securityindustry.org/OSDP

Security Industry Association
securityindustry.org

SIA

28