1105 MEDIA

www.securitytoday.com

SECURITY today

Technology | Education | Solutions

September/October 2021 | Vol. 25 No. 6

MOVING THE NEEDLE

Video security and storage play a significant role in the security space

MAKE
POWERFUL
CONNECTIONS

SECURITY today
Education | Technology | Solutions

Contents SEPT/OCT 2021

cover story

features

departments

Online Communities

Follow us on Twitter:
www.twitter.com/SecurToday

Become a fan on Facebook:
www.facebook.com/SecurToday

Link to Us:
http://linkedin.com/company/security-today

GO BEYOND SECURITY WITH SALIENT'S OPEN VIDEO DATA PLATFORM

Video is protecting your business today

But there is so much more you can get from your VMS

Imagine how you can fuel the rest of your business with video intelligence

Salient's platform empowers organizations to view, record, and manage video data. Built with an open architecture, CompleteView VMS is integrated with thousands of cameras, access control, and analytics solutions. Find out how Salient's platform can drive your business operations with actionable video intelligence.

SALIENT™

www.salientsys.com

With Ralph C. Jensen, Editor-in-Chief

Take Nothing for Granted

Contemplating a topic in the industry I have not given space in the last 20 years, I seem to be in a daze. Then I received an email about Women in Security. I dialed up a couple of friends to get their take on what is a relatively new organization.

What once was rare in terms of female editorial contributions are now frequent. I have noticed that Women in Security are among the most brilliant and brightest minds in the industry. Women are equally passionate about today's solutions and growing technology trends. I am pleased that this month we are publishing several stories contributed from women.

I reached out to a couple of friends and asked for an opinion on this topic. I think you will agree, and I know you will enjoy the contributed stories in *Security Today* and our *Campus Security & Life Safety* magazines.

"The high-tech industry includes many intelligent and driven female leaders, and more are entering the market today than ever before. A variety of leadership development, technology education, networking, and mentoring opportunities is critical to realizing the ongoing success of women in the high-tech space but especially in security," said Rhianna Daniels Hile, chief creative officer at Compass Integrated. "SIA's Women in Security group helps women make deeper connections, build new skill sets and engage in leadership experiences. It has been rewarding to see this group grow exponentially over the years, and I think it has been a valuable addition to the industry.

Women in Security captures the very essence of progress.

Looking back at my first tradeshow, maybe 21 years ago, there were few if any women attending a male dominated industry. Looking forward, the diversity within the industry is a welcome sight.

Part of the SIA Women in Security mission includes a security forum. The Women in Security Forum is a group for both women and men that offers programs, professional development opportunities and networking events with the goal of supporting the involvement of women in the security community

The mission of the forum is to engage all security professionals to promote, recruit and cultivate the leadership of women for a more inclusive and diversified industry. Another terrific part of this organization is the annual scholarship program. Six recipients received honors this year to further educational opportunities and promote advancement within the industry.

ID STATEMENT
Security Today (ISSN 2572-5246) is published 7 times a year, Jan/Feb, March, April, May/June, July/August, Sept/Oct and Nov/Dec by 1105 Media, Inc., 6300 Canoga Avenue, Suite 1150, Woodland Hills, CA 91367. Periodicals postage paid at Woodland HIls, CA 91367, and at additional mailing offices. Complimentary subscriptions are sent to qualifying subscribers. Annual subscription rates payable in U.S. funds for non-qualified subscribers are: U.S. $119.00, International $189.00. **Subscription inquiries, back issue requests, and address changes:** Mail to: *Security Today,* P.O. Box 2166, Skokie, IL 60076-7866, email SECmag@1105service.com or call 847-513-6011 or 888-768-8759 for U.S. & Canada; 00-1-847-513-6011 for International, fax 847-763-9564. **POSTMASTER:** Send address changes to *Security Today,* P.O. Box 2166, Skokie, IL 60076-7866. Canada Publications Mail Agreement No: 40612608. Return Undeliverable Canadian Addresses to Circulation Dept. or XPO Returns: P.O. Box 201, Richmond Hill, ON L4B 4R5, Canada.

LEGAL DISCLAIMER
The information in this magazine has not undergone any formal testing by 1105 Media, Inc. and is distributed without any warranty expressed or implied. Implementation or use of any information contained herein is the reader's sole responsibility. While the information has been reviewed for accuracy, there is no guarantee that the same or similar results may be achieved in all environments. Technical inaccuracies may result from printing errors and/or new developments in the industry.

CORPORATE ADDRESS
Corporate Headquarters:
1105 Media
6300 Canoga Avenue, Suite 1150, Woodland Hills, CA 91367
www.1105media.com

MEDIA KITS
Media Kits: Direct your Media Kit requests to Lynda Brown, 972-687-6781 (phone), 972-687-6769 (fax), lbrown@1105media.com

REPRINTS
Reprints: For single article reprints (in minimum quantities of 250-500), e-prints, plaques and posters contact:
PARS International
Phone: 212-221-9595
E-mail: 1105reprints@parsintl.com
www.1105Reprints.com

LIST RENTAL
This publication's subscriber list, as well as other lists from 1105 Media, Inc., is available for rental. For more information, please contact our list manager, Marie Briganti, Merit Direct. Phone (914) 368-1023; Email: MBriganti@MeritDirect.com; Web: https://go.meritb2b.com/1105

SECURITY today
Products | Technology | Solutions
www.securitytoday.com
Volume 25, No. 6

EDITORIAL STAFF

Editor-in-Chief	Ralph C. Jensen
Senior Editor	Matt Jones
E-news Editor	Brent Dirks

ART STAFF

Senior Art Director	Laurie Layman

PRODUCTION STAFF

Production Coordinator	Teresa Antonio

EDITORIAL ADVISORY BOARD
Pierre Bourgeix, Chief Technology Officer, Founder
ESI Convergent, LLC
William Crews, President/CEO,
Security & Resilience Consulting, LLC, Houston
Rob Hile, General Manager,
Florida GC&E Systems Group, Tampa
Jeff Karpovich, CPP, CHPA, CSSP, Chief/Director, Security & Transportation, High Point University, High Point, NC
Chris Lanier, LRG Inc., Jasper, Texas

SALES

Brian Rendine	972-687-6761
Sam Baird	+44 1883 715 697
Peter Kao	+886-2-2949-6412

INFRASTRUCTURE SOLUTIONS GROUP

President & Group Publisher	Kevin O'Grady
Associate Publisher, Security	Ralph C. Jensen
Group Circulation Director	Irene Fincher
Group Marketing Director	Susan May
Group Website Manager	Scott Newhouse
Group Webinar Administrator	Tammy Renne

1105MEDIA INC
YOUR GROWTH. OUR BUSINESS.

Chief Executive Officer	Rajeev Kapur
Chief Financial Officer	Sanjay Tanwani
Chief Technology Officer	Erik A. Lindgren
Executive Vice President	Michael J. Valenti

REACHING THE STAFF
Staff may be reached via e-mail, telephone, fax or mail. A list of editors and contact information also is available online at *www.securitytoday.com.*
E-mail: To e-mail any member of the staff, please use the following form: FirstinitialLastname@1105media.com
Dallas Office (weekdays, 8:30 a.m. – 5:30 p.m. CT)
Telephone (972) 687-6700; Fax (972) 687-6799
14901 Quorum Dr., Suite 425, Dallas, TX 75254
Corporate Office (weekdays, 8:30 a.m. – 5:30 p.m. PT)
Telephone (818) 814-5200; Fax (818) 734-1522
6300 Canoga Avenue, Suite 1150, Woodland Hills, CA 91367

Overcoming Big Challenges

A new generation of handheld tools can help security installers overcome key industry challenges and benefit from significant time and cost savings

By Tim Widdershoven

Despite the fact that the security market is changing, many businesses are configuring, installing and troubleshooting IP security cameras using laptops, even though it's time consuming and ineffective. Many are simply unaware of the productivity benefits possible by tackling their most common challenges on the job with a new approach to test equipment.

EMERGING TECHNOLOGIES

Arguably, the biggest trend affecting the security industry in recent years has been the switch to digital IP cameras from analog technologies. Installers are faced with having to fit unfamiliar, fast evolving equipment and obtain new knowledge to keep up with customer demand. With numerous types of CCTV cameras, plus many different configurations and connection methods, installation and troubleshooting can be time intensive and complicated.

The handheld SecuriTEST™ IP CCTV tester supports installers through this transition, with features to help save time and boost productivity such as QuickIP, which enables novice technicians to connect and configure IP cameras quickly and easily. Even on complex installations, users may only need to use one tester, helping remove the need for in-depth and time-consuming training.

Where security installations are using PoE, technicians also need to be able to verify that the camera has enough power to function. The compact PoE Pro tester from TREND Networks eliminates guesswork when installing, maintaining, and troubleshooting networks where PoE is deployed. Installers can easily verify Pass/Fail, even without a full understanding of the various industry testing standards, device power outputs, and cable lengths that are required for a device to operate successfully.

NETWORK INTEGRATION

Analog CCTV was installed with its own infrastructure, a series of hardware and cables for controlling the cameras. However, IP security cameras are usually installed to an existing network, already in place supporting computers, phones or IoT devices. Installers now need to understand the completely new area of how network integration works in order to conduct installation correctly or troubleshoot issues.

First, it is important to verify that the network has the bandwidth to support the cameras and prevent poor image quality. The SignalTEK 10G tester can be used to determine maximum bandwidth up to 10 Gb/s and identify areas with bottlenecks. Post installation, it can also be used to troubleshoot Ethernet connectivity issues faster using diagnostic tools such as the 72-hour event log which helps diagnose intermittent connectivity issues faster.

During commissioning and maintenance, SecuriTEST IP can also be used for a range of network troubleshooting and advanced testing requirements, including cable tracing, length, wiremap, and quality testing, removing the need for installers to carry multiple instruments.

An increasingly use for a wider range of purposes, cameras are not just for observing crime, such as number plate recognition, access control, and fire monitoring. Camera installations are used to aid compliance with Covid policies, observing that social distancing is being adhered to, for instance.

For outdoor cameras, installation can be especially complex where installers do not have the correct tools to test a fixed camera. Time spent travelling up and down a ladder to check the angle on a laptop. In the case of a new network installation or where building construction is in progress, set up can only be completed at a later date, returning to site when the IT infrastructure and computer room are in place and performance can be checked.

With a handheld IP tester, the entire installation can be completed, tested, and documented, removing the time-consuming need to return to site later. It is small, lightweight and does not require external power adapters and injectors, has 10-hour battery life and is operable with one hand, supporting productivity even for installers working on lifts and ladders.

CHALLENGE: RESIDENTIAL SECURITY BOOM

As demand for home security cameras and devices such as video doorbells has increased, the cost has become ever more affordable, even for those looking for more advanced solutions. The global smart home security camera market size was valued at USD 3.71 billion in 2019 and is expected to grow at a compound annual growth rate (CAGR) of 15.7% to 2027*.

However, residential customers do not necessarily have the same understanding of how these systems work as a commercial user, making it even more important to be able to clearly document the installation has been done correctly to prove performance and prevent unpaid callbacks.

SecuriTEST IP features advanced reporting to enable installers to document performance on site in detail, rather than filling in excel documents to create reports. When an issue arises, the proof of performance reports can demonstrate both camera images and network configuration, making return visits to site billable, especially in the case that the customer has changed the network parameters.

With SecuriTEST IP, users can depend on a simple, handheld tool that can replace an Ethernet cable tester, laptop, PoE injector, PoE tester, and reporting tool. Plus, it connects first time without the need to change complex settings and deliver reliable test results. Supported by a suite of other complementary test solutions, security installers can save huge amounts of time on every job and keep their customers happy.

__Tim Widdershoven__ is the marketing director for TREND Networks.

Camera 22 07:24:43 PM 01.29.2013

DomeWizard™

3 Cleaning Modes

Reminder

Clean Security Camera

Okay

Worldwide Shipping

Made in USA

dotworkz.com

(866) 575-4689

dotworkz systems

Fortified outdoor camera housings and accessories

Smarter and Stronger

Enhanced visitor management for a post-COVID world

By Martha Howlett

In the past year and a half, the Coronavirus pandemic has proven to be a continuing challenge for the security industry as well as the workplace in general. Many organizations have had to rethink their approach to creating a secure environment for staff, employees, and visitors. These new considerations have a simple goal: protect, manage, and monitor all staff entering and exiting the facility. The need for contactless interactions between visitor and facility have brought about some exciting and innovative solutions to emerging problems in visitor management.

The slowing, but still present, problem of Coronavirus has ensured that this kind of protection is no longer optional, but mandatory in keeping businesses alive and thriving. However, as the world returns to normal, it is clear that certain adaptations are here to stay.

INSPECTING CREDENTIALS

The world has moved on from visual/physical inspection of visitors and guests' credentials. Increasingly, it is rare to ask to provide physical identification by a receptionist. Not only does this pose issues of human error, but it also poses health risks and concerns for both parties and the entire building. Since the pandemic began, the world has had to adapt to contact-free methods of everything from grocery shopping to using a public restroom.

In the case of manual sign-in points, the public are now naturally wary of handling a common use pen to sign a paper visitor log, even with sanitization. Likewise, handing identification over to a person who has also handled hundreds of other visitors' credentials is no longer a safe or acceptable option.

Visitor management systems must now incorporate a cohesive and contactless visitor experience, prioritizing safety and health. In multi-tenant office buildings, for example, employing one receptionist to occupy a front desk for multiple companies in a building is expensive and can force building owners to allow free ingress into the building, which is an obvious security and health threat.

This problem could be solved by the effective implementation of a visitor management system, which would automatically read a visitors credential, such as a driver's license, confirm the information on a pre-authorization list, notify the host company/person, and print a temporary ID badge. Particularly in post-pandemic society, the use of QR codes has become commonplace for visitor check-ins. QR codes offer pre-registration and self-certification surveys to further speed up the signing in process, ensuring minimal congestion in reception areas and therefore minimizing the risk of transmission via lack of social distancing.

Integrating these systems with access control would make it impossible for a visitor to progress through the building without interacting with the sign-in system. Necessitating the need for a unique ID badge or other credential adds another layer of security while also ensuring minimal contact with doors/handles/buttons etc.

Visitor management systems also offer a reliable and clean data storage solution to visitor records. Paper logs can be lost, stolen, or damaged very easily, posing a significant risk to security. They can be easily bypassed or forgotten, meaning that potentially dangerous people could access the facility; this is especially of concern in laboratories and factories where expensive equipment is stored and sensitive data might be stolen.

Digital visitor management not only prevents expensive and dangerous accidents, theft and loss, but also allows for accurate track and trace information to be collated. Therefore, in the event of an outbreak in the building, all visitors and staff can be cross-referenced and easily contacted before the outbreak gets a chance to spread throughout the building.

These systems allow one-way routes to be put in place and used. Visitors can pose a threat to employees, both in terms of safety and in terms of health. With a visitor management system, a visitor can be given an access card that only allows them ingress and egress through certain doors and even in certain directions, ensuring that any one-way systems that are in place to protect employees are adhered to.

For example, a system integrated with thermal scanning could require temperature reading from all visitors. If the temperature is above a safe level, denied access for a set amount of time and a text message or email sent to a person of responsibility. Alternatively, that person would go through a 'COVID Route', whereby, if it were still necessary for them to enter, they would be directed through the building via a route that ensured no one else came into personal contact with that individual.

It is clear that previous solutions to visitor management are not only outdated in an ever-more digital world, but also present health risks to all, not to mention potential revenue problems. An outbreak in a facility can shut it down entirely for up to two weeks, which is of course a monetary concern for businesses. Previously, it was common for a receptionist to provide visitors with multiple pre-programmed proximity cards to hand out to visitors at will.

This presents potentially catastrophic security risks, as these cards can be stolen or misused. Further, as there is typically no record of who has a specific card, if a visitor neglects to return their card, they then have complete access to the facility without the company knowing who they are. With comprehensive digital visitor management, there is no risk of illegible writing on visitor logs, missing information, lost files, or time consuming sign-in processes. Instead, an adopted streamlined, safe approach that is both COVID-compliant, highly secure and creates a positive first impression on all those entering a facility.

__Martha Howlett__ is a content writer for Keri Systems Ltd.

CV-603 Series

CM-75 Series

CM-222 Series

YOUR ONE STOP SOURCE FOR EVERYTHING TOUCHLESS!

Camden offers a family of 'NO-TOUCH' solutions for your automatic door or access control application.

SureWave™ 'Smart' Touchless Switches

LazerpointRF™ TXLF Fobs with Relay Receiver

'Request to Exit' Detectors

Bluetooth Card Reader

CV-WR Series Fob with Wiegand Receiver

TouchlessWave.com™

Access our library of trade press articles and white papers on building and low-voltage system design in a post-Covid touchless world.

www.touchlesswave.com

CAMDEN DOOR CONTROLS

Opening New Doors to Innovation, Quality & Support!

Call: **1.877.226.3369 / 905.366.3377** Visit: **camdencontrols.com**

The Next Normal

Ways to evolve to better meet the needs of your customers after the 'great reset'

By Scott Harkins

After the COVID-19 pandemic and safer-at-home restrictions of 2020, many homeowners and businesses are well on their way to returning to their 'next' normal. Some have been eager to put the past behind them, and others are taking note of how 2020 helped evolve and shape their lifestyles for the better.

Homeowners are interested in investing more in their surroundings. In fact, a study by Harvard University projected a healthy pace of mid-single digit gains in annual home renovation and repair spending this year, with 4.8 percent growth by the first quarter of 2022.

Businesses are bringing back employees and equipment to meet pace with new demand, while others have adopted hybrid working schedules and an enhanced "phygital" (physical + digital) shopping experiences.

What remains at the core is our role as life safety and security stewards, and that job is more important than ever as families manage hybrid schedules and businesses continue to evolve their offerings. The resulting sense of comfort and confidence, not only through the life safety technologies we produce and supply but especially in the customer experience and interaction we offer.

That latter part – an enhanced customer experience – is a key element that all industries need to really examine, and convey to their customers, as we enter into the next normal.

CAPTURING INTEREST IN THE NEXT NORMAL

Smart home manufacturers are all measuring and monitoring the shifts made to daily life, lifestyles and household patterns that occurred as a result of safer-at-home lifestyles, and will continue to adjust based on those trends to meet customer needs. Because, in fact, those highly intending to make changes to a home express a higher inclination of buying smart home devices in the future, with 69% planning to buy at least one smart home device, compared to 40% on average, as reported by recent data from Parks Associates.

You have heard the phrase, 'A rising tide lifts all boats.' Well, that is exactly what's happening as intent increases for entry-level, self-installed awareness systems… it's also elevating the interest for professionally installed solutions.

To capture that interest, any marketer will tell you that you need to focus on the four Ps (Product/Service, Place, Price and Promotion) to be included in the consideration set and shopping experience. That online shopping experience – in the "phygital" era – is paramount.

As customers become aware of their need for the product/service, they will shop around and educate themselves on the market. The local, trusted dealer that has served its community (place) for 20+ years has an established reputation of a successful track record. Does the promotion of your service align to how customers purchase products today? Does your marketing put you into their consideration set? Is your pricing transparent? Is the shopper able to navigate your website easily and comparison shop? Do they understand the next steps in the purchase process?

As lifestyles meld into the next normal, industries are looking for strategies to remain competitive and relevant, and those companies that are evolving to capture interest and elevate the customer shopping experience can better out-pace the competition.

OFFERING CONVENIENCE WITHOUT COMPROMISE

According to industry research, the current popularity of smart doorbells helps raise the adoption prospects for a host of smart security devices, and the video doorbell forecast is expected to continue to grow. Yet, I have always said: "Don't rely on a video doorbell to save you during a life safety situation."

If the pandemic taught us anything, it is that we need to have good tools when dealing with a crisis. During a home fire or burglary, a simple awareness solution – without professional monitoring – is just not going to cut it.

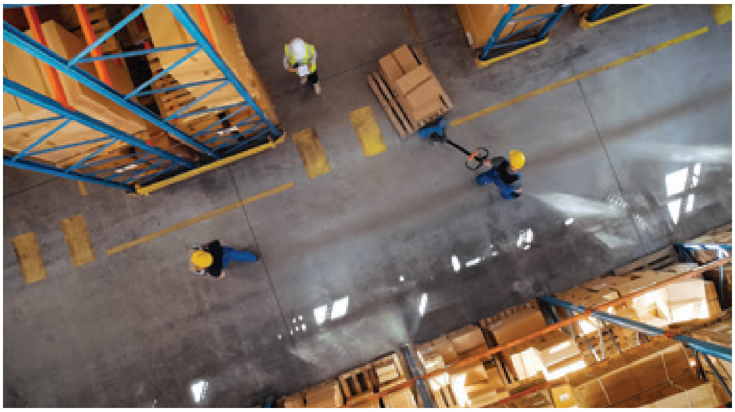
The professional security industry has historically been known to customers as a "Do it For Me" service. Yet, during the last 18 months, some dealers have started to use "Do It With Me" (DIWM) installations as a great middle ground. Many large dealers that performed DIWM installations during the pandemic have since returned to face-to-face installation and interaction to offer an experience beyond its intrinsic value.

"Do It With Me" represents a potentially perfect middle ground for companies that have already adapted some of their operations and installation processes during the pandemic. The DIWM approach combines the convenience of a DIY approach with assistance from a professional, and it can be an alternative solution, such as adding a sensor to a previously installed system, replacing parts or radio or a less intricate solution installed easily on demand with the help of a video tutorial.

It can minimize time on site or even a truck roll, and it offers the homeowner convenience, while mitigating the pain points that are commonly associated with DIY-installed solutions. In fact, we often hear that homeowners will abandon a DIY project after frustration with the technical complexity, integration issues with existing systems, and lack of customer service.

Regardless of the installation method, a fundamental aspect of security is helping people to keep their homes safe, secure and smart; and demand for those services is on the rise. According to Parks Associates, forty percent of security system owners are planning to upgrade their system, and more than 40% report these plans relate to COVID-19. The past year and half presented more than enough worries, but the customer's shopping and installation experience does not have to be one of them.

***Scott Harkins** is the vice president of sales and channel marketing, Americas, at Resideo.*



A Secure Home Run

Covering all the bases with the deployment of state-of-the-art integrated security solution

By Monique Merhige-Machado

There is no doubt, that New York City has an incredible history in major league baseball. New York can brag about the careers of Babe Ruth, Lou Gehrig, Joe DiMaggio, Jackie Robinson, Willie Mays, and more recently Mike Piazza and Derek Jeter. The latest piece of baseball history in New York City is the first MLB retail store.

The MLB NYC flagship store opened in midtown Manhattan in October 2020, and is the first permanent MLB retail store in the United States. MLB NYC collaborated with Legends, a premium experiences company with global expertise across merchandising, sales, partnerships, planning, technology, and hospitality. Legends decided to set the bar high in terms of square feet, breadth of merchandise, and premium experiences, which created a true baseball heaven for dedicated fans of any Major League baseball team, while also providing the ultimate fan experience.

The state-of-the-art retail destination features the widest in-store assortment of MLB products anywhere in the world, spanning two floors and approximately 10,000 square feet, and houses 100 different apparel styles. This one-stop shop for baseball gear is the widest in-store assortment of all 30 MLB club products anywhere in the world. Whether a fan wants a cap from the Miami Marlins or the Baltimore Orioles, they will find it amongst the 10,000 caps offered in-store.

If they wish to purchase a more personalized piece with their name on it, an embroidery station is available as well as a sock customization station. The wide range of memorabilia found in the store includes game-used hats, gloves, baseballs, and jerseys to signed baseballs, photographs, and even game-used & autographed cleats. Aside from wearable and frameable swag, the store also has a home and office section where fans can purchase customized team gift bags and even team logo guitars.

Not only is there a game-used section, but there is also a special line of game-used items from historic events including past World Series, All-Star games and Home Run Derbies. These top-notch products come from licensed partnerships with brands like Nike, New Era Cap, ’47, Topps, and more that carry merchandise of all 30 MLB teams.

A state-of-the-art high-profile retail store like MLB NYC required an enterprise level state-of-the-art integrated security solution to help protect its valuable collections. After being recommended by Legend’s consultant on this project, SAS Technologies Corp., a Certified Minority Women Owned (M/WBE) leading Long Island-based security integrator was brought on board to implement a security solution that will protect not only the merchandise and memorabilia onsite. The store will also host player appearances, special events, product unveilings and much more as a way for fans to celebrate all things Major League Baseball.

With more than 15 years of experience

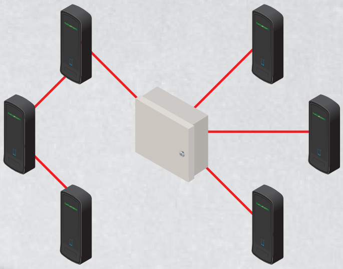
10 THINGS ACCESS CONTROL CUSTOMERS MUST KNOW ABOUT OSDP

1 OSDP is a real global standard approved by the Security Industry Association (SIA) and International Electrotechnical Commission (IEC), open to use by any manufacturer.

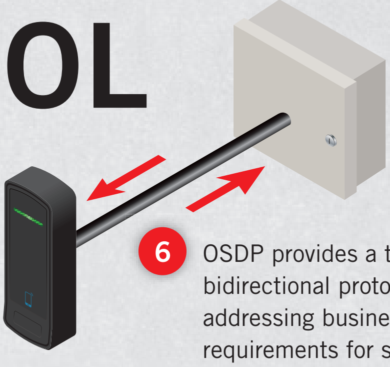
2 OSDP provides a guideline for interoperability among various companies' access control and security products, such as card readers and door controllers.

3 OSDP offers the option of encrypted communications between reader and door controller, independent of any encryption between credential and reader.

4 OSDP is built on the RS-485 serial transmission standard, needing just four conductors.



5 OSDP offers point-to-point and multi-drop topologies.



6 OSDP provides a true bidirectional protocol, addressing business requirements for secured and confidential authenticated messaging.

7 OSDP is more cyber secure than the most common access control communications protocol.

8 OSDP provides secure communications by specifying FIPS-197 encryption (AES).

9 SIA provides a guide to find and explore verified OSDP products that meet its standards.

10 Farpointe Data is honored to be among the first three manufacturers to have earned the SIA's new OSDP Verified mark on its mobile, contactless smartcard and proximity solutions. Plus, these readers are fully potted and IP67-rated!

Farpointe Data®
Readers • Credentials

The OEM's global partner for premium RFID solutions

For a complete, in-depth OSDP white paper, visit www.farpointedata.com/osdp

> "With a huge focus on loss prevention technology, the goal was to protect the store from petty theft plus keep patrons and employees safe."

helping clients in various vertical markets with its security needs, SAS Technologies was ready for this challenge even as the project was just starting to roll out during the COVID-19 pandemic. A big challenge for the new retail establishment was preventing theft as the store attracts traffic from all baseball fans, not just a specific team.

With normal foot traffic being heavier in the midtown area, MLB was preparing for when the COVID-19 pandemic would eventually slow down and was ready to invest in the right security solution to handle the influx of people that would be visiting the store daily. With a huge focus on loss prevention technology, the goal was to protect the store from petty theft plus keep patrons and employees safe.

AROUND THE HORN WHEN IT COMES TO SECURITY

Legends wanted to cover all the bases when it came to security and ensure proper, effective monitoring. With two entrances/exits located on the first level and one on the lower level, an integrated security solution was needed that could quickly detect a security issue. A huge focus to MLB NYC was securing the premise and ensuring that only employees could access the premises before or after hours. With four employees on staff that included three supervisors and one General Manager; having an access control system that could integrate with the video surveillance and alarm system was a huge priority.

"A huge challenge for MLB was trying to complete this project during the COVID-19 pandemic," said Simone Zar, general manager at Legends/MLB NYC. "Each member of the SAS Technologies team were true professionals that provided top notch service and made my job easier."

After careful review of the security needs, SAS Technologies knew the right combination of table setters to provide MLB NYC with the desired result. This included Lenel/S2 for access control and CCTV recording, Axis Communications for IP video surveillance cameras, Shooter Detection Systems for gunshot detection, Bosch for the alarm system, and Aiphone Series selected for the intercom solution.

Since MLB is a high-profile client, SAS Technologies delivered a powerful integrated security solution that would provide the desired results.

"By using the manufacturers selected, we felt confident that the solutions would integrate and work with one another. The minimization of the number of interfaces down to one made the management training on the security system much simpler," said Sergio Rocha, installation manager and project manager at SAS Technologies.

Being in the midtown area, which typically has high traffic, created the need for a reliable and foolproof solution. Legends felt confident in the security systems deployed to protect the 10,000 feet of priceless memorabilia and merchandise.

"The system that SAS Technologies deployed at the MLB store is by far the best security system I have ever used in my 24 years of experience working in retail," Zar said. "This was truly a great experience working with SAS Technologies not only during the installation, but after the store opened as they provided outstanding support for any issues, questions, or concerns that we raised."

From March 2020 through September 2020, the project was in high gear, but was delayed due to the COVID-19 pandemic. However, the SAS Technologies team worked collaboratively with the manufacturers and the team at Legends to ensure that the store stayed on target for the grand opening in October. Even with the many setbacks and challenges that faced this project due to the pandemic; SAS Technologies did not skip a beat.

"During the pandemic, we knew that when construction and the city would start to open and allow us back on construction and project sites that we had to be prepared." Rocha said. "The last thing we wanted was to come back after the time we had off and not deliver what our customer expected," states Michael Troiani, Service & Engineering Manager, at SAS Technologies.

SAS Technologies and stepped up to the plate, and would not have been able to deliver this solution without partners' assistance. Thirty 30 Axis IP cameras were installed; SAS Technologies collaborated with the general manager to reposition the cameras so Legends could get the best view possible from all angles. Offering merchandise from all MLB teams creates an influx of fans, which requires plenty of planning and preparation.

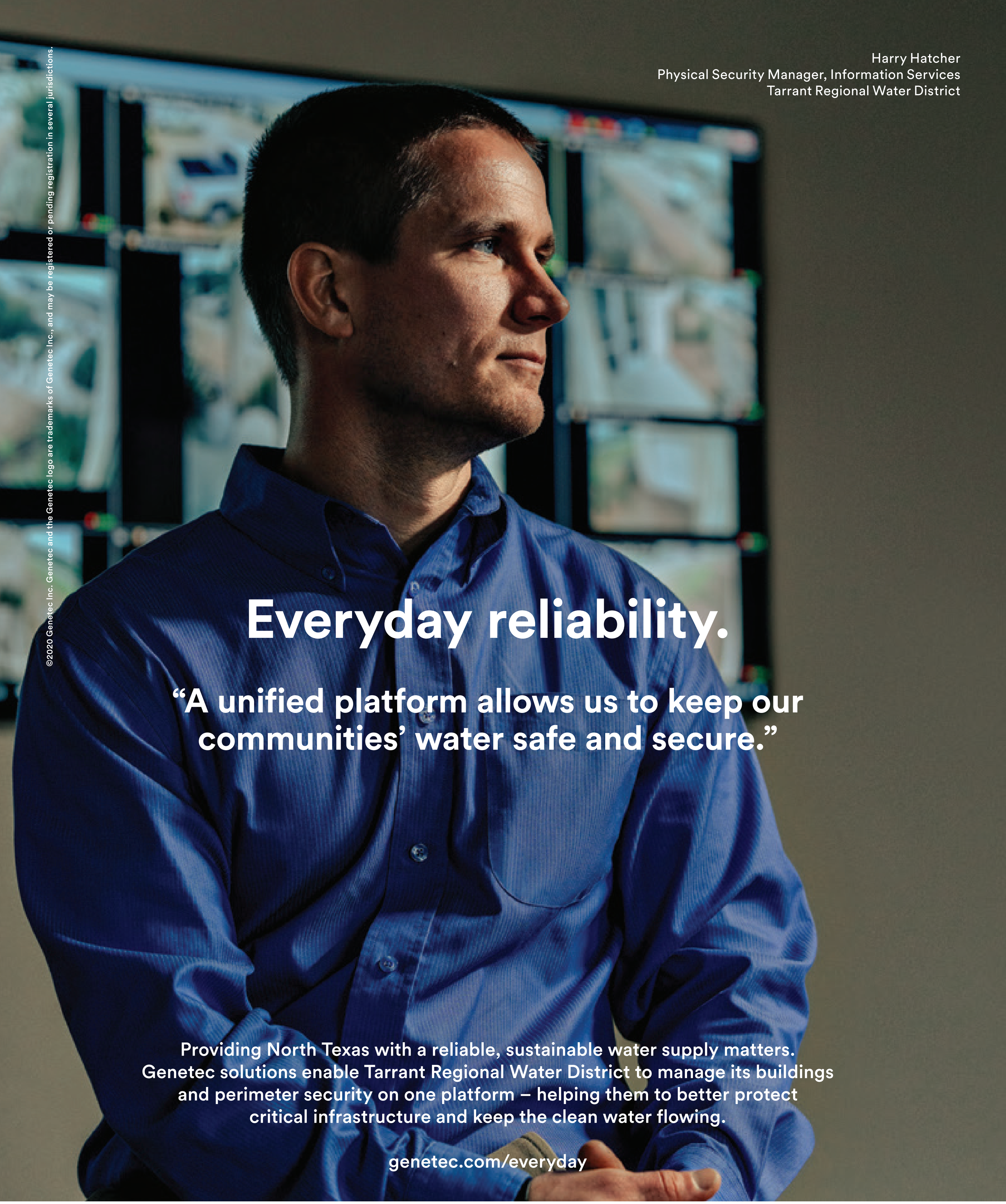
Having the cameras positioned correctly was crucial for the safety of the employees and fans. SAS was on hand every step of the way to help create a seamless installation and integration. It was especially important for them to provide specific details and some customization to this project. One item in particular was customizing the HID Multiclass reader covers with the MLB logos, for baseball fans.

Training on the system was handled by SAS Technologies, and was easily reachable after the installation for support.

"We trained Simone at Legends on the system and it could have not gone any better. Simone was extremely clear and specific on her objectives and how she wanted the system to function; and we customized the solution to meet all her needs," Troiani said. "When I was growing up, like many of us it was our childhood dream to hit the game winning homerun in the bottom of the ninth, being part of this project on many levels has helped fulfill this dream, we could not have asked for a better result."

As the needs of MLB NYC change and evolve over the years, SAS Technologies will continue to cover all the bases when it comes to securing the retail store and valuable merchandise and personnel. Legends scored a home run when it came to selecting the right integrator to install an enterprise-level security system.

__Monique Merhige-Machado__ is a freelance writer based in Port St. Lucie, FL. She is also the owner of Infusion Direct Marketing.



Moving the Needle

Video security and storage play a significant role in the security space

By Amanda Potas

Mark Agnor/Shutterstock.com

Video storage has come a long way since its simplistic and inflexible early days. Before more intuitive, scalable, and reliable systems emerged, customers purchased hardware from storage vendors and built their storage infrastructure based on their immediate needs. This meant all their hardware, software, servers and switches represented a timestamp in that organization's data diet.

These systems served static organizations well. However, for users who had growing data requirements and relied on ever-evolving technologies, these systems were not only difficult to scale, they were also expensive to maintain and often imprecisely met the needs of its users.

For this reason, in 1999, Jeff Burgess founded Burgess Computer Decisions. Beginning as an IT reseller, Burgess set out to build high-availability servers for Fortune 500 companies that outperformed the data storage standards of the day. In 2008, Burgess launched BCDVideo to transition his company to build enterprise-quality video recording solutions. Today, BCD has a footprint that includes more than 175,000 systems recording over 3.5 million cameras in 90 countries on six continents.

The Rise of Purpose-built Solutions

This burgeoning success directly mirrors the explosion of the data-sphere, expected to create, capture, copy and consume 181 ZBs of data by 2025, which is 181 billion terabytes or 181 trillion gigabytes, according to Statista. It also did not happen on accident.

Behind BCD's performance-driven IP video solutions is its partnership with Dell Technologies' OEM Solutions. Security integrators go to BCD and Dell to find innovative, customized and robustly engineered video storage solutions.

Nuts and Bolts

Since the start, BCD's goal has been to design purpose-built solutions and deliver the best customer support in the industry. These two tenants are the bedrock for consistent success in their customer relationships. When it comes down to the former, purpose-built solutions, working with Dell Technologies to provide infrastructure hardware was a no-brainer.

BCD tailors its security solutions, using Tier 1 hardware to enable their customers' needs. "To borrow from an old BASF slogan for video analytics and storage, 'We take it, and make it better.' Our customers would appear to agree," Burgess said.

HALO SMART SENSOR

According to the World Health Organization, 40% of the buildings in North America are making people sick.

Fight the spread of airborne diseases in your building with **HALO**

The COVID-19 and Influenza virus are commonly transmitted through the air as the virus is attached to very fine particulates. As part of its AQI measurements, **HALO** monitors Carbon Dioxide (CO_2), particulate concentrations, Humidity, Volatile Organic Compounds (VOC), and Nitrogen (NO_2) in the air. When **HALO** detects high CO_2 levels or particulate levels, **HALO** can notify the HVAC system via its BACnet interface, instructing the HVAC to open its dampers and allow more fresh air into the room.

Real-Time health index and alerts with HALO Cloud

CAPTURE COMPLETE HEALTH AND SAFETY AWARENESS IN YOUR BUILDING WITH THE ALL-IN-ONE HALO!

AUDIO ANALYTICS

• Spoken Key Word Alerting • Abnormal Noise Level Detection • Shouting • Gunshot Detection • Excessive Banging • Bullying

AIR QUALITY

• Vape • Smoke • THC • Particulates • Air Quality Index • Volatile Organic Compounds

CHEMICAL

• Ammonia • Carbon Monoxide • Carbon Dioxide • Nitrogen

ENVIRONMENTAL

• Temperature • Humidity • Tamper • Pressure • Health Index • Light Sensitivity

631.969.2601 • info@ipvideocorp.com • www.ipvideocorp.com/halo

IPVideo Corporation

"Dell Technologies' OEM Solutions began work with BCD when its former entry-level server vendor left the market, said Kyle Dufresne,, global senior vice president and general manager of OEM Solutions at Dell technologies. "Ultimately, the collaboration led to new design innovation and expanded to include other high-performance solutions such as HCI, storage, networking, and workstations, leading to a better experience for BCD's customers."

Video workloads are quite unique. The deployment of tens, if not hundreds, of high-definition, AI-optimized security cameras in a single site has increased bandwidth and data needs tenfold. Security deployments require significantly longer video retention periods while remaining high-performing, scalable and reliable. For security customers to get the most out of their video appliances, they need someone with the experience and innovation of BCD.

IP video security solutions require extensive pre-planning and design compared to off-the-shelf IT appliances not meant to withstand the requirements of video. That's why BCD takes Dell Technologies' bespoke infrastructure and incorporates the right memory, hard drives, testing and validation needed for IP video, as well as the individual needs of each end-user.

Ensuring the uptime of these purpose-built video data infrastructure solutions is just as important as its capabilities. One exclusive integration BCD offers for monitoring these systems is its Harmonize iDRAC (Integrated Dell Remote Access Controller) plug-in. The Harmonize iDRAC plug-in enables users to monitor servers proactively and predict hardware failures through their preferred VMS platform.

When dealing with large amounts of critical data, the Harmonize iDRAC plug-in is the perfect safeguard. Nobody has the experience or the lab for substantial research and development like BCD when it comes down to it. This makes BCD the ideal IP video data infrastructure provider.

Going Above and Beyond: Testing and Validation

Eugene Kozlovitser, BCD's technology director, explained that BCD has set certification and validation benchmarks well beyond what the current security hardware offers.

"Today, due to the rise of new technologies and 'lean' security infrastructure approaches, the most innovative software companies are always struggling to find the right hardware vendor that can offer a full spectrum of products and services including testing and validation," Kozlovitser said. "When a software provider is trying to establish the maximum breaking point of their software, BCD is usually the first ones they contact."

He also explained that BCD's software agnostic approach can easily scale out and redesign its testing facilities to optimize any suite of software products for their customers. In addition, the capability of hardware intake validation, factory authorized testing, soak testing, and risk analysis allows BCD to be the most trusted platform in the security industry.

frantic00/Shutterstock.com

"When it comes down to the former, purpose-built solutions, working with Dell Technologies to provide infrastructure hardware was a no-brainer."

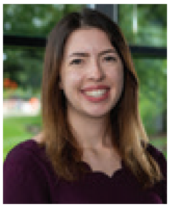
Going Above and Beyond: Supply Chain Expertise

When it comes to delivering products to customers who need them, BCD delivers. When shortages of video graphic cards, hard drives, CPUs arise, BCD is able to stay one step ahead because it orders components by the truckload and has multiple, strategically located warehouses throughout the world for just-in-time inventory. BCD works hand-in-hand with their customers to ensure organizations can address immediate security concerns the moment they arise, instead of having to wait weeks, if not months, for back-ordered hardware to arrive.

With these standards are consistently met—a best-in-class product development and design, customer support and supply chain maximization—BCD is setting a new standard in the safety and security sphere. In the most sensitive security environments, where protecting critical assets is the number one priority, BCD is building technology today, to secure the industries of tomorrow.

Looking Forward

For end-users looking to implement, upgrade or expand their security systems, thoughtfully designed appliances, like those engineered and built by BCD through their Dell Technologies partnership, will meet the needs of many security scenarios. The key to delivering better system performance and lower total cost of ownership across the board is bringing together top-tier technologies and industry-leading system design.



***Amanda Potas** is the marketing manager at BCD International.*

for heroes

for future leaders

for game changers

Alexander Supertramp/Shutterstock.com

The Time Has Come

Security technology is set to play a pivotal part in this rapid transformation

By Jason Burrow

Despite the rapid rollout of vaccines, the impact and ramifications of COVID-19 will be long felt in almost every part of the economy. Many businesses have needed to pivot and adapt quickly to new ways of working. They have felt the pressure of operating with fewer staff and the burden of having to monitor and manage operations remotely.

In addition to the impact of the pandemic, each industry sector also needs to contend with its own set of specific challenges. Among them, brick and mortar retail adapting to the rapid shift to e-commerce; logistics operators ramping up operations to meet unprecedented demand; the pressure for oil, petrochemicals and energy producers to cut CO_2 emissions; corporate enterprises attracting and retaining talent; or healthcare and assisted living providers dealing with an increasingly aging population.

Beyond these myriad challenges, all businesses also need to be prepared to deal with the uptick in extreme weather events, the shift to green energy, the increasing sophistication of cyberattacks, potential civil unrest, insider and terror threats and the continued need to manage with day-to-day safety and security operations.

Analyst firm Grand View Research predicts systems integration to dominate the physical security market through 2027, even before factoring in COVID-19 and the need to migrate operations and workforces to a virtual environment. Deloitte reports the acceleration of digitization, as a result of COVID-19 pointing toward technology for improved preparedness, cybersecurity, identity and access management, and flexibility.

Tech-savvy security and facility managers know that, in order to evolve and adapt, they need to eradicate disparate systems and silos of information. Systems integration is not confined to only the realm of large businesses - small to mid-sized organizations, and even homeowners, are realizing the benefits a more integrated approach for video, access, and audio can deliver to them.

A CENTRALIZED APPROACH

Upgrading to a centralized security and safety solution will help staff and control room operators respond to incidents and threats quickly, while also improving workflow to manage day-to-day operations. Even a minimal level of integration, such as pulling together access and surveillance, makes security and safety operations easier to operate from a single interface. This also allows for a rapid and practical way forward for complex, multi-location organizations.

Additionally, organizations can benefit from integration with dozens of building management systems – from IP audio,

intruder systems, fire detection to asset tracking – and streamline identity management by exchanging data with popular databases.

The data intelligence and comprehensive reporting provided by multiple systems also gives heads of security insights and well-informed decision-making power when it comes to orchestrating changes to manage staff and facilities.

Here we take a closer look at some of the other specific benefits a centralized security and safety solution can provide and share some insights on ways that security systems integrators can help customers realize them.

REAL-MONITORING AND SITUATIONAL AWARENESS

Real-time monitoring of single and multiple sites gives security staff instant situational awareness about what is going on within their facilities. Integrating alarms from multiple systems also gives operators an improved ability to visually verify notifications and automatically capture events using video, ensuring critical incidents are never missed.

Integrated solutions also offer remote access capabilities that allow security managers to maintain oversight even when they are away from the control room. From any location, single or multiple facilities can be monitored, and problems can be addressed as soon as they occur.

TACKLING DATA BREACHES AND THE INSIDER THREAT

The latest Kroll Global Fraud and Risk Report found that "employees more than any entity are responsible for internal fraud and leaks of internal information" as well as perpetrating the greatest share of data theft.

Deficiencies in cybersecurity and one siloed digital system can put organizations at risk. This has caused IT departments to take on an increasingly significant role when it comes to the purchase of physical security technology. They understand, better than many, that integrating systems allows for a more comprehensive approach to maintaining cyber protection across disparate systems and siloed databases. Integrating access control with standardized databases such as Microsoft Active Directory also provides businesses with the ability to better manage physical and logical identity management, which enables improved detection, and faster responses and recovery.

Integrated access control and video system can also pack a punch in detecting suspicious activity, such as when employees try to access server rooms or change their behavior patterns, which are often precursors to breaches.

BOOSTING PRODUCTIVITY AND EFFICIENCY

Inefficiency is a time-zapper and comes at a cost. The economic impact of COVID-19 has led businesses to recognize that integrated solutions have a key role to play in making operations run more efficiently – from reducing pressure on their control room and frontline staff through to minimizing hassle for employees. Staff, for example, often face frustration when trying to access multiple sites or organize meetings that require booking associated parking spaces, meeting rooms, and organizing guest ID badges.

> "Even a minimal level of integration, such as pulling together access and surveillance, makes security and safety operations easier to operate from a single interface"

By integrating previously disparate access control and video systems across different facilities, and combining them with the latest visitor management solutions, allows staff to leverage the security benefits and convenience of license plate recognition (LPR) and IP intercoms.

Integrating visitor management solutions is also proving to be an effective tool for contract tracing, a key requirement in the COVID-era. It also provides long-term enhancements, as it can streamline operational efficiencies that also improve the employee and visitor experience. This will benefit enterprises not only during the pandemic, and well into the future.

END-TO-END AND FLEXIBLE SOLUTIONS

Integration certainly has its perks and is clearly helping to tackle industry-specific challenges. In the retail sector, for example, forward-thinking stores can now integrate video tech with point-of-sale systems to take 'sweet heart' and internal shrinkage head on. Adopting these latest AI analytics will allow users to gain intelligence into customer behavior and turn browsing into sales.

The logistics sector is also finding that integrating video with asset tracking and inventory systems is better securing their supply chains. That is because it enables the visual tracking of goods, which, in turn, increases efficiency and improves customer service. For data centers, integrating HVAC systems with access control to detect when adjusted temperatures allow staff and engineers working in server rooms to reduce energy consumption. Additionally, intelligent analytics or sensors will alert staff when cabinet doors are ajar when an engineer is not present.

Sectors ranging from hospitality, healthcare, education and manufacturing are seeing for themselves that integration is delivering ever more capable and flexible solutions. These solutions are applicable to every type of medium-to-large business, from those that operate standalone large buildings and campuses to those with complex, dispersed, multi-site estates.

Users are looking for scalable, flexible, and future-proof solutions that can be adapted to meet new requirements and changing priorities without exponentially increasing license fees or complexity. They also are looking for solutions that give them the ability to easily integrate additional third-party systems, allow them to add sensors and IoT devices, and adopt new functions such as deep learning analytics with minimal expense and disruption. The time surely has come to unite disparate security systems. The benefits to end-users are many and far-reaching.

***Jason Burrow** is a regional sales director at IDIS America.*

BCDVIDEO

PURPOSE-BUILT, PERFORMANCE DRIVEN

Trusted Video Data Infrastructure Solutions

20+
Years in Business

170,000+
Systems Installed Worldwide

5
Average Days to Ship

40+
Private Label Customers

Today's IP-based surveillance solutions are more sophisticated and have complex network and storage requirements. BCD delivers **highly optimized, secure and manageable solutions** that meet the stringent requirements that IT departments demand.

Contact Us
+1-847-205-1922
sales@bcdvideo.com

BCDVIDEO.COM

Coming of Age

Innovation and automation are being built on strong data foundation

By Ajay Jain

There have been on-going discussions the past several years about how Big Data and Artificial Intelligence (AI) can be used to modernize physical security systems and operations. The truth of the matter is that digital transformation has already been taking place for quite some time, albeit in small steps with what is now a very fast-paced technology evolution.

What were once high-level theoretical discussions on mining data from both traditional physical security operations and scores of new and emerging IoT devices have now become a reality. This next generation of innovation and automation is being built on strong data foundations and data intelligence. And it is changing perceptions on how physical security systems need to be designed, implemented, and managed in this new era of data-driven physical security solutions.

Perhaps the most significant take-away from the genesis of data-driven physical security is the change in mindset from reactive to proactive systems technologies – the ability to autonomously process data in real-time to reduce friction in business process execution by eliminating human intervention, and to deliver actionable insights and even predictive analysis.

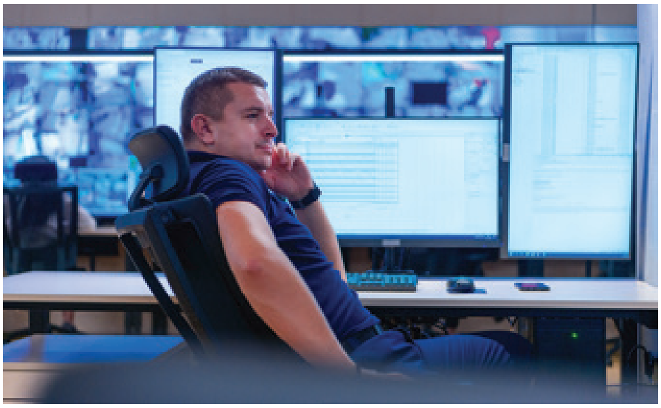
This has the potential to dramatically increase the overall effectiveness and efficiency of physical and cyber security operations, mitigating risk across the enterprise. As a result, physical security technologies and operations will continue to leverage real-time business intelligence across the enterprise to facilitate real-time decision making.

THE BIG DATA INTEGRATION CHALLENGE

One of the biggest challenges faced by security professionals today is the ability to harness and analyze the tremendous volume of data being generated by physical security operations containing spatial, sensor and transactional data and network of devices to derive meaningful actionable intelligence. With the bulk of such data being unstructured data, new data-driven solutions are required to contextualize this disparate and fragmented information in a seamless way.

One of the reasons this presents such a daunting challenge is that physical security operations typically employ several different point-of-control systems and associated sensors / IoT technologies such as Physical Access Control Systems (PACS), video surveillance, intrusion sensors, biometrics, visitor management, dispatch, incident management systems and more. For the most part, these systems are not highly integrated and provide siloed views of activity which fail to provide a complete picture, precluding intelligent insights from being drawn since all the data is not being analyzed in the same context.

The first step in resolving the fragmented challenge is to bring data from these otherwise disparate system technologies together onto a special purpose unified platform. It requires discovering, connecting, integrating, transforming, managing, analyzing, and storing valuable data insights and enable the execution of applications that are smarter and intelligent – net-net derive 5-10X value.



The next step is to understand how and where to use this newly found data intelligence to improve business processes. For example, can one apply data science to predict occupancy levels of a building or a floor to better schedule employees coming into a facility during today's pandemic times? Can one use data intelligence and predict what physical security IoT sensors or devices will fail within 30 days, and make the retroactive repairs as opposed to being reactive? There are numerous such promises of the data science discipline.

Last, but not the least, is to make this all very simple for users to consume. The data science, the machine learning and the artificial learning can only work if the intelligence and insights from the myriad data sources are driven to the applications without heavy lifting or understanding of computer and statistical science. It should be very easy for users to incorporate these applications into business operations. New developments in AI powered software platforms can help alleviate both physical and cyber threats by inferencing from large volumes of data, and quickly triangulate small subsets of pertinent information, provide actionable insights etc. This not only simplifies and improves physical security operations while delivering tangible ROI and lowering TCO, it also automates major security functions related to Physical Identity and Access Operations, SOC Automation and Cyber-Physical Security defense.

THE DATA-DRIVEN PLATFORM SOLUTION

New data driven solutions are now coming to market that promise to address many of the inherent legacy system and data integration challenges that plague the physical security industry. A prime example is the recently unveiled Vector Flow platform, which is capable of processing and analyzing vast amounts of data from otherwise disparate security systems, data stores and input devices.

This innovative new solution derives actionable intelligence

BRINKSHOME™

Security for life.™

Join the winning team at Brinks Home™

Flexible & Customizable Partner Programs

Our Network Sales team has expanded its program to collaborate with an even wider variety of authorized dealers, representatives, and other selling partners. Team up with a world-class brand and receive excellent compensation and individualized support whether you sell in the Continental U.S., Canada, or Puerto Rico.

For more information visit us at **brinkshome.com/partners** or call us to become a dealer partner at **800.595.2059.**

"With the bulk of such data being unstructured data, new data-driven solutions are required to contextualize this disparate and fragmented information in a seamless way."

from physical security data using advanced Artificial Intelligence (AI) and Machine Learning (ML) algorithms that empower a whole new range of highly advanced automated physical security applications that were previously unattainable. A truly converged data driven physical security solution, the new platform presents myriad opportunities for digital transformation and improving several major business processes such as:

Physical Workforce Identity & Access Management (PIAM) which unifies and streamlines identities, access and badges; on/off boarding processes; physical access provisioning; access audits and compliance to regulations; risks analysis and prescriptions and mobile self-service.

Physical Security Operation Center (SOC) Automation for autonomous false alarm reduction and reporting, unlimited device monitoring and auto optimization, auto configuration of devices, and auto detection of faulty devices, along with provisioning automated virtual SOC assistants using AI/ML playbooks.

Cyber-Physical Security to enforce "defense in depth" using advanced AI models that detect vulnerabilities in physical security, IoT and building automation devices to prevent cyber surface attacks and reduce organizations' exposure to overall risk.

Vector Flow's data-driven solutions are already implemented at several Fortune 1000 companies. This includes a global telecommunications provider with over 450,000 identities – the Vector Flow team replaced the legacy PIAM application with a new AI-enabled physical identity lifecycle application. The new solution promises to save millions of dollars in direct costs over the course of the contract while increasing overall security operations productivity, compliance to regulations and delivering valuable service to the enterprise.

In another example, a top Research and Pharmaceutical company, focused on anti-viral drugs and treatments, deployed Vector Flow's AI-enabled solution to streamline SOC operations, enable AI-driven device health prediction, reduce false / nuisance alarm counts and streamline SOC functions by establishing and measuring KPIs across all SOCs including compliance with newer regulations such as AB 685 & SB 1159 for building occupancy during Covid-19 times.

Ajay Jain is the president and CEO of Vector Flow Inc.

CEIA USA • THREAT DETECTION THROUGH ELECTROMAGNETICS

GAME DAY AT RECORD SPEED.

OPENGATE™ (NEW)
Groundbreaking Weapons Detection System

- Quickly and automatically screen guests with their backpacks and bags
- Extremely high throughput with near zero nuisance alarms
- Detects handguns and mass casualty threats, such as high caliber assault weapons and IEDs
- Easy to relocate at 25 pounds and installs in less than 1 minute
- Indoor and outdoor operations

Our threat detection and screening systems take the guesswork out of security screening. Incorporating the latest in threat detection technology, CEIA sets the standard for safety, convenience and accuracy.

For more information, contact your CEIA USA representative at **security@ceia-usa.com**
or call us today at **833-224-2342**.

CEIA USA
WWW.CEIA-USA.COM

A Hybrid Work Environment

Bring your own portable storage device to work? Not today

By Richard Kanadjian

As companies begin to repopulate their offices with workers who have spent the last 12-15 months toiling from their overcrowded kitchen tables and other non-traditional work settings, now faced with a potentially catastrophic problem.

Defined as any digital device, bring your own device (BYOD), owned by the employee and not be approved by the employer for use on the job. Such devices include cameras, wireless devices, tablets, laptops and USB flash drives.

While these devices are often essential to productivity and seem completely innocuous, they actually pose many serious cybersecurity risks and can single-handedly negate millions of dollars a company has spent on infrastructure security, not to mention myriad problems associated with the loss of vital company data.

Many post-pandemic returning workers are going back to a hybrid schedule. The plan might be a few days a week in the office, a few days back at the kitchen table. There is a very real risk that private company data is accompanying them to and fro, and stored on some manner of the memory device will become compromised, lost or stolen, resulting in a cybersecurity mess for the company.

A USB drive is one of the most popular BYODs. Known as removable media, flash drives, thumb drives, among other terms, and capacities up to 2TB. They have tremendous portability, and exceptionally easy ability to be connected to various networks, USB drives have proven their value as file-sharing and mobility tools and backup drives.

Unfortunately, they are also very susceptible to being lost, breached, and misappropriated. That leads to the possibility of critical, classified, sensitive data landing in the wrong hands.

Making matters worse, many times, the USB drive used by the employee is either bought by the employee or received as some type of perk or gift, virtually assuring they are not up to a company's standards, making them even more likely to pose a security risk.

While the BYOD concept offers varied pluses, there are also many special problems associated with it. Since USB drives are a favorite means for these hybrid workers to store and/or move files from work to home and vice versa, let's take a look at how the risk associated with their use can be mitigated.

There are four ways a hybrid worker using a USB drive poses a security threat.

- The employee accidentally loses a drive.
- An employee's USB drive is stolen.
- The trusted hybrid employee stores confidential company data on a USB drive and makes it available outside the company.
- A hybrid employee finds an infected USB drive and unwittingly plugs it in, whether out of curiosity or in a misguided attempt to find the owner.

So what is the magic word to ensure data stored on a hybrid worker's – or any worker's – USB drive stays secured? Encryption.

Bring Your Own Device

Maslakhatul Khasanah/Shutterstock.com

Encrypted USB drives use the strictest security regulations to protect sensitive data and protocols, and have helped businesses, large and small transport data when it needs to move beyond the company's firewall securely and confidently.

Encrypted flash drives are an essential pillar of a company's comprehensive data loss prevention (DLP) strategy. It is imperative that companies insist their employees use only encrypted USB drives, which combine the productivity advantages of allowing USB access while protecting the information on the drive.

Encrypted USB drives are powerful tools in eliminating security gaps and provide another layer of security in and outside the firewall by offering:

- FIPS Certification
- Latest encryption technology
- Anti-malware/virus protection
- Complex password protection
- Ability to be managed remotely
- Tamper-evident technology
- Wide-capacity range

Of the encrypted USB flash drives, the most effective are those where implemented security is in the device's hardware.

A USB drive with hardware-based encryption is an excellent, non-complicated, simple solution to protecting data from breaches while also meeting evolving governmental regulations. Priced between $40 and $600, depending on capacity, such devices meet tough security standards and offer the ultimate security in data protection to confidently manage threats and reduce risks.

Hardware-based encrypted USB drives are self-contained and do not require a software element on the host computer. No software vulnerability eliminates the possibility of brute-force, sniffing and memory hash attacks.

They also have unaltered digitally signed firmware, as well as a physical layer of protection. Some of these drives come in epoxy-dipped/filled cases that prevent access to the physical memory. In contrast, a USB drive with software encryption uses software that runs on the host computer and is vulnerable to attacks.

Button press up to 200 feet (61 m)

Traditional presentation mode

If your site requires that you access entrances and locations up to 200 feet away, as well as doors and situations with proximity/smartcards, Farpointe Data's secure Ranger solution provides both with a single transmitter. No other solution provides such two-in-one convenience.

- Compatible with all popular access control systems.
- Resistant to water, dust, grime and vibration.
- Extremely reliable, with over 900,000 in use.
- Powered by a widely available, replaceable battery tested to exceed 250,000 button presses.

Contact us today for a dealer near you.

1-408-731-8700

www.farpointedata.com

Farpointe Data®
Readers • Credentials

The OEM's global partner for premium RFID solutions

"There is a very real risk that private company data is accompanying them to and fro, and stored on some manner of the memory device will become compromised, lost or stolen, resulting in a cybersecurity mess for the company."

The top-of-the-line hardware-based encrypted USB drives use AES 256-bit encryption in XTS mode. This ensures anyone who finds such a drive cannot access the information, as the drive wipes itself clean after 10 attempts at guessing the password.

A patent-protected, hardware-centric/software-free encryption approach to data security is the best defense against data loss, as it eliminates the most commonly used attack routes. Furthermore, this same software-free method also provides complete cross-platform compatibility with any OS or embedded equipment possessing a USB port and file storage system.

Finally, it is also vital for companies to have policies and practices in place that deal with protecting data beyond encryption. Workers must know and follow these policies and practices to avoid loss of data, compromised data, or malicious virus and malware attacks.

Training and educated on the company's policies and practices regarding the use of USB drives is key to returning hybrid workers. Lack of training means you do not have a tightly sealed data loss-prevention strategy, and you are more prone breach, hacking and all of those other wonderful malicious things that can happen.

Several years ago, a USB security study found that 72 percent of employees use free drives from conferences and tradeshows or business meetings, even in organizations that offer 'approved' USB solutions.[1] How safe are those drives? Establishing a training program that educates employees on acceptable and unacceptable use of USB flash drives and BYODs is crucial for returning hybrid workers.

Don not ignore the serious risks of unencrypted BYOD USB drives. Take a proactive approach by implementing a best-practices standard and policy, and providing employees with company-approved encrypted USB flash drives for use in the workplace. Paying a little more up-front for encrypted drives will cost exponentially less than risking a potential data breach and potential fines for mishandling private customer data.

***Richard Kanadjian** is currently the business manager of Kingston Technology's Encrypted USB unit.*

[1] A Ponemon USB security study (January, 2019) found that 72% of employees use free drives from conferences and tradeshows, business meetings, etc. — even in organizations that offer 'approved' USB options."

Person
Vehicle
Vehicle
WISENET

Drivers and Implications

Innovations in hardware have bolstered compute power

By Quang Trinh

Artificial Intelligence (AI) has been around since the 1950s when scientists and mathematicians essentially wanted to see if they could make machines think like humans. Since these early notions of AI, technology has advanced at a gradual rate. However, significant breakthroughs in AI have occurred within the last decade--accelerated by digitalization, which has resulted in more data to analyze and improved outcomes.

It is fair to say that as technology continues to advance, the impacts of AI will be experienced in every industry—particularly in the security industry—and offer unprecedented opportunity to address real-world challenges.

Ryzhi/Shutterstock.com

HARDWARE EQUALS MORE COMPUTE POWER

Most recently, innovations in hardware have bolstered compute power and generated more AI-related applications. Think about it: the transition from Central Processing Units (CPUs) to Graphics Processing Units (GPUs), and now Application Specific Integrated Circuits (ASICs), is well underway and rapidly evolving.

The shift from CPUs to GPUs resulted in efficiencies and advancements in parallel processing, and the transition to custom ASICs—specifically designed to accelerate AI techniques in Deep Learning (DL)—has opened the door for on-premise and edge device solutions. As a result, many industries are now starting to realize the significance of both hardware and software when applying AI to more real-world use cases.

From CPUs, GPUs and ASICs to DLPUs and SOCs (System on a Chip), AI is changing the way many device manufacturers are approaching future device design and functionality. Even though AI has been around for many decades, it's recent advancements that have allowed the tech community to optimize the compute power required for AI and its techniques, including:

- Machine Learning (ML) the subset of AI, which uses fundamental cognition and leverages algorithms to solve basic problems by identifying patterns to make highly confident predictions--resulting in decision making with minimal human interaction.
- Deep Learning (DL) the subset ML that utilizes algorithms based on simulated neural networks inspired by the way humans learn (and trained on a massive amount of input data) in order to provide more accurate outcomes.
- Neural Networks (NNET) or Artificial Neural Networks (ANNs) are the core of DL algorithms, whose structure is designed to simulate the way the human brain and its neurons operate in order to process and recognize relationships between data.

REAL-WORLD OPPORTUNITIES

So what is the next step for AI? The common goal is the commercialization of AI technology. The data required for AI begins at the edge with devices for collecting and processing that data into information.

Billions of devices interconnected in private and public networks are already in existence (and more are added to the network every day) which presents immense opportunity when it comes to the development of on-premise and edge-based commercial products. That said, in order to be successful, companies will need to adapt to the ever-evolving AI framework. The challenge for most companies is how to apply AI into a real-world environment in order to solve a problem. Furthermore, the ability to resolve real-world problems requires a lot of data—quality data.

The approach toward acquiring quality data must be methodical and meaningful, so it's a walk before you can run process. Accordingly, in its initial stages, it requires an expert who can examine a problem, ask the right questions and get to the root of a problem before properly designing a solution around an AI framework. Of course the visual data in IP cameras is essential for AI to learn from.

Once solid methodology is determined and quality visual data is collected, there is still a huge task to organize and label the data when applying ML and DL techniques. Compute power demands will increase especially when shifting from ML to DL techniques during the training process. Once a ML/DL model is trained, and ready for execution, compute power at the edge also plays an important role. Deep Learning Processing Units (DLPUs) in today's high-performance cameras are providing great advantages to the leap from Machine Learning to Deep Learning.

MODELLING, QUALITY DATA DRIVE RESULTS

It is important to bear in mind that Machine and Deep Learning require hundreds-of-thousands, if not millions of data sets to learn. Ultimately, the output in DL is only as good as the data that the algorithm is being taught. Training an AI model to correctly output an efficient result is tedious and requires a lot of human interaction to test and retest the results. In fact, real-world situations are essential to training, so these exercises cannot be performed in a vacuum. Public safety cam-

comnet
Communication Networks

The Shortest Distance
Between Two Points

Audio, Video, Data, and Ethernet Transmission Solutions

ComNet is Your Solution for Fiber Optic, Copper, and Wireless Transmission

Your transmission challenge has always been getting your audio, video, data and ethernet signals from here to there.

ComNet offers the most comprehensive line of products designed to solve every transmission challenge.

MADE IN THE USA LIFETIME WARRANTY

RAZBERI – SIMPLE, SECURE VIDEO SURVEILLANCE AND IOT SOLUTIONS

Now part of ComNet

Simple-to-deploy, manage and cybersecure video surveillance systems and IoT devices

ComNet's Razberi line provides video server appliances, combined with cybersecurity and health management software to customers worldwide. We save customers install and maintenance costs and reduce the likelihood of a costly cyber breach.

View the Full Product Line at **comnet.net** and Identify the Fiber Optic, Copper or Wireless Connectivity Solution for your Application

Contact the ComNet Design Center Now for Free Design Assistance.
Call **1-888-678-9427** or **1-203-796-5300** or email **designcenter@comnet.net**

Visit www.comnet.net
Email info@comnet.net

Phone 1-203-796-5300
Toll Free 1-888-678-9427

an ACRE® brand

eras are ideal inputs and offer valuable data since they provide varying perspectives, unique environments and new unstructured data sets that many existing AI models are not based upon.

While Machine Learning is efficient because its algorithms are good at analyzing structured data, it's ineffective at processing unstructured data. Therefore, as AI looks to perform more complex analysis of unstructured data, Deep Learning with its algorithms based on simulated neural networks, is more capable. Visual data—including raw visual data in computer vision and encoded images or videos in JPEG and H.264/265—is unstructured data and incredibly valuable to Deep Learning. As we know, the Security Industry as a whole presents an abundance of visual data in real-world use cases—data that will undoubtably help drive advancements in Deep Learning over the next few years.

SETTING EXPECTATIONS

Despite the promising advancements in AI, it's important to set expectations around what AI can and cannot do. For example, many analytics use image classification to detect people and vehicles, but that doesn't equate to actually understanding a scene. Visual understanding is still very challenging and currently there is not enough real-world data and applicable training to allow an AI-based solution to fully understand a scene. Furthermore, the best AI-based analytics are not able to read a person's behavior. Emotional differentiation such as humor is something that an AI-based solution cannot determine or infer. In a scene where crowds gather, AI-based analytics cannot understand if the event is an altercation or a celebration.

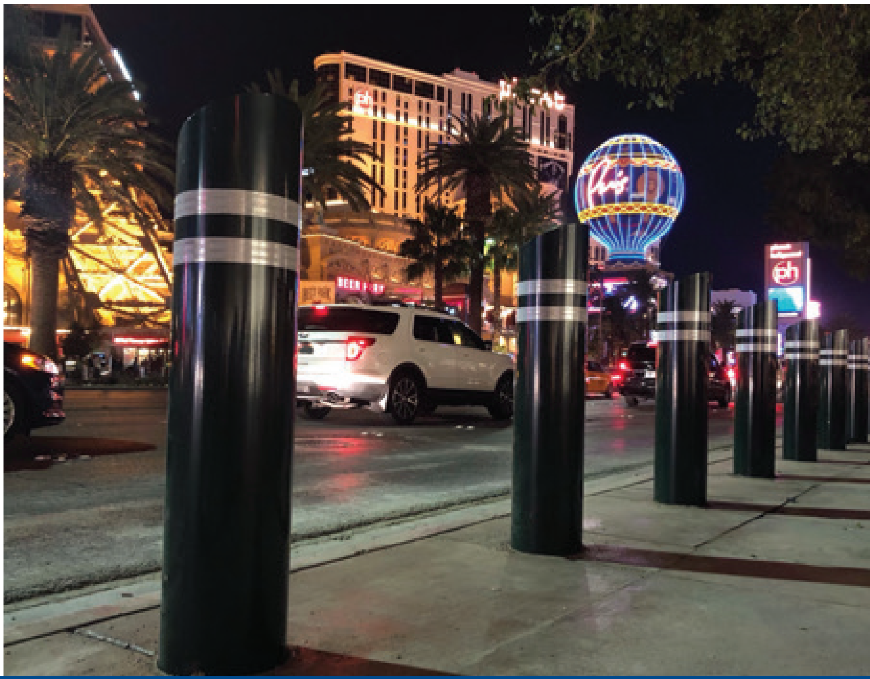
> "As a result, many industries are now starting to realize the significance of both hardware and software when applying AI to more real-world use cases."

Clearly there are still some tough questions that face our industry when it comes to real-world applications and possible AI-solutions for our customers. For these reasons, analytics used in the security industry require some degree of human interaction and judgement. In addition to these considerations, vulnerabilities exist in data manipulation of neural networks, which can cause AI to output inaccurate results. For instance, you cannot fully understand a scene at the single pixel level, so there is still work to be done from a technological standpoint.

This fact can also be illustrated by the dynamic nature of images captured on an IP camera—in a scene where lighting is inconsistent, harsh shadows can cause changes in a per pixel level that affect the classification of an image or object. All that said, the community of AI developers is growing and they, in combination with their partners, are making great strides.

CONTROLLED PRODUCTS
SYSTEMS GROUP

HOSTILE VEHICLE SOLUTIONS



Your customers need the correct protective barriers in place to secure their high value locations.

CPSG has the Hostile Vehicle Mitigation/ Anti-Ram products and expertise to assist through the system design, quote and purchase process.

CPSG is more than the nation's largest wholesale distributor, we provide complete solutions. Contact our barrier experts for a free design consultation.

Call or visit our website and sign up for upcoming HVM/Anti-Ram webinars.

Your **ONE** Source for Access Solutions.

GIBRALTAR
the power of innovation

NASATKA
SECURITY

Nice

HySecurity

FAAC
Simply automatic.

BFT

Calpipe
Security
Bollards

National Sales Line 877-531-6122 • National Technical Line 877-531-6123 • MyCPSG.com

OPPORTUNITIES FOR TOMORROW

There is no doubt that image classification within security applications is evolving with AI. Moving from pixel-based algorithms in video motion detection to ML and DL models that can classify people and vehicles is a start. What's more, a reduction in false positives can be attributed to the improvement of many DL models through real-world data.

Devices with a custom ASIC, DLPU or a SOC designed and optimized for DL will provide advantages at the edge. Edge devices with hardware acceleration for ML or DL will offer better performance and efficiencies. As AI becomes more mainstream, open-source projects will fuel the growth in edge-based processing along with some proprietary technologies around Deep Learning. For example, Google's Tensor Processing Unit or TPU is an AI accelerator ASIC that was developed in 2015 specifically for NNET Machine Learning.

Google opened licensing availability of the TPU to third parties in 2018 to further advance the adoption of DL to other hardware manufacturers. Their Edge TPU was designed around a low power consumption draw of 2W compared to their server based TPUs. The Edge TPU in its current generation can process 4 trillion operations per second and offers an alternative to GPU accelerated Machine Learning. This is just one example of the innovations in DL hardware acceleration that can lead to breakthroughs in AI and edge compute devices that are processing images in real-time. The future for DL on edge devices will be dependent on how efficient an ASIC, DLPU, or SOC design is implemented.

REDEFINING THE FUTURE

Artificial intelligence has already begun to impact the security industry, and it has promising and exciting implications. Intelligence is transitioning to a distributed architecture that impacts edge devices directly where data is collected. Increasingly, more AI-experienced companies are collaborating with customers and partners in our industry. Many companies are investing and exploring AI-centric solutions and are looking for partners to work with in the process. AI-based solutions in our industry will not be a one size fit all and will require a team well-versed in AI frameworks.

These teams must be willing to challenge conventions and ask hard questions in order to get to the root of a problem before architecting a solution around AI. With recent advancements and new opportunities, there's no doubt that innovations in AI will grow exponentially in the coming years—and these innovations will transform our industry and redefine the future of public safety, operational efficiency and business intelligence.

***Quang Trinh** is the manager of professional services at Axis Communications.*

DA™ Dakota Alert
MTPR-4000
Motion Transmitter and Portable Receiver
•Detects people or vehicles
•Monitor customer traffic
•For use in a retail shops, garden centers
Or at home
• 1 Mile range from transmitter to receiver
www.dakotaalert.com
605-356-2772
GARDEN
12 34
11/23/2020
Dakota Alert

Kryuchka Yaroslav/Shutterstock.com

The Time Has Come

Artificial intelligence is the talk of the town in most industries

By Aaron Saks

Every technology industry is talking about the benefits of Artificial Intelligence. More than a buzzword, AI is hyped as a panacea, while at the same time, it is often misunderstood by those who might benefit from it the most.

AI may mean different things to different people, there are plenty of aspects that apply to all disciplines. The ability for a machine to "learn" from data it is presented is at the core of all AI use cases. The term "machine learning" derives from that most basic idea. Deep Learning, a subset of machine learning, and is based on neural networks, and is frequently used to analyze and compare image data. The challenge is how to use these AI disciplines effectively to better protect people and assets. Beyond security, it's time to look at how data from these cameras can be used to positively impact operations and sales for an organization.

CHANGING HOW WE THINK ABOUT SECURITY CAMERAS

Traditional digital cameras do not identify objects they capture. They just blindly record pixels to a disk. With analytics, if the camera sensor detects movement in those pixels, it can place a bookmark in the recording or send an alert. Anyone who has tried to use traditional motion analytics, although they can be useful, will know they are also very prone to false positives. Depending on the installation, a motion event is triggered by something as mundane as a shadow from a passing cloud. For this reason, many security professionals shied away from using analytics in all but the most controlled circumstances or as a guide to where an event "might" have happened.

Using deep learning algorithms, we can effectively teach a camera sensor to identify objects and detect unique characteristics about them. It is a sophisticated process to train a machine learning algorithm and it can require hundreds of thousands of images to make it accurate. The algorithms must be told when it gets things wrong, as well. It is also important to remember that what differentiates today's technology from true AI is that machine learning and deep learning algorithms cannot learn new things by themselves.

Current AI-based cameras can reliably identify objects such as a car, truck, bicycle, license plate or a person in an image. They can also discern the unique attributes of these objects, such as color or whether a license plate or face is present. Thanks to advances in deep learning, these devices have evolved from capturing images to becoming highly accurate data gathering tools. They are network connected, and are truly part of the broader world of IoT devices that surround us. With their myriad new potential to protect and inform, it's time to think differently with regards to the value these devices can bring to an organization.

SECURITY BENEFITS OF AI CAMERAS

The most common application for AI-powered cameras today is to empower the traditional motion analytics that we are familiar with, such as loitering, intruder detection or entering/exiting an area. AI becomes a powerhouse when used to eliminate false positives from shadows, foliage or animals, by only triggering the analytics when the correct type of object is detected, such as a person or vehicle. The bar is raised further when a deeply integrated AI solution allows additional descriptive metadata search parameters to speed forensic investigations, such as searching for clothing color, or if the subject had a bag, glasses or hat.

AI presents a perfect solution to compensate for unmanned environments or those with limited staffing, or the loss of vigilance after looking at a screen too long. AI can help us not only watch continuously, but also feed systems that are able to sort, organize and categorize massive amounts of data in a way that human operators cannot. It can do so far more reliably than traditional video analytics ever did.

When it comes to protecting assets and people, real-time alerts generated by a video management system (VMS) enable security teams to be more proactive rather than reactive as events unfold in real time. Because AI-powered analytics eliminate false alarms, they can more accurately determine incidents that require further investigation by operators. Thanks to the extra data AI-based cameras can capture, analytic rules can be enhanced with more sophisticated logic and customization for precisely what an end user requires. For example, we can tell a camera to ignore all cars, but to alert us when a person comes to the door. AI can help us count objects like people or cars more precisely than ever. This includes the ability to count objects accurately even when they partly "occlude" or pass in front of each other. This is key since it allows use cases like people counting from more sensible camera view angles. This is far superior to conventional people counting techniques, which require a top-down view to avoid occlusion, and which give a less useful camera view when you want to identify faces as well.

POST-EVENT FORENSIC SEARCH

When it comes to post-event forensic searches, AI-based cameras are in a league of their own. Additional descriptive metadata about objects is captured within each frame. Because the metadata is small, it adds very little to the overall bandwidth and storage requirements.

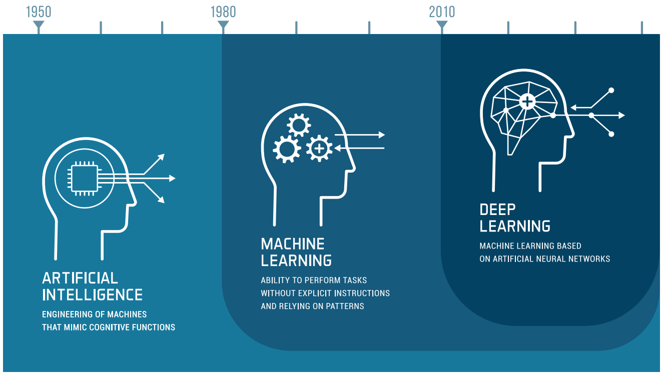
That metadata, which might include descriptive characteristics of objects like the color of a person's shirt or pants or their approximate age and gender, enables a VMS operator to quickly search through video to find a particular object or person. A search that might have taken security staff hours or days to complete now takes only seconds when the search includes additional metadata provided by an AI camera.

GOING BEYOND SECURITY

Although people counting, heat maps and queue management analytics have existed for some time, they too have been subject to the inherent inaccuracies of pixel-based motion detection. Conversely, AI-based object detection delivers profoundly accurate data and metrics for operations, sales and marketing teams looking for insight on everything from retail store performance to ensuring process efficiency and operational compliance.

As a result, these cameras have become an indispensable tool for business operations. Depending on the business, the value proposition for such data can be a game-changer worth many times the cost of the system.

For customers with more sophisticated data analysis needs, camera metadata is accessed and combined with other data. It is processed by other platforms for sophisticated visualization and data mining. This allows technology partners to access the aggregated data into their own charts, graphs and exception reports powered by specialized software they may already be using. There are familiar use cases spanning multiple industries that require linking data from access control, intrusion, point of sale systems, staffing data, schedule data, weather data and many other data sources. The potential for this unified data to create comprehensive business solutions is substantial.


1950
1980
2010
ARTIFICIAL INTELLIGENCE
ENGINEERING OF MACHINES THAT MIMIC COGNITIVE FUNCTIONS
MACHINE LEARNING
ABILITY TO PERFORM TASKS WITHOUT EXPLICIT INSTRUCTIONS AND RELYING ON PATTERNS
DEEP LEARNING
MACHINE LEARNING BASED ON ARTIFICIAL NEURAL NETWORKS

elenabsl/Shutterstock.com

> "It is also important to remember that what differentiates today's technology from true AI is that machine learning and deep learning algorithms cannot learn new things by themselves."

Since video cameras are already well accepted and commonplace, the opportunities for them to evolve into unobtrusive, important data gathering tools for business and operations intelligence will only continue to grow. Operations and marketing departments may also find common ground when budgeting for a system that can serve the needs of both departments.

BENEFITS OF AI ON THE EDGE

AI-based analytics can run on the edge or in a server, but there are significant aspects to each method of deployment that should be considered. With AI on the edge, valuable events and other metadata generated at the camera must be gathered from many endpoints and that data must be aggregated together to enable clear visualization of the trends and anomalies identified. This can be done on a lightweight local server that also runs the VMS. Running AI analytics at the camera significantly reduces the overall cost of the equivalent server resources required to run AI-based analytics since edge-based analytics run before video is compressed and streamed.

Running AI on a server requires that the video stream be first decoded which requires CPU/GPU resources that can scale dramatically as stream count increases. While the power of a server far outweighs what a camera can provide, there is a point of diminishing returns when electing to do everything on a server for all, but the most demanding processing. For that reason, a hybrid approach, in which AI analytics are performed on the edge and the lightweight data results are sent to an inexpensive server or workstation for aggregation and display, will remain a popular choice for some time.

__Aaron Saks__ is the product and technical manager at Hanwha Techwin America.

VICON

The Science of Sherlock

How modern-day crime solvers are putting technology to the task

By David Petrook

Sherlock Holmes is known the world over for his amazing use of, induction, deduction, forensic science, elementary observation, and logic to successfully investigate and crack crime cases. Although a fictional character born out of Sir Arthur Conan Doyle's imagination, Holmes has inspired generations of intellectuals to think analytically and scientifically, and his crime-solving methods adopted by police forces around the world, and with good reason.

The many complexities of modern-day criminal investigations, mounting case volumes, and vast troves of data have given rise to the next generation of crime analysts. With the proper tools, modern-day Baker Street detectives are making great strides in both preventing crimes and solving more cases and doing it all much more quickly.

The huge amounts of data available from video surveillance, body-worn devices, traffic cameras and other IoT devices means there is more real time and historical evidence for police to work with than ever before. Despite this, clearance rates, or the percentage of crimes that are resolved (but don't necessarily result in a conviction) haven't changed.

In fact, over the last few decades, where focus has turned to prevention, clearance rates for homicide cases in the United States have remained fairly constant at about 64%. Even for fictional hero-detective Sherlock Holmes, it would be difficult to process the vast amounts of information to understand which pieces really matter. Tried-and-true policing techniques supported by modern-day technologies have shown dramatic improvements in cities around the world.

Chicago for instance, has made enormous strides using the latest technology to help improve safety and responsiveness in some of the cities' most at risk neighborhood, decreasing violent crime by 24% and shootings by 70%. In this article, we go behind the scenes to see how the modern-day Sherlock Holmes is using technology to help solve cases, catch criminals and enhance the safety of our streets.

Crime analysts are proving to be an indispensable asset in improving and accelerating police work and are earning their place as valued consultants to many city departments large and small. The role of crime analysts is to identify trends and make recommendations based on their observations. Balancing more reactive, day-to-day crime solving with analysis, and re-opening old, cold cases to apply new data analysis techniques, they have changed the face of criminal investigation.

While they are surely employing Sherlock-like techniques, the volume of qualitative and quantitative data available to analysts, combined with modern technology to speed up analysis, changes the game. It not only allows them to help solve cases faster and catch criminals more quickly, but also apply modelling to identify patterns and abnormalities to support pro-active policing activities. Using modern technology tools, crime analysts can now also identify and analyze both short-term and long-term trends and patterns to help police and others target problems and create long-term solutions, and ultimately keep our communities and cities safer.

CHALLENGES CRIME ANALYSTS FACE

Traditional crime analysts are tasked with several functions. The first is detective work to find possible links in a crime. Based on any leads they have, they try to pinpoint any suspects' device readouts, analyze network connections and multiple databases to follow paths and look for any relevant clues that may shed more light on the case. If, for instance, a blue SUV with local plates is involved in a crime, and they know that other arrests were made recently involving a similar car, they can dig deeper to see what links, if any, there may be between them.

SAS Technologies Corp.

M/WBE
MINORITY/WOMEN-OWNED
BUSINESS ENTERPRISE

Offering State-of-the-Art Security Solutions For Commercial And Residential Properties for over 15 Years.

- **People Management**
  - + Access Control
  - + Visitor Management Systems
  - + ID Badging
- **IP Video Surveillance**
  - + Video Management Systems
  - + Network Video Recording
  - + IP Cameras
- **Telecom Solutions**
  - + Unified Communications
  - + IP Endpoints
  - + Voice Media Gateways

+ Complete System Design and Integration Services

See why consultants, IT experts, project managers, and installers work with our experienced team of security professionals to complete projects efficiently and achieve a level of excellence that is second to none.

Find out how SAS Technologies Corp. can help you find the right technology solution to meet your security needs and protect what matters most- your people, your business and your property.

Contact us today for your free security assessment:
Call us at **516-887-0022** or Email **info@sastechs.com**

SAS Technologies Corp.

375 Sunrise Highway, Suite 5, Lynbrook, NY 11563
www.sastechnologies.com
Licensed by the N.Y.S. Department of State NYS License # 12000291690

> "In this article, we go behind the scenes to see how the modern-day Sherlock Holmes is using technology to help solve cases, catch criminals and enhance the safety of our streets."

Secondly, software and data assisted crime analysts search for significant patterns in crimes in order to crack cases. If law enforcement, for example, is looking to home in on a drug network, crime analysts work to piece together who the suppliers are, who the buyers are, who the movers are, etc. Using their arrest and management systems records and data, they can better figure out how a criminal organization functions, and how to put in place strategies to move the case forward. Proof that modern technology is a game changer, one of the key contributors to improved clearance rates has been the application of new technologies and techniques to old, cold cases.

While the techniques for criminal investigations (with the exception of forensics) have not really changed that much, the ability to establish links between four or five pieces of data that previously would have taken days or weeks to find, can now be done in minutes or a few hours. This means that cases that would have previously sat on the shelf are more likely to be investigated and solved quickly.

Crime analysts' third function is to look for generic or statistical trends, such as a rise in homicides or assaults in a specific area. This helps them create maps and charts for the police department's executive team to get a clearer picture of what's happening in their precinct. Oftentimes, someone had to collect all the data and input the information into an Excel spreadsheet in order to see if the homicide and assault percentage were up or down over previous periods. With modern solutions, algorithms are now used to highlight statistically significant changes in the data that highlights changes in crime patterns.

PUTTING TECHNOLOGY TO TASK

Coordinating and collaborating all the data collected from myriad sources such as video surveillance footage, Automatic License Plate Recognition (ALPR), and information provided by private citizens or businesses is a huge undertaking. Gathering all that data from varying sources and interpreting it to make better, quicker, efficient decisions can be made.

Many crime analysts are turning to innovative technology solutions, such as Genetec Citigraf™. This decision support system empowers public safety departments to build a deeper, data-driven understanding of what is happening in their city. Citigraf collects and manages information provided by integrated CAD (Computer Aided Dispatch) systems, CCTV footage, ALPR data, RMS (Record Management Systems) and more in a single pane of glass, to immediately identify and display the exact location of an event using icons on a map from a built-in geographical information system (GIS). Thanks to a collaborative integration with gunshot detection technology. When a gunshot has been detected, response teams are notified with a map located gun icon coupled with nearby cameras. With this combined information, Rapid, actionable alerts to help law enforcement quickly intervene and take control of dangerous situations, stop crimes, and save lives.

Law enforcement has a new way of measuring, reporting, and determining the impact of new initiatives and interventions to increase overall public safety. Analytics dashboards, heat maps, and data analysis provide valuable insights into how crime and events move and change throughout a given area, over time. The collective, data-driven analytics give police departments forward looking, predictive indicators of potential issues within the city's coming operations cycle, helping law enforcement define and modify patrol beats and staffing requirements.

Trusted technology solutions can continually analyze information from thousands of sensors and data points, assisting frontline public safety teams by bringing to light relevant events and information. This allows responders to prepare for what they can expect before arriving on site and allows individuals and agencies to see what is happening across their jurisdictions.

The International Association of Crime Analysts reports that technology has proven instrumental in solving cases, developing effective strategies to prevent future crimes, educating the public, and allocating resources and prioritize patrol investigations. The result is often a reduction in crime rates and the development of proactive public safety strategies.

STRATEGIC DECISION SUPPORT CENTERS (SDSCS) FACILITATE THE USE OF MORE SOPHISTICATED TECHNOLOGY

We all need workspaces with easy access to the right tools to help us get the job done. While Sherlock Holmes carried out his own practice at his Baker Street home, the new modern crime lab typically features known as Strategic Decision Support Centers (SDSCs). These multi-screen equipped crime-fighting nerve centers facilitate decision making through increased data and intelligence and clearer context and correlation for better understanding. They use dedicated hardware and software solutions and help local police departments develop proactive investigative and public safety strategies. They function to give crime analysts and police departments more comprehensive local intelligence and deeper insight so that they can use r personnel and resources more effectively while improving officer safety.

While technology is proving a powerful tool in crime solving, it is and will always be the human element that ultimately cracks criminal cases. Just as Sherlock Holmes relied on his own powers of observation, induction, deduction, logic and reasoning, so too do modern-day crime solvers trust their wits to uncover clues and find the truth. Leveraging technology to help in the process is simply a smart choice and, well, elementary, my dear Watson.

__David Petrook__ is a product group director at Genetec.

SECURITAS
Electronic Security
+
M
FEMORAN
SECURITY SOLUTIONS
=Stronger Together

Safer Cities

As populations increase so do the complexity of challenges related to crime, traffic and more

By Adam Lowenstein

A lot has changed in cities around the globe in the last few years. According to the United States Census Bureau, population densities across the United States continue to shift from larger established metropolitan areas to smaller cities and into the suburbs. This is increasing the number of urban centers with sizeable populations.

COMPLEX CHALLENGES

As the numbers of new arrivals continue to increase in these locations, so do the number and complexity of challenges they face relative to crime, traffic, municipal services, public schools and housing. These are all longstanding issues that often drive people to relocate and are now emerging across an even larger number of cities and municipalities.

Fortunately, more cities continue to implement new advanced technologies to collect data for applications ranging from law enforcement, traffic and crowd control to environmental management, public services and operations management. With the continued deployment of advanced software management platforms and intelligent edge devices, data is being collected and processed from a myriad of public and private sources.

Integrated physical security systems continue to be one of the most efficient and effective ways to achieve wide-area situational awareness. In fact, many locations around the world have followed the early examples set by cities such as London or New York, where cameras provide coverage of areas that would otherwise require on-site personnel to observe events and behaviors.

Breakthroughs in physical security systems, such as integrated video and access management platforms, cameras with artificial intelligence (AI), and mobility solutions like in-vehicle camera systems and body-worn cameras, continue to revolutionize the way cities protect and serve the public. In addition to greatly increasing overall security and safety, these systems are providing new sources of data to enhance public services and the quality of life for residents.

USING VIDEO AS A PROACTIVE SOLUTION

The quantity and quality of video cameras deployed plays a huge factor in their collective effectiveness. When properly deployed across a centralized surveillance network, public officials effectively and easily monitor even the largest and busiest municipalities. Internet protocol (IP) video has become more affordable than ever and is the best option for installing a new system or upgrading an existing one.

Having a robust, extensive security camera network feeding into a centralized command center provides greater visibility of potential trouble and increases the ability to respond quickly and appropriately. An enterprise-grade VMS can support thousands of IP cameras with an unlimited number of authorized clients able to access live and recorded footage across the network.

Video analytics, whether embedded at the edge or implemented centrally via a VMS, add new levels of intelligent functionality to surveillance systems. With the addition of AI, these systems are quickly evolving from being reactive to proactive solutions.

Zapp2Photo/Shutterstock.com

"... many locations around the world have followed the early examples set by cities such as London or New York, where cameras provide coverage of areas that would otherwise require on-site personnel to observe events and behaviors."

This is increasingly evident given the wide range of AI-driven analytics readily available, including audio analytics for gunshot and scream detection, video analytics for intruder, loitering and cross-line direction, scene change indication to alert system administrators of possible camera tampering, people and vehicle classification, and facial recognition. These smart analytics lead to a wide variety of applications beyond conventional security.

Facial recognition, for example, helps authorities match a person's face to a database of enrolled faces to help identify known criminals. Additionally, video redaction allows law enforcement to blur the faces of persons who have no connection to an incident, when video footage is released to the public. This protects the privacy of innocent parties and saves valuable search and response time.

Analytics can also capture and process license plates, as well as track service and public transportation vehicles passing through a city or municipality. This can improve municipal services greatly as it aids in the recovery of stolen vehicles, the apprehension of people with outstanding arrest warrants or the identification of a person of interest.

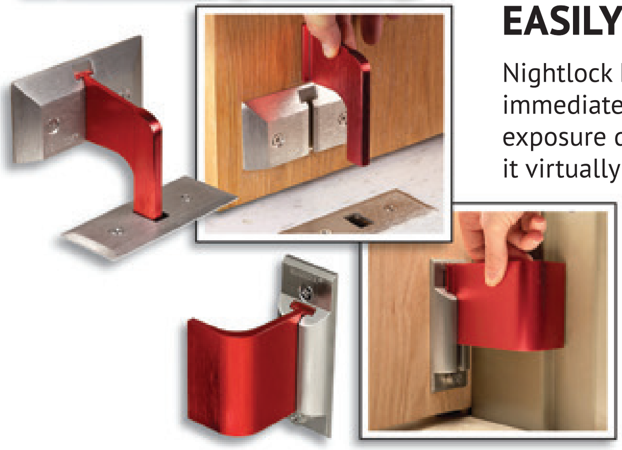
NIGHTLOCK®

LOCKDOWN SAFETY PRODUCTS

- CLASSROOMS
- OFFICES
- SAFE ROOMS

LOCKDOWN DOOR BARRICADES

✓SIMPLE ✓FAST ✓SECURE
FOR EXTREME EMERGENCY SITUATIONS



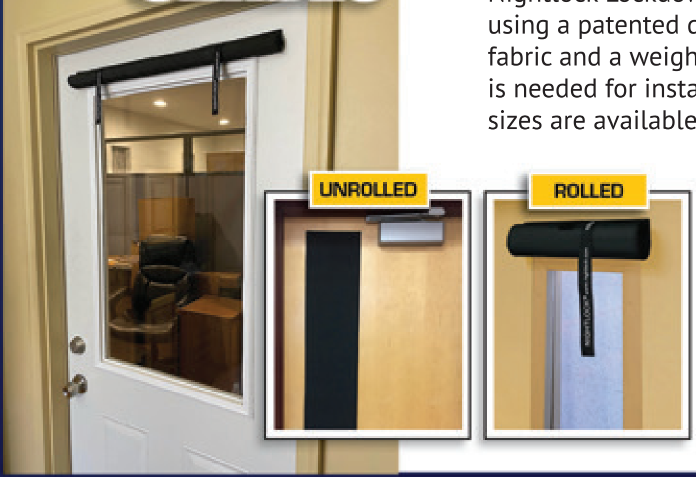
EASILY SECURES A ROOM IN SECONDS!

Nightlock Lockdown Door Barricades allow an individual to immediately lock the door from inside a room, eliminating exposure during a hostile intruder situation. This device makes it virtually impossible for an intruder to breach a locked classroom or office door.

- Simply add this safety device to doors
- Works with outward and inward swing doors
- No need to replace existing hardware
- One time solution - easy to install
- Lockdown in seconds

LOCKDOWN SAFETY SHADES

✓EASY INSTALLATION ✓FIRE RETARDANT
✓QUICK DEPLOYMENT



Nightlock Lockdown Safety Shades are manufactured using a patented design featuring high-quality blackout fabric and a weighted hem bar. No drilling or hardware is needed for installation; 10 standard sizes and custom sizes are available.

- Acts as a deterrent by blocking the view into classroom and office door windows/sidelights during emergency situations
- Cost Effective
- Customizable to fit all door and window sizes
- Installs easily

Helping you be "Lockdown Ready!"

nightlock.com | 855-644-4856 | sales@nightlock.com

GREATER SITUATIONAL AWARENESS

Police departments nationwide are under intense pressure to capture and maintain precise documentation of incidents and events. This is as much a security and safety issue as it is protection against false claims and lawsuits for cities and municipalities.

With the use of new digital technologies, police departments can maintain the integrity of evidence that benefits both citizens and law officers. Gaining situational awareness is critical in helping officers in the field make informed decisions when responding to calls. For example, the adoption of body-worn cameras by police departments is essential for both evidence documentation and risk mitigation.

Body-worn cameras record both video and audio to internal storage drives as well as removable memory cards. The footage can be quickly uploaded and stored on-premises or in the cloud. This allows law enforcement officials to quickly collect and release body-cam footage to the public in high-profile incidents.

IMPROVING TRAFFIC FLOW AND SAFETY

The same video surveillance networks used by police for public safety or city administrators to monitor city services are also ideal traffic-management applications. This is proving to be highly effective in cities around the world for improving traffic flow while also addressing the safety concerns of bicyclists, pedestrians and commuters using public transportation. For example, traffic cameras can detect wrong-way drivers, triggering roadside alerts such as flashing signs, and alert authorities on the ground to intervene before accidents occur.

KEEPING SCHOOLS AND CAMPUSES SAFE

With school violence all too common in municipalities throughout the United States, securing schools, colleges and universities is paramount. This requires integrated physical security systems that allow security staff to know the status of a given school or campus at all times. The ability to prevent assailants or predators from gaining access to schools and campuses is essential for the safety of students, teachers and staff.

Access-control software plays a vital role in these situations; capabilities such as door scheduling, user management, reporting and lock-down functionality help secure academic institutions from attacks. Intelligent video systems can also automatically identify known criminals and offenders and issue alerts when specific scenarios occur in real time, such as when someone enters an area that is off-limits or when a gun or knife is detected.

Empowering cities and municipalities with intelligent integrated systems makes them smarter, safer and more livable.

Adam Lowenstein *is the director of product management at Panasonic i-PRO Sensing Solutions Corp. of America.*

An Uninterrupted Lifeline

Radio communications link emergency responders to enhanced systems

By Mahesh Nanjakla

Kzenon/Shutterstock.com

For a first responder rushing into a building emergency, losing communication with their teams inside or outside of the building can be terrifying. In fact, according to an IAFC (International Association of Fire Chiefs) 2017 survey by Safer Buildings Coalition, 94% of surveyed first responders say reliable in-building communications is critical or frequently important during emergencies.[1,2]

Yet, 98.5% report dead spots in buildings, and 56% have experienced a communications failure over the last two-year period.[1,2] These dead spots and failures not only impact communication but directly affect first responders' safety and, ultimately, the safety of the individuals they're trying to help—as on 9/11, when firefighters and police officers could not properly communicate with each other in the World Trade Center.

POOR SIGNAL STRENGTH

Dead spots within a building for first responder radio communications are caused by poor signal strength, which is impacted by several factors depending on the facility. Low-emissivity glass windows designed to block solar heat can weaken radio signals into and out of buildings. While underground structures, obstructions (such as other large nearby buildings), and building materials, like concrete or metal, can all affect signal strength at a particular location.

Radio communication outages can be avoided for first responders within a building, who might be in a dire situation. Thanks to technology like emergency responder communications-enhancement systems or bi-directional amplifier (BDA) systems, first responders can walk into a building with confidence that their support teams still have their backs.

BDAs are signal boosters that sustain two-way radio communications throughout a facility—even in stairwells, underground tunnels and other typically challenging spaces. A BDA can provide 100% in-building coverage by boosting signals from a public safety radio repeater and distributing them throughout the building using the Distributed Antenna System (DAS). The BDA receives and amplifies transmissions from radios inside to the repeater antenna outside and vice versa, safeguarding reliable two-way communications.

IMPROVING CODE

As a direct result of the World Trade Center disaster in 2001, the National Institute of Standards and Technology (NIST) published recommendations in 2011 to improve code and public safety. Included was a recommendation to update national fire codes to provide reliable radio coverage in buildings. Most current adopted fire and building codes require emergency responder radio-signal strength, and coverage measured in all new and some existing construction. The International Fire Code (IFC) has been adopted by many states, requires acceptable signal coverage throughout 95% of the building in all areas on each floor in new buildings, while the National Fire Protection Association (NFPA) requires 99% building coverage in critical areas and 90% in general areas.[3] Meeting these code requirements can help prevent delays in acquiring a Certificate of Occupancy from Authorities Having Jurisdiction (AHJs), such as a fire marshal, once construction is complete on a new facility.

Deploying a BDA system not only supports compliance but also helps protect first responders and makes their job easier. It is important to check the specs though. Not all systems comply with Underwriters Laboratory (UL) code UL 2524. The UL product listing creates a performance standard for ERCES/BDA systems and assures AHJs, architects and engineers that the system works the first time and every time in accordance with IFC and NFPA regulations.

Every second counts in an emergency, and a communication failure can put lives at risk. Installing a BDA system that meets all applicable codes can help keep occupants safe while also protecting first responders who are putting their own lives on the line.

__Mahesh Nanjakla__ is the offering management lead, Emergency Responder Communication Enhancement Systems (ERCES), Honeywell Fire Systems

1. Safer Buildings Coalition, International Association Of Fire Chiefs (IAFC), IAFC Survey 2017, December 2017 [accessed July 2, 2021]
2. Creative Commons SBC In Building ERRCS Survey of IAFC Members, Creative Commons BY2.0
3. National Fire Protection Association, NFPA 1221: Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems, Current Edition 2019 (accessed July 2, 2021)

Kingston TECHNOLOGY

Manage Threats. Reduce Risk. *Kingston Is With You.*

TAA COMPLIANT

FIPS Level 3 Certified 140-2

AES-256 ENCRYPTION

With data breaches and regulations on the rise, it's important to protect sensitive information with data security standards. Protect company and client's sensitive data with Kingston's ultra-secure line of USB encrypted flash drives. Designed to protect data with the latest storage security, the drives are available in a wide range of models. Features include Customization, Anti-Virus protection and Management Solutions.

Visit **kingston.com**

Some of the listed capacity on a Flash storage device is used for formatting and other functions and thus is not available for data storage. As such, the actual available capacity for data storage is less than what is listed on the products. For more information, go to Kingston's Flash memory Guide at kingston.com/flashguide.

Connecting Networks

Creating safer workplaces during the COVID-19 pandemic

By Shahar Feldman

Andrey Suslov/Shutterstock.com

The Internet of Things (IoT) is turning dumb houses into smart homes. It is also revolutionizing access control systems for all types of commercial buildings, from small offices and retail shops to enterprise campuses and sprawling factories. Although digital locks, keyless entry, RFID card readers and security cameras have been around for many years, IoT technology has transformed building automation, bringing a new level of data-driven security, control, reliability and safety to the workplace.

The convergence of ultra-low-power IoT devices, cloud connectivity and advanced security technologies has enabled developers to create highly sophisticated, versatile and resilient access control systems. The ongoing Covid-19 pandemic has also added a new and unprecedented dimension of complexity to the workplace as evolving health screening regulations require even greater scalability, security and upgradability for access control systems.

To ensure the security of a building, its occupants and its contents, network and security system architects must consider all points of entry, anticipated threats and the ever-changing credentials of those seeking access to a building or campus.

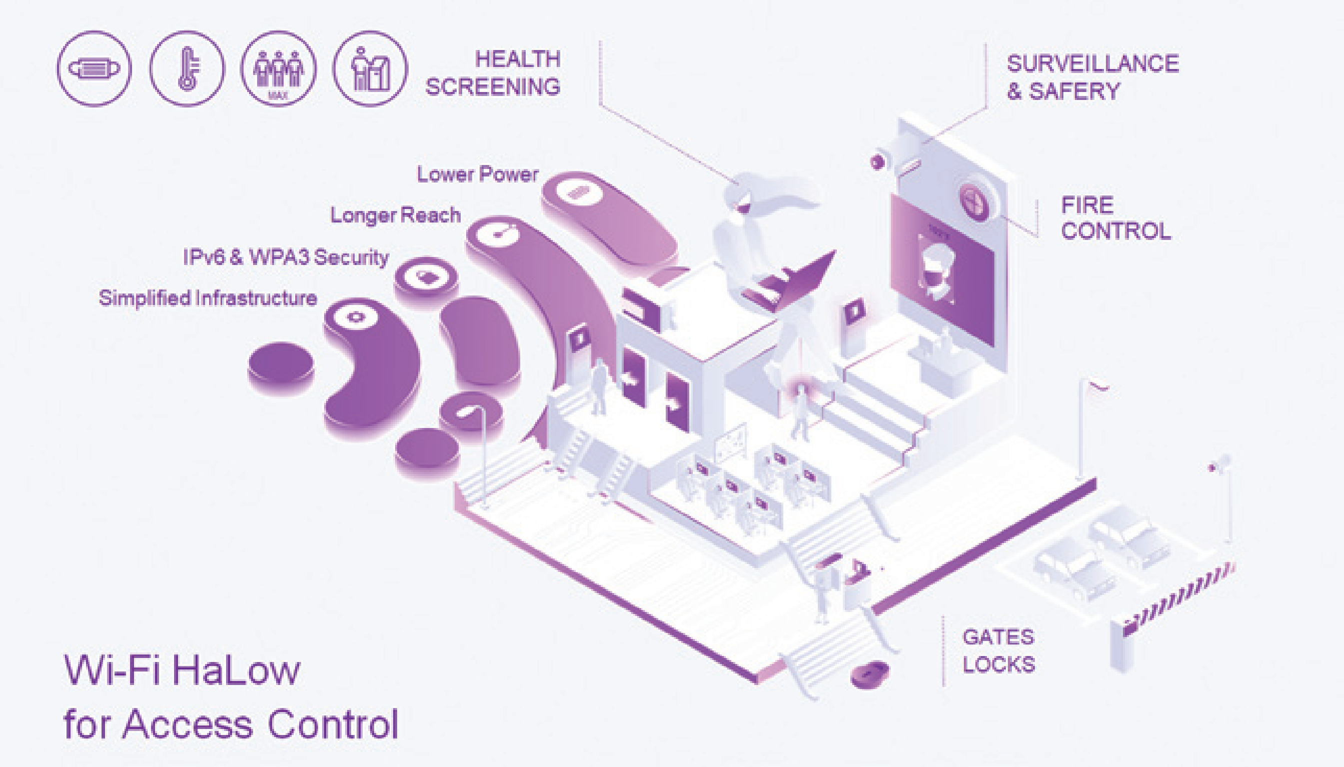
A comprehensive access control system can include a multitude of devices such as smart locks, security sensors, keypads, card readers, surveillance cameras, gates, health screening kiosks, and a wide array of sensors to help monitor maximum occupancy, elevated body temperature and facial mask compliance. Integrated through a robust network, these devices provide real-time status and control of the entire system.

Whether the scale of an access control system is a set of smart home door locks, health screening stations at building entrances or hundreds of secured doors in a large hotel or office, the costs and complexity of maintaining and upgrading the control network continue to increase. Whether running on an on-site computer or hosted by a cloud-based remote monitoring center, an access control system will benefit from using low-power wireless connectivity and IP, to unite all of the access components into an IP-based network that can extend across long distances inside and outside of a building.

Current best practices make it possible to implement robust wireless networks that deliver the flexibility and scalability to aggregate a multitude of devices under a single standard: Wi-Fi HaLow.

WHAT IS WI-FI HALOW AND WHY IT IS A GAME CHANGER FOR ACCESS CONTROL

Wi-Fi HaLow is a low-power, long-range version of the popular Wi-Fi standard that provides 10 times the range, 100 times the coverage area and 1000 times the volume of traditional Wi-Fi technology. These attributes make it an ideal wireless backbone for today's access control systems, especially those serving large enterprises with multiple entry points, locks, cameras and many other security devices.



The IEEE 802.11ah protocol was developed to meet the low-power, long-range connectivity requirements of IoT devices. The standard was ratified in 2016, and dubbed "Wi-Fi HaLow" by the Wi-Fi Alliance. The commercial rollout of Wi-Fi HaLow technology is well underway, with transceivers, SoCs and modules available now to system developers, and a certification program is expected in 2021.

Wi-Fi, in all of its manifestations, is the most pervasive short-range wireless protocol used today in homes, offices and public spaces. As Wi-Fi technology continues to evolve, the rapid growth of the IoT has sparked a rethinking of Wi-Fi, exposing technological gaps and revealing new ways the protocol can progress to meet the needs of our increasingly connected world.

Wi-Fi HaLow fills these gaps by providing an ultra-low-power wireless solution that connects larger numbers of IoT devices at much longer distances than conventional Wi-Fi, and at a higher data rate and security level than alternatives like Bluetooth, Zigbee or Z-Wave. Wi-Fi HaLow supports both indoor and outdoor applications, such as battery-powered wireless doorbells, security cameras, drones and surveillance systems. The lower the frequency, the better the penetration, and as a sub-1 GHz protocol, its RF signals can pass through walls and other barriers more easily than competing 2.4 GHz options, let alone even shorter range 5 GHz and 6 GHz radios. A single Wi-Fi HaLow access point (AP) can also reach thousands of connected devices, bypassing complex, bandwidth-constrained mesh networks, thereby simplifying installation and minimizing total cost of ownership.

The Wi-Fi HaLow standard's unique combination of native IP support, high data rates, low latency, exceptional energy efficiency, long-range connectivity and security features makes it an ideal protocol choice for integrated access control systems.

In addition to supporting smart locks, security cameras, card readers, gates and myriad wireless sensors, these systems also must support emerging security and health screening devices deployed in response to the COVID-19. For example, the seemingly simple act of entering the front door of an office involves multiple decisions: confirming a person's identity, validating the security profile, and assessing the current environment in which a person seeks access.

Adding to the complexity of existing secure access protocols, new COVID-19 screening procedures require low-latency, session-oriented connections of multiple inputs and outputs supported by an integrated system controlling hundreds or even thousands of connected devices. Wi-Fi HaLow is an ideal wireless protocol for these increasingly complex and diverse access control tasks.

THE HALOW EFFECT: SIMPLIFYING AND SCALING ENTERPRISE ACCESS CONTROL SYSTEMS

Security and access control devices in large-scale commercial buildings and campuses typically include electronic strikes, magnetic plates, hybrid smart locks, external keypads, RFID card scanners, and egress triggers on the inside of entries such as passive infrared (PIR) motion detectors and request-to-exit (REX) buttons. With new COVID-19-related health policies and procedures in place, many commercial buildings and offices have added health-screening kiosks, thermal cameras to monitor body temperature, and video cameras to help ensure health compliance such as wearing a facemask.

In a typical access network, a PC-based security system connects

The NEW
SMART CHOICE

GARRETT

"All of these devices must be integrated through a robust network that provides real-time status and control of the entire system."

to a control station, which in turn connects to low-voltage power transformers that energize locks or change their states. Many of these connections traditionally use wireline technologies, such as PoE, which provides control signals and power to a gateway controller located up to a maximum of 100 meters away. Some access control systems use a hybrid distribution network of PoE and RS-485 cables to reach proprietary access points connecting to wireless smart locks on the doors of nearby rooms.

Network and security system providers serving commercial buildings are increasingly turning to wireless technology as an alternative to wireline when it comes to scaling the access control system and adding new devices or rerouting existing network connections. Wireless connectivity makes it easier to expand or upgrade these systems without the expense and hassle of running new cables to often hard-to-reach places.

Wireless protocol options include those operating at 2.4 GHz or sub-GHz frequencies and those that support point-to-point, star and mesh network configurations at various power levels, data rates and ranges. The challenge for developers is to find a wireless "sweet spot" that minimizes system cost and complexity without compromising coverage, performance, latency, security or energy efficiency.

Wi-Fi HaLow can help simplify enterprise access control systems by reducing the costs of security network infrastructure, as well as the time and expense of cable installation. The protocol's energy efficiency helps reduce maintenance costs by minimizing the frequency of battery changes for IoT devices, and its fast data rates and low latency also streamline over-the-air (OTA) firmware updates. Imagine a scenario without HaLow where hundreds of hotel room door locks require a security firmware patch to be loaded by going door by door.

In addition, Wi-Fi HaLow uses a simplified star network capable of connecting large numbers of wireless sensors, health compliance systems and door locks without the need for intermediary proprietary controllers or sub-gateways to connect to the Internet. The access control network can be as simple as a Wi-Fi HaLow AP connected to a single PoE cable on each floor of a building, enabling each lock to operate as a locally controlled or cloud-based device.

Wi-Fi HaLow can also serve as a backhaul network to replace the tangle of low-speed cables running between the backbone network and clusters of connected devices. When an IT administrator needs to add new devices to a wireline network, installing or rerouting PoE and RS-485 cables can drive up labor and materials cost. Whether adding video, thermal imaging or other multi-factor authentication capabilities to a wireless smart lock, Wi-Fi HaLow is fully capable of handling the task with greater ease and at lower cost than upgrading wireline networks.

With its long-distance sub-GHz signal reach (up to 1 km), the benefits of Wi-Fi HaLow can also extend well beyond the interior of a building to control peripheral access points outside at the edge of the property. The protocol can connect multiple sensing devices, such as motion detectors and proximity sensors that provide early warning of approaching threats, as well as thermal imaging and facial recognition systems that help ensure the health of a building's occupants. Other long-range wireless networks such as LoRa and Sigfox can only support very low data rates for small packets of data.

Wi-Fi HaLow solves coverage and range issues with a single, simplified standard. For example, one Wi-Fi HaLow AP can support up to 8,191 devices, more than the number of rooms in the world's largest hotels. The sub-1 GHz RF signals can penetrate walls, doors, windows, ceilings, floors and other obstacles. Wi-Fi HaLow signals can extend farther than existing versions of Wi-Fi and other short-range wireless standards, with ranges that can reach devices that would normally require costly wireline connections. Because it is part of the IEEE 802.11 standard, a Wi-Fi HaLow network can also coexist with Wi-Fi 4, Wi-Fi 5 and Wi-Fi 6 networks without impacting RF performance. Wi-Fi HaLow is also an inherently secure wireless protocol. Its native support for IP and the Wi-Fi Protected Access 3 (WPA3) standard enhances the security of OTA firmware updates and cloud-based connectivity.

CONNECTING THE FUTURE OF SECURE ACCESS CONTROL NETWORKS

With the rapid rise of the IoT, access control systems for commercial buildings and offices are evolving to meet market demands for better security, energy efficiency, lower operating costs, and tenant convenience, health and safety.

The persistence of the COVID-19 pandemic has not only upended our lives, but it has also impelled IT and HR professionals to rethink access control best practices and add new health monitoring and screening technologies to the workplace. Even when the pandemic finally abates, it's likely that enterprise access control systems will continue to use some of the new monitoring systems in place to ensure the safety of building occupants and their guests.

The advent of Wi-Fi HaLow will help network architects and access control developers solve a number of building automation challenges. Wi-Fi HaLow overcomes the distance limitations, network congestion and higher power consumption of conventional Wi-Fi and other 2.4 GHz protocols, as well as the limited number of wireless devices that can be connected to a single access point.

These limitations impede new IoT-centric business models that are emerging across industries to enable a truly connected world. By addressing these challenges, Wi-Fi HaLow is gaining momentum in the market as a standards-based wireless solution that delivers the right balance of long range, high capacity, low power, high data rates and low cost of deployment.

***Shahar Feldman** is the vice president of marketing at Morse Micro.*

Temperature-Controlled Enclosures

Protect Fire Panels, NVRs, Wifi, Security and Electrical Equipment from Weather and Vandals

Over 80 Models In Stock

Rack Enclosures include an internal rack system

Outdoor NEMA 4 and stainless-steel or polycarbonate NEMA 4X Models available with Thermostatically Controlled AC and/or Heat

Outdoor NEMA 3R Models available with Thermostatically Controlled Fans

Indooor NEMA 1 Models available with Continuous Duty Fans

Available with or without windows

Mier
PRODUCTS, INC.

PROUDLY MADE IN THE USA ★ ★ FOR OVER 30 YEARS!

You name the box, can, cabinet or enclosure: *Mier Products has you covered!*

1-800-473-0213 | info@mierproducts.com | www.mierproducts.com

SECURITY TODAY SOLUTIONS

Compiled by Ralph C. Jensen, Editor-in-Chief

Support Healthy Buildings

LenelS2 supports Carrier's Healthy Buildings program and the safe return to work. LenelS2 has introduced a COVID-19 Contact Notification subscription-based service for businesses and other organizations using LenelS2's OnGuard® or NetBox™ access control security systems along with LenelS2's BlueDiamond™ mobile credential app. This new service complements LenelS2's touchless building access solutions by providing BlueDiamond-credentialed users with the ability to assess their health symptoms, receive real-time social distancing reminders and anonymized notifications if they have recently come into contact with a user that self-assessed as being positive for COVID-19.

Managing Lock Systems

CyberLock Inc., a global leader in key-centric access control solutions, announces the release of CyberAudit Web 9.4! CyberAudit-Web (CAW), the software suite for managing CyberLock systems, provides an intuitive interface to assign keys, set expirations, monitor personnel, configure access schedules, and more. The latest release, CAW 9.4, introduces interface upgrades, new security enhancements, mobile geolocation capturing to enrich location graphics, and powerful capabilities for 2nd generation CyberLock cylinders. This myriad of new features will enhance the CyberLock experience for users across the globe. CAW 9.4 includes a multitude of features intentionally designed to support the unique needs of high-security customers.

Built-in Storage

Paxton Inc. is pleased to announce the updated Paxton10 camera offering, adding a CORE Series of cameras alongside our existing PRO Series. The Paxton10 system combines access control, video management, and free Bluetooth® smart credentials, feature-rich software and now, the CORE and PRO Series of cameras. The new CORE Series cameras feature edge processing for ultimate scalability, built-in edge storage, and plug-and-play installation. The addition of the CORE Series gives installers new hardware, more choices, and better value than ever before. Paxton has also reduced the price of our PRO Series cameras providing a tailored video management solution at a cost-effective price.

Wireless Ethernet Solution

ComNet is announcing the introduction of its Generation 4 line of NetWave® wireless products that offer greater performance and increased stability in applications where throughput and increased bandwidth is increasingly important. The NW1 Gen 4 can exceed 500Mbps throughput under ideal conditions, accommodates 10/100/1000Mbps Ethernet, it also now has IEEE802.3at PoE Compliant PD on port 1 and an IEEE802.3af power source (PSE) available on port 2. Distance is specified for applications of up to 2 miles. The new hardware features a high-performance chipset with a quad-core CPU, designed to meet the high throughput demands that surveillance applications require.

Systems for Global Customers

Barrier1 Systems is working with global customers in the public and private sectors to install innovative new solutions that leverage the unique capabilities of Cepton's Helius system, which combines a network of Vista®-P lidar sensors with edge computing and advanced perception software, to deliver real-time, anonymized, 3D object detection, classification, tracking and velocity. The partnership demonstrates the versatility of Cepton's lidar technology. This will show how smart lidar solutions are by increasing security and safety, in various types of public and private commercial spaces and facilities. Barrier1 Systems has combined its barrier control systems with Helius to monitor the speed and direction of vehicles approaching entrance or exit points.

Tools for Installers, Technicians

Triplett Test Equipment highlights the innovative 8150 CamView5 IP Pro, a high-resolution, all-in-one security camera tester with Wi-Fi hotspot. The compact, lightweight CamView5 IP Pro is designed for the installation and maintenance of IP cameras, analog cameras, TVI, CVI, and AHD cameras, as well as for testing 4K H.264 /H.265 video. The CamView5 features HDMI output and a built-in Wi-Fi hotspot for easy connectivity with Wi-Fi-connected cameras. With its combination of a 5-inch touch screen and key buttons, the CamView5 IP Pro is user-friendly. This user-friendly design, portability, and many other functions make the CamView5 IP Pro, an affordable and essential tool for all installers and technicians.

AD INDEX

FREE PRODUCT INFO

Quick, Easy and Direct...get the info you need NOW!

Go online to www.securitytoday.com/productinfo to request free information from advertisers in this issue.

ADVERTISERS

Company Name	Page
ADT Commercial Security	23
AirShip Industries	13
Altronix	3
ASSA ABLOY DSS	21
Axis Communications, Inc	67
BCDVideo	25
Boon Edam Inc	28
Brinks Home Security	27
Camden Door-Touchless Waves	11
CEIA USA	29
ComNet Communication Networks	35
Controlled Products Systems Group	37
CyberLock, Inc.	7
Dakota Alert	38
Delta Scientific	39
Door King	51

Company Name	Page
Dotworkz	9
FARPOINTE DATA	15
FARPOINTE DATA	31
Garrett Metal Detectors	57
Genetec Inc	17
Hanwha Techwin America	33
IDIS Co., Ltd.	36
IP Video Corporation	19
Kingston Technology	53
LifeSafety Power, Inc.	55
MIER PRODUCTS INC	59
NIGHTLOCK	49
Panasonic Corporation of North America	68
Paxton Access, Inc.	61
Safety Technology Int'l, Inc.	63
Salient Systems Corporation	5
Salto Systems	41

Company Name	Page
SAS Technologies	45
Securitas Electronics Security, Inc.	47
Security Today	50
Theia Technologies	32
TREND Networks	2
Vicon Industries, Inc.	43
Viking Electronics	66
Winsted Corp.	65

Security Today Solutions

Company Name	Page
Barrier1 Systems	60
ComNet	60
CyberLock Inc.	60
LenelS2	60
Paxton Inc.	60
Triplett Test Equipment	60

Reprints: For single article reprints (in minimum quantities of 250-500), e-prints, plaques and posters contact:

PARS International
(212) 221-9595
1105reprints@parsintl.com
www.1105Reprints.com

List Rental: This publication's subscriber list, as well as other lists from 1105 Media, Inc., is available for rental. For more information, please contact our list manager:

Marie Briganti, Merit Direct
(914) 368-1023
MBriganti@MeritDirect.com
go.meritb2b.com/1105

Media Kits: Direct your Media Kit requests to:

Lynda Brown
(972) 687-6710 (phone)
(972) 687-6750 (fax)
lbrown@1105media.com

With Kate Adam

Once and For All

Anyone who knows Disney at all probably remembers the movie "Fantasia," and relating to Mickey Mouse in "The Sorcerer's Apprentice," as he cast a spell on a broom to do his chores for him and make his life a little easier. SPOILER ALERT: it did not go as Mickey intended, with the broom ultimately cloning itself ad infinitum and causing a massive flood that almost drowned Mickey.

The Internet of Things (IoT) offers parallel benefits, but also a parallel lesson. On the one hand, IoT makes our everyday lives easier. Smart speakers make it easy to play different types of music in different rooms, and people feel safer when their home is watched 24/7 by a smart security system. However, IoT represents a substantial risk for the networks to which they are connected.

IT IS ABOUT THE SOFTWARE

IoT software — all software — is written by humans, which means it will never be perfectly secure code, even if it's created under the most idyllic secure software development lifecycle implementation. Unfortunately, IoT software (especially consumer IoT) tends to be less secure, which means easy-to-exploit vulnerabilities and more of them.

Consumer IoT software is an interesting problem because it's not as though manufacturers are intentionally releasing smart thermostats, remote control drones or connected coffee makers that will "go rogue" and start sending sensitive data to attackers. Secure coding practices are more expensive and security is not accountable. The fact is that currently, secure code is not part of consumer IoT buying criteria.

SECURING IOT: WHAT DOESN'T WORK

For devices where the code may not be the most secure, endpoint agents that detect and stop exploits and malware deployed on the device itself, to help keep it safe. The agents are not deployed on IoT devices for a few reasons:

- Endpoint agents are too expensive, financially and operationally, for consumers to purchase, and install, and manage themselves.
- Endpoint agents are for specific operating systems and IoT devices use such a wide variety of operating systems that it is not feasible that an agent will specifically apply to each one.

Some IoT manufacturers will issue software patches to fix vulnerabilities and bugs, but deploying and applying patches comes with some operational overhead. For example, for someone to upgrade their phone OS they likely have to start the install manually and then restart their phone. It is annoying, so most consumers will put off software upgrades until forced to apply them.

For Industrial IoT (IIoT), patching and endpoint agents are a no-go. These systems are critical for infrastructure to function — think gas pipelines, power grids or water mains — so taking them offline to apply patches is out of the question.

Therefore, the network has the job of providing security measures for connected IoT devices.

SECURING IOT: GETTING STARTED

The first step is identifying that a connected device is indeed an IoT device and then understanding the risk that device presents to the network. For example:

- What is the use of the device?
- What access does it currently have?
- Is it running current software?
- Does that software have known high-severity vulnerabilities?
- Is that device exhibiting compromised behavior?

Answering these questions about an IoT device is fundamental to figuring out how best to secure it. There are many mechanisms that a threat-aware network can employ based on the context of these answers.

IoT devices can also be put into a separate security zone with access to resources limited based only on what the device needs to access (least privilege), and that access should be segmented based on individual sessions. For example, a printer on the Fourth floor of a building can only have access to files sent to it for printing and is not able to communicate with the engineering department's internal code repository. Access can and be defined per session, and the direction of each session should be enforced. If a new, unknown IoT device tries to connect via Wi-Fi or Bluetooth, perhaps it connects to the guest network until questions are answered sufficiently.

Additional security measures can be applied to IoT devices; such as always-on decryption with IPS/anti-malware, content inspection and sandboxing for all unknown files. Network behavior to and from IoT devices monitored for indicators of compromise, such as beaconing behaviors and connections to known command-and-control domains and IP addresses.

HOW THE NETWORK CAN HELP

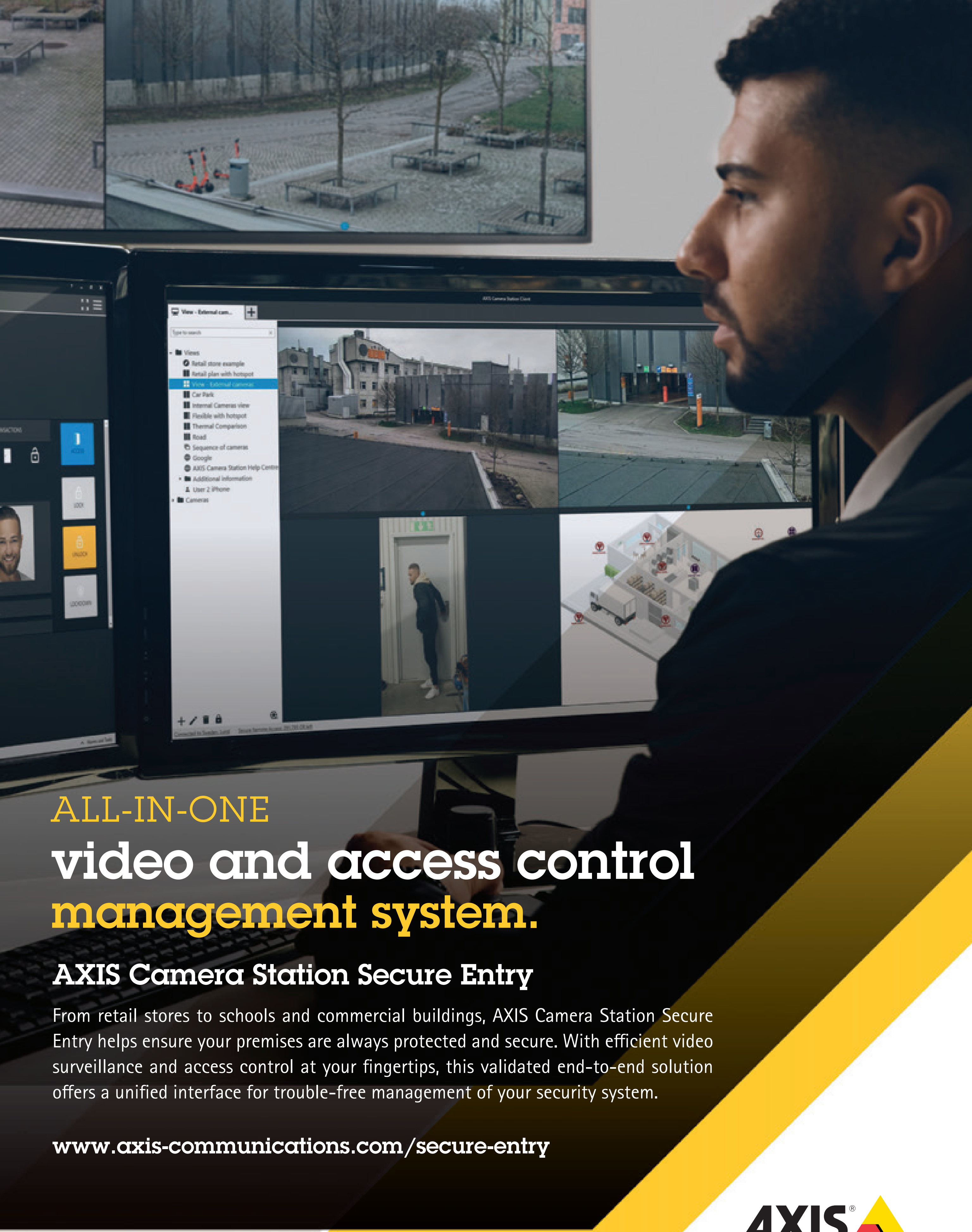
That said, when an IoT device is compromised and endpoint protection is not there or a patch cannot be deployed quickly, what can be done? The network can offer some mitigation.

In a threat-aware network, the infrastructure itself can stop certain connections. A Wi-Fi access point might be able to help assess the risk of the connecting device. The router might be able to prevent a compromised device being leveraged in a DDoS attack or prevent command-and-control communication to and from malicious domains and IP addresses. The switch might be able to help quarantine an infected IoT device at the switch port. All of this is beyond what a firewall can and should do.

In a threat-aware network, every point of connection participates in visibility, threat intelligence and enforcement, and IoT threats are thwarted at every stop. It is not just Mickey Mouse wringing his hands while the water level keeps rising; the threat-aware network helps solve for some of the security issues inherent in IoT so the benefits can be realized and life can be a little easier.

***Kate Adam** is responsible for the enterprise security product marketing team at Juniper Networks.*

Welcome!
EZ™ HELP
LETTERS
NAMES
CALL / HANG-UP
VOLUME
TTY
VIKING® MODEL C-2000B
ADVANCED DOOR/GATE AND ENTRY PHONE CONTROLLER
VIKING® MODEL C-1000B
DOOR ENTRY / CCTV VIDEO CONTROLLER
Call
Call


View - External cam...
Type to search
Views
Retail store example
Retail plan with hotspot
View - External cameras
Car Park
Internal Cameras view
Flexible with hotspot
Thermal Comparison
Road
Sequence of cameras
Google
AXIS Camera Station Help Centre
Additional information
User 2 iPhone
Cameras
ACCESS
LOCK
UNLOCK
LOCKDOWN

Panasonic
i-PRO

education | healthcare | corporate

SEPTEMBER/OCTOBER 2021

Campus Security & Life Safety

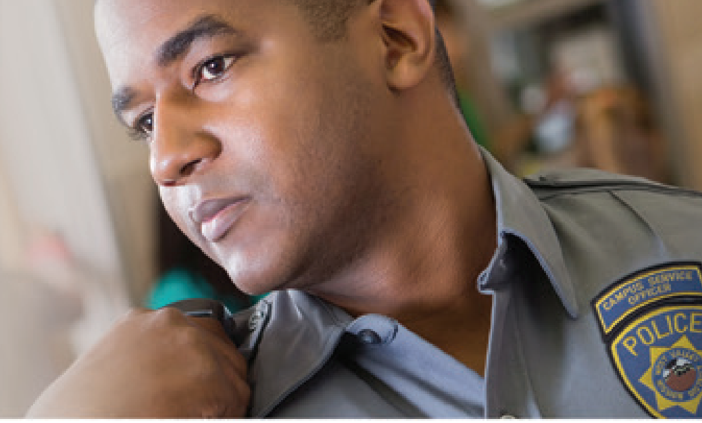
campuslifesecurity.com

Enhancing the Student Experience

Vanderbilt University enables faculty and student IDs on iPhone, Apple Watch

ESSENTIAL COMMUNICATIONS

RELIABLE | SECURE | AFFORDABLE



DHS and the Federal Commission on School Safety recommend two-way radios for effective communications in a disaster.

Schools rely on KENWOOD two-way radios to minimize contact, while maintaining order, now more than ever.

- Low cost, light weight and compact
- Antimicrobial surfaces. Easy to keep clean.
- Open the box and use the radio.
- Intuitive and simpler than a cell phone
- Rugged and waterproof
- Purpose-built for security and safety. Fire and police rely on radios. Your school deserves the same.

74% OF U.S. SCHOOL STAFF AND FACULTY USE TWO-WAY RADIOS

U.S. Department of Homeland Security

"With KENWOOD two-way radios, everyone knows the exact same thing, at the same time, the exact same message. And, no dropped calls."

– Kevin Wren, Head of Risk Security and Emergency Mgt., Rock Hill, SC School District

KENWOOD

NEXEDGE® NXDN® P25 DMR

1-800-950-5005 www.kenwood.com/usa

SECURING

the safety of our youth

GARRETT®
Multi Zone™

Fast, Easy, Versatile Security

- Budget-friendly safety
- 20 Pinpoint Zones
- Enhanced access control

The *Multi Zone*'s twenty zones provide precise location of one or more objects simultaneously. Multiple targets are indicated on both walkthrough panels via bright LED zone indicators.

GARRETT®
METAL DETECTORS

Email: security@garrett.com
Toll Free (U.S. and Canada) **800.234.6151**
Tel: **1.972.494.6151**

MADE IN THE USA

Inside this Issue

features

cover story

departments

Want Happy Customers? Hand Them Their Freedom with A Mobile Pass thru Their Access Control System for FREE

While technology keeps changing, smartphones remain front and center. So, it makes sense one of the top requirements in Access Control today, is for easy mobile control & credentials. That's why we created the secure Continental Access CA4K App with Built-in Mobile Credentials. Now, besides providing contactless authorized access through any type of door - working with any brand reader and most wireless locks–**the App's also FREE** to download from Apple or Google Play.

Ideal for anyone in your buildings, campus, schools or hospital, the CA4K Access Mgr App & Integrated Platform simply provide smartphone-based multi-tier access privileges for a few to large numbers of users; and Security Managers with smart, comprehensive enterprise control of users, threat-levels and a few, to thousands of doors, anywhere you are.

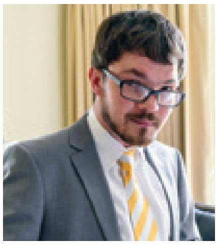
- **FREE Easy Intuitive Mobile App** provides Contactless Access for All Readers & Door Types from any smartphone
- **FREE Mobile Credential built in** app for Fluid Access thru any building or campus (Free. No annual subscription fees)
- **Emergency Alerts -** Sends push notifications (or emails) to users' phones in the event of an emergency, threat level escalation or lockdown event.
- **Integrated with CA4K Enterprise Security/Video/Access Platform** for Comprehensive Control of All Doors (1-32,000), wireless PIN/Prox locks, readers, elevators & entryways
- **Fast powerful processing** ensures fast, smooth access for simultaneous users even at peak times
- **Easy Migration & Generous Tradeup Incentive for Retrofitting Existing Systems -** Keep your existing readers & simply import your personnel database

Continental Access
A Division of NAPCO Security Technologies

For Free Demo or More Information
call 1.800.645.9445 or email CIMktg@cicaccess.com

CA4K
ACCESS MGR APP
Download on the App Store
GET IT ON Google Play

Campus Commentary



By Matt Jones

The Year of Recalibration

On one hand, it seems impossible to talk about themes of campus safety or campus security without mentioning the elephant in the room that is COVID-19. On the other hand, after a year and a half, it seems as though there's only so much left to say on the topic. Wear a mask? Check. Maintain social distancing? Check. Get the (now FDA-approved) vaccine? Check.

That said, the specter of coronavirus is starting to fade, at least a little. K¬–12 students recently returned to in-person learning full time, and college students are back on campus. Amid a flurry of mask mandates and vaccine mandates—or, in select states, despite the stalwart ban against them—students, faculty and staff seem more than eager to put on airs of normalcy once again.

It's a little early to declare the pandemic finished. The delta variant is still out there, and as of this writing, it's too soon to tell how the return to school will affect case numbers nationwide. And in this issue of Campus Security & Life Safety, you'll still find timely information and resources about indoor air quality and healthy schools. But as the third academic year tinged by COVID begins, even the precautions surrounding the virus are starting to feel old-hat. We're getting the time and mental space again to be able to turn our attention to other things.

It's nice to be able to widen the scope, to resume discussions of important issues facing educational institutions that have nothing to do with the virus. There's bandwidth once again to delve into topics like crime prevention and general campus safety tips, ever-present risks to stay aware of that now seem almost delightfully familiar and mundane. There are also graver dangers like active shooters—no more or less likely than they were two years ago, but still a threat that requires advance preparation and a coordinated response. None of these topics is new. But it's been a bit since we could give them our full attention.

I like to think of the 2021¬¬–22 academic year as the year of getting back to basics. The year when we shook our heads as if to clear them, trying to remember what we were concerned with before coronavirus took over the world. It's the year of remembering how to make small talk in the hallways; the year of being able to shoot your hand up and ask a quick, casual question during class; and, yes, the year of retraining your body to wake up at 7 a.m. instead of 7:55 for an 8 a.m. lecture. Getting "back to normal" won't happen with the flick of a switch. It'll take some time to exhale.

This year of recalibration also gives us the chance to see old problems with fresh eyes. It's a bit like getting stuck on a crossword puzzle and staring at it for so long that you're not even seeing it anymore. So, then, you'll step away to do the dishes, take the trash out, fold some laundry, take a quick mental break. And when you sit back down to the puzzle, more often than not, you'll find that no sooner have your eyes hit the page than that elusive answer to 34-Down pops into your head entirely unbidden.

That's obviously an oversimplification. But there's almost always value in returning to familiar problems with clear heads. Fresh perspectives and new experiences often lead to entirely new avenues of problem-solving. And, after the last 18 months, finding new ways to tackle campus crime feels more surmountable than living through a pandemic.

Matt Jones
Senior Editor

SEPTEMBER/OCTOBER 2021

EDITORIAL STAFF

Editor-in-Chief	Ralph C. Jensen
Senior Editor	Matt Jones
E-news Editor	Brent Dirks

ART STAFF

Senior Art Director	Laurie Layman

PRODUCTION STAFF

Production Coordinator	Teresa Antonio

SALES

Sam Baird	+44 1883 715 697
Brian Rendine	972-687-6761

INFRASTRUCTURE SOLUTIONS GROUP

President & Group Publisher	Kevin O'Grady
Editor-in-Chief/ Associate Publisher, Security	Ralph C. Jensen
Group Circulation Director	Irene Fincher
Group Marketing Director	Susan May
Group Website Manager	Scott Newhouse
Group Webinar Administrator	Tammy Renne

1105MEDIA INC
YOUR GROWTH. OUR BUSINESS.

Chief Executive Officer	Rajeev Kapur
Chief Financial Officer	Sanjay Tanwani
Chief Technology Officer	Erik A. Lindgren
Executive Vice President	Michael J. Valenti

REACHING THE STAFF

Staff may be reached via email, telephone, fax or mail. A list of editors and contact information also is available online at www.campuslifesecurity.com.

E-mail: To e-mail any member of the staff, please use the following form: FirstinitialLastname@1105media.com

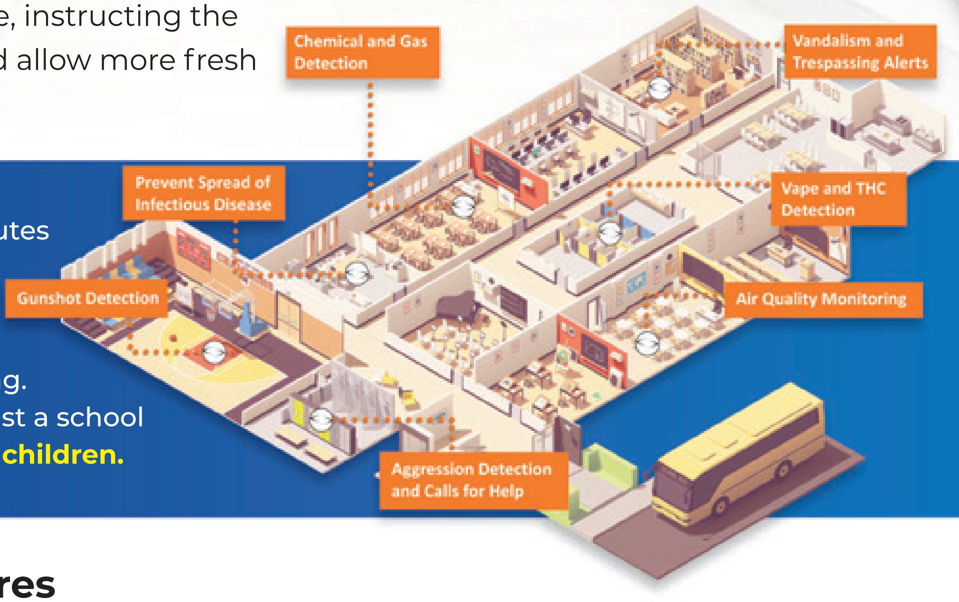
Dallas Office (weekdays, 8:30 a.m. – 5:30 p.m. CT)
Telephone (972) 687-6700; Fax (972) 687-6799
14901 Quorum Dr., Suite 425, Dallas, TX 75254

Corporate Office (weekdays, 8:30 a.m. – 5:30 p.m. PT)
Telephone (818) 814-5200; Fax (818) 734-1522
6300 Canoga Avenue, Suite 1150, Woodland Hills, CA 91367

HALO
SMART SENSOR

Fight the spread of airborne diseases in your school with **HALO**

The COVID-19 and Influenza virus are commonly transmitted through the air as the virus is attached to very fine particulates. As part of its AQI measurements, **HALO** monitors Carbon Dioxide (CO_2), particulate concentrations, Humidity, Volatile Organic Compounds (VOC), and Nitrogen (NO_2) in the air. When **HALO** detects high CO_2 levels or particulate levels, **HALO** can notify the HVAC system via its BACnet interface, instructing the HVAC to open its dampers and allow more fresh air into the room.


Chemical and Gas Detection
Vandalism and Trespassing Alerts
Prevent Spread of Infectious Disease
Vape and THC Detection
Gunshot Detection
Air Quality Monitoring
Aggression Detection and Calls for Help

Good Indoor Air Quality contributes to a favorable environment for students, performance of teachers and staff, and a sense of comfort, health and well-being. These elements combine to assist a school in its core mission — **educating children.**

Key Detection Features

- Aggression
- AQI
- Carbon Monoxide
- Carbon Dioxide
- Gunshot
- Help (Spoken Key Word)
- Humidity
- Light Level
- Masking
- Particulates
- Pressure
- Tamper
- Temperature
- THC
- TVOC
- Vape

631.969.2601 • info@ipvideocorp.com • www.ipvideocorp.com/halo

IPVideo Corporation

"It is essential, for example, for security personnel or staff to be able to react instantly to a troubling situation, whether in the congested hallways of a high school or middle school, or remote locations such as stadium bleachers or large fields of a college campus."

By Ken Francis

Transforming K-12 and Higher Ed

Cost has always been the biggest problem; complexity is a challenging issue

metamorworks/Shutterstock.com

A school needs more than great academics and smart students to be an intelligent campus. To support education and intellectual growth, campuses need to be safe, cyber-secure, and very smart.

This does not come as news to community and education leaders. Schools and colleges have wanted high performance security systems for decades. The biggest problem has always been cost, and then there is the complexity of the system, the challenge of integrating video and access control, or the need to hire extra personnel with special skills to manage the system.

For years, elite private schools and universities were the only campuses benefiting from advanced security platforms and video management systems. Thankfully, this trend is shifting, as cost-effective and scalable video management systems and remote access technologies have become available to K-12 school districts and universities across the country. Now, companies like Eagle Eye Networks offer cloud video management systems that are seamlessly integrated with existing technology, and managed with minimal effort.

Security Capabilities and Suspicious Activity

Violence on campuses is unfortunately something that all education leaders must think about in a proactive way. The most important benefits a school, its students and faculty gain from a cloud-based video surveillance system is bolstered security across the campus.

It is essential, for example, for security staff to be able to react instantly to a troubling situation, whether in the congested hallways of a high school or middle school, or remote locations such as stadium bleachers or large fields of a college campus.

Advanced analytics within a security system can notify security personnel in real time of situations worth addressing, while providing critical information to key decision makers so they can act quickly and decisively. The adaptability and flexibility of these security

systems allow for project scalability. Systems can be installed in phases to avoid impacting the school day.

A phased approach makes it easier for schools to budget for security investments, as does the subscription model of payment. Cloud video surveillance requires a small initial investment, and then the school or university pays for the system by subscription – a monthly fee based on the number of cameras, the amount of time video is retained for each camera, and what kind of video analytics are included in the system. Maintenance and upgrades are delivered via the cloud for technology fixes and cybersecurity assurance. Features, such as analytics, can be added or removed from the system remotely, at any time.

Take, for example, the University of Chicago, which leveraged the advanced capabilities of its cloud-based video management system to ensure student safety in an on-campus residence hall. The university quickly integrated a video management system to manage both exterior and interior cameras at the dormitory. Combined with remote viewing capabilities and motion detection, the cloud-based video surveillance systems enabled the university to enhance security without increasing its on-campus patrols.

Monitoring Insights from Object Counting and Line Crossing

Contributing to the intelligent campus are valuable video analytics such as "people counting" analytics that monitor the number of faculty, students and parents entering and leaving the building. This is particularly helpful for security managers and school administrators at the K-12 level, as it provides insight into the flow of people entering a building at the beginning, middle, and end of the day.

Implemented districtwide, people counting functionality can be scaled to multiple campuses to provide information for security and optimization of school facilities. "Line crossing" analytics can provide real-time alerts when movement is detected in restricted or sensitive areas with high value assets, such as medical supplies and electronic equipment.

Faster Recognition of Loitering, Camera Tampering and Intrusion

Ensuring a secure and safe campus requires around-the-clock monitoring. Advancements in cloud-based video surveillance technology have made this task easier by enabling security teams to manage multiple cameras from a single, centralized space and providing remote access to make it possible to monitor video from a computer or mobile device.

To ensure a swift response, custom loitering or intrusion alerts can be created to set a clear perimeter around designated areas and send a notification the moment an object or person breaches the boundary.

On a college campus that is far too large to physically patrol and monitor efficiently, this technology is a force multiplier, allowing campus security to keep an eye on multiple, large areas at once, like a stadium, field, or parking lot. Camera tampering can also be flagged in real time with instant notifications announcing when a camera is blocked, moved, or otherwise tampered with.

Wellness and Elevated Temperature Support

From heavily populated public schools to small standalone preschools, administrations across the country understand the need to screen for elevated temperature as a way to identify persons who may have a fever, and to lower the risk of spreading infection.

Temperature screenings have become a routine and time-intensive requirement for entering many campuses across the country. By pivoting to a cloud-based video surveillance system, organizations can implement a safe and contactless solution to screening temperatures, which, unlike alternate options, can be performed quickly, and without close contact.

Thermal cameras for preliminary temperature screening have some simple requirements for set up, including being installed indoors, away from wind and sunlight. Thermal camera vendors provide detailed instruction on set up and best practices for thermal camera usage. The cameras use specialized sensors that detect heat, instead of visible light. The camera measures skin surface temperature of an individual's forehead or inner eye area. It provides visible and audio alerts if an individual records an elevated skin surface temperature.

Meeting Special Education Regulations and Requirements

In recent years, an increasing number of states have introduced strict regulations surrounding the monitoring of special education classrooms in public schools.

Several states now require a video camera in every special education classroom, and require up to 90 days of retention for the video. To meet these requirements, many school administrators are finding that cloud video management systems enable them to meet these requirements economically and efficiently.

Addressing Cybersecurity Concerns

With the proliferation of malicious attacks, cybersecurity is becoming one of the top concerns for education leaders and parents.

First, they want to protect the privacy of students and staff in the classroom and around campus. To do that, it is essential that K-12 and colleges work with a provider of true cloud, one that manages cybersecurity updates continuously. A true cloud video surveillance system can maintain the privacy of student and teacher images through encryption. It can also mitigate malicious software that could harm a school's network and interfere with the learning and education process.

Access Control as a Service

The intelligent campus encompasses access control, as well as video surveillance. Access Control as a Service (ACaaS) is the modern way to bolster the security for any entity in the education space on and off campus. ACaaS is cloud-based and integrates with existing technologies, strengthening remote management in the event of an emergency and creating a more efficient security solution.

Cloud-based access control is a key element of an intelligent campus. From providing a unified security platform with an integrated video system to lockdown capabilities and health-safety tools, cloud-based access control strengthens the ability to monitor, track and instill safety measurements to keep students, faculty, and staff safe.

When cloud-based access control systems are integrated with cloud video surveillance, institutions can more easily and effectively manage security. The ability to act quickly, even while operating remotely, makes integrated access control and video management systems effective and desirable for school districts and higher education campuses.

True cloud video surveillance companies like Eagle Eye Networks have an open platform, which allows the school or university to choose their access control provider. An Eagle Eye system can integrate with Salto KS, Brivo, DMP Virtual Keypad or other leading access control providers.

As an example, the Brivo Access system integrated with video management systems connects access events – someone presenting a credential at a door – with the live or recorded video feeds together in one view, so the security director has lots of information to assess the situation. Security staff can easily see if the user associated with the credential is appropriate, and they can do this in real or near-real time. Moreover, the security manager can do this from onsite or a remote location. The combination allows school administrators to secure every door at a given facility through one interface.

In the case of an emergency event, a lockdown can be initiated from a desktop mobile app, which will immediately secure all doors while notifying all administrators. Priority first responders, including police, firefighters, and paramedics, can be granted access permissions, so they can perform their critical duties even when a lockdown is active. To reduce confusion or risk after an event has concluded, master and/or senior administrators are established to have full authority over the system and can proceed with the all-clear steps to get normal operations up and running again.

In a world where budget constraints are frequently encountered, collaborating with a third party ACaaS provider like Brivo not only provides a cost-saving solution, but also enhances your overall security when combined with your cloud-based video monitoring solution.

***Ken Francis** is the president of Eagle Eye Networks.*

Hear, be heard and be understood – every time, everywhere.

Schools and university campuses face a wide range of risks —from visitor management to emergency events.

Our intercom and public address solutions allow security teams to see and hear what's happening at entrances and throughout all buildings, and to broadcast general and emergency messages across a campus.

Learn How Our TCIV+ Video Intercom Station Empowers Security Teams:

- **Powerful Audio Technology with a 10W speaker and matching 10W class D amplifier**
- **HD Video with a wide angle lens**
- **Enhanced processing for stability, uptime, and a long product life**
- **Tough and Sophisticated Design with a diecast aluminum frame**
- **Cybersecure, meeting IEEE 802.1X network access control.**

zenitel
because communication is critical

Contact us today:
info.usa@zenitel.com

www.zenitel.com

"The audit process often reveals gaps in a school's safety plan and room for improvement, and an opportunity to adopt additional technology and resources."

By Danielle Myers

What Schools Need to Know

Follow this guide for evaluating, implementing a security plan to decrease shooter response times

a katz/Shutterstock.com

As schools resume across the country this fall, safety and security is top of mind for parents, faculty and administrators alike. Traditionally, as security alerts arise, schools address individual needs rather than formulating a cohesive safety and security plan with technology to reinforce it. This can cause a siloed approach to safety, and gaps in safety plans. The following is a systematic guide for evaluating, implementing and running a comprehensive, security plan for maximum safety.

Integrating Your Systems

Most school systems use a variety of technologies that typically have separate jobs, such as access control, security cameras, and communications. These are all important tools, but when siloed don't create a cohesive safety solution, rather, they only address a small set of safety concerns, such as addressing mass communication needs but not addressing point of entry vulnerability.

Instead, schools should examine ways they can actively prevent, detect and triage security threats, such as mass shootings in real-time. This starts with a safety audit of all policies, procedures and technology currently in place to combat emergency situations, like an active shooter situation. The audit process often reveals gaps in a school's safety plan and room for improvement, and an opportunity to adopt additional technology and resources.

Additionally, schools should combine these systems under a single platform to create an integrated safety solution. Implementing situational awareness and response technology is a more proactive solution for schools, as it unifies all of their security and safety systems onto one platform to improve communication, workflow and operations especially in an emergency situation. Time is of the essence in critical situations and using technology to reduce the amount of time the information takes to get to the proper people can save lives.

For example, schools may upgrade their cameras and access control systems, but most do not have the ability to access the live feed in order to alert staff about an incident unfolding in the building that is caught on camera. This reactive approach results in a communication breakdown. Implementing an automated alerting platform can turn alarms from stand-alone systems, into detailed alerts for delivery to communication endpoints. This means school administrators, teachers, and other onsite personnel can receive real-time information about possi-

ble threats and can immediately initiate the appropriate response plan.

The live feed would be sent to first responders, such as law enforcement, a school resource officer or a principal, in order to launch a quick response. With today's smarter networks and devices, plus an automated alerting platform to tie them all together, it is easier and more cost-effective than ever to create a safety and security bubble over a single campus or entire district.

Monitoring Access Points

One way a school can integrate technology for optimal safety and security is by auditing their entry points. While schools vary in their entry practices from having a manual sign in at the front desk to keycard entry, the doorway is the first point of access to each building. Entry access control systems are essential for optimum security. The ideal security system allows a person from anywhere in the building to both see and communicate with visitors before entering the building. This gives staff as much information as possible to make an informed decision about which visitors should be allowed to access the building.

Rather than having an employee assigned to wait by the doors and monitor entry, administrators can deploy automated alerting to allow staff members to receive an alert on their phone containing detailed information about any individual requesting building access; the alert can even contain live video footage pulled from security cameras. The employee can then permit access directly from their phone with the push of a button or secure the building in the case of a threat.

Adding an extra level of security with credential tracking and permissions, including key cards and pin codes, can be implemented throughout the building as an added layer of caution. Lastly, integrated cameras and building access sensors can allow access points to be monitored with a notification should the building be breached with a propped door to eliminate a threat early. Identifying areas of improvement at access points is a great first step to establishing a comprehensive plan.

Alerting the Right People at the Right Time

In the case of an active shooter inside the building, situational awareness technology notifies the right people, with the right information, in the shortest amount of time. From notifying law enforcement to employees and loved ones, technology can play a vital role in making sure everyone is aware of the situation to respond quickly.

This cuts down on people wondering what to do if they see something suspicious, or are in shock amid an emergency. Instead, a protocol is put in place, and executed for the use of a panic button to alert people of the situation immediately. Technology can make all staff feel empowered to act quickly and efficiently to deescalate an emergency situation, ensuring that every second is being optimally utilized and that emergency staff are alerted in real-time.

Technology has become vital in the safety and security of schools, businesses, and other public places because it provides peace of mind.

For instance, Blount County School District, just one county over from the recent Knoxville, TN, school shooting, implemented technology solutions to better equip them to respond to an active shooter situation a year ago. Their use of situational awareness and response technology integrated all safety and security technology into one platform and enhanced their mobile duress technologies throughout the school buildings.

Specific school staff members were given mobile duress buttons to be used in the event of an emergency. When one of the mobile duress buttons is triggered, an alert is immediately sent out to the proper staff and/or first responders with critical information. This goes out, via desktop alerts and includes a live video feed from the cameras closest to the triggered device and the location of the device triggered. This ensures quick and correct action would be taken to manage any situation.

The school believes this proactive approach will ultimately save lives in the case of an emergency. Each school had a different set of needs and requirements for its program. In a mass shooting situation, one minute can be the difference between life and death. While it can be overwhelming for schools to take on such a challenging and complex issue, starting with an evaluation, and identifying key areas of opportunity/improvement, and incorporating a comprehensive safety plan, schools can take steps necessary towards a brighter and safer future for our children, students and staff.

Making Your School Situationally Aware

Situational awareness technology is used for other mass notification updates to parents and faculty such as school closures, COVID-19 exposures, or new guidelines. An automated alerting platform can streamline lockdowns, evacuations, severe weather responses, medical emergencies, and many typical day-to-day events. By implementing an automated platform, schools are not only preparing for active shooter situations but also preparing for the future.

By maintaining the safety conditions and security of their school buildings, administrators can ensure that when the time comes for students to return, they are more ready than ever. Running a school is already a demanding job, and with COVID-19 and an increase in gun violence adding even more pressure and complications, it is easy to let things be swept under the rug, resulting in a minor issue becoming a major problem. To minimize risk, it's worth investing in a solution that can catch an issue before it escalates, relieving staff from doing unnecessary work and allowing them to focus on what's really important - teaching their students.

Navigating Increasing Violence in Schools

While several factors have led to school shootings, mental health is one that cannot be ignored. According to a recent report, staff members need to be able to identify students who may exhibit or be a victim of violence by examining and analyzing patterns and trends in their behaviors. A number of factors should be considered including attendance records, student grades, previous history or pattern of behavioral issues, and experience with bullying.

Having multiple touchpoints with students each day visible on one platform allows staff to view all interactions in one place to help identify trends or issues. For example, if a student is consistently absent from lunch on a certain day of the week, administrators may be able to identify that the student is facing food insecurity, or being bullied by another student during the lunch hour. Consolidating information onto a single platform not only improves efficiency, but also has the potential to spot issues that could escalate into situations that are more violent if not addressed properly.

Upgrading technology to protect students does not always have to be out of budget for schools. Many states, including Ohio and Kentucky are allocating funds and offering grants to schools to incorporate technology solutions. The technology allows schools to improve safety and communication by providing staff the ability to summon help from any web browser, which allows law enforcement to be notified quickly and discreetly, and to send and receive alerts via various devices.

Increasing public awareness of safety and security concerns and preparing for the worst can save lives in emergency situations. When the right people can receive detailed information about what is happening around them, they can react immediately and effectively. Situational awareness technology creates time to respond and that is critical for life safety as well as optimizing operations.

***Danielle Myers** is the general manager at Status Solutions.*

Rely on STI®

…for touch-free, turn to reset and more

Thousands of Buttons to Solve Your Problems

STI has the right button, right now. Tough buttons in a choice of touch-free or push activation. Steel or polycarbonate construction.

- Stopper® Station offers several color and activation choices
- Choice of standard or custom labels, snap-in messages and more
- NoTouch® Stainless Steel or Cast Aluminum helps promote health and safety and reduce the spread of germs

Learn more at www.sti-usa.com/sp445 or call 248-673-9898

STI®

Safety Technology International

2021

Enhancing the Student Experience

Vanderbilt University enables faculty and student IDs on iPhone, Apple Watch

Embracing the benefits of touchless access using smartphones, Vanderbilt University has expanded its investment into campus safety and security by leveraging HID Mobile Access® to deploy campus IDs on iPhone and Apple Watch through Apple Wallet.

The enhancement builds upon the university's initial investment in mobile-enabled technologies from HID Global. These technologies capitalized on the ubiquitous nature of smartphones and mobile devices among students—90 percent of whom reside on campus throughout their Vanderbilt education—and faculty to create a campus-wide identity and access management program.

The investment continues to pay dividends.

"Keeping students safe is our top priority. HID Mobile Access was the optimal solution for protecting students and allowing Vanderbilt to move to a mobile solution for securely accessing our campus and services. The integration of campus IDs on iPhone and Apple Watch brings added convenience for our entire campus community," said Mark Brown, Vanderbilt's director of business services technology. "Beyond the convenience and security—two very important considerations—this mobile solution gives us the freedom to provision and modify credentials remotely, which has been significant for protecting the health of our students and staff during the worst of the COVID-19 pandemic in 2020."

"This initiative has been of interest to both the student body and university administrators, as it supports both accessibility and convenience for our campus community," said Eric Kopstain, who is the Vanderbilt vice chancellor for administration. "We are also excited about this new option because it provides an added health and safety benefit for students. The contactless payment option will allow students to not touch surfaces or other people, thus helping to prevent exposure to COVID-19 and other viruses when making purchases."

Building on its Initial Investment in Mobile-Enabled Technologies

Vanderbilt initially tapped HID Global to implement a mobile credential solution that was compatible with Near Field Communication (NFC) and Bluetooth technologies. HID Mobile Access, powered by Seos® credential technology deployed alongside a reader infrastructure comprising HID® Signo™ readers, HID iCLASS SE® readers, and OMNIKEY® desktop readers to manage access to buildings. It complements the ecosystem by facilitating the usage of the already issued credentials for all other adjacent use cases. The solution allowed Vanderbilt administration to issue mobile credentials that let students, faculty, and staff access buildings and services with their mobile devices, as well as efficiently provision/deprovision credentials remotely without person-to-person contact.

The collaboration between Vanderbilt and HID Global began in 2014, when the university first validated the use of smartphones as a convenient and compelling new way to open doors. Pilot participants each used their smartphones for door access at one or more of a half dozen possible campus entry points, including a parking garage. The entry points were equipped with Bluetooth-enabled HID readers that configured to work with existing HID iCLASS smart cards as well as HID Mobile IDs.

In a survey of pilot participants, respondents cited convenience as the top attribute of the mobile access experience, since their

> “We are also excited about this new option because it provides an added health and safety benefit for students. The contactless payment option will allow students to not touch surfaces or other people, thus helping to prevent exposure to COVID-19 and other viruses when making purchases.”

By Daniel Gundlach

Blue Titan/Shutterstock.com

smartphones are always with them, and they are less likely to lose them as compared to their access card. Respondents further pointed out the benefit of using their phone as a backup in cases where their cards were lost or stolen.

At the pilot’s conclusion, the university began purchasing only readers with Bluetooth technology or later, NFC, so that it could roll out HID Mobile Access beyond faculty and staff to the entire student body. Approximately 90 percent of Vanderbilt’s contactless readers on campus were soon mobile-ready so that, “when we do get to that point, we’re ready to go,” Brown said.

Vanderbilt’s access control platform is CS Gold®, a higher education transaction system from CBORD for credential lifecycle management that integrates with the university’s HID Global access cards and door readers. HID wrote an application programming interface (API) for Vanderbilt so the CBORD platform could communicate with HID’s latest Seos credential technology that is powered by highly advanced encryption and a software-based infrastructure.

It secures trusted identities on any form factor, and can be extended for applications beyond physical access control. Brown said the plan was slowly phased in the Seos technology as it continued issuing cards, until it eventually removed the iCLASS chip from the card. This would enable it to migrate to the latest and most secure card format.

The simplified credential issuance of the mobile access solution began with new users receiving an email on their phone that included a link to the HID Mobile Access app. Once they accepted the invitation and clicked on the link, the credential pushed down to their handset. This process also reduced the time it took the university to issue credentials.

“When it comes to issuing the identities to somebody, what was probably a 10-minute process before could now be done in literally 10 seconds,” Brown said.

Provisioning credentials to contractors or other parties needing temporary access was made simple, and secure with HID Mobile Access than with physical cards, Brown said. It was now possible to pull a credential off a visitor’s or contractor’s phone as soon as necessary, so that, as an example, they were not in possession of a credential that they had forgotten to return at the end of their visit.

Elevating the Convenience Factor

Next, the university wanted to add support for credentials in Apple Wallet without compromising the existing access infrastructure or its security. Using HID Reader Manager the task was completed to upgrade firmware on the university’s physical access control readers to extend support for NFC-based credentials in Apple Wallet. The university uses the flexible HID Origo™ Mobile Identities API integrated with CS Gold.

With campus IDs in Apple Wallet, students can complete any action that would have previously required a physical ID card — both on and off campus — with just their iPhone and Apple Watch. Students simply present their device to a reader to enter dorms, libraries, and fitness centers, buy lunch, make purchases at campus stores, pay for laundry and print documents.

The university’s Commodore campus ID cards on iPhone and Apple Watch provide an extra level of security and privacy, so students do not need to worry about misplacing their physical card when they are enjoying campus life. Transaction history remains private and is never shared with anyone. If a student misplaces their iPhone or Apple Watch, they can use the Find My app to immediately lock their device and help locate it.

Vanderbilt administrators said the university is working to launch a similar offering through Android devices. HID Mobile Access enables mobile IDs to send via an app to either Android or IoS mobile devices.

This will enable more users to benefit from the ability to not only enter residence halls, campus libraries and other physical locations, but also buy food at campus dining locations, make purchases at Barnes & Noble at Vanderbilt, the campus post office, the Student Health Center and the Sarratt Student Center Box Office without needing their physical Commodore Card.

Students can use their phones to purchase food at nearby off-campus locations that are part of the Taste of Nashville program.

In 2014, Vanderbilt University had a vision for creating a safe and secure campus using mobile-enabled technologies. What started as a successful pilot quickly transitioned into a full-scale development of mobile access to faculty, staff and the entire student body. Today, the university has achieved its goal of delivering this safe, secure and convenient mobile access solution with the added flexibility of supporting the Apple Wallet platform. With integrated HID Mobile Access, issuing credentials to new users is as easy as having them download the app, validate identity and seamlessly add their credentials to Apple Wallet.

***Daniel Gundlach** is the vice president, Physical Access Control, North America at HID Global.*

Control the Panic

How to choose an alert system that complies with Alyssa's law and fully protect your schools

By David Rogers

On Valentine's Day in 2018, 14 students and three staff members lost their lives when a gunman opened fire at Marjory Stoneman Douglas High School in Parkland, FL. More than 20 people were shot within the first 70 seconds.

Alyssa Alhadeff, a 14-year-old student, passionate soccer player, and older sister to two brothers—was in one of the first rooms the gunman attacked. She immediately was shot but was still alive when the gunman moved to another room. Alyssa attempted to hide, but ultimately the gunman returned moments later, shooting her multiple times and ending her life.

With a faster emergency awareness and improved, coordinated response, the outcome of this tragedy could have changed.

Overview of Alyssa's Law

Driven by their grief and dedication to stop the unthinkable from taking another life, Alyssa's parents, Lori and Ilan Alhadeff created Alyssa's Law.

This legislation—named after Alyssa and in honor of all school shooting victims—addresses emergency response time to critical, life-threatening school incidents. Alyssa's Law requires public and charter schools to have silent panic alert systems that link directly to first responders and law enforcement agencies.

At the time of writing, Florida and New Jersey have passed versions of Alyssa's Law. Other states, like New York, Nebraska, Arizona, and Texas, are quickly following suit. Legislation was introduced at the federal level.

Top Actions Users Panic Button Should Empower You to Take

Successful emergency response, and the safety of everyone inside of school buildings, relies on more than just a system that only sends alerts. Below are four key actions a school panic button should empower its users to take.

Initiate the panic alert. Share specific emergency details from wherever you are located

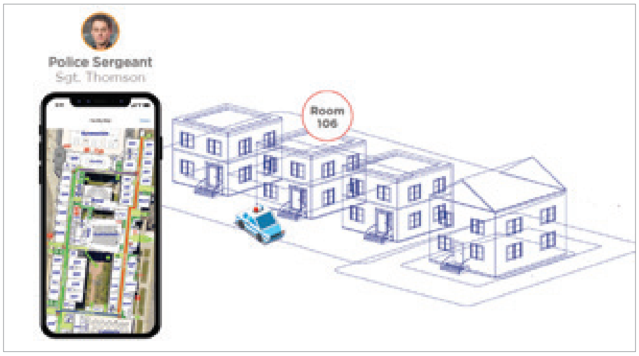
A best practice is to empower teachers and staff to summon the right help from wherever they are, whether in a classroom, a bathroom, on the track field or a school bus. Mobile panic alert systems greatly help by doing just that and enabling users to directly connect with 9-1-1 and send detailed, situation-specific notifications to a custom list of recipients. These alerts—ideally sent across text message, email, voice call, and push notification—should provide the type, location and time of the incident, and who initiated the emergency.

The school's system should confirm precisely where each user is when they initiate an incident and send alerts based on that location. This allows users to switch seamlessly between campuses without worrying about their panic button, or the signals sent out are being tied to the main office.

Provide easy access to critical school data. Stay in compliance with district policies

The panic alert system should enable schools to upload, organize, and display any PDF document they need to access during an emergency, including building maps and protocol procedures. It should be customized to the school or district's emergency response protocols, helping ensure that everyone stays in compliance with the policies and speaks the same language during an emergency.

Being in an emergency can jeopardize our abilities to think clearly and remember exactly what steps to take to keep everyone safe. Suppose the school's protocols are readily accessible on teacher and staff members' mobile devices or tablets. In that case, they can quickly remind themselves of their responsibilities and better protect those around them. Consider another scenario. Imagine being a police sergeant who is on your campus for the first time. When the school map is accessible on any web-enabled device, the sergeant can go exactly where he is needed without stopping and asking for directions.



Streamline response after initial delivery alerts. First responders and incident commanders cannot be everywhere on campus at once. The panic button should enable staff, first responders and incident commanders to communicate in real-time through group messaging.

Incident commanders and first responders also need a clear line of sight for every person, including students, staff, contractors and visitors, on campus. The most powerful solutions allow them to see details of each person in the buildings, including their location, status, medical conditions, and allergies. If they are students, it should also list their guardians' contact information.

To accomplish this, the panic alert system must integrate with an accountability solution that lets teachers and staff account for anyone, not necessarily just the students on their rosters.

Summon the right help for localized incidents. Schools frequently respond to localized incidents, like an irate visitor, student fight, or flooded restroom. There is also a growing concern that schools will see an increase in violent behavior as they reopen and students return to the classroom after the pandemic.

The panic button system must allow teachers and staff to summon help for localized scenarios so the appropriate personnel can respond to, identify, and resolve the issue.

Fully Protect Users Buildings and Everyone Inside of Them

The most powerful panic alert software seamlessly integrates with an emergency management system that empowers schools to:

- Practice and analyze drills
- Summon the right help for any situation
- Account for everyone on campus, including visitors, contractors, guardians, and volunteers
- Reunify students with guardians
- Integrate with the school's visitor and volunteer management solutions

Investing in the right tools and software—like the Raptor School Safety Suite—creates the ultimate benefit: safety and peace of mind for everyone in your community.

__David Rogers__ is a senior executive for Product and Marketing at Raptor Technologies.

Intelligent WiFi

ASSA ABLOY
Opening Solutions

Experience a safer
and more open world

Mobile

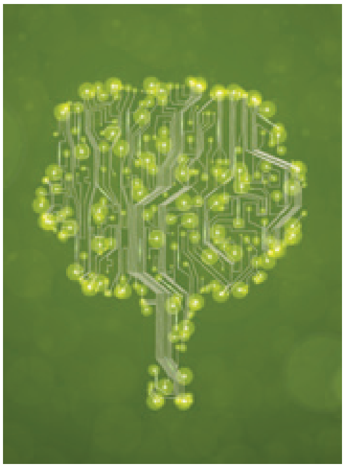
Real-Time Wireless

Complete Campus Security Solutions

ASSA ABLOY intelligent campus access control locks take advantage of existing infrastructure to provide advanced security and easier, more cost-effective installations.

- Future-proof your campus security with an easy migration path to higher security credentials and mobile access
- Use existing infrastructure to simplify installation and expand access control easily and affordably
- Integrate with industry-leading access control partner software

Learn more: IntelligentOpenings.com/campus



PoE

"A clear voice and sound clarify the intent behind the images that are captured on cameras, and increases situational awareness."

By Bruce Czerwinski

Vladeep/Shutterstock.com

Crystal Clear Security

10 ways Intercom Solutions Can Control Entry and Secure Your Facilities

Identification cards, video surveillance, keypads, software, databases, and even the doors themselves. They are all part of a security strategy to keep employees safe in a facility. All used to control entry to a facility or building, which mitigates risk and increases safety and security.

Other business benefits to controlling entry include mitigating the risk of cybercrimes and data theft, protecting your brand, and employee retention.

Almost overnight, due to the pandemic, the way that entrances were controlled has changed. For many facilities, the pandemic created a new security perimeter. Suddenly there was a need to interact and communicate with individuals moving in and out of doors and spaces without physical intervention. Even more, many security perimeters pushed farther out in order comply with social distancing guidelines.

While ID cards and video surveillance are one way to control entrances to a facility, they cannot completely do the job. Video surveillance may show a scene and access control can control access, yet IP intercoms can detect voices, high noise levels, breaking glass, or other sounds that are not within direct view of a camera. A clear voice and sound clarify the intent behind the images captured on camera and increases situational awareness.

To control entry, today's enterprise security systems need crystal clear voice, access control, and video surveillance working together to mitigate security risks. Working with an integrated IP intercom platform, a security officer can manage all communications through their access control workstation interface – answering and placing calls, managing a call queue, viewing associated video and locating callers on a map.

Specific events, whether common or critical, can automatically trigger pre-recorded messages, such as social distancing instructions or emergency lock-down announcements. The result is better situational awareness, enabling a more informed, faster response by an officer who can easily see, hear, speak to, and manage any situation or threat that emerges.

Here are 10 ways that intercom solutions can control entry to a facility and help keep it secure.

1. Entrances to commercial buildings. Intercoms can help security teams to identify visitors via both audio and video, before they gain access to the facility, and guide them to where they need to be. They also assist in responding to emergencies with both pre-recorded and manual announcements at the door.

2. Industrial facilities and manufacturing plants. Often with large perimeters, here is where intercoms complement well with physical barriers, sensors, CCTV, and other security measures, allowing security teams to listen to activity, and to see it, if security cannot physically be at the perimeter to patrol. Automated broadcast messages at the perimeter sound if an alarm triggers. It can alert the visitor, via voice, to leave the area.

3. Hospitals are "open" environments. Intercom solutions at doors and entrances can allow facility staff to communicate with patients and visitors remotely from their reception and intake desks, limiting the need for face-to-face communication during the pre-screening process and prior to admitting them into the facility. Adding elbow, foot, or other alternative switches can further reduce risk of contact between infected and uninfected individuals. Once inside the facility, those same intercom solutions can provide access and crystal-clear communication to entrances to restricted areas, cleanrooms, isolation rooms, and maternity wards.

4. Retail stores. Intercom solutions and speakers can assist customers, help security guards to perform their jobs better, and enable communication between office staff and sales personnel. To control entrances, intercoms can be used at the door on a loading dock, for example, to allow security not only see, but speak with and monitor all staff moving in and out of that area.

5. Prisons and correctional facilities. Intercom solutions facilities provide efficient audio and video assistance for visitors, cell communications, and with prison management systems to enhance a security guard's insight into situations and events. Placed at door, intercoms and gates to communicate with inmates and to control access to restricted areas, gates, sally ports, and door locks.

6. K-12 schools. Visitor entry can be controlled at the exterior doors, with an intercom solution that a receptionist or security guard can control inside the school. When visitors or vendors push the button outside, their images and the audio from their voices can help determine why they want access to the school. The intercom enables a two-way conversation to help the receptionist or guard determine why a visitor wants access.

7. University campuses. An intercom solution can control entry at main entrances, in addition to serving as an additional layer of security at administrative offices and other areas with highly sensitive information, but they are also ideal for use at delivery bays or other secondary entrances that have a lot of traffic.

8. Manufacturing facilities. Keeping downtimes to a minimum and steady production, without security issues related to uncontrolled entry. Intercom solutions can control access to multiple doors. They can also provide general information throughout one facility or to specific warehouses, production areas, or other areas, while also helping security teams to respond to emergencies with both pre-recorded and manual announcements.

9. Multi-tenant facilities. Hundreds of people might enter and exit each day, an intercom solution can allow tenants, a concierge, and security officers to identify visitors quickly and easily before granting access. The ability to hear and see the visitor will allow for accurate decisions in those busy environments.

10. Government Buildings. Visitor identification and area restriction are two very important security concerns for local, state, and federal levels. Intercom systems that provide visual and audio verification help deter unauthorized staff or visitors from entering secured offices and areas.

Whether it is a hospital, school, prison, retail store, or more, all facilities need to control access. Part of controlling access is the ability to see and hear the individual who wants it. Access control allows a team to safeguard a facility and allow entry, but it doesn't provide real-time information. Video surveillance allows security teams to see and detect, but used alone, it has its limits with providing a complete view of a situation, as well. Audio via an intercom solution brings those two elements together – it adds interactivity, and it allows people to hear, be heard, and be understood. It also allows security teams to control entry to a facility effectively.

__Bruce Czerwinski__ is the vice president of Sales and Business Development at Zenitel Americas.

SafeZone App
Call for help, receive alerts and proactively share location
OmniGuard
Responders continuously share location, communicate and visualize incidents
SafeZone Command
Real-time view of all incidents, resources available to assist, and means to coordinate optimal response
Indoor Positioning
Visualize incidents in 3D to speed response
SafeTrans
Live feed of vehicles to aid with monitoring shuttle buses or VIP protection

"Since some DVRs were not securely locked away, the university had concerns about data security and privacy. Maintaining the outdated security technology was becoming time-consuming and costly."

By Marc-Andre Bergeron

The Next Level

Unified platform gives access to built-in tools and analytics

Jeff Whyte/Shutterstock.com

The University of Calgary (UCalgary) is a top comprehensive research university located in Calgary, Alberta, Canada. With origins dating back to the early 1900s, UCalgary became autonomous in 1966. Over 50 years later, the university has more than 33,000 enrolled students and 5,000 staff across its five campuses, field stations, and other facilities.

The main campus is home to 11 of the university's 14 faculties and spans more than 200 hectares near the impressive Rocky Mountains. Other campuses include Foothills campus, Downtown campus, Spy Hill campus, and a remote campus offering nursing programs in Doha, Qatar.

Navigating the Inefficiencies of Older Security Technology

Ensuring community safety has always been a top priority at UCalgary. The security team works around the clock to secure its many campuses and keep everyone safe. This often includes using video, access control, and other security solutions to mitigate threats and promote a stronger sense of safety across its locations.

As years passed, the team began feeling the brunt of aging security technology. Each video and access control system was independently managed and owned, by various departments. Going to different sites to retrieve video evidence from DVRs or requesting the information from faculty contacts created roadblocks during investigations. Since some DVRs were not securely locked away, the university had concerns about data security and privacy. Maintaining the outdated security technology was becoming time-consuming and costly.

While the UCalgary team did their best to work around these inefficiencies and keep systems functional, they reached a point where they knew it was time for a major security upgrade. UCalgary began their journey to update their technology with the help of their trusted security integrator, Delco Security. The goal was to standardize on a video and access control solution across all university sites. They also sought to centrally manage all systems from one location and strengthen their cybersecurity and privacy posture. Having the freedom to upgrade other security systems later on, expand at their own pace, and select the devices that best fit their environment was also hugely important to the team.

With guidance from Delco Security, the UCalgary security team found what the right solution in the Genetec™ Security Center unified platform. According to Brian Whitelaw, chief of Campus Security at the University of Calgary, Security Center also supported a holistic approach towards physical security and cybersecurity convergence.

"Our goal was to have a standardized model for security convergence across our university. Genetec Security Center was the optimal solution that allowed us to bring all our security systems together under one umbrella. The unified platform also gave us access to built-in tools and analytics that would help us address cybersecurity and privacy, as well as enhance our overall situational awareness."

Standardizing the Security Center across All Campuses

Today, the UCalgary team works from a security operations center (SOC) on the main campus, using Security Center to manage access control, video surveillance, automatic license plate recognition, analytics, intercom and intrusion detection across all sites. While they are still migrating old systems onto the new platform, they currently have over 2,000 doors, 2,300 cameras, 45 intercom stations, 40 intrusion detection sensors, and various BriefCam analytics within the SOC. They have also implemented AutoVu Free-Flow to offer convenient gateless parking for students and staff, initially at three parking lots, with more to be added.

"We've definitely seen a better use of our resources with Security Center. In the past, if someone was at a door and called us via intercom to say they couldn't get in, we'd have to send staff," said Rick Gyson, director of campus security at the University of Calgary. "Now, our operators can visually identify and verify the person's credentials and remotely grant them access. When responding to an incident, we no longer need to rely entirely on witness observations. Our SOC operators can pull up video to see exactly what happened and share information with security staff while they are still at the scene. Security Center allows us to manage situations on campus more effectively."

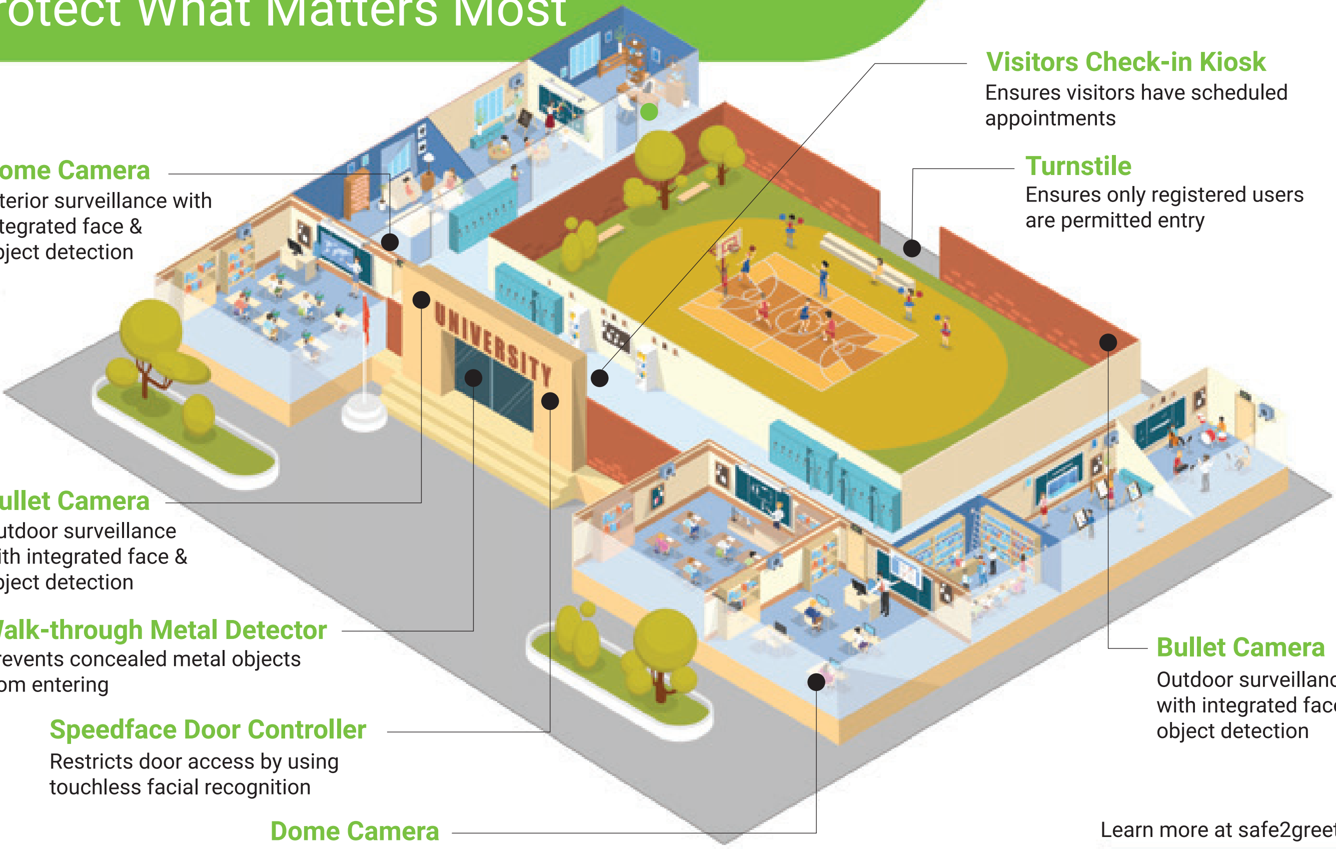
The SOC operators use Plan Manager – the map-based interface – to locate doors, cameras, intrusion points, and intercoms. This makes it easier to navigate the various campuses and buildings and eases the burden of having to memorize the locations of newly installed devices. They can also receive and respond to access control, intrusion, or other alarms directly from the map, speeding up incident response time.

"We've upgraded our security technology rather quickly, and we did have some concerns from an operational perspective whether our personnel would be able to adapt and feel comfortable using these new security solutions. Having a fully unified security platform like Security Center has made that easier. Now, rather than having to train staff on many different systems, there's only one system to learn and use," Gysen said.

COMPLETE CAMPUS SECURITY

Protect What Matters Most

ZKTeco USA



Visitors Check-in Kiosk
Ensures visitors have scheduled appointments

Turnstile
Ensures only registered users are permitted entry

Dome Camera
Interior surveillance with integrated face & object detection

Bullet Camera
Outdoor surveillance with integrated face & object detection

Walk-through Metal Detector
Prevents concealed metal objects from entering

Speedface Door Controller
Restricts door access by using touchless facial recognition

Dome Camera
Interior surveillance with integrated face & object detection

Bullet Camera
Outdoor surveillance with integrated face & object detection

Learn more at safe2greet.com

VISITOR MANAGEMENT | ACCESS CONTROL | VIDEO MANAGEMENT | METAL DETECTORS

Protect students, staff, and visitors with Safe2Greet

Health screening questionnaire

Metal detector screening for concealed metal objects

Automated skin temperature and mask compliance

Prioritize campus safety with ZKTeco's complete, personalized & dependable security solutions

(678) 826-3043 | info@zktecousa.com | zktecousa.com | 1600 Union Hill Road Alpharetta, GA 30005

Migrating Access Control with Intuitive Tools and Support at Hand

Achieving better situational awareness and response efficiency did not happen overnight for UCalgary. The team took a phased approach, which allowed them to upgrade one system at a time and keep expanding as budgets are renewed.

"Our main goal was to identify standards for our security installations and then grow and apply those standards across our campuses. The scalability and openness of the platform were hugely advantageous in that regard," Gysen said. "We could choose technology from many different manufacturers and upgrade our systems at our own pace."

Taking a phased approach was also particularly helpful during the access control migration. Moving access control data from multiple disparate systems onto a new platform can be a daunting task. UCalgary began with a pilot project of 80 doors. Throughout the process, the team was put at ease with the hands-on support they received from Delco Security and Genetec.

"We had some concerns about how we were going to manage access control data as we transitioned from old legacy systems to Security Center, but entire integration were extremely supportive throughout the process," said Satnam Dhanda, campus security electronic systems specialist at the UCalgary. "We had access to the import tool which helped ease that initial data transfer. This allowed us to upload batches of cardholder data into the new platform using CSV files. And now, we're working towards implementing the Security Center Active Directory integration which will streamline our processes moving forward."

Today, UCalgary has more than 85 buildings completed and are just about halfway through the access control migration. The team also took advantage of the Synergis Cloud Link to keep costs down and further expedite the access control migration. This intelligent gateway appliance offers native support for non-proprietary access control hardware. This meant the university could keep existing access control wiring and readers, and minimize hardware and labor costs. Currently, UCalgary has more than 45,000 cardholders, which include students, faculty, administrative staff and contractors. Using the Synergis system, the team can now secure access control rights, manage all cardholder privileges, and customize door rules and schedules from one platform. They can also quickly deactivate cardholder credentials across all sites and pull detailed reports to support compliance mandates.

"This allowed us to get very granular with customizing door rules and schedules, which helps our team, be more responsive to the needs of specific faculties and departments. During the pandemic, for example, our kinesiology department and medical school required some unique exception rules to restrict building access," said Brian Whitelaw, chief of campus security. "Our School of Architecture and Design also has a downtown location that has to be open to students but closed to the general public. We were able to accommodate those business requirements using Security Center."

Boosting Operational Efficiencies with Video Analytics and Intercom

Another key aspect of the security upgrade at UCalgary was adding video analytics and intercom. The team began by replacing old analog help phones with new SIP-based video intercom stations from Axis Communications. These devices enhanced video coverage around the main entrance buildings and offered easy two-way communication with SOC operators, at the press of a button.

"Having these new video intercom devices unified within the Genetec platform has given us a much better understanding of our environment. When we had the old help phones, we always relied on a person's ability to describe where they were and what was going on. With the video intercoms, we can see exactly where they are, pull up nearby cameras, and see what's happening, all while keeping the dialogue with them going," Gysen said.

Investigations have also gotten a boost since deploying BriefCam analytics within Security Center. Various analytics such as object removed or left behind, direction, dwell time, and crossline detection can all be used to speed up searches when an incident occurs on campus.

"We use the BriefCam analytics much more for investigation purposes. Whether its theft or another event, there are cases where something might happen after hours on a Friday, and it's only reported on Monday morning. Rather than having to search through three days' worth of footage, we can use the analytics to find what we're looking for much faster," Dhanda said.

"We're also able to narrow down our searches using criteria such as gender, adult versus child, and predominant colors of an item, so there's a lot of flexibility. This can be particularly valuable if ever we run into a case where someone has gone missing or for other more urgent investigations," Gyson said.

Streamlining Parking Enforcement with AutoVu Free-Flow

Using Security Center, UCalgary has also streamlined parking at the main campus. In the past, parking attendants would sit at a lot entrance, collect payment, and issue physical parking permits to drivers. The parking team at the university has since done away with all that using AutoVu Free-Flow, a module of the Security Center AutoVu™ automatic license plate recognition (ALPR) system.

"We have installed ALPR cameras at the entrance of three lots. Students or guests can now drive into the lot and pay for their time at a pay-by-plate kiosk. If the driver goes over the allotted time, our parking team will receive an alert within Security Center indicating the vehicle is in violation. Again, this is another situation where we're able to maximize our team's efficiency," Dhanda said.

Since the ALPR system is a core component of Security Center, the security team can also access the ALPR data during investigations. In the future, they are considering adding more ALPR cameras on campus roadways to better track vehicles of interest and further enhance security.

Investing in a Unified Security Platform that Evolves

UCalgary has many other plans for continued expansion on the horizon. First, the team wants to finish upgrading and standardizing all their access control, video surveillance, intrusion, and intercom systems within the Genetec platform. The security team is also in the process of setting up Genetec Mission Control™, the collaborative decision management system. When an incident occurs, this system will automatically guide operators through response protocols, so they can confidently handle any situation.

"We had seen another university using a Physical Security Information Management (PSIM) system, but the cost to implement that solution was well beyond our budget. Built into the Security Center platform, Mission Control gives us the same efficiency-boosting functionality at a fraction of the cost. Using Mission Control, we can reduce the sensory overload for our operators and help them focus on the most urgent situations," Gysen said.

"Right now, we think this is a very exciting time to be standardizing. Technology is evolving at such a fast pace, and we now have the foundation to be able to accommodate new innovation," Gysen said. "We also have so much flexibility in how we can adapt and expand our security platform. We are free to keep evolving our security initiatives to protect our campus community. A testament to our success is hearing from students themselves about how the security technology enhances their feeling of safety on campus," Gysen said.

***Marc-Andre Bergeron** is the director of sales for Canada, at Genetec.*

NIGHTLOCK®

LOCKDOWN SAFETY PRODUCTS

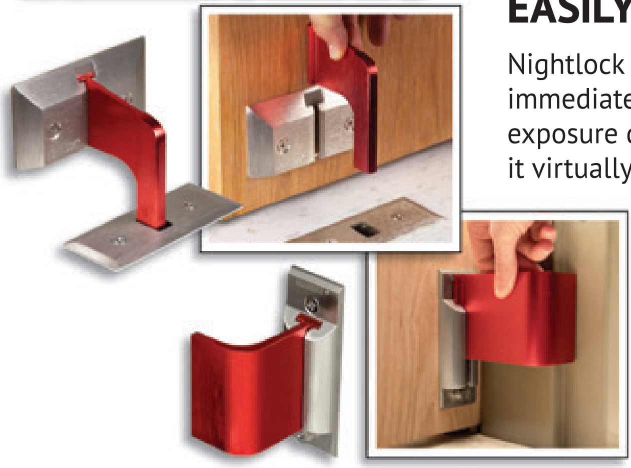
• CLASSROOMS • OFFICES • SAFE ROOMS

LOCKDOWN DOOR BARRICADES

✓SIMPLE ✓FAST ✓SECURE
FOR EXTREME EMERGENCY SITUATIONS

EASILY SECURES A ROOM IN SECONDS!

Nightlock Lockdown Door Barricades allow an individual to immediately lock the door from inside a room, eliminating exposure during a hostile intruder situation. This device makes it virtually impossible for an intruder to breach a locked classroom or office door.

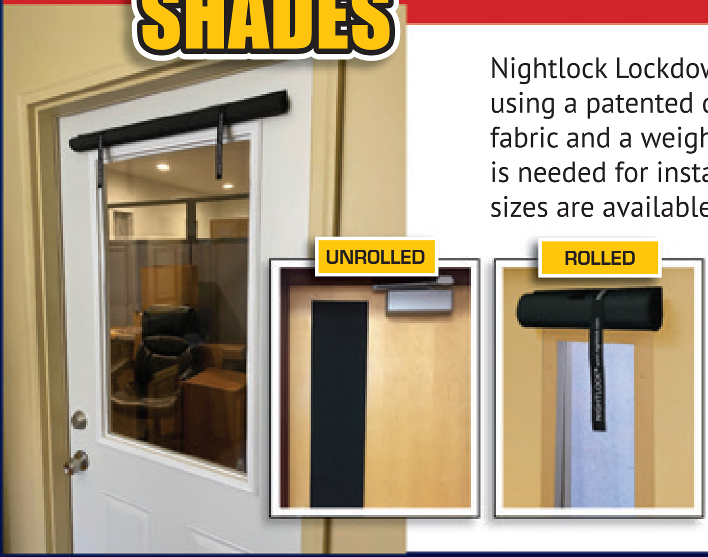


- **Simply add this safety device to doors**
- **Works with outward and inward swing doors**
- **No need to replace existing hardware**
- **One time solution - easy to install**
- **Lockdown in seconds**

LOCKDOWN SAFETY SHADES

✓EASY INSTALLATION ✓FIRE RETARDANT
✓QUICK DEPLOYMENT

Nightlock Lockdown Safety Shades are manufactured using a patented design featuring high-quality blackout fabric and a weighted hem bar. No drilling or hardware is needed for installation; 10 standard sizes and custom sizes are available.



- **Acts as a deterrent by blocking the view into classroom and office door windows/sidelights during emergency situations**
- **Cost Effective**
- **Customizable to fit all door and window sizes**
- **Installs easily**

Helping you be "Lockdown Ready!"

nightlock.com | 855-644-4856 | sales@nightlock.com

"To achieve this vision, campus communities must depend now on the social and political actions by university students, staff and faculty, administrators, and police leaders."

By Lt. Anthony Frisbee

A Contentious Debate Rages

Defunding police is not a new viewpoint of conversation

Simone Hogan/Shutterstock.com

Safety for some is not "inclusive safety" for all. A contentious debate rages on college campuses today to defund and abolish campus police. Yet college campuses across the nation are increasingly complex small cities, with rising student enrollment, more on-campus housing, an increasing number of high-profile controversial events, and yes, even crime (Wilson, 2015).

Theoretical lines of debate have been drawn in the sand with virtuous slogans and partial truths hurled as facts at their opponents. All this done to bring you to "their" side and earn your support. Neither of those for or against abolishing the police yet provide a public safety solution that balances safety obligations with community concerns and priorities.

Inclusive safety is a vision in which all members of the campus community should feel valued, welcomed and free from harm (UC, 2021). To achieve this vision, campus communities must depend now on the social and political actions by university students, staff, and faculty, administrators and police leaders.

Reimagining Campus Policing

This is not the first time campus communities faced paradigm-changing sociopolitical decisions affecting their safety. College police departments emerged 50 years ago in large part as an outcry for change. On May 4, 1970, National Guard members shot student protesters at Kent State University. After some 70 shots fired, four students lay dead. Nine other students were injured (History.com, 2017).

This tragic incident was a tipping point that sent shock waves across the country. Horrified how local city police and national guardsmen were violently clashing with campus communities during massive civil rights and anti-war demonstrations, campus administrators along with faculty and students demanded policing be reimagined on college campuses (Gelber, 1972).

State legislatures paved the way to allow colleges to create their own campus police that could relate to their unique campus communities and provide a safer environment at the behest of students, faculty, and staff (Sociopolitical Climate, 2009). By 2012, more than 4,000 university police departments across the United States serve and protect their respective campus communities (Reaves, 2015). More than 50 years after their initial creation, it is time once again to reimagine how campus safety can be achieved.

The Efficacy of Campus Policing

Many legislators, university administrators and campus police chiefs tout the success of campus policing as their ability to support safety stemming from specialized knowledge and close connections to the campus community (Peak, 2008). This premise is further supported by academic research that found campus police focus more on student safety than city police (Anderson, 1996). While one study found no significant short-term effects on crime rates caused by employing a college police department, it did reveal a significant long-term impact to reduce violent crimes by employing college police (Heaton, 2017).

Most colleges today offer comprehensive multidisciplinary resources to their community members. In addition to the police, colleges often employ counseling centers, student health, student affairs, academic affairs, equal opportunity and diversity, wellness education and mediation departments.

Using their specialized knowledge and close campus connections, college police can guide those in need to resources in their network that often fall outside of traditional criminal justice responses to resolve non-violent matters. Many of these campus resources, such as counseling centers and student wellness departments, help college students before their struggles reach the point of crisis requiring police intervention (Figueroa, 2021). In spite of the unique effectiveness of the campus police model, it has been swept up in the national dialog over abolishing the police.

Abolish Campus Policing Debate in the 2020s

Until recent years, the role of campus law enforcement has experienced a relatively unopposed 50-year expansion since its primary emergence in the 1960s and 1970s. Campus community support, in part, has been due to the belief that college campuses can be dangerous, thus requiring the need for college police. One may be perplexed as to why some community constituents who demanded the expansion of college police departments in the 1960s would now advocate for the disarmament of the very college police established to support their safety.

Abolitionists strategically chose to focus on college policing to initiate their efforts (McDowell, 2018). It is an interesting approach, considering research reveals young people are less likely to have positive attitudes about police (Wilson, 2015). The murder of George Floyd in 2020 during the Covid-19 pandemic though, galvanized social, political, business and media stakeholders toward a shared vision to "reimagine" and, increasingly, toward "defunding" and "abolishing" the police (DanDerWerff, 2020).

The death of George Floyd did not involve campus police officers; however, it spurred newfound social and political support to abolish college policing.

Several movements are striving to abolish police from college campuses altogether (DisarmUC, 2020). At least 44 student led petitions have been filed since by July 2020 to abolish police services from college campuses across the nation (Barajas, 2020). College administrators feeling the pressure of student activists and an increasing numbers of faculty begun holding "reimagining public safety" town halls and safety symposiums.

These efforts have already seen some success. In February 2021, Los Angeles officials announced they were removing 100 police officers from the schools and reducing the Los Angeles School Police budget to "reinvest" in the 'Black Student Achievement Plan' (Jake, 2021). In April 2021, during a public town hall meeting, University of California (UC) Board Regent chair John Perez shared he was open to discussions to reduce campus police across the 10 UC campuses by up to 40% (Turpin, 2021).

Pursuing a Holistic Safety Model

Decisions on the future role of campus law enforcement may ultimately be detrimental to college communities if not guided by principles for inclusive safety meant for all members of the campus.

"When any part of the American family does not feel like it is being treated fairly, that is a problem for all of us" (The Economic Times, 2014)," said Pres. Barack Obama. "Campus administrators and campus police chiefs need to embrace those desiring to reimagine college policing as community partners in the joint pursuit towards the creation of enhanced solutions to the ever-growing complex safety challenges. College police have the opportunity now to lead transformational change in partnership with their communities by taking proactive measures towards a shift to policing that is effective, and also inclusive."

Two Views – Armed or Unarmed?

The current debate on the future of campus policing often centers around two polar scenarios: campuses with no armed campus police or campuses with armed campus police. Neither of these proposed scenarios align with the principle of providing an inclusively safe campus environment for all community members.

The abolitionist argument to eliminate armed campus police and not to allow local city police to respond in their stead does not provide a solution to address violence or crime occurring upon campuses. Yet, others who would argue for the need of armed campus police with no change in campus policing are missing the opportunity to provide safety services more effectively to the whole community.

It is evident not all police calls-for-service require a response by an armed campus police officer. Yet this is exactly the safety model the majority of campuses utilize today. Conversely, an unarmed public safety or security officer is not equipped to respond to a call-for-service involving violence or complex criminal investigations.

Over the last fifty years, the role of college police expanded to community caretaker and social worker due to the convenience of having college police available 24 hours a day, 365 days a year, and the financial savings from not having to rely upon others. As we explore the opportunities to reimagine policing, it is equally important to reimagine the existing social service model used on campuses.

The Paradigm Shift

It is time for a paradigm shift in college policing by introducing a new holistic safety model that applies a tiered guardianship approach to support inclusive safety on campuses. Jumping ahead only five years shows us what can be done.

The new-tiered guardianship approach uses other professionals with specialized expertise as first responders to non-police related incidents. Just as fire departments responds to medical aid and fires, social workers and behavioral health professionals would now respond to incidents involving matters such as homelessness, substance abuse, and mental health/illness.

Additionally, unarmed public safety officers would now augment college police personnel, responding to non-violent and routine criminal matters, such as theft reports and building security checks/unlocks.

The college police would respond as a support resource to the other first responders in this tiered guardianship approach, just as they do for the fire department when an incident requires police assistance. Using a holistic safety model, the primary role for college police has become one of community guardian rather than enforcer like their city police counterparts. Campus communities benefit from having college police onsite to continue and respond to violence and complex criminal matters. Calls to defund or abolish campus police have subsided as the college community increasingly sees how the new model works, and that they are still safe even as fewer armed officers are in their midst.

Research has shown increased interactions outside formal police enforcement actions can significantly enhance the cooperation between the campus police and its community (Williams, 2015). Research has also demonstrated when people relate with the police, they tend to view them more positively, with legitimacy (Bradford, 2014).

The paradigm shift from enforcer to guardian on college campuses described above would further enhance community relations in support of inclusive safety, and can be a roadmap for college policing for the next 50 years.

The Future of Campus Safety

The role of campus law enforcement is at a strategic juncture. Whether campus police will enhance or diminish safety on college campuses ultimately depends upon the social and political decisions made today by university communities. Safety on college campuses requires that we challenge the status quo. As we do, the future safety of campus communities depends on the success of realigning campus policing with the purpose initially imagined 50 years ago when campus policing emerged – to support a safe and secure campus environment for the whole community. It is time to enact a holistic safety model using a tiered guardianship approach in partnership with social services to support inclusive safety upon college campuses.

***Lt. Anthony Frisbee** is a member of the University of California-Irvine Police Department.*

REFERENCES

- Anderson, T. H. (1996). *The movement and the sixties.* New York: Oxford University Press.
- Barajas, J., 2021. At some U.S. universities, a time to rethink cops on campus. [online] Los Angeles Times. Available at: <https://www.latimes.com/world-nation/story/2020-07-09/amid-nationwide-calls-to-defund-the-police-universities-rethink-ties-to-police-dept> [Accessed 5 July 2021].
- Bradford, B. (2012). Policing and social identity: procedural justice, inclusion and cooperationbetween police and public. *Policing and Society*, 24(1), 22–43. doi: 10.1080/10439463.2012.724068
- City News Service (2020, November 7). NBC Lost Angeles: LAPD Budget to be cut by $150 million; Decision triggered by widespread protests. Retrieved March 13, 2020, from https://www.nbclosangeles.com/news/local/lapd-budget-to-be-cut-by-150-million-decision-triggered-by-widespread-protests/2456578/.
- Clery Center. (n.d.). Retrieved March 8, 2020, from https://clerycenter.org/policy-resources/the-clery-act/
- DanDerWerff, Emily (2020, June 8). Vox: The Narrative Power of "Abolish the Police." Retrieved March 6, 2020, from https://www.vox.com/culture/2020/6/8/21281069/abolish-the-police-black-lives-matter-george-floyd-protests-minneapolis-new-york.
- DisarmUC. (n.d.). Retrieved March 8, 2020, from http://www.disarmuc.com/
- Ekins. (2017, August 1). Policing in America: Understanding Public Attitudes Toward the Police. Results from a National Survey. Retrieved December 21, 2019, from https://www.cato.org/survey-reports/policing-america.
- Figueroa, S., 2021. Why your campus should invest in mental and emotional wellness programs |. [online] University Business Magazine. Available at: <https://universitybusiness.com/why-your-campus-should-invest-in-mental-and-emotional-wellness-programs/> [Accessed 5 July 2021].
- Gelber, Seymour (1972).The Role of the Campus Security in the College Setting. (Washington, D.C.: U.S. Government Printing Office).
- Heaton, Paul, Hunt, John, & Jessica. (2017, June 30). The Short- and Long-Run Effects of Private Law Enforcement. Retrieved March 8, 2020, from: https://www.rand.org/pubs/external_publications/EP67207.html
- History.com Editors. (2010, May 25). The 1960s History. Retrieved February 19, 2020, from https://www.history.com/topics/1960s/1960s-history
- History.com Editors. (2017, September 8). Kent State Shooting. Retrieved February 18, 2020, from https://www.history.com/topics/vietnam-war/kent-state-shooting
- Horowitz, H. L. (1986). The 1960s and the Transformation of Campus Cultures. *History of Education Quarterly*, 26(1), 1. DOI: 10.2307/368875
- Jake, Dima (2021, February 18). Los Angeles schools removes over 100 officers and cut police budget to reinvest in 'Black Student Achievement Plan.' Retrieved March 16, 2021, from https://www.msn.com/en-us/news/us/los-angeles-schools-remove-over-100-officers-and-cut-police-budget-to-reinvest-in-black-student-achievement-plan/ar-BB1dMdft.
- McDowell, M. G., & Fernandez, L. A. (2018). 'Disband, Disempower, and Disarm': Amplifying the Theory and Practice of Police Abolition. *Critical Criminology*, 26(3), 373–391. https://doi.org/10.1007/s10612-018-9400-4.
- Nelson, L. (2015, July 29). Why nearly all colleges have an armed police force. Retrieved March 2, 2020, from https://www.vox.com/2015/7/29/9069841/university-of-cincinnati-police
- Peak, K. J., Barthe, E. P., & Garcia, A. (2008). Campus Policing in America: A TwentyYear Perspective. Police Quarterly, 1 1(2), 239-260. doi:1 0. 1 1 77/1 098 6 1 1 1 07306840
- Rubinstein, Dana (2020, June 30). The New York Times: Nearly $1 Billion Is Shifted From Police in Budget That Pleases No One. Retrieved March 6, 2021, from https://www.nytimes.com/2020/06/30/nyregion/nypd-budget.html.
- Simone Figueroa | December 16, & Figueroa, S. (2020, December 16). Why your campus should invest in mental and emotional wellness programs |. Retrieved July 06, 2021, from https://universitybusiness.com/why-your-campus-should-invest-in-mental-and-emotional- wellness-programs/
- The Economic Times. (2014, December 2). Young people of colour feel not being treated fairly: US President Barack Obama. Retrieved from https://economictimes.indiatimes.com/news/international/world-news/young-people-of-colour-feel-not-being-treated-fairly-us-president-barack-obama/articleshow/45343805.cms
- Tikkanen, A. (2020, April 9). Virginia Tech shooting. Retrieved April 12, 2020, from https://www.britannica.com/event/Virginia-Tech-shooting
- Turpin, L., 2021. U*C community discusses potential UCPD reforms at Future of Campus Policing event - Daily Bruin.* [online] Daily Bruin. Available at: <https://dailybruin.com/2021/04/23/uc-community-discusses-potential-ucpd-reforms-at-future-of-campus-policing-event> [Accessed 5 July 2021].
- UC Presidential Campus Safety Plan. (2021, June 01). Retrieved June 06, 2021, from https://www.ucop.edu/campus-safety-plan/
- Wilson, C.P., & Wilson, S.A. (2015). Evaluating legitimacy and marginalization: Campus policing in the State of Rhode Island. *Cogent Social Sciences*, 1(1), DOI: 10.1080/23311886.2015.1006091

"A comprehensive plan should be designed to ensure all parties are equipped to respond to the incident in real-time."

By Robert Watson

Crisis Management Technology

Better preparation for emergency managers for active shooter incidents

In recent years, the United States has witnessed a surge of active shooter incidents, which have put emergency preparedness into the spotlight for "when," not "if" the next tragedy occurs. Unfortunately, mass shootings have become a part of our daily lives - as gun violence is responsible for the loss of 38,000 lives per year, designating it the leading cause of premature death in the United States.

The United States alone has seen at least 147 mass shootings in the first few months of 2021, so far a 73% increase from years past, a trend that does not seem to be in decline. And as most active shooter events end in five minutes or less, emergency managers must be prepared to collaborate with first responders to activate life-saving response protocols and procedures to respond to the crisis and its aftermath in real-time, without warning.

The question then becomes, "How do emergency managers prepare for a mass casualty incident (MCI) that happens without warning?" While a community will never be able to prevent tragic incidents like mass shootings from happening, an emergency manager can put an active shooter plan into place that focuses on mitigation, response and recovery. A designed comprehensive plan will ensure all parties are equipped to respond to the incident in real-time.

When deploying the steps outlined in a community's active shooter preparedness strategy, having the right technology gives the emergency managers, community crisis teams, and first responders a flexible, connected incident command system solution. First responders and hospitals need to have an efficient real-time information flow with emergency managers to deploy life-saving techniques and personnel to save as many people as possible during an active shooter incident.

How can Technology Help Emergency Managers during an Active Shooter Situation?

Emergency managers must incorporate robust technology platforms into their emergency response and preparedness strategies to notify all stakeholders, minimize the potential for false or inaccurate notifications, and track the flow of information to ensure the parties involved are receiving it.

An effective platform also enables emergency managers to share critical information and updates with state and local agencies during an MCI event. This allows first responders and healthcare staff to focus on saving lives rather than going back and forth on the phone attempting to communicate the severity of the situation.

Responding to an Active Shooter, for Emergency Managers Preparation is Key

Active shooter incidents have become commonplace within numerous settings where groups of people gather – on college and high school campuses, in office buildings, movie theatres, churches, hospitals and retail stores and during community events. Assailants usually select target-rich locations and often carefully plan attacks weeks in advance.

Daniel M. Barnett/Shutterstock.com

There is no predictability as to when, where and how these MCI events occur; only those victims are blindsided; and emergency managers are thrown into chaotic, and often life-threatening environments. The importance of preparation and response time cannot be stressed enough.

In a report detailing the best methods to respond to active shooters, the Department of Homeland Security (DHS) describes a few key components, which can be helpful to emergency managers when developing an Emergency Response Plan (EAP):

- **Reporting:** Staff must know how to report an active shooter to first responders and colleagues.
- **Evacuation:** All exit routes and procedures should be outlined.
- **Management support:** Specific staff should be assigned emergency management roles to facilitate an efficient response.
- **Hospital information:** Details of local hospital accessibility, resources, and contact information should be included.
- **Emergency notification system:** Organizations must have a system to alert staff and monitor the situation.

"To best prepare your staff for an active shooter situation, create an Emergency Action Plan, and conduct training exercises," according to DHS. "Together, the EAP and training exercises will prepare your staff to effectively respond and help minimize loss of life."

Here are five best practices based on recommendations from the FBI, the Department of Homeland Security and other federal agencies that emergency managers can incorporate into their EAPs. They include advice for prevention, protection, mitigation, response and recovery.

Prevent Critical Events before They Strike

Prevention is the least glamorous and yet, most valuable strategy for protection. After all, an effective prevention strategy is designed to be invisible, stopping threats before they appear.

Active shooter preparedness manifests itself in the training and tools that bolster employee safety and wellbeing. During a crisis, quick and coordinated communications are needed, and there is little to no time for planning. This urgency demands staff already have proper training through education and drills. Proper preparation also means an organization has defined reporting methods, and an emergency manager has tools in place for a tactical response.

Reports are vital to effective analysis and response. Common types include checklists, action plans, response playbooks, situational reports (SitReps), and After-Action Reports (AARs). Each of these forms should be thoroughly vetted to ensure your organization is recording and reporting data of value. Unfortunately, no innovative technology can compensate for poor or missing data.

Rather, digital systems are designed to enhance critical data during and after an active shooting event. Organizations should have a digital reporting method to handle reporting, communications, and assessment. The bundled set of tasks is vital to prevent delayed responses, communication gaps, and inaccurate data. The system should have robust features that can connect easily with first responders, incorporate an intuitive user interface, and have the capacity to manage workflows easily.

Protect Staff through Emergency Action Planning

The next strategic step to protect your organization is to create an EAP. This plan is an emergency response playbook for staff. EAPs help staff react quickly, improve decision-making, reduce panic, and help organizations spot potential emergency management obstacles before they turn into problems.

Create a Threat Assessment Team to Mitigate Damage

Most emergencies do not call for a superhero. Typically, they demand a team of superheroes.

This is the case when confronting the threat of an active shooter. Organizations can benefit from professionals in different sectors, geographies, and industries.

They also benefit from individuals with diverse skill sets. For these reasons, the FBI recommends creating a Threat Assessment Team (TAT), a group of professionals that works with law enforcement to forecast risk and provide recommendations.

A TAT strategy can be used, even with one emergency manager on staff. For an active shooter, this means building a team — whether paid experts or experienced community volunteers — that analyzes an organization, its staff, and stakeholders and provides an objective, data-driven risk analysis. TAT members conduct interviews, gather information, evaluate threats, aid in decision-making, and follow up to re-assess strategies and impacts.

A TAT connected to a digital network and operational intelligence is even more useful. Juvare has seen this first-hand across diverse industries and organizations. An emergency intelligence network can provide a consistent and comprehensive view of operations, highlight essential resources, and deliver updates.

Data visualizations, mapping, third-party data, and custom dashboard analytics can increase awareness and ensure a targeted response. This applies to one person, or many people, tasked with handling operations.

Centralize Systems for a Rapid Response

For the fastest response, it is imperative to reduce unnecessary decision-making and unneeded tasks. Organizations respond with speed when there is an emergency plan in place, regular employee training through education and drills, and an effective emergency response management system.

A centralized crisis and emergency management system has the power to accelerate and simplify processes. These systems do this by eliminating the need for multiple software applications and manual work.

Further, they quicken emergency response by automating reporting tasks and communicating in real-time with first responders for additional support. All key stakeholders during an active shooting — be they law enforcement, medical teams or leadership — kept up to speed of critical events as they develop. When an emergency manager has a clear picture and a fast response to an active shooter, they are able to provide law enforcement with vital details that save lives.

Review Data for a Resilient Recovery

Recovering from an active shooting event is one of the most challenging things an organization can go through. Many staff will be trying to cope. Leadership must notify loved ones in the case of injury and casualties. There will be pressure from the media and authorities to get an accurate account of what happened.

To effectively plan for the future, the DHS recommends emergency managers and organizations analyze the incident in-depth and create a report that assesses how critical events transpired. The report recommends looking at the successes and failures for improvements. It also suggests that leadership re-examine its Emergency Action Plan and look at data to make improvement recommendations. Digitizing this effort can alleviate some of the stress and work tied to this "after-action" report. Emergency response software breaks down when authorities were contacted, details how updates were delivered, notes losses and identifies impacted facilities.

The lamentable truth today is that violence threatens every organization. In the case of active shooters, this means dealing with attackers that are "actively engaged in killing or attempting to kill" colleagues, faculty, or students you know and care about. Unlike some natural disasters, these active shootings escalate rapidly and are hard for emergency managers to predict. What's more, organizations have a greater responsibility to prepare employees since much of an attack happens before police arrive. By having an effective real-time action plan in place, emergency managers can focus on mitigation, response, and recovery during an active shooter incident. Put simply, this level of preparation for an MCI event is no longer a choice but a must.

Robert Watson *is the CEO at Juvare.*

"In 2020, the U.S. experienced a particularly active North Atlantic hurricane season with a record-breaking 11 storms making landfall—including six hurricanes."

By Heather Bender

Providing Safer School Communities

Understanding grant requirements helps fund life-saving building projects

Studio MDF/Shutterstock.com

Many of us have experienced it. The dark greenish-gray sky and the strange stillness that happens just as ominous storm clouds gather. Even before a cell phone signals a weather alert, instinct tells us to find secure shelter, and with good reason.

While only a small fraction of storms create extreme weather conditions, the United States has more tornadoes than any other country in the world. With an average of over 1,000 tornadoes per year, no state is free from their threat. In 2020, the U.S. experienced a particularly active North Atlantic hurricane season with a record-breaking 11 storms making landfall—including six hurricanes.

Because huge storms move so swiftly and in such unpredictable ways, schools need to be prepared to protect students quickly. Extreme weather tragedies are caused by flying debris, so it is of utmost importance to construct storm shelters to code, including adequately protecting windows and securing areas with storm doors rated to meet ICC500 testing criteria for extreme weather.

Evolving Building Standards for Increased Protection

To meet the current IBC requirements, all educational facilities with more than 50 occupants must provide a safe room to protect students and staff from tornadoes and other extreme weather events in certain areas of the country such as Tornado Alley in accordance with ICC500 standards.

In addition, educational facilities are subject to ICC-500 standards in states or localities that have adopted IBC 2015 or newer and are in an area that has an increased risk of tornadoes (ICC500/FEMA-P361 provides a map for guidance). This requirement applies to any new construction, retrofit addition, or significant improvement project and is included in 2015 IBC and 2018 IBC. ICC-500 provides the minimum requirements for safety relative to the design, construction, and installation of storm shelters built for protection from high winds and impacts associated with extreme weather.

Manufacturers offer advanced rolling steel doors designed specifically for safe room protection against life-threatening tornadoes and hurricanes. However, only a few rolling door products are tested and certified to meet both ICC-500 and FEMA P-361 standards – a requirement to be included in an ICC500 rated shelter. It is important to specify a door from a manufacturer that meets these necessary standards to receive a FEMA grant, including the newly instituted BRIC option.

There is another factor to note when schools are planning to apply for funding. All FEMA safe rooms designed and constructed for educational facilities must follow the most recent edition of the FEMA publication Safe Rooms for Tornadoes and Hurricanes: Guidance for Community and Residential Safe Rooms (FEMA P-361).

Funding Safe Rooms and Storm Shelters in School Facilities

Storm shelters and safe rooms are common throughout Tornado Alley, a region that encompasses part of South Dakota, Nebraska, Kansas, Oklahoma, Texas and eastern Colorado. It is an area infamous for having the most powerful and destructive storms. However, these life-saving spaces are not as common nationwide, even though tornadoes have touched down in all 50 states.

Lack of funding and challenges navigating building codes and construction guidelines are frequent obstacles to making storm shelters a reality for many school districts.

The Federal Emergency Management Agency (FEMA) replaced its Pre-Disaster Mitigation program with the Building Resilient Infrastructure and Communities (BRIC) competitive grant program in 2020 to facilitate funding and encourage advanced planning for extreme weather. The new BRIC program supports state and local governments by encouraging them to shift their focus to proactively protecting their communities.

BRIC applications are reviewed on an annual basis, and school districts may submit safe room or storm shelter projects that meet the following requirements:

- Cost-effective
- Reduces or eliminates risk and damage from future natural hazards—such as extreme weather
- Follows one of the latest International Building Codes (IBC)—either 2015 or 2018
- Aligns with an applicable hazard mitigation plan
- Meets environmental and historic preservation (EHP) requirements

Wind Load and What It Means for Your Facility

By specifying commercial rolling doors and shutters that meet strict wind load requirements and are certified by a third party as being compliant to ICC500 standards as part of a storm shelter project, schools are able to design unique, open, light-filled spaces while meeting IBC requirements and ensuring they are compliant with International Code Council (ICC) 500.

Considering the codes are guidelines that echo the minimum requirements for safety, understanding what wind load is —and why it is important in storm shelters— should be a cornerstone of one's knowledge on the topic.

Wind load refers to any pressure or force that wind exerts on a building. There are three types of wind forces, including uplift, shear and lateral wind load. These are all common in a tornado, hurricane, or strong storm with straight-line winds. Shear wind load is a horizontal pressure on vertical structural elements. This kind of pressure is especially concerning because it can change wildly based on weather conditions.

Extreme weather, such as hurricanes, tornadoes, and thunderstorms with straight-line winds put acute forces on a building. This can cause doors to blow out due to the storm's wild swings in positive and negative pressure.

That is why rolling door and shutter products are tested, for both static and operable wind load. Static wind load specifies the maximum wind load at which a door is able to remain safely in place while closed. Operable wind load specifies the maximum wind load at which a door is able safely operate without the curtain of the door being hung up in the guides and stuck in an open position. Operable wind load may be a concern for schools that serve as community shelters during hurricanes. For instance, loading dock-rolling doors may need to operate during the storm to accept emergency supplies and necessities.

Calculating wind loads and determining which product works best can be a tricky science, especially because the calculation not only includes wind speed, but also 10 other factors for accuracy and safety.

It is vital for decision makers to reach out to rolling door manufacturers to learn more about wind load requirements, wind load calculations, and rolling door options. Manufacturers' architectural specialists and consultants use a Door & Access Systems Manufacturers Association (DASMA) calculator to identify comprehensive wind load needs and create custom closure solutions. They also work closely with school safety administrators and specifiers to ensure they are making the best decision when it comes to student, faculty and administration safety.

At The Intersection of Safety and Design

With the implementation of these stringently tested rolling doors, architects can include windows and natural light in their design of modular classroom pods, gymnasiums, and cafeterias—creating positive, learning-focused spaces that can also transform into ICC-500/FEMA P-361 rated safe rooms when needed. A single maximum protection-rolling door can be used to cover multiple openings or even banks of windows, and activated by a building alarm or the turn of a key.

The rolling door can deploy on alarm with no manual intervention, allowing faculty and staff to focus on the safety of the students, while also preventing them from witnessing the storm and—most importantly—protecting them from violent winds and flying debris. After the storm, the door coils back into the structure and out of sight until it needed again.

Proper planning enables school districts to obtain funding and gain valuable insight into the standards and codes needed to meet life-saving storm shelters and safe rooms. By selecting the appropriate rolling doors and working closely with their manufacturers, architects can design dual-use areas that provide inspiration for students and protect them from extreme weather when the need arises.

__Heather Bender__ is the strategic marketing manager at CornellCookson.

"The best way to begin is by breaking down each core vertical slice to determine its needs, and then find a solution that is open enough to make a multi-faceted system a reality."

Finding the right security solution for, let's say, multi-tenant housing, requires significant consideration. There is a variety of factors to think through, such as which doors need to be secured? How will visitors be managed? Where cameras will need to be deployed? What if that was just one small vertical slice of a much larger campus with distinct needs? Now you are thinking like a higher education buyer.

A university campus comes with diverse security needs. There is residential housing, academic buildings, point-of-sale locations like dining halls, and high-security areas such as research laboratories, sports stadiums involving mass gatherings, healthcare facilities and even off-season usage by third-party organizations such as camps or symposiums. Finding a solution that can cover all of those use cases is no simple feat. The best way to begin is by breaking down each core vertical slice to determine its needs, and then find a solution that is open enough to make a multi-faceted system a reality.

Management

Before diving into the solutions for the various use cases, it is critical to consider how any campus-wide security solution will be managed. Consider using an "area access manager" style of governance.

This partitions system administration rights across different departments to manage buildings, cardholders and any other relevant systems. This distributes the workload, reducing strain on the often resource-constrained security team.

Campus Buildings (with specialized areas)

The most common type of security needs on a higher education campus are the buildings students use every day for living and learning. For student housing, access control at the main entrance of the building is a necessity. Whether indoor wireless or PoE locks are included on individual room doors is a matter of budget. There is room here to go with mobile credentials but to accommodate other on-campus needs, as if dining halls and smart cards are also used. Integrating video management into the overall ecosystem is ideal for student protection, allowing a university to monitor everyone coming and going, and ultimately identify unauthorized individuals who manage to gain entry. Furthermore, campus buildings are used in the school off-season to house visitors for temporary stays (such as symposiums or camps), so the ability to provide temporary credentials becomes an important consideration when implementing a security solution.

One of the most onerous components of residential buildings is the constant turnover (as semesters come and go), along with ever-changing roommate assignments, because let's face it – not all roommates are a match made in heaven. Many institutions of higher learning do not have a good solution for this challenge and find themselves spending significant time manually changing access rights. Finding an access control solution that can easily integrate with the existing human resource or student information system to automate this process saves many headaches, while also reducing the risk of a student accidentally gaining access to the wrong residence hall room. In situ-

haireena/Shutterstock.com

By Brandy Edgecombe

50 customers in One

What it takes to think like a higher education buyer

ations like the recent COVID-19 pandemic, this integration also used to block a person's access to facilities for specified time-periods based on the results of a health self-assessment questionnaire, helping to create safer, healthier buildings for the entire campus community.

For standard academic buildings, access control should be deployed where needed – places of ingress and egress, as well as any rooms and closets that should not be accessible to the general population. Many schools have research programs and facilities that operate high-dollar equipment, store hazardous materials or controlled substances and contain valuable intellectual property.

The research areas must be protected with a higher level of security than a standard classroom. It is not uncommon for research programs to have federal funding and affiliation, which may require compliance with additional federal regulations. It is critical to select a system that supports compliance with all of the various regulatory requirements of a campus. At a minimum, readers need to use Open Supervised Device Protocol and multifactor authentication if any hazardous chemicals or controlled substances are being used and stored.

It is a solemn necessity that any solution includes ways for authorized persons to put a campus on lockdown, whether that be a special card swipe, a software-initiated lockdown or an input such as a panic button. Ideally, lockdowns should be customizable to certain campus areas for a more targeted approach.

Point of Sale

College campuses also include retail experiences with dining halls or on-campus stores, where students need an easy way to make purchases. As stated earlier, using smart cards that act as both an access credential as well as a place to store school funds is ideal.

Things can get tricky when students try to take advantage of "all you can eat" meal plans by giving friends their cards. One way to solve this problem while also speeding up entry is by integrating with biometric software and readers. Rather than multiple swipes of a card, students can simply walk through immediately as the biometric reader verifies their access. Exchanging cards is no longer possible when students are required to present a unique biometric, which in turn, reduces the financial loss a campus experiences with meal plan sharing.

Stadiums and Mass Gatherings

The influx of people on a big college game day presents a host of unique security challenges. A big rival football game can draw more than 100,000 people over a relatively short timeframe, and unlike other controlled and secure areas on campus, necessitates letting large numbers of people into a given area at a given time.

While it's not feasible to provide credentials to every visitor to the campus, risk can be mitigated by implementing extensive video surveillance to improve situational awareness around violence or theft, as well as intercom integrations to improve mass notification capabilities in the event of an emergency. Due to the open nature of athletic facilities, it makes the most sense to focus access control on select areas that require tighter restrictions, such as locker rooms, IT closets and areas where currency is stored.

Find an Open, Trusted Solution

If you take anything away from this simplified breakdown of the multiple uses of a college setting, it's that a good technology solution is an open one that has a wide variety of features, and a proven pedigree of seamlessly integrating with third-party technologies. With the right products and implementation, your security solution will certainly make for a safer campus – but it can do much more than that too.

It can simplify operations and enhance the everyday experience of students and faculty, all while providing the peace of mind and confidence needed to create an ideal learning environment.

***Brandy Edgecombe** is the director, Higher Education Solutions, at LenelS2.*

By Kelly Kleinfelder

9 Ways to Reduce Contaminants

Facility managers should consider practical steps first

To protect students and employees from the SARS-CoV-2 virus that causes COVID-19, air quality should be a top concern for school and college administrators. As we have learned more about how COVID-19 spreads, it has become clear that the vast majority of cases occur through airborne transmission—and improving the ventilation in campus buildings should be part of a layered approach to health and safety that includes multiple mitigation strategies.

Ventilation system upgrades can increase the flow of clean air and reduce the presence of contaminants inside buildings. Here are some practical steps that facilities managers and other leaders can take right away to improve campus indoor air quality.

Below are four simple, low-cost strategies for increasing the air flow in buildings, as well as five additional suggestions for improving the existing ventilation systems in schools and colleges to prevent the spread of SARS-CoV-2 and other contaminants. These suggestions draw on guidance from the American Society of Heating, Refrigeration and Air-Conditioning Engineers (ASHRAE) and the Centers for Disease Control and Prevention (CDC).

Simple Strategies

Introduce more outdoor air into buildings. If you can, open outdoor air dampers beyond their minimum settings to reduce the amount of air that is recirculated from HVAC systems. When weather conditions allow for this, open windows and doors to increase the flow of air from outside. Even a slightly open window can introduce beneficial outdoor air.

Increase air flow and circulation. Use portable fans wherever possible to circulate clean air and direct potentially contaminated air outside. Avoid placing fans in a way that could cause contaminated air to flow directly from one person to another. According to the CDC, one useful strategy is to use a window fan to direct room air outside. This will help draw outdoor air into the room through other open windows and doors without generating strong indoor air currents. Similar results are achieved in larger facilities using gable fans and roof ventilators, the CDC says.

Make sure ventilation and air filtration systems are working properly.

Check to ensure that all building ventilation systems are operating correctly and provide acceptable air quality for the occupancy in each space. Make sure air filters are properly sized. Inspect filter housing and racks to make sure filters fit correctly and to minimize the amount of air flowing around, instead of through, the filter. Make sure restroom exhaust fans are functioning properly and operating at full capacity when the building is occupied. Inspect and maintain exhaust ventilation systems in areas such as kitchens, and consider operating these systems any time the building is occupied.

Adjust HVAC system settings to maximize air flow. Adjust the settings on HVAC systems to increase total air flow to occupied spaces wherever possible. Turn off demand-controlled ventilation (DCV) controls that reduce air supply based on temperature during hours when a building is occupied.

In buildings where the HVAC fan operation can be controlled by a thermostat, set the fan to the "on" position instead of "auto," which will operate the fan continuously—even when heating or air conditioning isn't required.

More Complex Solutions

Upgrade HVAC systems to MERV 13 or better. Many schools and colleges have decades-old HVAC systems that will do little to prevent the spread of airborne viruses within buildings. An air filtration system's ability to remove particulates from the air is rated on a number system called Minimum Efficiency Reporting Values, or MERVs. This rating system is helpful in comparing the performance of different filters; the higher the MERV rating, the better a filter is at trapping airborne particles.

Both ASHRAE and the EPA recommend using the highest-efficiency air filters you can afford to combat the spread of COVID-19 in buildings, with a minimum efficiency target of MERV 13. According to the EPA, "Filters with MERV-13 or higher ratings can trap smaller particles, including viruses."

The New York City Public School System has spent millions of dollars to upgrade the HVAC systems within its schools from MERV 8 to MERV 13 filtration. Upgrading the air filtration within HVAC systems to a MERV 13 rating or better gives schools and colleges the best chance at capturing airborne SARS-CoV-2 particles and removing them from the air inside buildings.

Use HEPA filtration systems to help clean the air.

HEPA stands for "high-efficiency particulate air" filtration, and these filters are highly effective at pulling impurities from the air and holding onto them so they can not recirculate. HEPA filters technically aren't MERV rated, as the MERV scale stops at 16. However, if the MERV scale continued beyond 16, HEPA filters would be rated between MERV 17 and MERV 20. HEPA filters are considered 99.97% effective at filtering particulates as small as 0.3 microns.

HEPA filters can be used inside many HVAC systems, and portable HEPA filtration systems are also available to clean the air inside individual classrooms and other indoor spaces.

Consider using UVGI technology to supplement air filtration. Hospitals and other sterile environments have been using technologies such as ultraviolet germicidal irradiation (UVGI) for years to remove harmful contaminants on surfaces and in the air—and this technique is proving to be effective in mitigating the spread of COVID-19 as well.

UVGI involves the use of ultraviolet-C (UVC) light rays to kill the SARS-CoV-2 virus and other contaminants. Direct exposure to UVC radiation inactivates the virus; however, schools and colleges must use UVC lamps with caution, as UVC exposure to human skin or eyes can cause injuries. Using an air purifier or filtration system that contains

Virrage Images/Shutterstock.com

"Ventilation system upgrades can increase the flow of clean air and reduce the presence of contaminants inside buildings."

built-in UVC lamps as well as filters adds another layer of protection, and this strategy can be more effective than just using a filter alone.

Change air filters regularly. The air filters inside ventilation systems must be replaced periodically as recommended by the manufacturer. As the filters become dirty, they also become less effective. Changing them regularly requires a lot of discipline, not to mention money and staff time. However, failure to do so could lead to HVAC system inefficiency and put building occupants at risk from SARS-CoV-2 and other contaminants.

Establish a reliable supply chain for air filters and other supplies. During a crisis such as the COVID-19 pandemic, supplies such as air filters and personal protective equipment (PPE) can be hard to come by. The pandemic has shown that relying on a single supplier can leave schools and colleges vulnerable when there is a shortage of materials. Especially when demand is high, it's best to have access to a large and diverse pool of suppliers and manufacturers. This strategy not only helps with ensuring access to supplies; it also helps institutions procure materials at the lowest possible cost.

In New York City, school custodians are changing the air filters inside building HVAC systems every three months. With more than 1,700 public schools, this requires several thousands of filters at a time when supplies are scarce. Working with SDI, the city school system was able to source replacement filters from multiple suppliers. The district now keeps a store of filters in a separate warehouse just for this purpose.

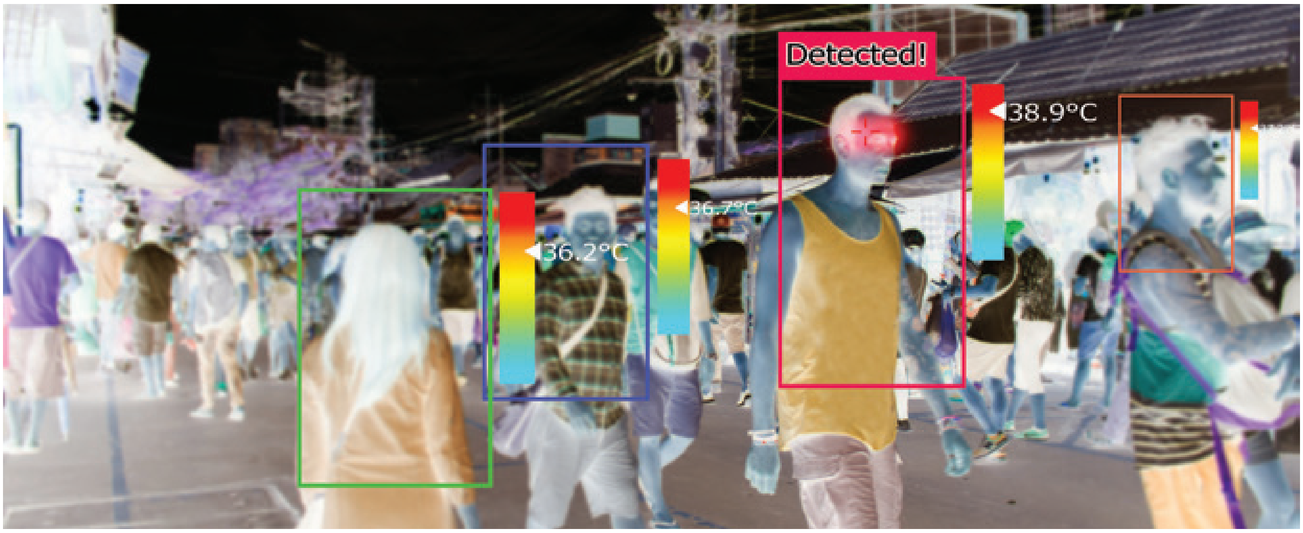
A Multifaceted Approach

The threat from COVID-19 has drawn attention to the need for better ventilation and air filtration in schools and colleges as part of a multifaceted approach to health and safety.

By applying these nine strategies, campus facility managers and other leaders can reduce the likelihood of SARS-CoV-2 transmission and other airborne illnesses and create a safer environment for students and employees.

Kelly Kleinfelder *is the CIO and senior vice president of information technology at SDI Inc.*

By Bruce Canal
and Paul Baratta



panuwat phimpha/Shutterstock.com

Adapting Security Technology

Innovations that will stand us in good stead for years to come

Necessity is the mother of invention, especially when it comes to battling COVID-19. We have tried common sense practices like frequent hand washing, masking, and social distancing. Yet the scourge is still among us. With school districts eager to get students back in the classroom, and hospitals desperate to curtail the surge of COVID patients, it is clear they could use a helping hand to return to some semblance of "normal."

Where might that helping hand come from? Network security technology. The same technology used to monitor and secure a campus can also be used to address the variety of problems posed by the presence of COVID-19. After all, protection is protection – whether you are trying to stop an intruder or a virus.

The beauty of these investments is that even though they're being used to combat COVID-19, the technology will continue providing safety and security value to a campus – whether an educational institution or medical complex – long after the virus has run its course.

Two application perspectives: traditional security and COVID

Surveillance. Most schools and hospitals install video cameras to keep an eye on who enters and exits the campus. They want to know if someone is suspiciously loitering around the property or trying to sneak into restricted areas. Those same cameras can be used for contact tracing, determining who might have been within three feet of or interacted with a COVID-19 positive individual. Since we know close proximity contributes to the spread of the disease, early identification and isolation of others who might have been exposed is critical to stemming a massive population outbreak.

Remote monitoring. Many hospitals remotely monitor patients so that medical staff can safely oversee multiple patients without compromising quality care. During COVID, virtual monitoring limits the spread of infection by reducing the number of times staff need to enter an ill patient's room. This also decreases consumption of personal protection equipment (masks, gowns and gloves) per shift, a significant cost savings.

Touchless entry. Hands-free entry systems have become a ubiquitous convenience. A video camera or sensor detects motion and automatically opens and slowly closes the door or triggers an alert for a remote person in authority to activate the automated door mechanism. People swipe a keycard to unlock the door themselves. During COVID, many schools and hospitals are taking hygienic access to another level with keyless entry systems that can be triggered by a QR code loaded on a smartphone, thus eliminating the need to touch virus-laden surfaces like door handles and keypads.

Replacing traditional doors with contactless power doors, like those used at handicapped entrances, can be especially useful in elementary school settings where students typically cluster in groups and take turns holding the door for classmates going in and out for recess. In entrances where additional security is an issue, campuses can integrate audio-video intercoms to enable visitors to be vetted for COVID exposure before activating the power door.

Intelligent audio. These systems provide a mechanism for conveying timely communication – live or pre-recorded messages – whether directing a trespasser to vacate the premises, announcing emergency evacuation procedures, or simply paging someone to report to a certain location. During COVID, many institutions integrating intelligent audio systems with video cameras to automatically trigger pre-recorded health information to people entering the building, such as a reminder to mask up and use the provided hand sanitizer.

Especially in schools where students tend to cluster, administrators

> "The beauty of these investments is that even though they're being used to combat COVID-19, the technology will continue providing safety and security value to a campus – whether an educational institution or medical complex – long after the virus has run its course."

can program a pre-recorded message to play throughout the day reminding everyone to follow CDC guidelines, wear their masks correctly, and keep three feet apart from one another.

Analytics. Many institutions enhance campus safety and security with the use of video and audio analytics. Video analytics provide early detection and proactively trigger alerts to potential security threats like motion, loitering, and perimeter intrusion or track operational issues like queue wait times or occupancy capacity. There are audio analytics that listen for sounds of aggression, breaking glass, weapons fire, and other acoustic signature that indicate danger to individuals or property. During COVID, analytics could detect whether persons are wearing masks or maintaining social distancing.

In school cafeterias, for example, video analytics can alert cafeteria monitors to intercede when too many students are sitting closely together or trigger an audio message to students to move to separate tables. If a student has tested positive for COVID, intelligent search analytics can be used to pull up video footage the shows everyone on campus they recently met, so they could be informed and tested.

Radar. Radar is also gaining traction as a warning system for after-hours intrusions into areas, such as athletic fields and hospital rehabilitation pools. The technology is often integrated with surveillance cameras to track trespassers or wandering patients to prevent safety and liability issues. When tied to intelligent audio systems, they can trigger a specific targeted message depending on the event – whether a warning to vacate the premises or an alert to staff that a patient has exited their room. In hospital settings, radar is often used on helipads to warn of any obstructions needing to be cleared before a helicopter arrives. During COVID, radar could detect someone approaching a school or hospital and trigger a message directing him or her to a single point of entry where they can be screened for health issues and issued a mask before entering the building.

Financing Technology Investments during COVID

With so many school districts and hospitals strapped for funds, financing any new technology investments might seem out of reach. However, in 2021 the federal government passed two economic stimulus packages – the CARES Act and the American Rescue Plan Act, which earmarked funding to schools and hospitals that can be used to pay for these types of projects.

Schools would need to submit a proposal to their respective state's Department of Education, while hospital would need to apply to their respective state's Department of Public Health. The important thing to remember when applying for these grants is to frame the proposal in terms of how the investment would help your institution prevent or mitigate the spread of COVID.

Schools and hospitals can apply for these monies through December 2024 or until their state's allocation has been exhausted.

__Bruce A. Canal, CPP,__ is the business development manager for K-12 and Higher Education for Axis Communication, Inc. __Paul Baratta__ is the healthcare business development manager for Axis Communications.

"A continuous, sustainable approach to school healthcare services can ensure that the physical and mental health needs of students are being met—and also that school staff members are equipped to provide adequate support."

By Dr. Robert Darzynkiewicz

A Reopening Strategy

Resources to support students' physical and mental health needs

Proxima Studio/Shutterstock.com

As schools begin to welcome students back in full force, there is increased attention on learners' physical and mental wellbeing. Since the latest round of COVID-19 relief funding includes dollars for in-school healthcare services, district leaders are encouraged to take this as an opportunity to revamp and strengthen existing student health programs.

For many families, school is more than a place to learn. It is also a place to receive access to healthcare, counseling, nutrition and other essential services. A continuous, sustainable approach to school healthcare services can ensure that the physical and mental health needs of students are being met—and also that school staff members are equipped to provide adequate support.

Here are some strategies for meeting students' physical and mental health needs as they return to school.

Strategies for Supporting Students' Physical Health Needs

District leaders will need to consider how they currently support the physical health of students, and if there are updates are needed before fully reopening.

Ensuring Compliance with CDC and Local COVID-19 Guidelines

In the CDC's COVID-19 K-12 Operational Strategy guidance, five key prevention strategies are listed to help prevent the transmission of the virus, including:

- Universal and correct use of masks
- Social distancing
- Handwashing and respiratory etiquette
- Cleaning and maintaining healthy facilities
- Contact tracing in combination with isolation and quarantine

To safely resume operations, I strongly recommend that district leaders look at their existing processes and make updates as needed. For example, establish social distancing and mask-wearing guidelines with staff and students, and keep an inventory of essential supplies (like face masks) on hand at each school site.

Providing In-school Telehealth Care to All Students

While telehealth has been around for many years, its popularity is skyrocketing due to the pandemic. Telehealth is the marriage of technology and healthcare, using a wide variety of technology and electronic communications to promote remote health-related services. Telehealth companies can partner with schools to provide in-school and in-home telehealth care services to all students.

In addition to assessing symptoms related to COVID-19, telehealth providers are able to address common health concerns, like stomachaches or allergy symptoms, and to create a care plan tailored to students' specific needs. Having telehealth providers available to support the work of school nurses and other staff members can help districts address a wider range of student health concerns and reduce absenteeism.

Educating Families about the COVID-19 Vaccine

The COVID-19 vaccine is an important piece of the school reopening puzzle. With efforts to vaccinate educators continuing, a recent trial showing 100% vaccine efficacy in children ages 12–15, district leaders must work proactively to quell vaccine hesitancy.

The CDC compiled a COVID-19 Vaccine Toolkit for School Staff & Childcare Workers that may be used to support communications with teachers and other staff members. In addition to this, I recommend that district leaders find a way to provide vaccine guidance and support to families, especially those in underserved communities.

Strategies for Supporting Students' Mental Health Needs

One of the most important considerations during this crisis and its aftermath is the mental wellbeing of students, staff and the community at large. The mental and emotional toll this crisis has taken on people is immense and will be felt for months, and years to come. Many students were in very vulnerable positions before this crisis hit. That has worsened. Social determinants of health have changed drastically, and situations are worse for many families than they were even just a few months ago.

With this in mind, district leaders and teachers must prepare for increased stress, anxiety and trauma and be ready to support students' mental health needs.

Expanding Existing Mental and Behavioral Health Services to Accommodate More Students

School counselors were already outnumbered pre-COVID, with an average student-to-counselor ratio of 430:1. Just as they are able to support the work of school nurses, telehealth providers can also support the work of school counselors, case workers and other staff. During a telehealth appointment, students can share their feelings and symptoms with a provider, who can then collaborate with the child and their family to create an action plan.

Providing Mental Health Support to Staff

To effectively meet the mental health needs of students, district staff members need support, too. In "Resources to Support Mental Health and Learning during School Reopening", the National Education Association (NEA) provides actionable strategies and resources for ensuring the wellbeing of staff, students and families.

Applying Social-emotional Learning (SEL) Strategies Throughout Education

The Collaborative for Academic, Social, and Emotional Learning (CASEL) recommends that district leaders make SEL an integral part of every student's education. CASEL compiled a list of COVID-19 SEL resources, which includes recommendations such as:

- Providing consistency in daily routines to foster a sense of safety and predictability.
- Taking the time to listen to students.
- Supporting students in building or maintaining a sense of community and connection.

Keeping Every Student Healthy

Whether you are an administrator, a teacher, a counselor or a nurse, you play an important role in keeping students well. By offering physical and mental health resources in school, we can help more students receive the care they need so they can focus on learning.

With the support of district leadership and increased funding, there is an opportunity to reinvent school health and wellness services and to make a real, positive impact in the lives of students and their families.

__Dr. Robert Darzynkiewicz__ is the chief medical officer at Hazel Health.

Ad Index

Advertiser	Page	URL
1105 media	39	www.spaces4learning.com/sif
Assa Abloy DSS	19	www.IntelligentOpenings.com/campus
Assa Abloy EMS	29	www.assaabloyesh.com/es100
CEIA USA	13	www.ceia-usa.com
Continental Access	5	www.cicaccess.com
CriticalArc	33	www.criticalarc.com
Garrett Metal Detectors	3	www.garrett.com
HID Global Corporation	43	www.hidglobal.com/touchless
IP Video	7	www.ipvideocorp.com
JVCKenwood	2	www.kenwood.com/usa
Nightlock	25	www.nightlock.com
Safety Technology Int'l, Inc	15	www.sti-usa.com/sp445
Salient Systems Corporation	44	www.salientsys.com
Salto Systems	9	www.salto.us
ZKTeco USA	23	www.zktecousa.com
Zenitel	11	www.zenitel.com
Viking Electronics	41	www.vikingelectronics.com

STEINER
Technology Corp.
Ann Ferguson
Senior Accountant

Safeguard your campus with Salient's open video data platform

At Salient, we focus exclusively on our open video data platform so you can easily incorporate best-of-breed technologies that expand your campus and operational capabilities. Salient's CompleteView video surveillance solution empowers organizations to view, record, and manage video data. Built with an open architecture, CompleteView is integrated with thousands of cameras, access control, and analytics solutions.

Find out how our platform can drive your campus operations with actionable video intelligence. Contact Salient today and let us focus on your security.

SALIENT™
www.salientsys.com