

SECURITY Update

CREATING BUSINESS OPPORTUNITIES



For Manufacturers, Distributors, Dealers,
System Integrators & Installers of Security,
Fire & Safety Systems.

Vol. 11 No. 02

www.securityupdate.in

February 2021

Pages 16

Price ₹ 50

Important considerations for a safe return to business



Organisations worldwide are witnessing the power of cutting-edge video to drive a return to business as (almost) usual. But while the technology itself is vital, it's only one part of the process. However, there are also health, safety and welfare policies that businesses would do well to bring into operation alongside their technology investments.

Today's intelligent AI-powered cameras provide vital screening services for organisations striving to get people back to business. These cameras can measure someone's skin temperature and check if they are wearing a mask or not; they can carefully monitor crowd density, flagging when there are too many people in a certain location; and they can accurately measure the distance between people, helping to uphold local social distancing regulations.

But for this technology to deliver its full potential, businesses should also consider key HR and legal matters that may affect all those coming into view of the cameras. These considerations can be woven into a custom Health, Safety and Welfare policy, which is understood and adhered to by all.

Ensure staff are on hand and informed

First of all, businesses need to ensure there are staff available to support the screening process at the premises, and that they know exactly what they are expected to do.

Consider temperature screening, for instance. Who is going to be present to monitor temperature readings? And if someone does have a high temperature, what happens next? Moreover, what will you do if someone objects to having their temperature screened? Such things need careful consideration.

Equally, when it comes to mask detection, will members of staff be on hand to guide people towards the mask detection cameras? And if the camera finds no mask, will one be provided?

For flow control, it is vital to consider how many people can safely be accommodated on the premises at any one time. A policy will also be needed to deal with what happens if people continue to enter a location that has reached full safe capacity. And if the system sounds an alert to one or more individuals, asking them to maintain social distancing, one key question is: how will the business enforce this?

ing, one key question is: how will the business enforce this?

Employee consent and privacy

It is also vital that staff fully understand that they are being screened, and that they agree to it beforehand. Organisations should clearly inform employees of the video technology, the nature and extent of the monitoring, and its purpose, clarifying what has changed from the normal policies. It is recommended to obtain official written employee consent for being screened.

If facial recognition is selected for use for employee access control, this technology will reveal 'personal data', which is defined as 'processing personal data', and privacy regulations apply (such as GDPR in the EU). Consent for processing facial images is essential, so businesses must obtain it from each employee, who should be clearly advised that this data will be used only for future access control/ time attendance. Employees should also be given the option to withdraw their consent in the future if they change their mind.

The data of a human



subject's body temperature generated during automated temperature measurement is not defined as a 'personal data' under certain data protection laws. However, it cannot be ruled out that data protection law does apply in the case that it is possible (even subsequently) to identify the people passing before the cameras.

Of course, every business is different. So when devising health and safety procedures,

it is vital that each element should be tailored to the specific business, the environment and the policies. It is vitally important to also check changing regional guidance and requirements regularly. Organisations may also want to consider getting legal advice, in order to ensure that this part of the process is absolutely right.

Hikvision, as a company, believes it has endeavoured to optimise its products and help

customers reduce the compliance risks regarding data protection law. The company also recognises that technology is only one part of the back-to-business story, and has produced a Back-to-Business eBook that gives an overview of its camera portfolio, explains how to install them for the best results, and outlines the health and safety considerations for using them.

Credits: Hikvision



C1C

As Sharp-Eyed as an Owl



Super Vision, Even at Night

Get better night vision at increased distances with the C1C and enjoy round-the-clock protection. The advanced infrared LED lights along with an upgraded optical configuration means that even in dim light, you can still see up to 12 meters (40 ft.).



Corporate Office:
PRAMA HIKVISION INDIA PVT. LTD.
Oberoi Commerz 2, International Business Park,
18th Floor, Near Oberoi Mall, Off W.E. Highway,
Boregaoon (East), Mumbai - 400 063.
Tel: +91-22-4041 9900, 2846 9900
Web: www.hikvisionindia.com

Sales
+91-22-4041 9944, 2846 9944
sales@pramahikvision.com

RMA Support
+91-22-8822 9977, 3322 6070, 2846 9977, 0250 863 6677
rma@pramahikvision.com

Technical Support
+91-22-8822 9999, 3322 6060, 2846 9999
support@pramahikvision.com
Toll Free - 1800 222 699

Dear Reader

For as many years as one could recall, London was the city with the maximum number of CCTV cameras in the world, it was reported in 2004 that a Briton was liable to be shot (pictured) 300 times a day by CCTV cameras, from when one left for work in the morning till the time one returned. Then, cities in China overtook London to be the most surveilled. However a recent study titled 'The Top Surveillance Cities Worldwide' conducted by Surfshark and published in the South Asia Journal surprised everyone when it listed two of India's cities in its top 10 list. Chennai apparently is at the top with 657 CCTV cameras per sq km and 25.5 per 1,000 people. Hyderabad is at number two, beating major cities such as London, Beijing and New York. Not surprisingly, six Chinese cities feature in the top 10 - Beijing, Harbin, Xiamen Chengdu, Taiyuan, Kunming, while Delhi features at number eight!



As the proliferation of CCTV cameras in public areas keeps growing by the day, and as the government starts to store more and more data about its citizens, one often wonders if we will have any privacy left in another few years. Governments all over the world want to keep tabs on every citizen, often in the name of national security. While that may be true to a certain extent, citizens are increasingly getting uncomfortable with the way technology is transforming with intelligence gathering capabilities. The risk to every citizen is increasing because of the vulnerability of personal information falling into wrong hands.

Tony Porter, the former surveillance commissioner of UK & Wales, who I had the honour to meet a few years ago, when he was still holding office, feels that people don't understand the capabilities of newer, biometrically enabled systems such as drones, mobile-phone tracking and automatic number plate recognition (ANPR). He says, "It is not clear that the right balance between privacy and security was being struck, accusing police of acting like 'sentinels in the mist'." An erstwhile senior police officer himself, Porter says, "the balance between privacy and security hasn't yet been demonstrably met."

Taking cognizance of privacy concerns and keeping the rise in public interest litigation cases in view, many countries are cautious of the technology and the European Union is considering banning it in public places for up to five years while it works out how to prevent abuses. Amnesty International has launched a global campaign to ban the use of facial recognition systems, a form of mass surveillance that amplifies racist policing and threatens the right to protest. The 'Ban the Scan' campaign kicks off with New York City and will then expand to focus on the use of facial recognition in other parts of the world in 2021. It is viewed that publicly deployed facial recognition systems are a form of mass surveillance that violate the right to privacy and threaten the rights to freedom of peaceful assembly and expression.

While others deliberate, on 14th May 2019, San Francisco banned the use of facial recognition software by the police and other agencies. Civil liberty groups have expressed unease about the technology's potential abuse by the government amid fears that it may push the United States in the direction of an overly oppressive surveillance state. But critics said that rather than focusing on bans, the city should find ways to craft regulations that acknowledge the usefulness of face recognition.

However, the technology has many benefits as well, giving law enforcement agencies a great advantage to identify suspects while investigating crimes. Used alongside artificial intelligence and machine learning this technology can be used to even predict and stop crimes from happening. It is ridiculous to deny the value of this technology in securing airports and border installations. As a biometric feature, use of face recognition has gathered significant momentum over fingerprints and other contact technologies in access control during the ongoing pandemic time. It would be interesting to continue tracking how this tech pans out in public usage over the next few years.

Till we meet next month, Stay Safe and Keep Others Safe.

G B Singh
Group Editor

gbsingh@1stasset.org
@EditorGB
linkedin.com/in/gbsingh9



SECURITY UPDATE is a focused educational publication on protection technology, products and solutions. It reaches the business community of manufacturers, distributors, dealers, installers, integrators and consultants of security, fire and safety systems. Printed monthly as a lightweight tabloid, it is easily carried and read on the move, reaching the remotest corner of India, even where the internet may not have reached!

General Information

SECURITY UPDATE welcomes manuscripts, news items and photographs, however SECURITY UPDATE is not responsible for loss or damage incurred while in transit or in our possession. SECURITY UPDATE is published monthly on the 28th day of every month. Deadlines are three weeks before this date.



©1st Academy of Security Science Education & Training Pvt. Ltd.
ISO 9001:2008 Certified

All rights reserved. No part of this publication may be reproduced in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written consent of the publisher. Opinions expressed in articles or advertisements appearing in SECURITY UPDATE are those of the authors or advertisers and do not necessarily reflect those of the publication, or of its publishers.

Printed, published and edited by G B Singh on behalf of
1st Academy of Security Science Education & Training Pvt. Ltd.

Printed at Ask Advertising Aids Pvt. Ltd.

88 DSIDC Sheds, Okhla Indl. Area Ph-I, New Delhi 110020

Published at "Security House", 24-B, Udyog Vihar-V, Gurugram 122016, Haryana, INDIA.

info@1stasset.org

Aiphone launches IXG Series IP Video Entrance Station with Telecoil to assist individuals with hearing loss



Aiphone, the international manufacturer of intercom and security communication products, is announcing its IXG Series tenant, guard, and entrance stations are integrated with Telecoil (T-Coil) to assist individuals with hearing loss or impairments who wear compatible devices.

This integration allows the IXG-DM7-HID IP Video Entrance Station to send out an elec-

tromagnetic signal that the T-Coil within a person's hearing aid picks up – allowing the hearing aid and the intercom system to directly connect to produce a clearer sound and to remove audio interference.

This feature allows those who suffer from hearing impairments to more easily communicate using an intercom system in multi-tenant facilities, as well as medi-

cal or elder-care facilities. "The Telecoil integration is important to ensure Aiphone's intercom and security communication products can be easily used by individuals who are hearing impaired and require the assistance of a hearing aid," said Brad Kamcheff, Marketing Manager for Aiphone Corp.

"More than 13 percent of people in the United States report some difficulty with hearing and Aiphone wants to ensure that our devices support accessibility and the Americans with Disabilities Act." The T-Coil integration works like this: when a hearing-impaired individual approaches an intercom, the sound signal is connected to an amplifier, which generates a current to pass the signal to the induction loop – which

is usually made of copper tape or wire.

The loop then produces an electromagnetic field and is then picked up by the T-Coil. As each hearing aid individually tailors the sound to the specific needs of the individual, the integration with T-Coil allows for reduced background noise and the full spectrum of sound frequencies required for intelligibility.

The IXG Series from Aiphone features the benefits of an IP intercom with the versatility of a multi-tenant solution, all powered by a single, full-featured system. IXG Series solutions are ideal for commercial sites, industrial facilities, schools, campuses, parking garages, retail, emergency calling, and correctional applications.

LenelS2 integration with Seek Thermal's contactless thermal imaging system



LenelS2, a front-runner in advanced security systems and services, announced the integration of its OnGuard® and NetBox™ access control systems with Seek Thermal's Seek Scan thermal imaging system. The new integration allows businesses to identify individuals with elevated skin temperature through a contactless solution and

allow or deny entry based on this reading.

The integrated solution joins the Carrier Healthy Buildings Program suite of offerings to help deliver healthier, safer, more efficient and productive indoor environments. LenelS2 is a part of Carrier Global Corporation, a foremost provider of healthy, safe

and sustainable building, and cold chain solutions.

As one of the most affordable thermal temperature screening solutions meeting FDA guidelines during the COVID-19 pandemic, the Seek Scan system is designed to automate body temperature screening. With accuracy readings within a fraction of a degree, the Seek Scan system delivers the same performance as a handheld infrared temporal thermometer, but it is automated from a safe social distance.

Through its application programming interface (API), the Seek

Scan system is accessible anywhere on a network, enabling integrators and business owners to access and manage the system. "As we strive to help reopen offices and other gathering spaces, daily temperature scanning is one important aspect of a comprehensive strategy to help ensure healthier environments," said Mike Muench, CEO and President, Seek Thermal. "As the demand for thermal screening and integrated API solutions grows, our strategic collaboration with LenelS2 will help deliver this affordable system to a myriad of businesses and organisations."

Third Millennium announced the launch of new Anti-Ligature Reader



Third Millennium has announced the launch of a flush-mounted Ligature Resistant reader. The RX5M is a Third Millennium styled flush-mounted Ligature Resistant reader. The unit is a multi-technology reader suitable to interface with all standard

access control systems.

This unit offers impact-resistant construction with a high degree of protection against vandalism and malicious attack.

The stainless-steel flush fit assembled housing may be secured

to a recessed standard UK Double Gang Back Box using two security screws, making installation quick and easy.

Steve Greenaway, Business Manager, said

“The primary function of the reader is to prevent anyone from harming themselves, or others, and ensuring that a ligature cannot be attached to the reader.” “However, the RX5M is also

suitable for areas where standard readers might become damaged, such as unsupervised public places, corridors and detention facilities.”

Alarm.com unveils new video doorbell and LTE sensor



Alarm.com, made two major product introductions recently. The first is a new Alarm.com-branded video doorbell with a COVID-friendly spin; the second is a LTE-powered sensor that can be deployed in challenging environments.

The touchless doorbell eliminates the need to physically press a button – anyone coming to the front door simply stands on a doormat placed at a safe distance to ring the chime. Rather than using motion detection, the product's internal video analytics do the work.

According to a press release, when a person is detected, the doorbell immediately triggers the existing chime in the home, sends a mobile alert to the homeowner and starts recording a video clip. Homeowners can see and speak with visitors through the doorbell's live HD video and two-way audio.

The device also features:

- 150-degree vertical field-of-view that gives homeowners a full head-to-toe image of visitors and clear look at packages left on the doorstep
- Optimized portrait viewing on mobile so there's no need to rotate the mobile device
- Full HD resolution, HDR, and infrared night vision
- Onboard heater for low temperature operation
- Live video and saved clip viewing using the Alarm.com mobile app or website

The Alarm.com Flex IO is a new battery-powered sensor device that has been weatherproofed for outdoor durability. It uses the latest LTE-M technology to operate anywhere there's LTE coverage and without a panel, hub or even Wi-

Fi. According to a press release, security service providers can offer the device as a standalone solution or as an expansion to a customer's existing system.

According to the release, the sensor sets up in seconds and can be attached to almost anything, such as doors, gates, sheds, barns, detached garages, guest houses and other access points around a property. A wired magna-loop input option keeps users informed if freestanding items, like a motorcycle or lawn mower, are moved.

An expected battery life of more than two years and the vast LTE coverage via AT&T and Verizon paved the way for this product's development. It also includes wired inputs that enable the device to integrate with other sensor devices, such as motion detection or water leak detection.

er sound gives intuitive and user-friendly clear information to visitors, and suits almost all applications and environments for indoor and outdoor installations and offers the highest level of security.

The CT9 incorpo-



rates ISO18092 NFC and BLE, QR code mobile phone access ID, and several chip technology RFID dual 125KHz & 13.56MHz contactless smart cards which makes it ideal to use when several card populations with different RFID-technologies and/or frequencies should be used at the same time. The CT9 is designed to read Secure Access Modules (SAM) embedded on a SIM-card sized contact chip, and is compatible with Mifare SAM AV2 which gives the possibility to further increase security for storing encryption keys (Evaluation Assurance

Level, EAL5+) and also allows for diversification of encryption keys. This combination makes the product flexible for all kinds of security applications and future technology requirements applicable to the security industry.

The CT9 TCP/IP reader supports QR code display on a 3.5" touch screen, visitors use their personal mobile phone with the app running to scan a code to unlock the door. The system is flexible so is able to authorise a visitor with his/her valid access time or for a particular duration. An SDK is offered

for both server software and smartphone app integration.

As the CT9 comes with an SDK for third party server software integration, it is ideal for general purchase applications for access control, visitor management, time attendance, facility control, loyalty membership management and cashless payments. The SDK also offers a mobile phone app demo with source codes for customer mobile app development using BLE/NFC or QR codes for lock control.

Tagmaster launches world's first intelligent bike detection system



Tagmaster is launching a radar detector system for directional counting of bicycles and pedestrians in urban environments. The system is thought to be the first intelligent bicycle and pedestrian detector on the market.

The launch is another result of Tagmaster's investment in solutions for so-called Active Travel, which contributes to the necessary transition to a more sustainable transport system. The new radar detector system is launched simultaneously in France and the UK and will help cities de-

velop better solutions for bicycle traffic and pedestrians.

“We are seeing a strong development towards bicycle traffic and pedestrians, so-called Active Travel, starting to have the same status in traffic flows as motor driven vehicles. This development has intensified during the ongoing pandemic and major investments are being made in solutions for bicycle traffic and pedestrians in major cities in Europe”, said Jonas Svensson, CEO, Tagmaster.

The system is easy to implement as the de-

tectors are mounted to existing street furniture with no in-ground sensors required, and it can be used for both temporary measurements and permanent for long-term measurements.

The system allows responsible traffic authority to measure both the direction and frequency of bicycle traffic and pedestrians. The Cityradar unit can be powered by mains, solar or battery supply. It is equipped with a 4G modem for remote data collection and Bluetooth for localised wireless configuration and data collection via an app.

New web access control reader from Civintec

The Crystal Touch, CT9, is a Linux based HTTP server centralised reader with TCP/IP Ethernet suitable for both LAN and Internet cloud server software communication. Designed with embedded relay control for lock control,

the CT9 is ideal for both standalone access control systems and online server centralised access control monitoring in real time - no need for an additional controller.

With a stylish and elegant design, the 3.5" touch screen and speak-

Safetrust introduces SABRE MODULE to upgrade HID iCLASS® Readers with MIFARE® DESFire® EV3 Security



Safetrust, a pioneer in virtual credential solutions, introduces the SABRE MODULE, a 30-second plug-in upgrade that adds DESFire EV3 and remote management capabilities to installed HID iCLASS readers. The module simplifies the transition from legacy prox, iCLASS or SEOS credentials to DESFire EV3 and supports Wi-Fi which allows customers to remotely manage and configure their readers, eliminating the need for

onsite visits.

The fast, plug-and-play solution requires no rewiring and allows organisations to extend the ROI of their existing infrastructure with their installed readers, it's the end of rip-and-replace. "Safetrust technology extends the useful life of access control infrastructures and provides a transition path away from expensive and proprietary vendor card products to interoperable industry standards such as DESFire EV3,

Global Platform and OSDP SC," said Jason Hart, CEO of Safetrust.

"With support for Bring Your Own Key (BYOK), a customer can choose the card manufacturers that best suit their design needs and pricing." Over-the-air (OTA) updates enable future features to be delivered seamlessly from a central management portal. This includes future product features, software patches and any evolution of new card specifications.

New non-contact access control and attendance solution



The iT100 Iristime, is Aditech's newest non-contact biometric offering that features both iris and facial recognition technology. Automatic recognition of iris and/or face is possible and a large capture volume allows for increased flexibility, speed and convenience.

Iristime offers enhanced security through Secure Boot and an open Android Platform provides an opportunity for third party application

development. The Aditech Iristime time and attendance also uses an iris/face fusion feature which means the system can be operated in iris only / face only / and, or, fusion mode. Options can be selected and used depending on the requirements for the specific biometric security environment.

Simultaneous biometric capture automatically captures dual iris and face at the same distance, and a proven

set of anti-spoof counter measures are also included.

The solution offers non-contact authentication as the system automatically captures faces and iris naturally at a distance of up to 24 inches or 60 cm. The 7inch multi touch display offers easy on device setting and user enrollment via a self-guidance feature with live images on the multi touch LCD screen.

Iris ID iCAM M300 biometric reader compatible with MozaicID smartcard software credential application

Iris ID, a pioneering provider of iris recognition technology, announced the compatibility of its iCAM M300 handheld, multi-modal biometric reader and the MozaicID iCAM M300 smartcard software credential application.

This application enables the mobile device to accommodate a range of Personal Identity Verification (PIV) compatible credentials including PIV Interoperable (PIV-I) and the Transportation Worker Identification Credentials (TWIC), a smartcard

used by workers requiring access to secure areas of U.S. maritime facilities and vessels.

The MozaicID app uses the iCAM M300's detachable FBI-certified Sherlock fingerprint sensor from Integrated Biometrics to authenticate workers' identities by comparing a live fingerprint to a stored template embedded in the credential. The application will also check the trust status of the presented credential. The iCAM M300 also enables mobile enrolment of workers with its



embedded camera simultaneously capturing both iris and facial modes for contactless identity authentication.

3DX-Ray launches AXIS-CXi cabinet X-ray screening system to identify the nature of the materials scanned



on pseudo colourisation of images and powder detection algorithms to indicate to operators the potential of a threat – these tools do not have any independent standard accreditation or assessment unlike the materials discrimination 3DX-Ray has introduced which is assessed according to the transport and aviation sector standards.

A further major innovation is in the design itself. The AXIS™-CXi has an extra-large inspection chamber, whilst maintaining a small footprint. So, not only can it scan mail and parcels, but it can also scan bags up to and including aircraft cabin bags.

The system is mobile and aesthetically sympathetic, meaning that it can be used in corporate entrances and hotel lobbies in times of raised threat levels. With user-friendly touch screen controls, unrivalled image resolution and image processing software, AXIS™-CXi is a unique product with unmatched functionality and utility.

In a world first, 3DX-Ray launches the AXIS™-CXi, a cabinet-based X-ray screening system that utilises the same colour differentiating image technology used in airport baggage screening. The AXIS™-CXi is a huge step forward in mailroom scanning, as colour differentiated images enable operators to determine not just the shape but, the nature of the materials being scanned. Orange shows organics, such as; explosives, chemicals and drugs, as well as more

innocent items such as foodstuffs. Blue shows metals, such as; guns, knives, and potential IED components.

Green shows inorganic materials like those used in homemade explosives. Grey scale is used for recognition of shapes and the form of objects. This allows the operator, with very little training, to analyse items more accurately, quickly and easily.

This is a step change from the existing cabinet mail screening manufacturers who have relied

Hikvision launches 4G solar kit for remote security



Hikvision has launched a 4G Solar Panel Kit for standalone security sites in the UK & Ireland. The company believes this will “revolutionise the protection of remote assets in hard to reach places” by providing a security camera that runs on solar power.

The kit (DS-2XS6A25G0-I/CH20S40) includes a 4G camera, a solar panel, a battery, and a bracket, and can provide one-stop monitoring in remote environments. This means providers can deliver connected security to scenarios such as agriculture, animal and forest observation, as well as temporary monitoring of construction sites.

Hikvision says it has received numerous requests from rural communities and places where power and cabling aren't practical, while installers are regularly seeking temporary mo-

bile solutions for short/medium term projects. The issue of having no power or network is no longer a problem, explains the company, with the kit providing power to the camera through the solar panel and connectivity through 4G. It sends data to a communication station and then on to the security monitoring centre, where it can be managed using HikCentral Professional or the Hik-Connect app. Both monitoring and management activities, like viewing footage live, can be done remotely over the 4G network, which is considered to have more than capable bandwidth capacity for video delivery. Hikvision does recommend that all customers check with their providers on the network strength and speed before purchase.

Its lightweight design is said to be easy for one person to install, while

the IP67 rating provides protection against most adverse weather conditions, and it also survives well against strong winds often experienced in remote areas. The kit demonstrates long endurance, detecting power levels and automatically adjusting to power-saving mode when they are low. This means it can work continuously for up to seven days in cloudy and rainy weather when fully charged.

Hikvision believes that solar is now a genuinely practical solution, with technology having advanced significantly in recent years. For instance, it is said to take around 18 hours of sunlight to charge the cells from 0-100%, while a fully charged battery enables the system to run continuously for seven days in overcast conditions.

analytics simultaneously detects and classifies various object types, including people, vehicles, faces and license plates, and is supported by Wisenet AI algorithms. Unique to Hanwha Techwin, these identify the attributes of objects or people, such as age group, gender or colour of the clothing a person is wearing.

The attributes are saved as metadata on the NVRs alongside the images captured by the cameras, enabling users to quickly search for specific objects or incidents. The algorithms are even able to recognise if a person is wearing glasses or holding a bag.

Together, the NVRs and AI cameras offer a high degree of detection accuracy, whilst minimising false alarms. As such, they provide control room operators and security personnel with a powerful tool to identify and respond quickly to any suspicious activity. They also offer businesses, and in particular

the retail sector, with the opportunity to capture and analyse business intelligence, which will enable them to review customer demographics, gain a greater understanding of customer behaviour and improve the customer experience. In this respect, because AI can handle extremely busy and dynamic scenes, it is much more suitable for retail environments than traditional video analytics.

In addition to H.265, H.264 and MJPEG, the new NVRs support WiseStream II, a complementary compression technology, unique to Hanwha Techwin, which dynamically controls encoding, balancing quality and compression, according to movement in the image. When WiseStream II is combined with H.265 compression, bandwidth efficiency is improved by up to 75% compared to current H.264 technology.

Installation time is

minimised with the ability for engineers to remotely connect to the NVRs via a smartphone or tablet without having to set up a complex network, by using P2P and unique QR product codes. In addition, the NVRs can be easily and quickly configured to match an end-user's requirements via an updated Wisenet user interface, and with the help of a new installation Wizard.

If communication between one of the NVRs and a Wisenet camera equipped with an SD card is disrupted, Automatic Recovery Back-up (ARB) will facilitate the transfer and seamless storage of the images stored on the SD card when the network connection is restored. This provides continuity of recording and negates the risk of what could be valuable video evidence being lost.

New facial expression technology for human behaviour analysis



Herta is launching the company's new video analysis solution, Bioobserver, a sophisticated software aimed at marking a significant change in the study of human behaviour and facial expression analysis.

Based on advanced artificial intelligence techniques, Bioobserver automatically detects and annotates a person's facial expressions and micro-expressions, as well as the direction of the gaze and head orientation, in order to monitor behavioural metrics such as affective states

or the individual's level of attention.

The platform also allows for the configuration of automatic rules and annotations of events to extract key frames of the video that are considered of interest.

With Bioobserver subtle micro-expressions such as “frowning”, “blinking” or “raising eyebrows” can be detected. The tool offers the possibility to work at a very low level. Then, the combination of some micro-expressions may form a higher-level pro-

typic facial emotion (such as joy, anger, sadness, fear, surprise...) which can be configured in the software as well.

This new solution has been co-created together with key end-customers from the law enforcement sector, resulting in a user-friendly, intuitive and time-saving tool that any interviewer would love. The solution is being offered as an SaaS model and will allow the customer the opportunity to process hours of video, extremely fast and at a favourable price point.

Advanced NVRs offer accurate AI meta-data search



Three new feature-rich NVRs from Hanwha Techwin which offer up to 400Mbps network camera recording, are able to read AI metadata, enabling operators to quickly and accurately search video for objects and attributes associated with

them. Introduced at the same time as the 64 channel XRN-6410B4 and sharing the same features, the Wisenet XRN-3210B4 has 32 channels, whilst the 64 channel XRN-6410DB4 NVR is also equipped with a dual switched-mode power supply

(SMPS), to ensure continuity of recording for mission critical applications.

The 3 NVRs are compatible with all Wisenet AI cameras which have license-free deep learning AI video analytics onboard. The

AndroVideo releases a security camera that follows OSSA's Technology Stack for video security devices



The Open Security & Safety Alliance (OSSA) has announced that AndroVideo has released its first security camera that follows OSSA's Technology Stack. OSSA drives an open platform principle and philosophy to open up the security and safety marketplace to fuel innovation beyond the limits of a single organisation. Supporting the security industry's emerging open ecosystem, the new Smart Edge Camera from AndroVideo is available now and bears the 'Driven by OSSA' seal.

This mark indicates the product follows the OSSA Technology Stack for video security devices that prescribes the use of a common operating systems (OS), with the first two OSSA Specifications being:

OSSA Application Interface Specification

OSSA Compliant Camera Definition Specification

The seal also ensures seamless connectivity within the newly established digital marketplace operated by Security & Safety Things – also an OSSA member organisation. This single marketplace is a central hub that provides tools and information to enable third-party app development. System integrators can then use the infrastructure to purchase, install and manage the apps on 'Driven by OSSA' camera devices. This consolidated approach is a core component of the Alliance's vision to steer open standards.

AndroVideo is a developer and manufacturer

of smart edge cameras that offer impressive technological advancements. The AndroVideo Smart Edge Camera runs the operating system provided by Security & Safety Things and seamlessly connects to their recently announced digital marketplace.

AndroVideo takes security up a notch with its competitive edge computing capabilities. The MD2, EBL2 and VD2 in dome, bullet and vandal dome form factors incorporate various robust technical features. Engineered with expertise in image quality tuning, the new product line provides market players with a highly optimised, application-ready platform for rapid AIoT development.



14.2.

- Easily archive and backup footage to a remote destination for safekeeping.

- Complete data ownership and perpetual licences. All video processed on-premises, with optional internet connectivity

needed only for remote backups and viewing. No subscriptions are needed.

Tamron announces the expansion of M117FM fixed focal lens series for machine vision compatible with 1/1.7" imagers



Tamron Co., Ltd., a renowned manufacturer of optics for diverse applications, currently offers an array of globally renowned Ø29mm compact-size fixed-focal lenses, M117FM series, compatible with 1/1.7" imagers and full 6-mega pixel resolution, for machine vision applications. Five new models, M117FM12 / M117FM16 / M117FM25 / M117FM35 / M117FM50, will be released to support the growing needs of applications.

Mega-pixel cameras used for machine vision applications including production equipment, print circuit board mounting equipment, various test equipment,

and various machine tools, are migrating toward higher resolution. Tamron currently offers a variety of mega-pixel machine vision lenses with 30 different models compatible with 1.1", 1/1.2", 2/3", 1/1.7" and 1/1.8" imagers.

Currently, rapid growth is expected in the use of machine-vision lenses compatible with 1/1.7" and 1/1.8" imagers of 6-megapixel resolution. To meet the need, Tamron's M117FM series is added with five new models. The new M117FM portfolio, in addition to the two models currently available (wide-angle 1/1.7" 6mm F/2.4 (Model: M117FM06) and 1/1.7" 8mm F/2.4 (Model: M117FM08)), offers a

total of seven models to meet the requirements of a wide range of field of view in machine vision applications.

The expanded lineup of compact-size M117FM models, with an outer diameter of Ø29mm, offers an optimum selection for all machine vision applications, and assures compact size, high-resolution, high-contrast imaging for all shooting distances including up-close distances. Tamron develops popular and affordable high-resolution fixed focal lenses that address customers' critical requirements and needs in all machine vision applications and pursues optical performance that assures distinguished fidelity in all image details with excellent user utility.

Synology launches DVA3221 Deep Learning NVR for on-premises video surveillance and analytics

Synology Inc. launches the next Deep Learning NVR, the DVA3221, for advanced on-premises video surveillance and analytics. Using GPU-accelerated deep learning algorithms, DVA3221 can generate real-time insights that enable security personnel to take action immediately.

Facial recognition, people counting, vehicle detection, and additional video analysis capabilities enable the users to deploy a more intelligent solution for a safer environment.

DVA3221 combines Synology's expertise in data storage and man-

agement with powerful VMS solution, Surveillance Station. Support for over 7,600 cameras, ONVIF compatibility, and integration with I/O modules and speakers mean that one is not tied down to a specific brand or platform. With all analytics stored and processed on-prem, the solution can be entirely standalone, with no internet connectivity required unless setting up cloud or off-site backups.

Surveillance Station is platform-agnostic, supporting playback and management through mainstream browsers, through the Windows

and Mac clients, and mobile apps.

- Deep-learning powered video analytics for facial recognition, people and vehicle detection, people counting, and more.
- Supports up to 32 camera feeds, with six real-time video analytics tasks.
- Search intelligently through existing footage by filters such as motion detection, missing items, no-idle zones, and more.
- Store large amounts of footage with four internal 3.5" bays, expandable up to

3xLOGIC unveils VIGIL suite of video solutions in the EMEA region



3xLOGIC, the globally renowned provider of server and cloud-based technology, has announced the launch of its VIGIL suite of video solutions, across the UK, Europe, Middle East and Africa (EMEA) regions.

The ecosystem, comprising software and hardware components, such as cameras, recorders, thermal imagers, people counters, and accessories, is designed to provide a scalable security solution that's tailored to every business need. Business executives have increasing amounts of data available to analyse, with the total amount of data in the world estimated to be 59 zetta-

bytes. The 3xLOGIC ecosystem taps into this, by capturing and analysing these 'big data' elements and combining disparate data sets.

The VIGIL suite of video solutions help business executives to optimise their operations, find efficiencies, secure their buildings and assets, and solve problems they never knew they had in the first place. The video suite additionally integrates with security systems, Point of Sale systems, alarm management platforms, and cloud-based management systems to make security management easier and more efficient.

Bill Hobbs, Vice President of Global Sales at 3xLOGIC stated, "For over 15 years, 3xLOGIC has been proud to be at the forefront of server and cloud-based technology. The launch of the VIGIL video suite is the next step, helping business executives make data-driven, informed decisions across their supply chains, their sites, their buildings, and people."

He adds, "With VIGIL, business executives don't just get a single security system, access control, or video management system, they get an ecosystem that's bespoke to their needs and goals."

New thermal cameras measure body temperature



Panasonic I-Pro Sensing Solutions Corporation of America has released a new thermal camera solution aimed at helping organisations maintain the health and safety of those entering their facilities. This solution combines Mobotix M16/S16 cameras with the functionality of a new plug-in from Panasonic I-Pro's Video Insight vid-

eo management systems (VMS) to automatically detect when an individual's body temperature exceeds a pre-set threshold and provides an alert to the appropriate personnel.

Panasonic I-Pro's Video Insight VMS plug-in and Mobotix thermal cameras combined functionality trigger an alarm

when a user-defined, pre-set temperature threshold is detected. The solution can define multiple areas of interest to set up temperature readings and can be set up in either Celsius or Fahrenheit. The system also allows you to edit the temperature threshold and review the detailed thermal readings at any time.

YOUR SECURITY BEGINS WITH YOUR PERIMETER



DETER, DETECT & DELAY INTRUDERS.
BEING FOREWARNED IS BEING FOREARMED!

ECONOMICAL. RELIABLE. EFFECTIVE.



- They provide a higher level of detection capability to detect an intrusion attempt and set off the alarm which is then transmitted to the security personnel, police or the CMS.
- They are installed easily on existing walls or fences, or as a free standing secure energy perimeter fence, forming your first line of defence.
- The wires of a free standing secure energy fence serve as a barrier, alleviating the need to erect another conventional fence or wall, reducing cost.
- Safe, complies with International IEC Standard 60335-2-76
- Fences can be remote controlled and integrated with other systems such as, Perimeter Lighting, CCTV, and Alarm Systems.
- They reduce cost of security personnel.
- They last for years and have low maintenance cost.

APPLICATIONS:

BUNGALOWS, FARM HOUSES CAMPUSES,
PRISONS, GOVERNMENT & MILITARY SITES,
CRITICAL INFRASTRUCTURE FACILITIES...



Email us today
for more information:
info@kawach.com

IDS launches uEye XLE camera family with USB3 interface



Particularly affordable, particularly compact and particularly powerful when the essentials matter: the new uEye XLE camera family from IDS has been specially developed for high-volume and price-sensitive projects.

The industrial cameras can be easily integrated into any machine vision system. Customers can choose between single-board cameras with or without C-/CS-mount or S-mount as well as variants with coated plastic housing.

The first models will be equipped with the

light-sensitive 5 MP sensor ON Semiconductor AR0521. There are almost no limits to the possible applications of the new camera family. The cameras also show their strengths in classic industrial applications such as surface inspection. The models fit into the smallest of spaces, for example as embedded vision solutions. The price-optimised design makes the cameras particularly interesting for applications where costs are the main concern. Therefore, the company also offers a large number of inexpensive lens-

es for the cameras.

All uEye XLE models feature a USB3 interface (SuperSpeed USB, 5 Gpbs) and are 100 percent GenICam-compliant. The cameras can be used with any software that supports the USB3 Vision Standard. For an optimal user experience, the company recommends the use of IDS peak. The free SDK includes all necessary components from source code samples to transport layer, so that customers can start developing their own applications right away.

IDEMIA provides frictionless biometric access control for Václav Havel Airport Prague staff with MorphoWave Compact



Václav Havel Airport Prague (PRG), with its prime location in the Centre of Europe, is the largest and most important international airport in the Czech Republic. Prague Airport handled 17.8 million passengers in 2019 and received the Airport Service Quality Award 2019 awarded by ACI for the second time in a row. At Prague Airport, there are different types of areas restricted to authorised personnel.

These are governed by an access control system fitted with approximately 1,000 readers and over 1,500 secured points (doors, locks, etc.). Mifare Desfire cards are predominantly in use for the time being. Among these, Security Restricted Areas (SRAs) are the highest security areas, with 60 access points of high importance.

Due to the critical nature of those areas, Prague Airport needed a very high level of security, and decided to implement a biometric solution, as the card itself (including with the use of a PIN code), would not be deemed as secure enough. The biometric system had to be able to cope with over 20,000 individuals,

with the capability to increase to up to 30,000 users in the future.

Prague Airport decided to keep the existing access cards but to add a biometric verification level for the SRAs. This means that the biometric solution would have to be used in combination with the existing cards through a two-step process. In order to avoid any physical contact with the devices, for user convenience as well as for hygienic considerations, it was decided to deploy a contactless biometric technology.

Prague Airport tested two technologies capable of connecting to its access control system, among which IDEMIA's MorphoWave Compact contactless fingerprint terminal. After a thorough testing period, the choice was to go for IDEMIA's technology for a number of reasons including: great user experience with an easy and quick hand gesture, as well as a strict GDPR compliance with users' biometric information stored only in their cards.

Prague Airport deployed more than 60 MorphoWave Compact in its SRAs. The readers

were installed at existing control points and are fully integrated into the airport access control system. More than 20,000 users now have their biometric data in their access cards and the system is fully operational.

IDEMIA's seamless biometric technology helps address health and safety issues. Employees appreciate the user experience provided by the solution deployed: it is easy to tap the access card onto the embedded card reader situated at the top of the reader and then to just wave the hand in a quick simple movement to get 4 fingerprints verified in less than 1 second, without the need to touch any part of the device.

Airports is a key vertical among the many different ones served by IDEMIA. The biometric devices are used by 35+ of them throughout the world for staff access control, as here in Prague. The company's biometric solutions are also used for border control and passenger flow facilitation, in more than 30 different airports.



approaches. For such a modern wood factory, safety is of paramount concern. Advanced video surveillance systems need to be introduced in the internal and external areas of the factory.

Due to the extremely high risk of fire in a wood factory, the customer has high demands for a smart system to keep sufficient video backup as evidence. Specifically, the system needs to be capable of storing up to 30 days of videos, with copies stored on a separate network at the same time so that the videos can be safely saved under different network conditions.

A total of 400 IP cameras from Dahua Technology were installed inside of the factory for general monitoring, including DH-IPC-HFW1230SP, DH-IPC-HDPW-1231FP-AS and DH-IPC-HFW2231TP-ZS. In this chain factory, DH-IPC-HFW1230SP was used to monitor machine operation, and DH-IPC-HDPW-1231FP-AS was used to monitor corridors. These two types of cost-effective Mini-Bullet Network Camera feature 2MP resolution with a motorised 2.8mm/3.6mm fixed lens.

With IR illumination, detailed images can be captured under low light conditions or total darkness. The cameras' Smart IR technology ad-

justs the intensity of the camera's infrared LEDs to compensate for the distance of an object. Smart IR technology prevents IR LEDs from whitening out images as they come closer to the camera.

In order to ensure the safety of staff and vehicles in the factory vicinity, DH-IPC-HFW2231TP-ZS was installed outside the factory to monitor large and open scenes. This IR Megapixel Vari-focal Camera features 2MP resolution with a 2.7mm ~ 13.5mm vari-focal lens, meeting monitoring needs of different distances.

For challenging ultra-low light environments, IPC-HFW2231TP-ZS powered by Dahua's Starlight Technology offers excellent light sensitivity, capturing color details in low light conditions down to 0.006lux. The camera uses a set of optical features to balance light throughout the scene, resulting in clear images in dark environments.

In addition, these cameras allow $\pm 25\%$ input voltage tolerance, suitable for the most unstable conditions in outdoor applications. Its 2KV lightning rating provides effective protection against lightning for both the camera and its structure. Certified and subjected to rigorous dust and immersion

tests (IP67), these cameras are ideal choices for installation even in the most unforgiving environments.

In order to help the customer improve the security of video storage, three types of Dahua 4K H.265 Network Video Recorders – adopting powerful processors with up to 4K resolution for preview and playback – are used in the factory to store 10-day videos, which can provide critical details for identification.

On the other hand, a 48-HDD Enterprise Video Storage is used to separately store 30-day videos at the headquarters in case the factory area videos are damaged. It supports 512 channels of IP camera inputs and 1024Mbps incoming/recording bandwidth, offering an unparalleled storage performance. Moreover, DHI-DSS4004 was selected as the central server, through which all videos are integrated in one system for a unified operation and management in the headquarters' control room.

The vast factory vicinity is now equipped with Dahua video surveillance system, enabling all security checkpoints to monitor the factory in real time. At the same time, the massive video storage and backup allows the administrator to review emergency situations if necessary.

Dahua Technology's video surveillance solution employed at Cedr Factory to improve security level

With a history of over 20 years, the Cedr factory is one of the leading manufacturers of wood-

en doors, kitchen cabinets and other wood products in Russia. Today, it has a few of its

own modern and automated plants with a wide range of products and innovative production

Dallmeier deploys Panomera multifocal-sensor system to secure Gazprom Arena

Since its completion in 2017, the Gazprom Arena has served as the home ground stadium for the Russian football club Zenit St. Petersburg. And as one of the host stadiums for the 2018 FIFA World Cup and the 2021 Euro Football Championship, the Gazprom Arena must also satisfy the strict security regulations of FIFA, UEFA and ESS-

MA. When selecting the video security system, the managers responsible at Zenit therefore opted for a solution from the German manufacturer Dallmeier.

With its patented Panomera multifocal-sensor system, Dallmeier guarantees the security of many stadiums all over the world. The objective was providing cover-

age with video security technology for the entire area surrounding the stadium, the entrance gate approaches, the rooms below grand stands, and the grandstands themselves in one of the largest video security projects ever undertaken in a football stadium.

Under enormous time pressure, a high-performance system had to



be implemented in the stadium with a capacity of 60,000 fans and yet had to remain adaptable and flexible in response to changing customer wishes as the project progressed. One requirement which from time to time presented the greatest challenge was capturing all areas of all the grandstands all of the time, so that unequivocal identification of offenders could be assured in all circumstances.

In order to achieve this, the Russian Interior Ministry stipulated two key requirements for the video security system: Firstly, it must capture the entire grand stand area with a “minimum resolution density” of 250 pixels per metre (px/m). This also corresponds to the performance criterion defined in the globally valid standard DIN EN 62676-4 for video security systems for purposes of enabling identification of an unknown person.

And secondly, the image frequency must not fall below a frame rate of 25 frames per second (fps). Because it is typically only the combination of the specified minimum resolution density and a fluid representation of events that can ensure incontestable evidence that is usable in a court of law.

In order to meet these stringent requirements, the security managers invited a number of vendors to present their solutions in advance at Zenit’s former home ground - the Petrovsky Stadium - to enable them to choose the right solution for the Gazprom Arena. A Dallmeier video security system has already been operating in the Petrovsky Stadium since 2012, and after a thorough evaluation of all the solutions, the operators decided to install a stadium solution from Dallmeier in the Gazprom Arena as well.

Because compared with conventional camera technologies such as megapixel or PTZ cameras for example, the patented Panomera multifocal-sensor system from Dallmeier can guarantee coverage of even the largest expanses with the stipulated minimum resolution density and frame rate. And Panomera systems continuously capture everything that is happening in full resolution and allow high-resolution zooms - both live and in the recording and by several operators at the same time.

This enables stadium operators to track and reconstruct relevant occurrences in detail both live and after the fact. Besides the technical superiority of the Panomera technology, another decisive advantage of the Dallmeier stadium solution was the innovative 3D planning approach, with which a digital reproduction of the Gazprom Arena was created.

This makes it very easy to fulfil the requirement according to which at least 250 px/m must be assured literally “in every last corner”: colour coding in the 3D simulation makes it possible to see exactly where the value has been reached and where a correction should be made, perhaps by setting up in another position or using a different camera model.

A further major advantage of this planning approach is the extreme efficiency of the solution: For example, Zenit St. Petersburg is able to provide security on the terraces throughout the Gazprom Arena with way less than 100 Panomera camera systems, covering all areas with at least 250 px/m and 25 fps. An alternative solution would have required a substantial four-figure number of conventional single-sensor cameras.

Apart from enormously high infrastructure costs (masts, cables, etc.) this would also have generated a practically unmanageable deluge of images for the video system operators. Another benefit of Dallmeier’s 3D planning programme is the automatic generation of “CamCards” - exact configuration documents for every single camera. Armed with this information, installers on site know exactly which camera must be mounted where, how high and at what angle.

The big advantage besides the immense amount of time saved consists in the planning reliability: It can be predicted with great accuracy how much labour the installation of the total solution entails, because this approach minimises uncertainty factors.

Thanks to Dallmeier’s unwavering assistance throughout the project, testing by the state technical personnel in Russia was also successful in the subsequent project phases, with the result that the stadium operators were able to begin operating the video security system after final project commissioning in good time for the 2018 FIFA World Cup.

Recently, over 1,000 single-sensor cameras have been installed in the Gazprom Arena in addition to the Panomera systems - these safeguard the remaining areas of the stadium. Due to the large number of cameras, the total storage capacity for the video security system amounts to more than six petabytes (equivalent to about 6,000 TB).

High-performance recording appliances from Dallmeier are used to process this information.

NOW CONTROL YOUR SECURITY FROM WHEREVER YOU ARE

Addressable Intrusion Alarms with Easy BUS (Single Cable) Wiring

JABLOTRON
CREATING ALARMS

JA-100+



- Emergency alarm alerts to the user & authorities
- 24/7 burglary, fire, flood, & CO protection
- Notifications with 3 layers of backup via integrated GSM/GPRS/LAN
- SMS & voice reports from the system to up to 15 users
- Panic & duress modes
- Integrate with CCTV cameras
- Programmable outputs for lights & other automation
- 20 independent calendars to schedule automatic events
- Remote control the system via web/mobile app/call/sms
- Detailed reports pinpointing the individual device
- Door lock control with RFID card
- User friendly keypads with control segments

APPLICATIONS:
HOMES, OFFICES,
BANKS, FACTORIES,
BOARD ROOMS,
LABS, R&D CENTRES,
SHOPS...



KAWACH
PROTECTION SYSTEMS
Technology on Guard

Email us today
for more information:
info@kawach.com

Mayflex installs Hikvision thermal elevated temperature screening for COVID-19



Mayflex, the distributor of Converged IP Solutions, has installed Thermal Elevated Temperature Screening Solutions from Hikvision to improve the health and safety of their employees and visitors during the COVID-19 pandemic.

The system works by automatically checking the forehead skin temperature in real time as employees pass by, maintaining a 2m gap in accordance with UK Government social distancing advice. If a person is over a normal temperature threshold, an audible and visual alarm is given and they will be asked to verify their body tem-

perature using a medical thermometer. If in the future face masks become mandatory, the system can also verify if a visitor or employee is wearing a mask.

James Vian, Technical and Training Manager said “The temperature screening solution has been installed in our main reception as well as the warehouse entrances at both the Head Office and our Environ House warehouse. The system includes the Hikvision Thermographic Bullet and Turret Cameras with the addition of the Hikvision Blackbody Calibrator that increases the accuracy of the read-

ings from $\pm 0.5^{\circ}\text{C}$ to $\pm 0.3^{\circ}\text{C}$.”

Andy Cooper, Supply Chain Director at Mayflex said “It’s a non-contact means of quickly and consistently measuring the skin temperature of a person’s forehead, whilst maintaining social distancing in line with current Government guidelines. In doing so, we can reduce the likelihood of someone with an elevated temperature coming into contact with other building occupants. This also reduces the possibility of losing an entire shift for 14 days, ensuring that we can deliver on our customers’ needs even in these challenging times.”

UVeye secures Corpus Christi Naval Air Station from intruders with the help of Helios



Security is the biggest concern for military facilities. Modern military facilities face a wide variety of risks, from cyber attacks to data theft to terrorist attacks. The Corpus Christi Naval Air Station in Corpus Christi, Texas for example, dealt with three separate attempted intrusions in a year and a half. In one incident, a man driving a stolen SUV entered the base and attempted to exit through a separate entrance, but crashed his car and was then shot by security personnel.

In another incident, just eight months later, the base went on lockdown again before an armed man was taken into custody. Then, in the third incident, seven months later, there was a third attempt to break into the base, this time by a man with known ties to terrorist groups.

The man fired at the security guard at an entrance gate and struck her bulletproof vest before she raised the barrier to prevent the attacker from getting inside the base. The base's security did a good job of preventing any serious damage during these attacks, but with the frequency of these incidents, more modern security may be needed to ensure that the next attack doesn't end in catastrophe.

Modern times call for modern security solutions, and Helios by UVeye is the perfect option to protect sensitive facilities. Helios is safer, improves security, makes security officers' jobs easier, works in extreme conditions, and can even identify vehicle passengers with high body temperatures to help prevent the spread of COVID-19. Helios UVIS uses machine learning and artificial in-

telligence to inspect the undercarriage of any vehicle that drives over its multiple high-resolution cameras.

It alerts the user on any irregularities or foreign objects hidden in the undercarriage. Inspecting the undercarriages of vehicles is very difficult for security personnel. Before Helios, there was never an effective solution for under-vehicle inspection, and even if security officers inspect the undercarriage, they may not know what to look for. They may not recognise a threat and allow a vehicle with a weapon, bomb, or other illicit or dangerous item to enter the facility.

Security officers put themselves at great risk by manually inspecting vehicles, as evidenced by the attempted terrorist attack in Corpus Christi in May. With Helios, the security guard can inspect the vehicle from a safe distance by simply looking at the high-resolution images and checking for anything suspicious or unusual in the undercarriage.

No matter how well trained a security officer is, all humans make mistakes. However, with Helios, the chances of human error are greatly reduced. The system produces high-quality images of the undercarriages and alerts the security officer of any irregularities. It will even detect issues in the undercarriage of a vehicle passing through the system for the first time. Detecting potential threats is easy with UVIS.

The high-resolution images allow a security officer to see the entire undercarriage very clearly to determine whether there is anything suspicious. Instead of manually inspecting

the vehicle and putting themselves at risk, security officers can inspect the vehicle from a more relaxed and safer environment and zoom in on the smallest details.

Plus, Helios provides a side-by-side view of previous scans from the same vehicle if it has gone through the system before to make it easier for the officer to notice any differences. Helios can withstand up to 20 tons per axle, meaning that it will survive being run over by even massive vehicles. It is fully operational at temperatures between -20 and 40 degrees Celsius and is IP 68/54 compliant, meaning it offers full protection against sand, dust, or rain.

UVeye's thermal sensor can also detect the body temperatures of vehicle passengers, which can identify visitors with potential fevers, improving the safety of everyone on the base. UVeye fully supports 3rd party integration and provides a multiple layer of security for any facility.

Integrating to the centralised server provides the capability of connecting multiple systems or lanes across different sites while enabling central management and control via one screen. The centralised management system enables the client to access the different systems deployed and manage the different users and historical data.

The undercarriage of a vehicle is one of the most important parts of the vehicle to inspect, but also one of the most difficult areas to inspect. Helios is the perfect solution to prevent any weapons, bombs, drugs, or other illegal and dangerous items from entering military facilities.

It can make everyone

in the facility safer, including security officers, who will no longer need to manually inspect vehicles and put them-

selves in harm's way. Integrating with other security and access control systems can provide a multi layer approach

to tighten the entry and exit points to any sensitive site while keeping personnel and data safe.

Eagle Eye Networks completes citywide surveillance program of installing cameras in Mexico city



Eagle Eye Networks, the provider of cloud video surveillance, announced one of the fastest completions of a large scale, fully integrated citywide surveillance program, installing 13,720 cameras in 4 months. This project has been a large success for Mexico City C5, contributing to Mexico City's larger 'Citizen Safety' mobile application. This mobile application facilitates content sharing for more effective neighbourhood watch and a panic SOS button. "Effective citywide surveillance is more than installing cameras in a few key locations, it's about creating a platform that meets the unique needs of each municipality."

"In partnership with Eagle Eye Networks we leveraged the Eagle Eye Video API and SDK to customise a unique web application that is designed to integrate fixed, mobile body worn, and vehicle cameras into one interface, providing an unprecedented level of insight and awareness into our cities operations," said Jaime Abad Valdenebro, CEO, Omnicloud.mx.

4G connectivity with Eagle Eye Networks'

bandwidth optimisation was utilised in order to facilitate this quick deployment, installing approximately 250 cameras per day at its peak. The cameras are all operational, remotely monitored, and providing safety and security to citizens today.

This fast-paced install occurred amidst the global supply chain challenges caused by COVID-19, however, Eagle Eye Networks' strong partnership with both the Reseller, Omnicloud.mx, and suppliers provided alternatives and solutions to keep the project on schedule.

Eagle Eye Networks solution was chosen because the Eagle Eye Cloud Video API Platform provides an open solution that allows integration of new technologies (AI, advanced analytics, search, license plate recognition), new suppliers, and new cameras at any time. Future and cybersecurity proofing the city's investment and eliminating the headaches associated with managing large premise based data centres was crucial in their decision.

"When deploying a city-wide surveillance

project, scalability, retention, and cellular transmission must be considered. Eagle Eye's cloud video retention and massive on demand scalability make it ideal for large scale deployments. To operate your own large data centre system for video recording is expensive and challenging."

"With Eagle Eye's subscription service we provide a more robust and lower cost answer for large scale deployments. Furthermore, our open platform provides a future proof solution, integrating AI, video analytics, and advanced search at the click of a mouse," said Dean Drako, CEO of Eagle Eye Networks.

"More than half of the world's population resides in cities, creating an increased demand for smart, accurate insights to help streamline everyday operations including public safety, traffic flow management, infrastructure and transportation. Enormous amounts of data collection, aggregation, and storage are necessary to drive the deep analysis that is required to produce these smart insights."

How COVID-19 may be affecting fire safety procedures for SMEs



While the pandemic has altered many aspects of 'routine operations', businesses must be careful that any changes have not had a detrimental impact on fire safety. From office-based premises, through to independent retailers and service providers, it continues to be crucially important to keep staff, visitors and assets safe. Dakota Murphey explores some of the ways that COVID-19 has affected fire safety procedures at smaller businesses, many of who may not have dedicated safety officials, and what they need to consider upon reassessment.

The first thing to note regarding fire safety at small businesses is that you must not assume that due to the change in circumstances as a result of the COVID-19 pandemic that this excuses you from your obligations. Support continues to be available, with fire safety professionals being considered 'key' or 'critical' workers.

"Due to these unprecedented circumstances," says Tony Clark, Managing Director of EFL Fire and Security, "we have adopted measures to ensure we can still provide essential services in line with government guidelines to new and existing customers."

It is essential that you continue with your fire safety requirements as normal, with all testing and maintenance regarding fire safety equipment must continue. If your business has changed anything regarding fire safety services, such as putting

off inspections of fire extinguishers or cancelling maintenance of fire alarm systems, citing COVID-19 as your reason for doing so, this needs to be changed.

It might seem like if you have closed up your premises due to the coronavirus pandemic, that it minimises the fire risk at your property. However, this is not the case, and even empty premises have issues that small businesses need to consider. The first thing to note is that businesses need to ensure that their empty premises have clear entrances and exits and that excessive amounts of stock or supplies are not being stored in an unsafe manner. Additionally, it is up to companies to make sure that they are not leaving electrical devices turned on or even plugged in.

It could be a great idea to install a connected fire alarm system that automatically alerts the fire services, or even one that provides real-time monitoring updates on an app or web portal that can be accessed remotely. And, it is also worth noting that empty buildings are at a potentially greater risk of arson attacks, so measures should be put in place to minimise this possibility. This could include the installation of CCTV systems that can be remotely monitored, as well as acting as a deterrent – especially useful if you don't have access to guarding services to provide protection.

For those small businesses that have been able to remain operational and not had to close, buildings may

have been altered to adapt to the changing health and safety government guidelines, such as social distancing measures. Examples may include the wedging open of fire doors in order to remove the need to open doors by touch, or the sealing off of doors that were previously part of the fastest route out of the building. In such cases, businesses need to ensure that they reassess their fire and emergency evacuation procedures, to ensure potential issues are spotted before it is too late. For example, if certain doors that were previously a part of the fastest fire exit are now closed, this needs to be made clear, and a new fast fire exit route should be created to ensure that no-one is put at risk. In any case, businesses need to be aware that practical changes that have been made as a result of the pandemic can have an effect on fire safety. Perhaps the building's occupants have changed, with the previous fire safety officer working from home indefinitely, and so a new employee needs training, for instance.

Undoubtedly one of the most important things to say here is that small businesses clearly need to take this time to reassess fire safety requirements. It is up to all SMEs – whether they believe they have been changed or not – to carry out fire risk assessments that take into account the range of new circumstances. When anything changes at a business, fire safety precautions and procedures have the potential to be affected.

SMEs still have a duty of care to take everyone involved protected against the risk of fire – so all small businesses should carry out new fire risk assessments as a priority.

For example, have you considered that if

your business remains open while others close you may see a spike in demand? Greater footfall at the business premises can necessitate re-thinking scenarios and establishing new emergency plans. Whether a small busi-

ness has closed its doors temporarily or it has had to modify its behaviour to stay in line with government regulations, it will need to reassess whether its previous fire safety procedures remain relevant to the circumstances.

Odisha sets up India's first 'Fire Park' to spread awareness on fire safety measures



Odisha Chief Minister Naveen Patnaik recently inaugurated a first-of-its-kind 'Fire Park' to educate citizens on the safety measures and how to remain alert during emergencies. During the virtual inauguration, the Chief Minister also launched a dynamic online portal 'Agnishama Seva' of the Odisha Fire Service to enable smooth access to the citizens to the services provided by the department.

The park has been set up inside the premises of the Odisha Fire and Disaster Academy in the state's capital. Each section of the park would conduct demonstrations on safety measures to be taken during a fire mis-

hap before the firefighters arrive, operating procedure during rescue and disaster operations, exhibition halls showcasing equipment, screening of films and distribution of leaflets on fire safety. As per reports, the park would be open to the public every Saturday from 3.30 pm to 5.30 pm.

CM Patnaik said that the Fire Park would play a key role in creating and improving awareness on basic fire safety measures among the people, particularly the students. "It is no doubt an effort in the right direction to create a safety compliant citizenry," he said. He further informed that as many as 16 fire-related

services were now available to the citizens on online mode and the fire service department has been instructed to give priority to the feedback mechanism under the 'Mo Sarkar' to ensure hassle-free and time-bound services to the public.

Praising the role of Odisha Fire Service, Patnaik said, it has earned a glorious distinction for itself at the national level for its outstanding services on rescue and disaster response. "I expect the Odisha Fire Service to continue to adopt technological innovations and bring about transformational changes in the public delivery system," he said.

Fire Blankets vs. Fire Extinguishers: Pros, Cons and Considerations

Fire extinguishers are much better known than fire blankets, but they both have a place in your fire safety plan. Both fire blankets and fire extinguishers can extinguish small fires—so, how do they differ and what should you know about each? Let's compare how they perform in terms of ease of use, reusability, and appropriate use cases.

Fire extinguishers are a go-to piece of fire safety

equipment for a reason. Fire extinguishers are perhaps the best-known method of fighting small fires in their early stages. With options ranging from the versatile ABC fire extinguisher, which can tackle a range of common fires, to CO2 extinguishers, which do not leave residue and work on fires involving flammable liquids, gases, and electrical equipment, there's a fire extinguisher for practically every application.

Unfortunately, many homes don't even have a fire extinguisher, though across India, there were 6,364 fires in residential properties in 2019, which resulted in 6,329 deaths, 321 injuries. Gujarat reported the third highest number of incidences of fire in residential property. There were 658 incidents reported in 2019, as per the NCRB.

In contrast, extinguishers are common at



work and in public spaces since they're required by fire codes in commercial and high rise buildings. Fire extinguishers are also a great idea for vehicles and, in some cases—such as commercial trucks, tractors, and buses—they're required.

The pros of fire extinguishers

They are very effective when used properly. Fire extinguishers are relatively easy to use, and a study by the National Association of Fire Equipment Dealers (NAFED) showed they were “effective in extinguishing fires 95 percent of the time.” This, of course, applies when a fire is in a relatively early, containable stage. But even when a fire extinguisher could not completely put out the fire, the study found that it often limited damage and provided some degree of control over the situation until firefighters could arrive.

A fire extinguisher is an active fire protection device used to extinguish or control small fires, often in emergency situations. It is not intended for use on an out-of-control fire, such as one which has reached the ceiling, endangers the user (i.e., no escape route, smoke, explosion hazard, etc.), or otherwise requires the expertise of a fire brigade. Typically, a fire extinguisher consists of a hand-held cylindrical pressure vessel containing an agent that can be discharged to extinguish a fire. Fire extinguishers manufactured with non-cylindrical pressure vessels also exist but are less common.

A wide range of sizes are available for different structures and threats. When seconds count, fire extinguishers can either stop a fire or give you time to retreat safely.

Fire extinguishers: cons and considerations

A fire extinguisher can be used by most people,

but employing one safely and effectively does call for a bit of training. Note that Occupational Safety and Health Administration (OSHA) regulations require formal training for facilities under their jurisdiction.

The right way to use a fire extinguisher is often described by the acronym P.A.S.S.:

- P – Pull the Pin.
- A – Aim the Nozzle at the Base of the Fire.
- S – Squeeze the Handles Together.
- S – Sweep Back and Forth.

While doing this, you should take care to begin spraying while standing at a safe distance, even if the spray is not quite reaching the base of the fire. You can move closer if the fire is dying out as you advance.

The larger a fire extinguisher is, the longer it will be able to fight a fire—and the heavier it will be. People who lack upper body strength may struggle to pick up a larger fire extinguisher like a 9kg model or take it off a wall bracket safely.

Cleanup after discharge can be significant. If you've got a choice between a fire and a mess, you'll choose the mess every time. But the cleaning required after using a fire extinguisher is something to consider.

Cleanup needs vary by type, and common ABC fire extinguishers, unfortunately, leave a residue that is one of the more difficult discharges to handle. You may need professional help cleaning up after a discharge, especially if the residue has gotten into ductwork—the dry chemical is toxic, and you must avoid getting it into any waterways.

Fire extinguishers must be replaced or recharged after use. Once a fire extinguisher is used,

it must be replaced or recharged, even if it was not completely discharged. Commercial grade fire extinguishers can often be serviced and recharged after use, but many inexpensive extinguishers, like those sold in retail stores, are designed for one use only and must be replaced.

Fire blankets: a great option for containing fires and protecting people from flames—but not for fighting a fire that's already spreading.

Fire blankets work on a simple principle: smother the fire and deprive it of oxygen. To do this effectively, they have to be nonflammable themselves and provide as much of a barrier for heat and oxygen as possible. A modern commercial fire blanket will contain a fiberglass layer to achieve this purpose and the blanket will be designed to keep the fiberglass from coming in contact with skin.

A fire blanket should be mounted on a wall near (but not directly over) the area where it might be needed. For example, NFPA codes and standards stipulate that fire extinguishers be placed within 30 feet of cooking equipment, and it's proper to place a fire blanket within this range as well. A fire blanket typically comes with a protective cover that clearly identifies it and instructs the user on how to extract the blanket.

Pros of fire blankets

They can be used for personal protection. If a person's hair or clothing is on fire, wrapping them up in a fire blanket can be an important part of the “stop, drop, and roll” technique which is taught to minimize burns and injury. According to NFPA, blankets are especially useful if the person involved is not physically able to move rapidly due to age, medical condition, or physical limitations.

In a similar situation,

discharging a chemical fire extinguisher around a person's face could cause serious lung irritation, which could compound problems caused by smoke inhalation.

If a fire is out of control and you are surrounded by flames, a fire blanket may also help protect you and those you are helping if you must evacuate near areas exposed to flames.

Fire blankets contain fires in early stages, especially cooking fires. Cooking fires often start with a relatively small amount of grease in a container like a pan or pot. People are often reluctant to discharge a fire extinguisher because of the cleanup effort and expense involved, and Class K fire extinguishers

cerned about what will happen when they use a fire extinguisher and are confused by the different types of extinguishers available; they may not know exactly which one should be deployed. While these concerns can and should be addressed by training, using a fire blanket may be a more straightforward decision if a fire is small enough.

Cons and considerations of fire blankets

Fire extinguishers must be replaced or recharged after every use, whereas fire blankets should always be replaced after any use in a fire, even if they appear to be intact.

Older fire blankets may contain asbestos. The



are specifically required “for fires involving combustible cooking media (vegetable or animal oils and fats).” Sometimes, people pour or throw water onto a grease fire, with disastrous effects.

Putting a lid or pan over a fire in a container is the right idea—if done effectively, it will smother the fire. But it can be risky, because you may not have enough protection from the flames as you bring this cover down over them. Using a fire blanket lowers this risk. FIRST, turn off the source of heat, if possible. A quality fire blanket will have straps to help you wrap your hands up completely to protect them. You must quickly drape the fire blanket over the fire without throwing it or fanning the flames. Once it's on, leave it in place until you're certain the fire is out.

Fire blankets can be used by people who might have difficulty with extinguishers. If upper-body strength is an issue, fire blankets sized like the Wilson and Cousins 60” x 78” fire blankets are easily handled, as they typically weigh no more than two to three pounds.

Some people are con-

EPA instituted a partial ban on products containing asbestos in 1989 because of the serious risks of lung disease associated with the material. Asbestos was extremely common in fire blankets before that time. If you have any old fire blankets in your home or workplace that you suspect may contain asbestos, contact an asbestos removal specialist. Don't use them.

Fire blankets require you to get close to a fire. The correct technique to use a fire blanket requires you to place it right on top of a fire. If flames are high above the source or widespread, this may be difficult or impossible to do safely. Fire blankets can't be used safely on larger fires.

If a fire is becoming widespread, a fire blanket can't be deployed effectively. A typical fire blanket size is about five feet wide by six feet long. Sizes much larger than this can become unwieldy for one person to handle. If the fire is extensive, it's not a good idea to attempt to use a fire blanket, except as mentioned above for personal protection.

Fire blankets also require a bit of training.

Without proper training, it could be easy to panic while approaching a fire, causing you to drop or throw the blanket. This could make things worse by spreading flaming liquids or fanning the flames. If you fail to wrap your hands in the corners of the blanket, you could burn yourself. For all these reasons, deploying fire blankets should include some training in how and when they are used, just as you would for fire extinguishers.

Fire blankets and fire extinguishers each have a role in fire safety

You should not be

without a fire extinguisher—they are required for commercial spaces and highly recommended for all homes. They can prevent or minimize damage before the fire department can arrive and often put out fires in their earlier stages. But while fire extinguishers are more familiar to most of us, you should consider adding fire blankets to your fire protection strategy.

A fire blanket may help avoid a cleanup effort and they are particularly useful for small cooking fires that are caught early. This piece of equipment could also be a life-saver for yourself, a family member, or a coworker if someone catches on fire or needs to evacuate near flames. Fire blankets are an especially good idea for kitchens and areas where vessels and containers might catch fire. And they are also worth considering if you have elderly or infirm people in your home or place of business—who may not be able to drop and roll to smother a fire on their person.

The need to adopt AI in your surveillance operations



The explosion of artificial intelligence used to enhance business processes, propel innovative products, and further automation has touched essentially every industry to date. The security sector, notable for its maturity and complexity, is not exempt from the AI tidal wave.

In fact, quite the opposite, the security sector and more specifically the domain of video surveillance have seen an emergence of AI-powered solutions both hardware and software.

The widespread

eo flow, autonomously identifying and classifying the videos according to predefined rules. When AI video analytics are used effectively, they yield very promising benefits. A jump in video flow analysis from an average of 10% by humans to 100%, a reduction in operational costs, and an increase in safety and a decrease in risk.

The use of AI video analytics for surveillance sounds simple enough, however, there are several perceived factors inhibiting security organisations from adopting the technology.

The security industry is capital intensive, complex in its IT structure, and diverse in situational business needs. There-

expensive, time-consuming, and often unfeasible.

However, not all AI video analytic solutions need to be deployed on edge with smart cameras. Instead, video analytics can be deployed both directly on to the camera or have server-based integration maintaining and scaling to your existing camera network. AI video analytics can also analyse a range of videos from low to high resolution in a variety of formats: thermal, infrared, visible.

Complex IT structure

A single central command centre or in-house security network operates in a multi-manufacturer environment. This means cameras, video



adoption of IP cameras, cloud computing capacities, and smart sensors have paved the way for new AI products and solutions to function at scale.

One application of artificial intelligence for the video surveillance sector is the use of video analytic solutions to analyse video streams in order to extract pre-determined objects, behaviours, or situations. To give some examples, AI video analytics can be used to monitor perimeter crossing for border control, detect fevers or masks in airports or public spaces, arms detection in casinos, or be used to filter out alarms triggered by benign movements versus real intrusions.

This application of artificial intelligence leans on its specific branch, machine learning, which uses a complex series of AI models to analyse the content of the vid-

fore, resulting in a perception of high effort, time and costs required to successfully integrate AI into your video surveillance operation. However, these effort constraints can be debunked due to the flexibility of video analytic solutions.

Three areas that deter security organisations from adopting AI

Existing capital

A surveillance operation contains a network of cameras that film with a range of video qualities. AI video analytics often operate on smart cameras that have the appropriate video image quality for the capacity of content analysis. The costs involved in overhauling legacy camera systems, converting videos into higher quality, or waiting until the current camera network is ready to be replaced in order to integrate AI is

management systems, and technology partners can be provided by several manufacturers therefore increasing the complexity of successful IT workflows and integrations.

Theft or perimeter infringement can take place in a matter of minutes, therefore the transfer of information between solutions is required to function at top speed. To overcome this complexity, the successful integration of solutions in a multi-manufacturer environment is assured through industry enforced standards set by non-profit organisations. This allows for third-party solutions such as AI video analytics to be easily integrated into the bulk of software and hardware technologies.

Diversity in security needs

The objective of a

surveillance operation can vary greatly from one organisation to another. Retailers prioritise theft detection, while city governments may be concerned about arms detection or people counting.

The capacity for AI to function with high performance, meanwhile adapting to several organisation's security needs requires algorithms to be trained accordingly. To obtain high performance in a diverse security setting

is inherently built into how AI video analytic machine learning model's function. AI can be trained to adapt to different environments and uses progressive learning to increase performance overtime. A collaborative effort between security experts, data scientists and business strategists will ensure high performance and an appropriate application of AI to fit each organisation's specific needs.

While for some video surveillance organisa-

tions, the costs and time associated with successfully integrating AI into their network may seem daunting, there are ways to adapt new technology into an existing operation with minimal effort. The emerging presence of smart cameras and IoT products will only accelerate the adoption of AI moving forward. If your organisation is looking to enhance its operation with emerging technologies, now can be the time.

Here's why you need a surveillance-centric microSD card for your security camera



Security cameras are arguably the easiest way to improve the security of your homes and now it's easier than ever to get one for yourself. Most of the security cameras currently available in the market tend to come with a tiny microSD card slot which you will need to record video. After all, you can't be expected to stare at the live feed 24x7.

Most people assume that using any microSD card would work, and in a way, they would be right. But buying the right microSD can make a world of difference. A security camera would be near constantly writing on the card and as such, the card should be able to handle consistent recording with a high degree of endurance. Not only that, but there is a chance that the security cameras might be placed outdoors. So it should be able to handle the weather.

Here's a quick look at what you should look out for when buying a microSD card for your security camera.

As you would most probably already know, microSD cards are available in various capacities. These are pretty clearly

mentioned on SD cards themselves. It's difficult to gauge the ideal capacity that one should buy as that can vary wildly depending on use cases. If you plan to record high-quality video feeds and retain it for longer periods like weeks, then you'll have to buy higher capacity cards as the video will take up more storage space. Most cameras let you reduce the quality of the recorded video, but that might come back to haunt you later on as while examining the footage or zooming in, you may not be able to gather much info.

It should be noted that higher capacity cards will cost more. On the plus side, you'll be able to record days, weeks or even months of feed at any given time which can be handy when you need to rewind to a particular point. So you'll have to strike a balance based on your needs and budget.

The capacity of a microSD card is only one aspect. The speed class of the card determines write speeds, which in turn plays an important role in the quality of the recorded videos. Speed class is shown via a scale

that goes from 0 to 10, with Class 10 cards offering sustained performance of 10MB/s, which is good enough to record Full HD videos. There are some latest cards that use UHS1 (denoted by the symbol U1, which is the letter 'U' with a number in it). This is good enough for Full HD recording with superior frames and UHS3 (denoted by the symbol U3), which is optimized for higher resolution 4K recording. However for most practical purposes, a Class10/ UHS1 card is good enough in case of home surveillance.

Unlike most other devices, a security camera will be constantly writing over data on a loop 24 hours a day, 7 days a week. This affects the longevity of the card, which may lead to data loss in the future. Thankfully, select cards are specifically designed to be used in security cameras. These cards come with advanced features such as 96-layer 3D NAND tech with excellent performance, reliability and endurance. Plus, the WD Purple QD101 surveillance-grade microSD cards are sold with a limited warranty of three

years.

As mentioned earlier, there is a chance that the security camera may be placed outdoors where it (and the microSD card) will be subject to weather conditionals like rain, snow, moisture and more. As such, the camera and the microSD card need to be robust enough to handle that. So look for microSD cards that are water and temperature proof.

While microSD cards are harder than optical media, they can wear

out with use. All cards have a limited number of write cycles that they can endure. Of course, the most obvious thing to do would be to regularly replace the microSD card. Thus one should prefer buying a surveillance-grade card that has a specific endurance rating to help determine the best time for replacement.

These simple things should ensure that your security camera performs at peak levels. Thereby giving you the quality

and sense of security you should expect from such a camera. Not only that, some microSD cards support temperatures that range from -25°C to 85°C, with humidity resistance. On top of this, the cards come with Card Health Monitoring capability. When used with compatible cameras, it can notify you when the card's health is low. So you can take preemptive measures for card replacement.

Credits: Western Digital

Biometrics can't Replace Mobile Password Security



People used to be suspicious of the notion of having their facial recognition, fingerprints or other biometric data "on file" somewhere. Not anymore. Pretty much everyone uses their fingerprint to log into both their phone and a growing number of accounts, including not just personal phones and apps but also corporate devices and apps that contain confidential business information.

It's easy to understand why end users love biometrics. Instead of having to remember multiple passwords and manually type them in, all users have to do is touch a small scanner and voilà! What could be easier and more convenient? No wonder the market for biometric solutions is expected to reach nearly \$60 billion by 2025.

Biometrics hold a lot of promise as an authentication factor, particularly now that so many people are working remotely. However, when users lean on them too heavily, they tend to allow password security to fall by the wayside. This includes not only the time-honored practice of using a strong, unique password for every account but also adding additional layers of security, such as multi-factor authentication (2FA). This is fueled by a persistent myth that password security no longer matters because biometrics are set to "replace" passwords. Let's dispel this myth

right now.

Biometric Authenticators Depend on Passwords

The confusion is rooted in a fundamental misunderstanding of how biometric authentication works. Fingerprint, iris and facial recognition scanners don't replace passwords. Here's what goes on behind the scenes when an end user scans their fingerprint, iris or face:

- The biometric authenticator performs a "true-false" query to determine if the biometric it just scanned matches what it has on file.
- If there's a match, the biometric authenticator retrieves the user's password out of the device keychain and transmits it to the app.
- The app authenticates the user based on this password.

Biometric authentication solutions don't "replace" passwords. They just abstract away the complexity of manually typing them in. This means that if a user chooses a weak or common password, a cybercriminal can access the device or app simply by bypassing the biometric authenticator and using the password.

Biometrics Can Be Circumvented

Another misconception about biometric authentication is that it is somehow inherently

more secure than a password. If a user's mobile device is lost or stolen, the logic goes, cybercriminals will be unable to access it without the user's fingerprint or facial recognition.

Not so fast. When Samsung launched its Galaxy S10 smartphone in 2019, one of the device's major selling points was the phone's ultrasonic fingerprint sensor, which was ostensibly more secure than traditional optical readers.

A security researcher defeated the sensor using a wine glass, some software and an LCD resin printer. Some people may have taken comfort in the fact that this particular method required expensive, specialized software and a printer with an accuracy level of 10 microns. That comfort didn't last long: Last fall, a group of Chinese researchers demonstrated how to compromise the fingerprint lock on any smartphone, ultrasonic sensor or not, with \$140 worth of equipment and an app that analyzes a photograph of a fingerprint.

Biometrics Can't Be Changed

Perhaps the strongest argument against leaning too heavily on biometrics is that stolen passwords can be reset, but stolen fingerprints or other biometrics cannot. Further, if users properly secure them, passwords are quite difficult to steal. Biometrics are frighteningly easy to steal. Humans leave fingerprints everywhere, and our faces and even irises can be recorded, photographed or scanned from a distance without us ever knowing.

Cybercriminals don't even have to follow targets around to lift fingerprints or take photos. Databases containing biometric data can also be breached. In 2019, a database owned by a U.S. Customs and Border Patrol contractor was compromised, exposing photos of 184,000 travelers. At least some of the images ended up on the Dark Web. Three months later, the developers of a biometric lock system

used by the UK Metropolitan Police, along with banks and defense contractors worldwide, was found to be storing 23GB of fingerprints, facial recognition images, login credentials and other sensitive information on an unencrypted and unsecured database.

Reports of the Death of Passwords Have Been Greatly Exaggerated

Biometrics aren't inherently bad, but they're

not a replacement for passwords, not now and not for the foreseeable future. This doesn't mean organizations should ditch biometrics completely. Instead, they should be one part of a multi-layered approach to cybersecurity that includes, not replaces, comprehensive password security and robust identity and authentication management (IAM).

Top things to keep in mind when buying a CCTV Security System



After a break-in or vandalism at home or at work, you may be prompted to install a capable smart video CCTV system. Regardless of the reason, you are looking for one thing, and that is safety. With advancements in technology over the years, it is no longer safe to just rely on heavy doors and locked UPVC windows.

A complete CCTV system primarily comprises installation gear, camera and a storage device. Anyone looking to purchase a security video system tends to look for clear image quality within a particular price bracket. Here are some points one should keep an eye on while purchasing a CCTV security and monitoring system:

Know the purpose

It's important to understand what you are purchasing a CCTV security system for. For example, a camera with 2 megapixel (MP) HD picture quality works the best in domestic CCTV security systems within a range of 20 to 25 metres. A higher range (5 MP and 8 MP) is essential for a CCTV system installed outdoors.

Understand the camera

There are basically

two types of cameras: HD cameras are used for domestic purposes while IP (networking) cameras are mostly installed in factories and enterprise settings. These CCTV cameras are further categorised into Wired vs Wireless. Wired cameras are connected to the digital video recorder (DVR) through a cable, whereas, Wireless (or Wi-Fi) cameras are simply connected to consumers' smartphones via an app and information is stored within the device on an SD card. Cameras with inbuilt audio-recording and night vision are also popular options as they can capture high-quality video even in pitch-dark conditions.

Do not neglect 'storage'

Collecting video footage is the singular most crucial duty of a CCTV camera, it is also one of the most critical points of failure in many implementations. And reasons for that are many, but the most common ones are 1) inadequate storage capacity as a result your important old data can't be retrieved because it is overwritten by the new data and 2) lost connection between your camera and the backend because you didn't have storage on your camera. Both of these can be easily fixed.

First of all you must buy a surveillance-grade storage device that is high capacity, high performance and high endurance which is built ground-up for CCTV or smart videos. Secondly, most cameras come with slots for microSD cards and a few with a slot for SD cards. There are various capacity options available up to 512GB from WD Purple Surveillance microSD and SD cards that one can choose from.

Always buy from certified CCTV camera providers

Before ordering an installation, be sure to reach out to reputable and certified CCTV camera providers. Reputed system providers offer after-sales services in addition to the company warranty. This is either included with the cost of installing the CCTV system or is charged separately. Shifting cameras for a better angle, relocation, wiring problems, or even forgetting the app password are some of the likely scenarios when you might have to reach out to your CCTV camera provider and not to forget cleaning of your CCTV camera.

Budget should not compromise purpose

CCTV systems have considerably evolved over the years. Image quality is a key consideration while buying a smart video system, however, the greater the resolution the higher the storage capacity required for recording the video. Hence, selecting the right type of storage without compromising on budget is critical for the best performance and reliability of a security video system.

Partnering with **Kawach**
will always be a **BRIGHT** idea



INTRUSION ALARMS | ELECTRIC FENCING | GUARD TOUR SYSTEMS

Established in 1983, Kawach has been the most trusted source of highly dependable electronic protection systems for over three decades. Our systems protect the Hon'ble President of India and the National Museum among thousands of other government, corporate and individual end-user clients across India. We manufacture and offer systems from world-renowned brands such as Jablotron, Nemtek, and Tomst in India. On offer are state-of-the-art Addressable Wired and Wireless Intruder Alarms that can be controlled by the mobile application. Electric Fencing and Outdoor Beam Sensors that can be integrated with the central control panel and our mobile application. Our Guard Tour Systems are uniquely vandal-resistant, requiring no batteries or recharging for over 5 years! Incidents and observations can be logged by guards, reports generated and emailed to relevant people from our desktop or cloud-based software.

**We Train, Certify, Support and Promote
our System Integration Partners**



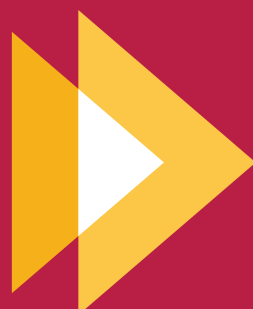
JA-100. The addressable 4 wire alarm system range

**PARTNER
INQUIRIES
WELCOME**

**CALL US
TODAY**

"Security House"
24-B Udyog Vihar - V, Gurgaon-122016, India
Tel: +91 - 124 - 4001111 | E-mail: info@kawach.com
Web: www.kawach.com

INDUSTRY EVENTS



ITALY
4-5 March, 2021
ICDEM
Rome, Italy

www.waset.org



NORWAY
9-10 March, 2021
Sectech Norway
Norges Varemesse
Lillestrom
Norway

www.securityworldmarket.com



NIGERIA
16-17 March, 2021
Fire Expo West Africa
Landmark Centre, Lagos
Nigeria

www.securexwestafrica.com



INDIA
24-26 March, 2021
6th Smart Cities India 2021 Expo
Pragati Maidan
New Delhi
India

www.smartcitiesindia.com



INDIA
22-24 April, 2021
FSIE 2021
Bombay Exhibition Centre,
Mumbai, India

www.fsie.in



NETHERLANDS
28-29 April, 2021
EFSN Fire Sprinkler
International, 2021
Amsterdam, Netherlands

www.firesprinklerinternational.com



SOUTH KOREA
12-14 May, 2021
Secon 2021
Korea International Exhibition
Centre - Kintex, Goyang-si
South Korea

www.seconexpo.com



INDIA
13-14 May, 2021
International Police Expo 2021
Pragati Maidan, New Delhi
India

www.internationalpoliceexpo.com



UK
18-20 May, 2021
Security & Counter Terror
Expo - SCTX 2021
EXCEL, London
UK

www.counterterrorexpocom



UK
18-20 May, 2021
IFSEC International 2021
EXCEL, London
UK

www.ifsec.events/international



INDIA
3-5 June, 2021
Security & Fire Expo -
South India
BIEC, Bengaluru
India

www.safeindiaexpo.com



MALAYSIA
15-17 June, 2021
IFSEC Southeast Asia 2021
Malaysia International Trade
and Exhibition Centre,
Kuala Lumpur, Malaysia

www.ifsec.events/sea/



USA
19-21 July, 2021
ISC WEST
Sands Expo Centre,
Las Vegas NV,
USA

www.iscwest.com



PHILIPPINES
21-23 July, 2021
IFSEC Philippines 2021
SMX Convention Center Manila,
Mall of Asia Complex,
Pasay City, Philippines

www.ifsec.events/philippines/



UK
7-9 September, 2021
The Fire Safety
NEC, Birmingham, UK

www.firesafetyevent.com



UK
7-9 September, 2021
The Security Event 2021
NEC, Birmingham, UK

www.thesecurityevent.co.uk



INDIA
16-18 September, 2021
Secutech India
Bombay Exhibition Center
Mumbai, India
<https://secutechindia.tw.messefrankfurt.com/mumbai/en.html>



SAUDI ARABIA
19-21, September, 2021
Intersec Saudi Arabia
Jeddah Center for Forums &
Events
Riyadh, Saudi Arabia
www.intersec-ksa.com



UK
28-29 September, 2021
UK Security Expo 2021
OLYMPIA London
United Kingdom

www.internationalsecurityexpo.com



FLORIDA
27-29 September, 2021
GSX 2021
Orlando, Florida

www.gsx.org/exhibit/



USA
5-7 October, 2021
NFAA Annual Conference and
North American Expo
Las Vegas, NV, USA

www.nfaa.org/annual-seminar/

HIKVISION[®]
See Far, Go Further

Secure Your Loved Ones at Home with Video Door Phone



DS-KIS202 (Video Door Phone)

- Self-adaptive IR supplement
- One-touch calling
- Pinhole camera with 720 x 576 @ 25 fps
- Unlock controlling

Indoor Station

- Hands-free video intercom communication
- Supports monitoring the door station and the external along camera
- Convenient installation and easy operation



Corporate Office:
PRAMA HIKVISION INDIA PVT. LTD.
Oberoi Commerz 2, International Business Park,
18th Floor, Near Oberoi Mall, Off W.E. Highway,
Goregaon (East), Mumbai - 400 063.
Tel: +91-22-4041 9900, 2846 9900
Web: www.hikvisionindia.com



Sales
+91-22-4041 9944, 2846 9944
sales@pramahikvision.com



RMA Support
+91-22-6822 9977, 3322 6070, 2846 9977, 0250 663 6677
rma@pramahikvision.com



Technical Support
+91-22-6822 9999, 3322 6060, 2846 9999
support@pramahikvision.com
Toll Free - 1800 222 699