The underrated benefits of 'plug-and-play'

Security solutions are meant to protect and make customers feel secure. But that wasn't the case recently for a Mississippi couple who installed a camera to watch over their daughters. Someone hacked into the camera, scaring the kids and potentially putting them in danger. Before dismissing it as a one-off home security issue, look at what happened before the presidential inauguration when hackers hit more than 100 cameras that watched over the U.S. Capitol.

These are just a couple of examples of vulnerabilities that hackers have exploited. Researchers unearth new cyber weaknesses in network cameras frequently, prompting manufacturers and developers to release patches before someone tries to take advantage of them and it makes headlines.

Now consider for a moment, what happens when a surveillance camera system is hacked, or an end-user finds vulnerabilities in their installation through penetration tests. There is panic - of data leakage, of the device's functioning, and, of course, reputation, not necessarily in the same order.

And guess who gets the first call in most situations? If it's a government project as serious as the U.S. Capitol incident, the FBI may be called into action, but for most commercial enterprises this isn't an option. After reporting a breach to the police, the next call will be to the systems integrator.

The integrator will be blamed for the solution not being secure even if they are not at fault, even if it's the camera and the network devices themselves that are vulnerable. Often this impacts the integrator's reputation, who ends up having to rework on the project or even replace the whole system, free of charge.

Where Do the Vulnerabilities Lie?

Ask any cybersecurity expert, and they will tell you that any device connected to a network is at risk. Digital solutions could be vulnerable because of potential bugs in an algorithm, shoddy networking practices, or just carelessness from users. There is enough research done to back up these concerns.

The good news, of course, is that most solution providers are prompt to provide firmware updates to close any unexpected backdoors. The bad news is that this is a reactive approach, as there are obviously other weak points yet to be discovered, and it could be just a matter of time before a hacker is one step ahead of a researcher.

Making things worse are botnets. These clusters of connected, compromised-devices can cause devastating damage to networks, businesses, and countries. They are a security admin's worst nightmare not just because of the potential scale of damage, but also because of their flexibility that allows updating. For instance, after the Mirai botnet wreaked havoc across the globe, came another named Reaper that attackers could easily update to increase the damage it caused.

What You Should Know

An obvious conclusion is that there is no single answer to cybersecurity problems. A combination of robust technology and best practices is the ideal solution, and implementing it will require reconsidering the kind of solution providers you work with. In the meantime, the following factors need to be remembered.

1. More is Not Always Merrier

The security industry has been seeing the debate between open and proprietary protocols for quite a few years now. While the supporters of open protocol solutions argue that different companies need to specialize in different segments, there is no denying that integrating solutions from different companies is always going to be difficult.

Not all the devices from a company may work well with another company's devices seamlessly. Updates to firmware may also be difficult because integrators will have to manage each device separately. Sticking to solution providers who can meet all your security demands is a solution to this. But you will have to make sure that even these solution providers use technology that prevents third-party access effectively.

2. Firewalls Only Work When Configured Well

Firewalls are one of the first and most important lines of defense in network security. Simply put, it's a software that filters information coming into a device and going out from it, looking for anything that could be harmful. Its significance in NVRs is undeniable. But what many people don't realize is that a firewall is only as good as its configuration.

As a systems integrator or end-user, you must ensure the NVR solution you purchase has a firewall that is configured and designed to the best level.

3. Security of Transmission Systems is Equally Important

The use of transmis-

Dear Reader

With the lockdown due to COVID-19, having been extended to May 3, 2020 and even beyond in some states, many people are wondering what the future holds for them and their families, businesses and workers.

Since it is now abundantly clear that the lockdown will only be lifted in phases, with production at a stand still, supply chains disrupted, and many workers having gone to their home-towns, manufacturers and distributors are finding it difficult to plan ahead.

However, this is not the time to get into a state of despondency. Let us understand that the 'normal' as we knew it, is now a thing of the past. We shall have to work collectively towards creating a new 'normal'. For example, the west will be forced to concede that the 'namaste' or bowing from the waist which has been the "normal" for a large part of Asia, is a far better form of greeting than the traditional western handshake. Similarly, Asian families will be forced to give up their traditional huge family gatherings, with much hugging and backslapping in favour of more distanced meetings with the help of technology, and virtual meetings will replace large numbers of physical meetings. Many jobs may permanently take on a work from home 'avatar', thereby stepping up the need for more secure high speed internet connections, while petrol and diesel consumption and personal transport such as cars and motorised two wheelers may permanently see a very reduced rate of growth due to a lesser need to physically commute to one's workplace.

At the same time, traditional dependence on imports will shift towards more local manufacture and dependence on exports will shift towards greater development of domestic markets. In other words, we shall see a lot of change in the coming months and years.

However, I once again reiterate that this is not the time for despondency but the time to gird up one's loins and get down to the task of building a new India. Our workers are not a liability for us but rather an asset, who if treated with fairness and compassion will help us build a better, more efficient and stronger enterprise. While many things will change, there are some that must not. We must not lose faith in mankind, trust in our fellow human beings and the spirit to help others while trying to reestablish ourselves.

If we have not already done so, let us plan on how best to manage our affairs while still stretching out a helping hand to others. Keeping in touch with partners, clients and prospective clients is a vital aspect of this rebuilding exercise. Last month, I have already mentioned how progressive brands are smartly leveraging tools such as linkedin, facebook posts, tweets or blogs on their websites, publishing and promoting webinars, presentations or training videos, or simply engaging with the industry at large.

After all, if our parents' generation could overcome the effects of the partition in India and the holocaust in Europe, we too can rise to the challenges posed by this new kind of war.

Let us together once again raise the slogan "We Shall Overcome".

Till we meet next month,

Cheers, Stay Safe and Keep Others Safe.   **G B Singh**
Group Editor
📧 gbsingh@1stasset.org
🐦 @EditorGB
in linkedin.com/in/gbsingh9

TOP INDIAN WOMEN INFLUENCERS IN SECURITY

Globally women are playing a key role in the advancement of the profession of security in all sectors, verticals and levels of the industry.

In order to recognise and honour the accomplishments, value and contributions of women within this male dominated vital sector of the economy, SECURITY TODAY & SECURITY UPDATE, in association with InfosecGirls and the Women In Security & Resilience Alliance (WISECRA) have launched the 'Top Indian Women Influencers in Security' recognition.

This new accolade has been developed to help recognise women in security across india who have made significant contributions, advanced the industry and shaped the path for future generations of professionals among other vital contributions.

**There is 'No Fee' for Nominations.
Last Date to Nominate is 9th May 2020**

For nominations, please visit our website:
www.securitytoday.in

SECURITY TODAY
www.securitytoday.in

BLOCK YOUR DATE — AUGUST 26 & 27

KNOWLEDGE SUMMIT

August 26 & 27, 2020

New Delhi

YOUR QUEST FOR KNOWLEDGE STARTS HERE!

The Knowledge Summit presented by SECURITY TODAY has gained universal recognition for providing in-depth coverage of leading edge technical and security management issues facing Protection Professionals.

www.1stasset.org | E-mail: info@1stasset.org

The underrated benefits of...

sion protocols that are not secure enough could easily result in hackers accessing your data. Using cryptographic protocols like Transport Layer Security (TLS) is important here but this alone is not enough to get the most out of your system.

4. Never Underestimate Human Error

Security experts and solution providers often tell customers that the weakest link in cybersecurity is the user. Simple mistakes like not changing default passwords could end up costing the customer dearly.

But despite such warnings, many customers still fail to do the right thing. Unfortunately, in many instances, solution providers are content with just warning them of the issue. Clearly, it's not enough, and this is where plug and play solutions become relevant.

Why Plug-and-Play Solutions Are the Answer

With more and more devices getting integrated into security infrastructure, systems integrators and end customers need to have a method to manage each of them. However, if you factor in the chances of human error, managing more devices, with separate configurations and passwords for each of them, it could result in the solutions having several vulnerabilities.

For instance, having to setup a separate password for each device is time-consuming and monotonous, leading to installers or operators using weak passwords that can be easily broken by hackers. Or even worse, using the default passwords.

True plug-and-play solutions are the only credible answer to this. When devices require minimum configuration, there is less chance of human error, and this leads to better security. There is no need for users to come up with unique passwords and change them periodically for each device.

Plug-and-play solutions also make the integration process smoother. Systems integrators no longer have to worry about compatibility issues or frustrating device-configuration processes. A strong integration guarantees less chance of bugs in the system that hackers can exploit. Having a single solution provider watching over the whole integrated solution also allows integrators to rest assured that they can deal with any problem that may arise during or after the project through a single window.

Plug-and-Play to Reduce Total Cost of Services

Working with a cyber-secure physical security solution has several benefits for systems integrators, but if you look at the bigger picture, it all comes down to bringing the Total Cost of Service (TCS) down. TCS helps integrators understand the profitability of a customer account by determining the overhead costs and actual activities. A true plug-and-play solution that reduces cybersecurity concerns and offers a hassle-free installation process reduces overall TCS and gives integrators more room to utilize their resources better and boost their earnings.

Aiphone introduces IXG Series multi-tenant video intercom solution

Aiphone, the international manufacturer of intercom and security communication products, introduced its IXG Series IP-based video intercom, a comprehensive solution providing multi-tenant and mixed-use building managers with reliable network communication and entry security along with the convenience of a tenant mobile app.

The IXG Series integrates multiple security layers to meet property managers' needs for a single facility or an entire portfolio of mixed-use properties. The cloud-based IXG Series Mobile App enables tenants to screen visitors and un-lock entries using their smartphones from virtually anywhere in the world. The app may be used with or without an individual interior station. Building managers may select to have tenants screen visitors or have all entry requests go directly to a guard station before being transferred to the appropriate suite or apartment.

The IXG Series further enhances security with an available elevator control adaptor to ensure visitors access only the floor on which the tenant works or resides. All entrance, tenant and guard stations include touchscreen displays and enable onboard event recording with a microSD card.

Other features and benefits of the IXG Series video intercom include:

- Illuminated touch-screen entrance panel for interface and video display

- Available later in 2020, a physical video guard station

- Video conferencing between guard stations

- Confidence that the system is functioning as intended with scheduled or manual health checks of all stations, components and network connections

- Ease of installation. All stations are Power over Ethernet using standard structured cable (Cat-5/Cat-6)

The IXG Series may be combined with Aiphone's IX Series 2 peer-to-peer video intercom system with its many door, master and sub stations, adapters and modular emergency towers and wall boxes, to create broader, more powerful solutions for large and enterprise-level applications. The IXG Series is compatible with legacy and future IX Series and IX Series 2 products.

Abloy unveils Mobile Digital Key & 'Extremely Weatherproof' Bluetooth Padlock

Abloy Oy, has introduced its newest innovation in digital keys, the ABLOY BEAT. The new keyless solution combines three main components: a digital key, a mobile application and a heavy-duty, Bluetooth padlock. All is managed with the visual ABLOY OS user interface.

Among businesses worldwide, there is a growing need for the convenience and accessibility of highly secure keyless access solutions — either as an addition to existing workflows or as a standalone solution. Especially in remote areas or situations where carrying a physical key can bring the possibility of corruption or even danger for the holder, a mobile solution is also in demand.

BEAT is designed especially for professional physical protection of critical infrastructure, businesses and industry sites. While securing property, it also offers customers improved operational efficiency, reducing both logistics and costs. It also saves on fuel emissions, making it a sustainable option. The solution is intended to be used in sectors like telecom and data centers, transportation and logistics, utilities (water, electricity, gas) and mining.

The digital BEAT key connects to the physical heavy-duty, Bluetooth padlock, designed to perform in harsh environments and remote areas. The padlock has an IP68 protection rating, a case-hardened steel body and LED indications for lock status. It complements the current ABLOY® SUPER WEATHER PROOF range of padlocks.

BEAT can be integrated with existing security workflow solutions in use, but it can also be implemented as a standalone locking solution with ABLOY OS. ABLOY OS enables managing keys, locks, and access rights on-the-go and remotely from a single, easy-to-use and highly visual interface.

BEAT is the latest addition to Abloy's comprehensive and evolving digital portfolio of future-ready security and access control solutions. The news announced today is the first phase of the BEAT solution, and the company plans to unveil new features in the future.

'Proxy' Promotes Smartphone-Based Reader as World's Smallest

Proxy is bringing to market a new smartphone-based identity signal reader the startup company bills as being "so small it can be installed behind existing access card readers in just minutes."

The universal reader, called the Mobile Reader Nano, is said to provide employees, tenants and visitors with smartphone-based building access with no impact to existing security systems. Before now, companies that wanted to enable smartphone-based building access had to replace their existing readers, according to the company.

The Nano operates on 2.4GHz (Bluetooth Low Energy) frequency. Signals emitted from a person's smartphone replace the multitude of keys, cards, badges, apps and passwords people typically need to gain access to the buildings, devices and services they frequently use, according to the company.

The new reader is said to work with all access control providers, so there is no need to modify or replace backend access software. When both landlords and tenant companies implement Proxy Mobile Reader Nano, they can provide completely frictionless lobby-to-office access to tenants and visitors.

Alvarado launches SU4500 compact barrier optical turnstile to enhance perimeter security

As security requirements expand to smaller buildings and lobbies, architects and specifiers are looking for compact optical turnstiles that provide a high level of security in the limited space available. With this problem in mind, Alvarado has introduced its most compact barrier optical turnstile to date, the SU4500. Designed for high-end facilities where space is at a premium, the new SU4500 has a compact 38" cabinet length but doesn't compromise on security, throughput performance or looks.

The unobtrusive modern design does not impede or obstruct the line of sight, and the shallow depth of the lane ensures that it will fit in even the 'coziest' of spaces. Typical installation sites for the SU4500 include corporate lobbies and elevator banks, university recreation centres, government facilities and hospitals.

Because aesthetics is such an important factor in modern construction, the SU4500 includes architecturally inspired features and liberal use of crystal-clear materials. The SU4500 can be further enhanced through an optional lighting package that allows users to illuminate the side panels (and the top and end lights, if desired) in any RGB colour and create unique transition effects. The result is a modern look that complements any environment.

Integration is quick and easy, as the SU4500 integrates with virtually any existing access control or visitor management system. Dedicated inputs for fire or life safety systems are provided and outputs are available to turn on cameras, lock interior doors and provide remote notification of alarm events.

The SU4500 can accept various credential readers, including RFID and emerging technologies such as biometrics and elevator dispatch. The result is a secured access solution that not only looks amazing but provides superior access control and visitor management.

Climax X1 Alexa Built-in Alarm System

X1 is a new Alexa built-in voice-controlled smart home alarm system, incorporating home security, home automation, and emergency monitoring all-in-one. Users can talk to X1 directly and control the smart home system with the voice commands. Turn off the lights, arm the system, or apply a scene when there's a need—all hands-free and without hassle.

What's more, with Climax's Alexa built-in voice extenders (VRCP-WIFI-AVS) placed around the house, users can easily control the system with their voices via the nearest device to them, no matter if they are in the living room or the kitchen. The two-way voice communication on X1 and voice extenders also offers peace of mind during emergency events. Having a safer and comfortable living environment is easier and intuitive now.

With Alexa built-in, users can talk to X1 directly and control the smart home system with the voice commands, realizing home security, home automation, and emergency monitoring without hassle. X1 features two-way voice communication with echo cancellation, allowing for real-time conversation with anyone at home.

In a house equipped with Climax's Alexa built-in Voice Extender (VRCP-WIFI-AVS), users can easily control the system with their voices via the nearest device to them. The two-way voice function on voice extenders also provides great assistance during emergency reporting. X1 is compatible with Climax's F1 technology. With its fast transmission and reliability, the alarm reports will be sent timely to build a safer home environment.

With integration of Z-Wave automation sensors, X1 enables users to remotely control lights or home appliances according to customized schedules, scenes, or rules. X1 is tailored to all users' needs and enhances their quality of life. X1 can also assimilate round the-clock sensors, like smoke & heat detectors, water sensors to prevent disasters and quick response during emergencies.

Identiv integrates Bluetooth and cloud-based access control with MobilisID solution

Identiv, Inc. has announced the launch of MobilisID, its latest solution for frictionless access. The MobilisID solution brings ease and simplicity to physical access and management without compromising security. Using the latest in Bluetooth and capacitive technologies, MobilisID allows users the freedom to access a controlled environment without the need to present a credential.

Identiv's MobilisID solution combines security, simplicity, and convenience into an easy-to-install, cloud-managed physical access control system (PACS). By harnessing users' current smartphones and tablets to transition from conventional physical cards to secure mobile credentials using powerful, multi-tech Bluetooth MobilisID Readers, the smart mobile solution creates a secure and effortless way to approach physical access, keeping users on-the-go.

Issuing and managing credentials has never been easier with MobilisID Manager. The MobilisID cloud-based portal works on any web-browser and gives administrators and operators the ability to issue, update, and remove user credentials on-the-fly, making the once cumbersome process of creating physical credentials simple, quick, and efficient. Managing users and credentials with MobilisID Manager is also cost-effective by cutting out the hardware necessary to produce cards and eliminating costs to deploy, ship, and track physical cards.

The MobilisID app, available on the Apple App Store and Google Play Store, converts almost any iOS or Android smartphone or tablet into a direct replacement for a traditional, physical credential. The MobilisID app securely transmits a personalised credential using the latest Bluetooth technology to MobilisID readers allowing the user to freely move throughout a building or facility without the need to present the mobile device. For those sites that require support for legacy, proximity-based credentials, including cards, tags, or fobs, the MobilisID Reader supports 26 – 37 bit 125 kHz low frequency (LF) credentials, making the transition from physical to electronic-based access control seamle

Napco Security announces availability of iSecure Complete Cellular Alarm Systems

Napco Security Technologies has announced the availability of its award-winning iSecure Complete Cellular Alarm Systems. iSecure is designed to help security professionals to be more competitive, adding more residential accounts and new RMR, while offering the professional-grade security systems, remote Smart App & notification alerts consumers want.

For speediest setup, iSecure is uniquely installable in about an hour, and programmable using any smart phone/tablet and a cloud-based portal with easy drop-down menus. (No laptop required!)

iSecure is available in 3 all-inclusive kits, with choice of wireless keypad, security touchscreen or connected home touchscreen, and includes two wireless window/door sensors and wireless PIR.

iSecure guarantees the lowest equipment cost and professional installation in under an hour and features a Go-Anywhere Smart Hub with built-in StarLink Cellular/IP LTE dual path alarm reporting that literally goes anywhere, wall-mount or tabletop, allowing dealers to position it for best signal reception and less vulnerability to smashing, plus spoken voice prompts, 85db siren, RF-receiver & 24-hr standby for maximum power-outage protection.

A full line of professional accessories are also available including wireless CO, smoke, heat detectors, video cameras & doorbell, extra plug-in siren with strobe and the iSecure Takeover Module, eliminates rewiring or replacing installed sensors, and more.

LILIN unveils Aida Traffic Management Solution
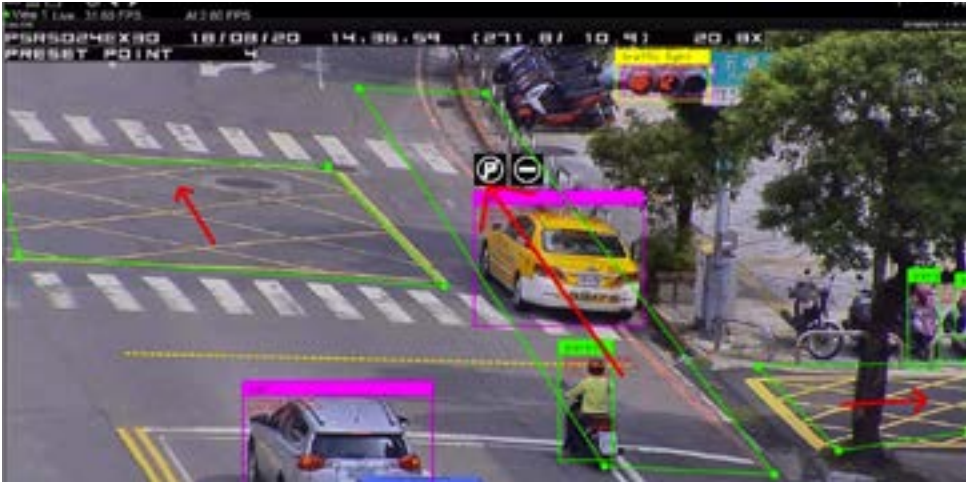
LILIN has announced the release of its Aida traffic management solution. With the success of LILIN Aida automatic number plate recognition (ANPR), LILIN Aida adds AI traffic management to the Aida product line. LILIN Aida can be installed on the edge for traffic analysis where the metadata gets sent to the remote Navigator Control Centre.

LILIN Aida ANPR and traffic management can integrate with LILIN Navigator VMS products including Navigator Control Centre, Navigator Corporate, and Navigator Enterprise for event notifications, statistics, and system automation.

Both LILIN Aida and LILIN Navigator products utilise Intel Media SDK for Windows and maximise the GPU processing power for video decoding and rendering. LILIN offers Aida ANPR, traffic management, VMS software, and AI recorders (NAV2000AI and NAV3000AI series) which can run on Intel CPU, GPU, VPU, and NVidia Cuda on Windows OS. LILIN Aida software is able to run Multiple AI models on distributed AI CPU, GPU, and VPUs of a Server. LILIN Aida ANPR series and Aida traffic management use the latest deep learning technology.

Aida traffic management can provide accurate AI traffic object recognition for parking spot detection, parking violation, turn left violation and turn right violation, wrong way detection with number plate recognition, truck, motorbike and pedestrian violations, queuing detection, average speed detection, and loitering detection. LILIN Aida traffic management by deep learning technology requires thousands of pictures for image labelling and machine training of object datasets. These processes are time consuming tasks. The datasets are then used for traffic management.

Image labelling needs more attention for inference accuracy. LILIN deep learning processes consist of image labelling, video recognition, and accuracy validation. LILIN designed and developed AI-enhanced software combined with intelligent video surveillance edge devices can optimise traffic systems.

Dahua Technology launches WizSense full-colour series network camera

Dahua Technology has successfully launched its brand new solution for smart night surveillance, the WizSense Full-Colour Series Network Camera.

This new camera series embraces Dahua Technology's four major technological innovations:

Large Aperture Lens - Features F1.0 super large aperture that collects 2.5 times the amount of light compared with F1.6 aperture, creating a brighter image.

High-Performance Sensor - Offers 30% photosensitive capacity increase through its larger sensors.

Advanced ISP - Dahua ISP 4.0 greatly improves Signal-to-Noise Ratio (SNR) and colour reproduction.

Warm Light - The weighted radiance of blue light is 40% below European Union standards, which presents lower light pollution and less harm to human eyes.

With these four technological advances, Dahua Full-Colour Camera delivers unparalleled performance at night. It achieves 24/7 monitoring by capturing vivid details and presenting coloured images in low light conditions. At the same time, it provides warm and smart auxiliary light to guarantee image clarity and quality even in total darkness. Thanks to its built-in AI functions, higher monitoring accuracy at night is guaranteed.

Dahua Technology delivers both SMD and Full-Colour for night surveillance advantages to its customers. On one side, SMD can easily process visual information collected by Full-Colour Camera. On the other side, the Full-Colour Camera significantly increases the accuracy of SMD at night.

In addition, Dahua SMD has the ability to effectively filter false alarms triggered by pets, leaves, branches, raindrops, lights and other irrelevant objects, and only focus on real threats, human and vehicle.

Utilising the two advanced technologies, Dahua WizSense Full-Colour Camera can accommodate a wide range of application scenarios, such as museums, cinemas, factories, villas, schools, etc. Users no longer need to worry about the high cost of patrolling or leaving their property unguarded at night. This solution is fully capable of meeting the demands of ordinary users, delivering a safer and cost-effective solution for night surveillance.

Panasonic® i-PRO and WCCTV connect to provide high performance Mobile Surveillance Solutions

Panasonic i-PRO U.S. Intelligent Surveillance, a division of the recently formed Panasonic i-PRO Sensing Solutions Co., Ltd., has recently entered into a technology partnership with Wireless CCTV LLC (WCCTV) to offer high performance wireless transmission solutions over state-of-the-art 4G LTE networks. The reciprocal agreement enables authorized Panasonic i-PRO systems integrators and reseller partners to integrate WCCTV wireless solutions for delivery to their customers, and for WCCTV to offer their customers wireless surveillance solutions that integrate Panasonic i-PRO cameras.

The combination of industry leading imaging and surveillance solutions from Panasonic i-PRO with WCCTV's proven 4G LTE Wireless Network technology fulfills users' growing demand for rapidly deployable surveillance solutions that feature the ability to be easily relocated to areas of immediate interest.

"WCCTV's innovative approach to wireless transmission employing 4G LTE technology delivers the performance or integrity our customers demand for professional applications," said Bill Brennan, President of Panasonic i-PRO Sensing Solutions Corporation of America. "We believe the addition of WCCTV's wireless transmission technology to our growing portfolio of solutions further enhances our position as an end-to-end supplier of comprehensive surveillance and access control system solutions and strengthens our mid-size municipality vertical focus."

"The marriage of WCCTV's wireless solutions with the globally renowned performance of Panasonic i-PRO's imaging and surveillance solutions is a win-win for both our companies, our reseller partners and the customers we all serve," said Adam Haworth, Executive Vice President at WCCTV. "We look forward to working with Panasonic i-PRO and their integration partners to help existing and new potential users resolve longstanding surveillance issues related to traditional wired network connectively."

New Avigilon intelligent and cost effective camera

The new Avigilon H5M camera is the latest addition to the Motorola security solution portfolio, and has been designed to provide customers with a cost-effective solution for budget-conscious video security projects that require a small-footprint camera for outdoor use. The H5M camera can handle tough environmental conditions while offering AI-powered Unusual Motion Detection (UMD) — all backed by a five-year warranty.

The camera features a compact size and can seamlessly integrate with other open-platform systems. In addition, this intelligent camera helps save time through its built-in AI technology that flags unusual events to users. The H5M camera is offered in 2 and 5 MP resolution, it is priced cost-effectively, and is engineered to be easy to install, addressing a wide variety of security needs and helping projects remain on time and on budget.

"We are introducing a budget-friendly solution for our customers who have sites that need value-oriented, outdoor-rated cameras," said John Kedzierski, senior vice president, Video Security Solutions at Motorola Solutions. "This camera is suited to serve a wide-variety of customer segments, where we are always working to provide intelligent end-to-end solutions that target our customers' specific security needs."
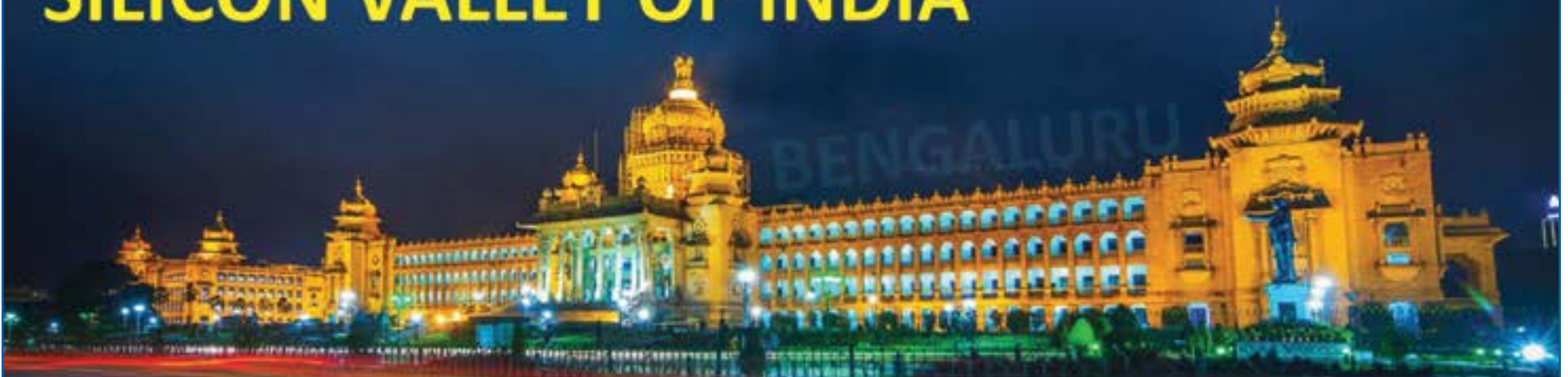
FLIR launches smart solution for elevated skin temperature screening
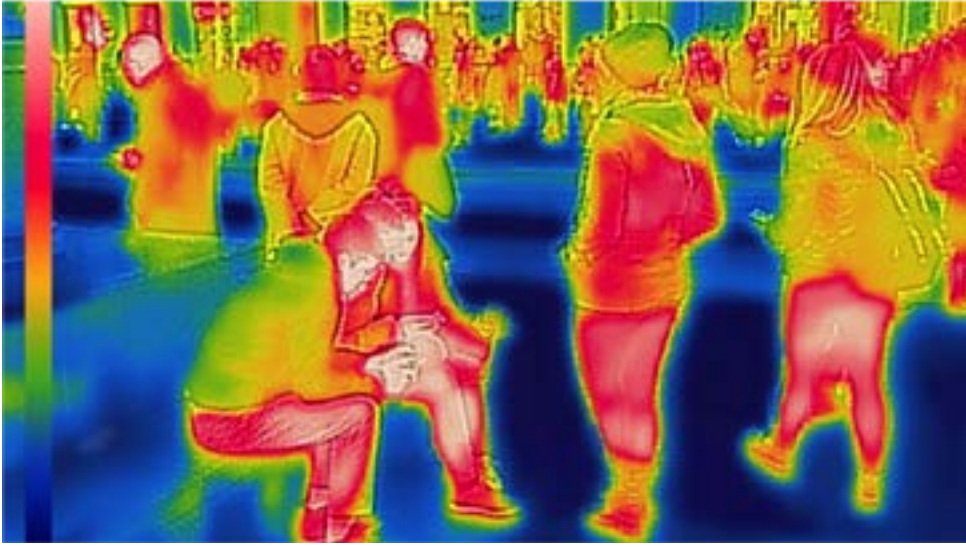
FLIR Systems, Inc. has announced the FLIR A400/A700 Thermal Smart Sensor and Thermal Image Streaming fixed camera solutions for monitoring equipment, production lines, critical infrastructure and screening for elevated skin temperatures.

These highly configurable smart camera systems provide accurate, non-contact temperature monitoring across a wide range of disciplines: manufacturing process control, product development, emissions monitoring, waste management, facilities maintenance, and Environmental, Health, and Safety (EHS) improvements. The FLIR A400/A700 Thermal Smart Sensor solution initially will be prioritized for those responding to COVID-19. For all applications, the series offers multi-image streaming, edge computing, and Wi-Fi connectivity to help speed data flow and enable faster decisions, improving productivity and safety for professionals.

FLIR designed the A400/A700 cameras with two configurations to better meet application-specific needs. The Thermal Smart Sensor configuration, recommended for measuring elevated skin temperatures, incorporates advanced measurement tools and alarms with edge computing to enable faster critical decisions. The Image Streaming configuration provides multiple thermal streaming capabilities to help optimize process control, improve quality assurance, or identify potential failures that could shut down a production line.

Users design their systems by choosing either the Smart Sensor or Imaging Streaming configurations, selecting either the A400 or A700 camera body based on the resolutions they need, and then adding lenses and a range of optional features to fit their application.

Also, FLIR currently is in beta testing for an automated elevated skin temperature screening software solution that is fully integrated with its United States Food and Drug Administration-certified thermal cameras. The solution is designed to rapidly increase the accuracy, ease-of-use, and speed of existing screening procedures. FLIR will share an announcement about its solution in Q2 2020.

HGH showcases enhanced thermal and visible panoramic sensor

HGH is to showcase its new generation SPYNEL-U 360° panoramic thermal and visible camera surveillance system shortly. The optronic expert reinvented this maintenance-free, uncooled thermal imaging camera from design to performance to provide unrivalled situational awareness. The dual-channel SPYNEL-U when used in conjunction with CYCLOPE advanced image processing software provides multiple threat detection, day and night, even in adverse weather conditions.

The SPYNEL range is world-renowned in the defence and security sectors. Spynel-U offers both a thermal and visible high resolution panoramic channel on the same sensor. While the high contrast thermal panoramic video is ideal for real-time long-distance detection and tracking, the high-resolution visible panorama enables the rapid identification of the detected threats.

The new SPYNEL-U design utilises the same base as SPYNEL-X and SPYNEL-S, supporting straightforward sensor interchangeability on platforms and tripods. Employ the SPYNEL-U to protect critical infrastructure such as ports, airports, nuclear plants and prisons, as well as at public events and demonstrations.

New Wisenet four-channel multi-sensor cameras

Hanwha Techwin has enhanced its premium Wisenet P series with the addition of three new four-channel multi-sensor cameras, designed to provide a cost-effective solution for detecting and tracking objects over wide open areas.

The 8MP Wisenet PNM-9084QZ features motorised varifocal lenses for precise control of focal length, angle of view and zoom of each of its sensors, as do the 8MP PNM-9084RQZ and 5MP PNM-9085RQZ, which are also equipped with built-in smart IR illumination for each sensor. This illuminates objects at a distance of up to 30m by focusing the beam in line with zoom. All three new H.265 multi-sensor cameras are equipped with motorised PTRZ gimbals which reduce on site times as they enable installation engineers to remotely pan, tilt, rotate and zoom the lens' positions in order to set the camera's field of view.

Head of Product and Marketing for Hanwha Techwin Europe, Uri Guterman, said: "These new models, which enable operators to choose from a broad range of customisable angles and zoom settings per sensor, offer cost savings for both system integrators and end users. This is because multi-sensor cameras use less cable, conduit and mounting hardware compared to what would normally be required to enable up to four separate cameras to do the same job. They also need fewer VMS licenses as only a single IP connection is required."

Key features include advanced wide dynamic range (WDR), which performs at up to 120dB to accurately produce images in scenes that simultaneously contain very bright and very dark areas, true day/night camera functionality with a removable infrared cut filter (ICR).

Other features include digital image stabilisation (DIS), which reduces motion blur caused by wind or vibration and ensures the capture of sharp, stable images; Support for H.265, H.264 and MJPEG compression, as well as WiseStream II, a complementary compression technology unique to Wisenet cameras; Built-in Intelligent Video Analytics (IVA), including Tampering, Loitering, Directional Detection, Defocus Detection, Fog Detection, Virtual Line, Enter/Exit, Appear/Disappear, Audio Detection, Face Detection and Motion Detection.

Finally, you have sound classification: An audio analytics feature which recognises critical sounds such as raised voices, screams, broken glass, gunshots and explosions, and generates an alert to enable security personnel to quickly react to any incidents; together with IP66, IK10, and NEMA 4X ratings for protection against water, dust, and mechanical impact, makes the three multi-sensor cameras an ideal choice for outdoor applications.

AI Camera specialist Deep Sentinel launches product for SMB Market

Deep Sentinel, a startup provider of artificial intelligence (AI)-based security cameras and monitoring services for the residential market, has launched a similar offering for small-to-medium businesses.

Deep Sentinel for Business is said to provide after-hours protection against crimes like vandalism and theft, while featuring many of the same benefits as the company's home security product.

The company's weatherproof cameras use AI to detect potential threats, alerting one of the company's LiveSentinel guards to unusual activity, including loiterers. Guards can then intervene through the system's two-way audio and 104dB siren, with the ability to contact local law enforcement.

The system kit includes three wireless cameras with wall mounts, a hub and four rechargeable lithium-ion batteries. The 1080p cameras offer full HD recording and streaming, and include night vision and PIR motion sensing to 35 feet with a 130° field of view. The AI engine detects people, animals and objects, and is said to interpret behavior in real time. This capability distinguishes between a potential intruder and a dog or other non-threats.

AV Costar wins two industry awards

Arecont Vision Costar (AV Costar) is set to receive two security industry awards for the new adjustable view, omnidirectional ConteraIP Omni LX Remote Setup camera. The newest Omni platform offers easy installation and setup plus advanced features in a megapixel camera that covers any view up to 360 degrees for non-stop situational awareness.

AV Costar's Omni LX Remote Setup camera was first unveiled at last fall's GSX Chicago conference, and is now generally available. AV Costar brings a proud legacy of surveillance industry leadership, pioneering the first panoramic 180-degree multi-sensor megapixel cameras, followed by the first adjustable view, 4-sensor omni-directional models, with multiple follow-on generations adding new features, capabilities, and designs.

The new Omni LX Remote Setup offers some of the most advanced capabilities and features of any omni-directional multi-sensor camera, including hands-free setup. The camera is easily installed with a unique, time saving mounting design on a wall, ceiling, pole, emergency call box, or other structure. All 4 sensors can then be remotely moved into position from the safety of the ground over the network. The installer remotely uses the pan, tilt, zoom, and focus controls to lock in non-stop coverage of virtually any viewing area. 180-, 270-, and 360-degree presets speed setup, with the ability to further adjust and save additional viewing choices. These capabilities eliminate the need for a service call or use of a lift or ladder to change or fine tune the view, saving both time and money. The Omni LX Remote Setup brings even higher performance and reliability than earlier models, all in a compact PoE dome.

New line of affordable domes from Axis

Axis Communications launches a new generation of the Axis M31 network camera series. The Axis M3115-LVE and Axis M3116-LVE are suitable for both indoor and outdoor surveillance and offer a wide-angle view and effective video quality in 1080p and 4 MP and are designed for use in a wide variety of applications.

These fixed domes feature Axis Forensic WDR for high-quality video even when there's both dark and light areas in the scene and Axis Lightfinder for increased light sensitivity and clear colours in low light. Additionally, there's no need for additional lighting – with built-in IR illumination unobtrusive surveillance can be achieved in total darkness.

Key features include HDTV 1080p and 4 MP video quality; Forensic WDR, Lightfinder and IR illumination; Wide-angle view; Zipstream supporting H.264 and H.265; and Signed firmware and secure boot.

These impact-resistant cameras are IK08-rated, and the casing can be repainted in any colour to blend in with specific surroundings. Signed firmware and secure boot guarantee that the firmware hasn't been altered and ensure only authorised firmware is installed. These products offer Axis Zipstream with support for H.264/H.265, which significantly reduces bandwidth and storage requirements without compromising image quality.

EIZO launches FlexScan 27-inch WQHD ultra-slim monitor

With a 27-inch diagonal and 2560 x 1440 pixels, the new FlexScan EV2760 from EIZO offers plenty of scope for efficient use in the office. Whether its text, graphics, photos or videos, users enjoy crystal clear, incredibly detailed image reproduction on its large screen. Antireflection coating, flicker-free brightness control and a flexible stand facilitate ergonomic work. Its smart, three-sided, virtually frameless design means that one can focus on what's most important while maintaining a clear overview of their work.

Thanks to its EIZO EcoView functions it boasts a low power consumption if, for example, one needs a lower brightness level and a glare-free view. The EV2760 offers a wide range of connection possibilities with Display Port, HDMI and DVI-D signal inputs, not to mention four USB downstream ports.

When it comes to image quality and ergonomics in particular, the EV2760 fulfils all professional requirements for monitors used in modern office environments. Antireflection technology and Auto EcoView ensure a glare-free view of the screen, while the stand helps to prevent posture problems thanks to its amazing flexibility.

The WQHD-LCD featuring IPS technology ensures the greatest possible viewing angle. The EV2760 achieves a contrast ratio of 1000:1, thanks to a typical brightness of 350 cd/m2.

EIZO provides a five-year warranty for the EV2760, just like for all FlexScan models.

Hikvision Introduces Temperature Screening Thermographic Cameras

Hikvision has introduced Temperature Screening Thermographic Cameras in India to help the preventive measures at Airport and other transport terminals, schools, hospitals and at places with long queues.

These Temperature Screening Thermographic Cameras can sense IR radiations (8-14μm) and produce thermal images. Thermal cameras convert IR radiations into gray value, and establish the accurate corresponding relation between gray value and temperature through the temperature measurement algorithm model.

It is well-known that one major symptom of virus infections is temperature caused by fever. Therefore, a thermal camera with high temperature accuracy can detect the elevated skin temperature to make the temperature screening so as to achieve rapid preliminary screening in public areas. Actual core body temperatures should be further confirmed using clinical measurement devices. Under any circumstances, it is highly recommended to use Hikvision's thermographic cameras in accordance with local laws and regulations. It takes only one second for a thermal camera to detect the temperature of each person. Thus, there will be no congestion when passing through the site where temperature needs to be checked as the Thermal camera supports non-contact temperature measurement, from up to around 1 meter away. That reduces the risk of infection coming from physical contact.

Multi-person Detection: It can enable multi-person detection simultaneously

Alarm Notification: In case of any detection the Temperature Screening Thermographic Camera immediately sends alarm notification to notify operators. It also has AI detection to reduce false alarms from other heat sources

Dahua Thermal Solution prevents spread of COVID-19

The year 2020 is bound to be a special year with the outbreak of coronavirus disease (COVID-19) globally. The highly contagious disease has taken away many lives and counting, especially in China, South Korea, Japan, and some countries in Europe and the Middle East.

Dahua Technology has been an early participant in the epidemic prevention and control in Asia, joining the global efforts in combating the virus to minimise the impact on mankind.

Since sending its first batch of thermal cameras to the hardest-hit area, Wuhan, on January 24th, 2020, Dahua Thermal Solution has been deployed in thousands of sites in China, including transportation hubs, commercial complexes, banks, and other places, and some are on the way to multiple countries in Asia.

Hong Kong, a financial capital in Asia, also suffers from the COVID-19 epidemic situation. Dahua Thermal Solution has been applied in some local business complexes, banks, company parks, and other places. To enable safe and smooth work resumption recently, quite a few major corporations have been using Dahua Thermal Solution in their headquarters and subsidiaries to improve their workplace safety. Dahua Thermal Solution measures the body temperature of their employees, handling thousands of staff flow every day.

Compared to the traditional way of body temperature measurement – a forehead thermometer, using Dahua Thermal Solution will significantly improve speed and accuracy, and at the same time, help reduce cross-infection via non-contact measurement.

To measure the temperature of 5,000 people, it will take about 4.2 hours using a forehead thermometer, as it takes at least 3 seconds to measure a person. However, it takes only 30 minutes if using the Dahua Thermal Solution, which measures 3 people per second. It also features a high accuracy of ±0.3°C.

"Dahua Thermal Solution helped us detect a couple of suspected cases in just a few hours of operation, which we greatly appreciate," a Hong Kong user commented. Dahua Thermal Solution has been on the front line since the very beginning, helping with the epidemic prevention and control in airports, railway stations, hospitals, schools, and other sites all over Asia. Featuring high accuracy, high efficiency, strong adaptability and easy deployment, Dahua Thermal Solution can also be applied to all kinds of entrances and exits, kitchens and kindergartens.

Singapore Police deploys HID Lumidigmâ Fingerprint Sensors

HID Global has announced that the traffic branch of the Singapore Police Force has deployed an electronic Know Your Customer (eKYC) system that uses HID Lumidigmâ V-series Fingerprint Sensors to verify the identities of driver's license applicants.

The HID Lumidigm sensor's patented multispectral imaging technology has helped improve identity-verification speed and efficiency as compared to their previous paper-based process, and its proven liveness-detection capabilities significantly diminish the risk of fraudsters compromising the eKYC system.

Deployed by HID partner Secur Solutions Group at Singapore's three driving schools, the new eKYC system improves security by using fingerprints to verify the "true identity" of driver's license applicants. The speed and reliability of the Lumidigm sensors has enabled the entire enrollment process to be performed at kiosks in seconds, from fingerprint capture through matching against the actual identity documents (NRIC/Work Permit).

The Singapore Police Force is enrolling 500 to 700 individuals a day at the kiosks since deployment and has cut almost 1,500 man-hours of labor per month by eliminating its staffed counters and manual workflow. "The HID Lumidigm sensors have outperformed all alternatives with respect to speed, accuracy and consistency of image acquisition regardless of finger or environmental conditions," said Tseng Wun Hsiung, CEO of Secur Solutions Group. "New opportunities are being considered for service enhancement and parts of the eKYC system are being evaluated for integration."

HID Global's patented multispectral fingerprint imaging technology captures unique characteristics from the finger's surface and subsurface, which is particularly important for the Singapore Police Force's eKYC system because it serves a large population spanning many ages, ethnicities and skin types. The Tseng Wun Hsiung technology works reliably with normal, wet, dirty, dry or damaged fingers, and in sunlight or wet or cold conditions.

Field-updatable liveness detection is employed to distinguish between the captured biometric data from a real living person versus a plastic, fake or other artificial fingerprint copies. HID's V-Series Lumidigm sensors were the first fingerprint products certified to the International Standards Organisation (ISO) standard focused on anti-spoofing and liveness detection.

Luton Airport Marriott gets cybersecure video protection with IDIS

The new Courtyard by Marriott hotel at London's Luton Airport is being protected with the latest, cybersecure video surveillance technology from IDIS. The complete end-to-end solution, from Korea's largest video equipment manufacturer, is enabling trouble-free remote 24/7 monitoring, ensuring improved service efficiency, safety and security for guests. IDIS DirectIP technology was chosen for its ease of installation and use together with the reassurance of multi-layered protection against cybersecurity risks.

Although the installation team from DGS Systems had never previously worked with IDIS technology before, they found that it lived up to its true plug-and-play promise. Despite having almost 100 cameras to set up – including 74 full-HD IR domes and 17 vandal resistant full-HD IR domes – one-click network configuration allowed the engineers to work rapidly, connecting devices easily and not needing to manually enter passwords for each one. This not only reduced installation time but ensured greater protection against network infiltration by minimising the likelihood of human error, which can occur when passwords need to be written down and entered manually. Encryption technologies and NVR firewalls together with proprietary protocols and file structures make IDIS surveillance solutions less vulnerable to attacks than many common open architecture components.

IDIS DirectIP made it easy to set up the three IDIS NVRs (32-channel DR-6332PS-S) to provide impressive recording capability and meet the customer's requirement for three months' storage of all recordings. The NVRs' 370Mbps throughput ensures no latency on live footage and high-quality image capture in full HD.

Most of the cameras are used for incident investigation, although with the hotel's service areas now covered, operational efficiency has been improved too. For example, routine checks on the rooftop plant room can now be handled remotely, rather than in person, which is particularly useful during adverse weather

conditions.

The hotel's owner also wanted to protect the car parks and building exteriors to reduce the risk of crime, and shortly after the system was completed, a gang of opportunist scrap-metal thieves was recorded stealing cables from the site. The IDIS full-HD IR domes provided video evidence that was key to a successful police investigation, delivering

pin-sharp images in all lighting conditions and easily handling rapid variations in brightness and shade thanks to their true wide dynamic range (WDR).

"The IDIS solution was very installer-friendly and easy to configure," says Dariusz Surowy of DGS Systems UK, confirming that the same technology is now being used on more sites.

Meanwhile, James Min, Managing Director, IDIS Europe comments that IDIS solutions are designed to be easy to install, simple to use, and to give the lowest total cost of ownership (TCO). "For busy hotels such as the Courtyard by Marriott at Luton, they provide the perfect tool for safety, security and more efficient management."

Infinet Wireless. "Our years of experience developing state-of-the-art wireless solutions, able to operate in the most diverse climatic conditions and terrain topologies, whilst delivering bandwidth-intensive applications in real time, allows us to deliver to SESESP a solution that is helping the state continue its critical work safeguarding its citizens and entire communities."

Infinet Wireless designed and implemented the network based on its R5000 product family, which includes Point-to-Multipoint (P2MP) solutions as well as Point-to-Point (P2P) ones. The new platform provides the necessary bandwidth and capacity, with room for future growth, for crucial systems all aimed at improving people's lives, ensuring their security

wherever they are and significantly preventing and ultimately reducing crimes of all types.

Ultimately, SESESP is now able to rapidly gather all relevant information from all corners of the state, then share it with various authorities in order to take preventive actions as well as remedial ones whenever necessary.

Infinet Wireless to safeguard residents in Mexico

Infinet Wireless has installed a new high-capacity wireless infrastructure to improve public safety and expand its geographical coverage in the Zacatecas state, located in north-central Mexico.

The company has provided connectivity to around 150 locations in numerous municipalities in the state, further enabling the local authorities and law enforcement agencies to provide dynamic monitoring of the streets and neighbourhoods, emergency care wherever it is needed, enhanced citizen protection, and connecting the REPUVE public register of vehicles with all relevant command and control centres.

Infinet Wireless was selected to deliver the project following a decision from the Executive Secretary of the State Public Security System (SESESP), which is responsible for citizen safety and security in the entire state, with the main objective being a major technological

overhaul and renewal to ensure the safety of residents and visitors to the region.

"SESESP required a solution which could address the limitations of the legacy wireless platform we had, make more efficient use of the limited radio spectrum available, mitigate radio interference generated by third party and rogue base stations, as well as significantly improve the reliability of our camera feeds even in the highest density locations," said Jaime Francisco Flores Medina, Executive Secretary of the SESESP of Zacatecas state. "These were critical criteria for SESESP, and Infinet Wireless was able to provide a reliable solution which met and exceeded our expectations, as well as providing much easier installation and maintenance."

One of the key challenges faced by SESESP was to ensure that its subsidiary, The Center for Integral Coordination, Control, Command and Communications (C5),

could have access to dynamic and comprehensive visibility at the street level, enabling quick decision-making on all matters related to public safety, medical emergencies, the environment, civil protection, flow of road traffic and the provision of various services to the community at large. Gathering and sharing real-time information from a multitude of sources presented a real challenge, especially as the collected information needed to be subsequently distributed to various monitoring and control centres spread across the state.

"This was a project with understandably very stringent requirements due to the mission-critical nature of SESESP's work protecting the state's citizens and visitors. As the eighth largest state in Mexico, there were obvious geographical challenges in order to connect more than 150 locations across Zacatecas," said Carlos de Lamadrid, Regional Business Development Manager for LATAM at

Mountain Warehouse selects Nedap for RFID roll out

Mountain Warehouse, a major UK outdoor apparel and equipment retailer, has selected !D Cloud, Nedap's leading inventory management solution for a global deployment to 400 stores. The deployment started in January 2020 in the United Kingdom, continuing with Europe, North America and New Zealand with the main objective being to improve inventory accuracy, leading to better product availability.

Mountain Warehouse has been growing year on year for 2 decades now. To continue this success, it's vital that the retailer continues to be agile and move with customer behaviour. Aligning bricks and mortar with the digital experience of using RFID is an essential ingredient to maintain this growth.

"We have been very successful over the past 22 years at Mountain Warehouse. To build on this growth, we made the decision in 2019 to RFID source tag our inventory. As a result of this, we will benefit hugely from having full inventory visibility. Knowing what is in stock allows us to provide better product availability, improving our

customer proposition, whilst increasing sales", comments Jamie Morgado, Head of Retail Operations at Mountain Warehouse.

Mountain Warehouse ran a previous project looking into the benefits of RFID. The improvement in accuracy, although with a different supplier, supported the business case which in turn started the Request for Proposal process.

"We were looking for an experienced supplier with a platform that was simple to integrate, could scale internationally with ease, and was lightweight to set up from an IT perspective. We also wanted an application that is easy and fun for our store staff to use. We feel that Nedap's experience in the market and approach to RFID, fits in very well with our objectives and culture at Mountain Warehouse, not only now, but where we want to be in the future too", comments Alexandria Smuts, Head of IT Delivery at Mountain Warehouse.

In addition to experience and references, not having to invest in shielding materials was an important driver for Mountain Ware-

house when selecting !D Cloud. Alexandria Smuts says: "One key aspect in choosing Nedap was their Virtual Shielding solution, which will help stores with their shop floor replenishment process, maximizing on-shelf availability. Virtual Shielding removes the requirement to physically shield stock rooms with RFID blocking paint or foil, which facilitates a lower level of investment for roll out.

"It is an absolute pleasure to welcome Mountain Warehouse to our !D Cloud community", comments Nick Markwell, Business Lead !D Cloud UK at Nedap. "We share the same philosophy that inventory accuracy is the fundamental building block to enabling product availability. This will open more doors for future growth, opening up omni-channel initiatives and ultimately providing their customers with better choice. We are looking forward to helping Mountain Warehouse deploy RFID globally and supporting them to develop their RFID roadmap, so that they can continue to build on their very strong 22 years of trading."

Stringent regulation upgrades drive fire alarm market

The global fire alarm and detection market size is expected to reach USD 75.3 billion by 2027, expanding at a CAGR of 8.5% over the forecast period, according to a study conducted by Grand View Research, Inc. Increasing awareness towards the safety and security of assets across the globe is expected to offer significant opportunities for technological innovations in the market.

Additionally, rise in the consumer spending on fire protection devices especially across the enterprise and industrial sectors in order to reduce the risk of accidents is expected to spur market growth. Moreover, stringent government regulations and mandates regarding workplace safety, and increasing demand for state-of-the-art fire alarm & detection systems is expected to fuel the market.

The need for upgrading the existing alarm and detection systems to more advanced versions that consequently comply with the new stringent regulations will drive the market. A growing number of fire accidents has developed into the need for installation of advanced alarm and detection systems across the residential, commercial, and industrial sectors. For instance, legislative requirements from different countries including the National Fire Protection Association, USA, and Building Code of Australia have mandated the installation of fire detection devices, thereby boosting the demand for these devices.

North America dom-inated the market in 2019 and is expected by the researchers to continue its dominance over the forthcoming years. Whilst the Asia Pacific region is anticipated to exhibit the highest CAGR from 2020 to 2027. Growing industrialisation and urbanisation in emerging markets such as India, China, and Japan is expected to accelerate infrastructure spending including mass transportation such as airport security for example.

The fire detector segment is expected to dominate the market owing to stringent government regulations across various countries mandating the installation of the devices. For instance, in India, the National Building Code (NBC) was published in 2016 to implement building standards ensuring safety through the use of active and passive smoke detection systems. The segment is expected to reach USD 38.1 billion by 2027

Within the detectors segment, smoke detectors are expected to dominate and the analysts expect that trend to continue over the forecast period, anticipating it to reach USD 17.0 billion by 2027.

Prominent industry participants cited by the researchers include Bosch; Eaton Gentex; United Technologies Corporation; Honeywell; and Johnson Controls.

A non-flammable lithium battery

Researchers from Deakin University in Victoria, Australia, have developed a lithium metal battery prototype which features electrolytes designed to be resistant to catching fire.

The breakthrough from Deakin's Institute for Frontier Materials (IFM) is said to represent an alternative to the rechargeable lithium-ion batteries used in portable electronics, stationary energy storage and electric vehicles and is the culmination of more than 10 years' work by electromaterials staff at the institute.

Patrick Howlett, director of the university's Battery Technology Research and Innovation Hub (BatTRI-Hub) said a 1 Ah (amp-hour)-sized lithium metal pouch cell was the first device Deakin created using ionic liquid electrolytes which allow for better safety and high temperature and high voltage stability, to offer increased energy storage capacity.

The ionic liquid is a salt which takes liquid form at room temperature. Researchers at Deakin and Melbourne's Monash University have been working for 30 years on the materials, which have begun to attract widespread interest in the battery community.

"Ionic liquids are non-volatile and resistant to catching fire, meaning that unlike the electrolytes currently used in lithium-ion cells – used by, for example, Samsung and Tesla – they won't explode," said Howlett. "Not only that, but they actually perform better when they heat up so there's no need for expensive and cumbersome cooling systems to stop the batteries from overheating."

However, it is an outstanding ability to cycle energy-dense lithium metal electrodes which inspired the research effort. IFM research fellow Robert Kerr, who has worked on translating the materials into real devices, said changing battery materials could change key features of the devices.

"For example, if we change the electrodes to include lithium metal, we can increase the storage capacity for up to 50% longer run-times," said Kerr. "When we change the electrolyte, it can give a higher discharge rate or allow the battery to operate at much higher temperatures – but the electrolyte must be compatible when in contact with the reactive lithium metal electrode. By choosing the right electrolyte chemistry we can completely avoid the catastrophic explosions caused by ignition of the volatile electrolyte when the cell is damaged or overcharged."

While lithium metal batteries could offer far better energy density and much lower weight than lithium-ion technology – thanks to the replacement of heavier graphite with lithium metal as anode – lithium metals do not work well with conventional electrolytes. Another headwind for the innovative technology is the lack of knowledge about the best way to manufacture cells at practical levels for demonstration, given the use of lithium metal electrodes in lithium metal batteries is not common in the industry. The breakthrough has been described as "just a stepping stone on the way to 1.7 Ah cells, which are soon to be in production" nevertheless.

The project has been progressing at a rapid pace since the formation of the Deakin BatTRI-Hub in 2016. The potential of ionic liquid electrolytes is also being explored under a separate three-year project run by IFM and BatTRI-Hub with chemical manufacturer Boron Molecular – which was spun out of the federal Commonwealth Scientific and Industrial Research Organisation – and technology company Calix.

In the first stage of the project, coin-cell fabrication, electrochemical screening and testing of Calix's highly porous nano-active electrode materials – such as manganese oxide (Mn_3O_4) cathodes and titanium oxide (TiO_2) anodes – and ionic liquid electrolytes will be carried out by IFM at Deakin. After that, the BatTRI-Hub will manufacture pouch cell and battery pack prototypes. The project will involve a field trial of the battery packs, including solar applications linked to small solar systems and Deakin's smart microgrid, which features a 7 MW solar farm and a 1 MW battery. The products could then be supplied to global manufacturers and customers for performance evaluation.

Telguard gets NY City approval for Fire Alarm Communicator

Telguard announces its cellular fire alarm communicators have been issued a certificate of approval by New York City that will allow dealers to use the company's TG-7FS LTE cellular fire communicator.

New York City has strict regulations on which types of fire communicators can be deployed within the city. Manufacturers must obtain a certificate of approval for fire systems dealers to be able to specify a brand like Telguard. The TG-7FS is a universal cellular communicator, meaning it works with virtually every fire alarm control panel. Using LTE cellular networks, the TG-7FS transmits alarm signals from the fire panel to the designated monitoring station. The unit meets UL 864 requirements and is compliant with NFPA 72 for primary or backup communications for commercial fire alarm systems.

By using the TG-7FS, accounts can go from two to one dedicated landline, which provides cost savings, according to the company.

Dealers and integra-tors can choose from either AT&T or Verizon models — whichever carrier works best for them in their locale. Telguard has been a go-to cellular communicator for authority having jurisdictions (AHJs) and fire marshals across the country for years.

Telguard is a brand of Telular Corp. The company combines devices, communications, video, interactive services and alarm processing into turnkey systems for monitoring intrusion, fire systems and home automation without a traditional landline.

Problems your access control software could fix right now

So often, our focus in security and access control zeroes in on the hardware. Its latest functionality or compatibility with emerging technologies grabs the headlines. Yet it is your access control software which knits a system together — and the signs are, this is finally getting the attention it deserves in security procurement.

"Today, access control software is more accessible to a wider variety of actors," writes Bryan Montany, a research analyst at IHS Technology, "providing end-users with broader and more comprehensive data relating to patterns in building occupancy."

"Software has also supported integrations with other security systems, enabling security managers to respond in real time to emerging incidents and potential security breaches."

In other words, you can escape the limiting functionality of outmoded access management with a new generation of software solutions. They can fix everyday access irritants.

Below are just seven:

Freedom from the access management terminal

Multi-seat management should be a given. Your intuitive, customised dashboard could have a personalised login screen configuration for every administrator. Software should offer flexible management options, including secure system administration from anywhere and multi-time zone capability options.

An access management "terminal" should be tied to you — not the other way around.

Maximum flexibility, whatever your legacy system Access control software puts in the hard yards when it bends your existing system or setup to new needs. It can integrate across several databases, making workflows easier and less error prone. You may even wish to manage any existing mechanical locks from the same interface as your electronic or electromechanical locks. The right access control software handles that for you.

Tailored access for every site user and visitor

Streamlining access rights management for staff, contractors and visitors can boost business efficiency. Your access control software should filter access to specific locks according to the precise security needs of your site and users. For any system, you should be able to create individual schedules for key-holders, doors or audit trails. In a few clicks you can require users to revalidate keys regularly, making it safer to issue a contractor with time-limited access.

Smarter, more effective building management

Smart buildings need intelligent software. Do you know who uses which doors at your site, and when? Are you planning an office expansion and weighing up appropriate security for each type of room use? A properly configured software control panel should accurately track user movement around your site. It feeds back the data you need to make better business decisions.

Saving security budgets with a Software as a Service (SaaS) option

Ideally, you want to spend your security budget on actually securing people and assets. Alas, in the real world, IT costs and contingency budgeting eat up much of it. When you run access management software with a reliable SaaS provider, security infrastructure budgeting becomes more predictable. Your data enjoys complete redundancy and is therefore more secure. And your company's software is always, automatically up to date — critical for cyber-security resilience.

Mobile solutions for the modern mobile workforce

Are your mobile workers and contractors returning to base — or the nearest credential update — to redefine or revalidate their access rights? Access control software can (and should) be mobile. So, instead of updates, workers update credentials on the go, wherever they are, via an app and its encrypted Bluetooth connection.

All your business process software in one place

Multiple systems create double or triple the work. Duplicating data entry increases the chance of errors. With access control powered by the CLIQ Web Manager, for example, you can integrate powerful access management features with your existing business process software. One hub for everything. Thanks to the CLIQ Web Manager's open architecture, you can build a single interface to control all your "live" workflows. You manage HR, support ticketing, financial reporting and more, alongside daily access control tasks like validating and revalidating credentials, cancelling lost keys and ordering automated audit trails for locks or users.

Your Guide to Lighting

We all know the saying "crime never sleeps." The truth is reality isn't far off. According to U.S. News, crimes like murder, sexual assault and robbery happen more frequently at night nationwide, with cities like Cincinnati, Ohio, Austin, Texas and Dallas experiencing more overall police incidents during the evening than any other time.

For the integrator, this means the most competitive security solutions will be able operate reliably, day and night, to address these incidents—the only problem is, without proper illumination, most traditional video surveillance systems simply can't.

The Importance of Illumination

In the age of video analytics, especially, we've seen this issue create a serious security challenge. A standard security camera operating — without lighting — at night can yield dark, grainy images at best. Because video analytics require clear, high resolution images to deliver actionable results, low-quality images stop detection, identification and incident prevention in its tracks. When integrating a round-the-clock security solution, it's important to understand what options exist to mitigate this problem.

Built-In Versus External

A popular lighting option is when LEDs (light emitting diodes) are integrated into the camera. The appeal of these cameras, with built-in LEDs that encircle the lens, is that they provide an all-in-one solution. However convenient they may be, these options often create limitations. The range for visible LEDs built into a surveillance camera is around 150 feet — and typically only covers a 30° field of view (FOV), even though a standard camera's FOV is often 90°.

This creates "hot spots" in the middle of the camera view and can cause a total "white out" of the rest of the image. Additionally, LEDs encircling a lens are known to cause heat buildup, which can degrade the lens over time. External illuminators, however, are able to minimize heat accumulation and offer much longer illumination ranges — up to 900 feet, in fact, when using infrared (IR) illuminators. Because mounting external lights also enables deployments to adjust the angle of the illumination and pair any given camera lens with the perfect range/wavelength, independent illuminators represent a versatile solution.

Visible Versus Invisible

An equally important consideration is the type of illumination to install. Visible illumination — or white light — operates at a low cost, making them especially attractive when compared to other options, such as fluorescent or incandescent bulbs. These options are also durable and insensitive to vibration; and they feature an extremely long life. Because they utilize visible light, moreover, they enable color image capture and can even act as a deterrent to suspects when used as a floodlight.

Drawbacks to consider include the fact that they do, however, create light pollution and operate at comparably shorter distances. Invisible illumination, on the other hand, is detectable only by black-and-white or true day/night cameras, making any camera placement with invisible illumination covert. IR illumination of this sort offers a much longer range than visible light, making them an effective choice for security cameras tasked with monitoring larger areas. Drawbacks to consider include the fact that they can only produce black-and-white images, which can hinder object recognition and search analytics based on color.

Best Practices for Choosing an Illuminator

When it comes down to it, there is no "one-size-fits-all" lighting option for security deployments. Each surveillance system requires a unique solution. In a smaller space, for example, the ideal invisible lighting option is a short range, infrared illuminator.

In these cases, higher wavelengths (>940nm) are truly invisible and offer a wide area of coverage. In a larger space, or in an outdoor setting, medium range infrared illuminators with lower wavelengths (<850nm) provide illumination at longer distances, though they also produce a faint red glow. When video analytics require lighting at longer distances for ranged detection, however, this may be considered a worthy trade-off.

Consider these factors when specifying lighting for your surveillance system:

- The angle of illumination. The FOV of every camera is different, making it important to choose a lighting option that best matches the camera lens being used.

- Dual or triple mounting bracket. If a p/t/z camera is deployed, or if the area being surveilled is too large or wide for one illuminator to do the trick, mounting brackets allow the installation of two or three, side-by-side devices. This strategy doubles the angle of illumination and increases illumination distance by up to 40%, in the case of a dual mounting bracket and increases illumination distance by 75%

when using a triple mounting bracket.

- Both options allow integrators to install a hybrid lighting solution depending upon the specific needs of the deployment (i.e. a mix of both visible and invisible lighting).

- Make sure to target specific points of interest, such as gates or doorways, with both your camera and your illuminator to ensure the most important areas are covered.

Temperature Screening Solution: Helping in unsure times

Temperature is an important indicator of physical health. In many scenarios, people with abnormal temperatures could have a health issue. Thus, it's crucial that this is detected and monitored quickly and accurately. But traditional methods of temperature measurement are time-consuming and can put operators at risk. At times like these, technology can provide an efficient alternative.

With advanced detectors and algorithms, Hikvision's Temperature screening Thermographic Cameras are designed to detect elevated skin-surface temperatures. This means they can be used for rapid and preliminary temperature screening in hospitals, stations, airports and other public places. The cameras have an accuracy of up to ±0.5°C, giving a valuable indication of which persons should be further tested for fever.

It takes just one second to detect a person's skin-surface temperature, and the system can measure multiple people at the same time. This means it is efficient in an entrance, for exam-

ple, where a number of people will be passing at the same time. The use of AI technology means non-human heat sources, for example a hot coffee, are ignored, reducing false alarms.

Once a person is identified by the camera as having a higher skin-surface temperature, they can be flagged for further measurement. The system can also be useful to monitor a situation, providing useful anonymous data from a safe distance supporting end users' potential analysis or research. All this is also achieved with fewer people, not only making it easier to manage and more efficient, but also reducing the overall risk of unnecessary exposure.

Hikvision's thermal portfolio has a number of options to help with temperature screening. For example, a Turret/Bullet Camera with AI combined with iVMS 4200, a laptop and a bracket can be used as a quick solution that can be easily and quickly installed. For higher accuracy, a solution with a Blackbody calibrator gives an accuracy of ±0.3°C. There's

also a more mobile option, using a Handheld Camera that can connect to a smart phone or PC through WiFi to a Hik-Thermal app. This also features a built-in speaker for audio alarm.

There are also solutions that combine temperature screening with access control, allowing lobbies to be monitored and, if necessary, people measuring above a certain skin-surface temperature refused entry until they are double-checked by alternative methods.

It's important to remember that Hikvision's temperature screening thermographic cameras are designed so as to achieve rapid preliminary screening in public areas. Actual core body temperatures should be further confirmed using clinical measurement devices.

This is just one element of a complex infrastructure to overcome challenges in unsure times. It can also give managers and researchers useful information, collected in a safe manner.

AI is not a security cure-all, says Identity Automation

With the start of the 2020s, many security industry experts are reflecting on the emerging technologies over the past decade and looking forward to what is in

store in the future. Artificial Intelligence (AI) is a buzzword that has infiltrated everyday nomenclature throughout the past decade. Every industry from healthcare,

to banking, to security has implemented some form of AI that is touted as the hidden key to maximising productivity and/ or security. However, AI technology is still in

its infancy and is not the panacea that many cybersecurity experts claim.

Today, AI is a nascent technology and has limited practical applications because it's still difficult to understand the rationale that is used by the machine learning algorithms for making their decisions. As a result of this limited understanding, these technologies are only leveraged for pinpointed functionality. For example, AI can be designed to analyse data for specific threats, such as malware, but AI technology is only as good as the data it analyses and cannot be fully trusted to discover new threats that emerge on their own. Furthermore, even when a threat is detected by AI, humans are still needed to confirm that a real risk is present.

AI undoubtedly has its place in today's security space. Government agencies and the military use AI to comb through hundreds of hours of call data to try to isolate terrorist or criminal activity.

In its current state, AI can successfully review large amounts of data and automate repetitive tasks. The results of these services are helpful as additional data points, but at this time it makes more sense to use AI as helper technology rather than fully relying on AI to ultimately make decisions for organisations.

Furthermore, AI can be utilised in access management to watch the habits of individuals and identify actions that stray outside the norm. For example, if a user logs into a system outside the normal working hours, AI can identify this anomaly and utilise step-up authentication to further validate that the user should be granted access. AI can also be leveraged for access certification campaigns by providing scoring that helps approvers prioritise their efforts on certifications with low scores. However, algorithms should not be trusted to make higher stake decisions. This is because AI cannot

currently be taught or programmed with the intuition that humans naturally possess, making the risk of a breach or other security threat is considerably higher.

In this next decade, AI will continue to grow from its infancy into a more useful and robust tool that companies can utilise to keep their assets and people safe. There will be a point where AI reaches a mature stage where it can truly think and learn on its own; computing power has grown exponentially in the last decade and will only continue to grow more in the next. This increase in computing power opens up a limitless number of possibilities for AI usage, especially as humans perfect and refine AI's algorithms.

For now, AI has a place in today's security industry and has already proven to be adept at identifying threats and making society safer. While this is helpful, humans remain as a critical factor in evaluating threats. I believe that the future of AI is bright, and fully expect that our capabilities around explainable AI will rapidly advance thus providing many opportunities to leverage these technologies in a fully autonomous capacity in the not-to-distant future.

Athena claims its AI platform detects Coronavirus

Athena Security is an AI surveillance startup that created a platform it claims can stop threats before they happen. The latest threat detection it has added is for COVID-19, the coronavirus that is quickly spreading across the globe.

According to the company's website, "Our Fever Detection COVID-19 Screening System is now a part of our platform along with our gun detection system which connects directly to your current security camera system to deliver fast, accurate threat detection — including

guns, knives, and aggressive action. Our system can also alert you to falls, accidents and unwelcome visitors."

Athena says its AI platform utilizes a NVIDIA 2080 RTX graphics card and computer vision to continuously monitor every camera frame for threats such as a gun being pulled out, hands in the air or someone being punched. When it comes to detecting coronavirus, "Athena watches the thermal camera for people with elevated body temperature. Fever and dry cough

are the first two signs of coronavirus infection, and fever is a quantitative way to rapidly screen large numbers that walk by the camera without friction," the company says.

Once a person with an elevated temperature is detected, Athena will send a real-time video feed to security staff, an administrator or whomever the user designates.

Athena says its platform can send alerts to a user's VMS and integrate with access control or other systems with an API, available by request. The company is aiming its coronavirus detection at schools, corporations, retail organizations, industrial companies and other industries that are putting workplace safety measures in place to help prevent the spread of the virus.

HIKVISION®

See Far, Go Further

Capturing the World as It Really Is
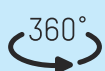## Empowering Business with Intelligent Insights
Hikvision Fisheye Cameras

FEATURE HIGHLIGHTS

- Cost Efficiency
- Less Distortion, More Natural Visuals
- No Blind Spots
- Heat Mapping
- Intersection Flow Analysis
- Less IR Reflection