Is Right to Access CCTV as per DPDP Act Allowed?

Proactive Security: The Future of Perimeter Defence

www.securityupdate.in

SECURITY update

THE SECURITY & FIRE SAFETY TECHNOLOGY MAGAZINE

For Security & Fire System Manufacturers, Distributors, Dealers, Integrators, Installers, IT Systems Integrators & VARs, Consultants & Enthusiasts.

Vol. 14 No. 07 | July 2024 | Price ₹ 150 | Pages 52

Bespoke Technologies to Safeguard the Perimeter

SECURITY SYSTEMS PROJECT HANDOVER

Revolutionising Door Security with Electric Strikes

Productivity Vs Security: How CIOs and CISOs Can See Eye to Eye

Protecting Against LIB Fires in Recycling Facilities

BEST SECURITY INDUSTRY PUBLICATION

www.securityupdate.in
SECURITY update
THE SECURITY & FIRE SAFETY TECHNOLOGY MAGAZINE

ON 28TH NOVEMBER 2018, SECURITY UPDATE WAS AWARDED AS THE 'BEST SECURITY INDUSTRY PUBLICATION' BY THE HON'BLE UNION MINISTER OF COMMERCE & INDUSTRY AND CIVIL AVIATION SH. SURESH PRABHU DURING THE 28TH IISSM GLOBAL CONCLAVE IN NEW DELHI.

SecuriteeUpdate | SECURITY-UPDATE | www.securityupdate.in

HIKVISION®
See Far, Go Further

ACCESS CONTROL PRODUCT PORTFOLIO

FACE RECOGNITION TERMINALS

FINGERPRINT AND RFID TERMINALS

MULTIDOOR CONTROLLER

BOOM BARRIERS

ENTRANCE CONTROL SYSTEMS

SOFTWARE OPTIONS

iVMS4200 AC	Hikcentral Access Control	Hik-Connect 6
Desktop (PC based)	Web Based (Server based)	Cloud Based Software

/HikvisionIndiaOfficial

Prama Hikvision India Private Limited

/HikvisionIndiaOfficial

Registered Office:
Office No.1-4, 2nd Floor, Siddhivinayak Arcade, Akurli Cross Road No.1,
Near Kandivali Station, Kandivali (E), Mumbai - 400 101, India.
CIN: U36100MH2009PTC190094

Corporate Office:
Oberoi Commerz II, International Business Park, 18th Floor, Near Oberoi Mall,
Off. W. E. Highway, Goregaon (East), Mumbai - 400063. India.
Board No.: +91-22-4041 9900, +91-22-6855 9900 | **Web:** www.hikvisionindia.com

Technical Support: +91-22-6822 9999, +91-22-3322 6060
Email: support@pramahikvision.com

Sales: +91-22-6822 9944, +91-22-4041 9944
Email: sales@pramahikvision.com

RMA Support: +91-22-6822 9977, +91-22-3322 6070,
+91-250-663 6677 | **Email:** rma@pramahikvision.com

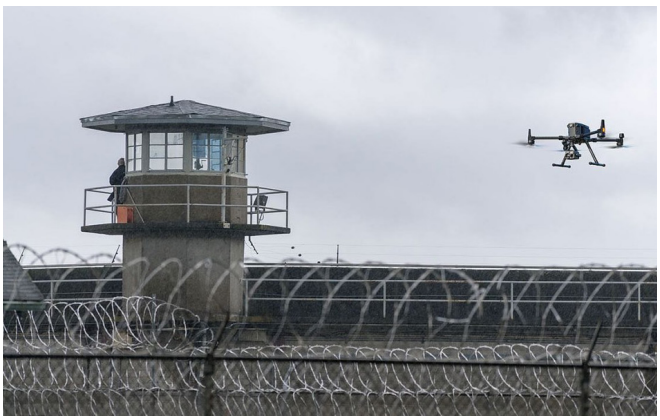
Toll No.: 18602100108

CONTENTS

COVER STORY 16

SECURITY SYSTEMS PROJECT HANDOVER ESSENTIALS

In today's business climate, the importance of implementing a comprehensive security system cannot be overstated. A properly designed and installed security system can provide the end user with a number of important advantages, including deterring crime, protecting assets, and providing peace of mind. Understand the significance of a security systems project handover and the essential requirements involved.



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. Editorial deadlines are three weeks before this date.

EDITOR'S NOTE

Dear Reader,

End users frequently delay upgrading technology, both hardware and software, even after it has reached end of life (EOL) and is no longer supported by the manufacturer, simply because it still functions. However, devices and spare parts from OEMs may no longer be available, leading system integrators to purchase untested components from the open market to keep systems operational. In many cases, EOL software also stops receiving updates or patches, increasing the system's vulnerability to sudden failure and cyberattacks. Criminals often exploit these weaknesses to access assets, resulting in losses, costly downtime, reputational damage, and expensive recovery efforts.

This can force end users into making hasty decisions to purchase new technology when the ageing system suddenly fails. Rushed acquisitions of security technology come with significant risks. Without thorough research, organisations may end up with inadequate or incompatible systems, leaving critical vulnerabilities exposed. Such hurried decisions often neglect the need for proper integration with existing infrastructure, leading to inefficiencies and protection gaps. Additionally, insufficient training on the new technology can result in user errors that compromise security. The absence of proper evaluation may also cause organisations to overlook better, more cost-effective solutions. In the long run, these missteps can lead to higher costs, reduced effectiveness, and preventable security breaches.

It's crucial to plan ahead before systems reach their end of life and fail. Allocating sufficient time for evaluating new technology that meets current requirements is essential, as this evaluation is a systematic process that demands careful consideration. Key questions to consider include: Does the technology offer out-of-the-box features that meet your needs, or can gaps be filled through configuration? Is the user interface intuitive and easy to understand? Can you trust that your assets, both tangible and intangible, are secure on the new platform? How well can the system adapt to your organisation's changing needs over the next five years? How seamlessly does it interface with other building management and IT systems? Assess the ecosystem: How strong and connected is the community of users and partners around the technology? Seek referrals and speak to current users. Consider the costs, both direct and indirect, of designing, configuring, and rolling out the new system, as well as ongoing licensing and support expenses. There may be additional factors to weigh depending on your specific situation, so it's better to proceed cautiously than to face higher costs and increased risks later on.

Ultimately, taking the time to thoroughly evaluate and plan for new technology not only ensures a smoother transition but also safeguards against unforeseen costs and vulnerabilities. An old English proverb defines the above aptly, "A Stitch In Time, Saves Nine" Till we meet next month, Stay Safe and Keep Others Safe.

G B Singh
Group Editor

gbsingh@1stasset.org @gbsingh9 @EditorGB

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

IFSEC BANGLADESH

12 - 14 SEPTEMBER 2024

Hall 4 (Naboratri) ICCB Dhaka, Bangladesh

informa markets

Power UP Your Security Brand Outreach

Why Exhibit at IFSEC Bangladesh 2024?

Brand Exposure: Showcase your brand and solutions to a diverse audience, raising your profile and enhancing brand visibility.

Networking: Connect with industry leaders, government officials, and potential partners to explore new business opportunities.

Product Launch Platform: Launch new products and innovations directly to your target market, gaining immediate feedback and generating leads.

Market Access: Gain direct access to a burgeoning market in Bangladesh and beyond, where the demand for security solutions is on the rise.

Educational Opportunities: Engage with industry experts and thought leaders through conferences, seminars, and workshops, gaining insights into emerging trends and technologies.

Exhibit Partners

EROSIS · DigiMark Solution · HARKON Electronics Corporation · Swaraj Secutech · synest · TEBillion · Voltaic Cable · XYZ Digital Pvt. Ltd.

In Association with

i-station wings of idea

Supporting Association

ASIS International · Bangladesh Computer Society · MitKat

Media Partners

Security Update · সিনিউজ · দৈনিক সংবাদ · Fire & Safety Security · Industrial Safety Review · Secure Asia · Safe Secure · Life Safety & Security · Security Link India · Security Update

CONTACTS:- SANJAY KHANDELWAL | M: +91 98117 64515 | E: sanjay.khandelwal@informa.com
MADHU SUDAN SAHA | M: +880 1713145595 | E: mssaha1978@gmail.com
FOR SPEAKER OPPORTUNITIES: ADEESH SHARMA | M: +91 98103 07335 | E: adeesh.sharma@informa.com
RAZIB RAFIQUL HOSSAIN | M: +880 1912-527273 | E: rafiqistation@gmail.com
FOR MARKETING & ALLIANCES: PANKAJ SHARMA | M: +91 99713 65776 | E: pankaj.sharma@informa.com
AVIJIT MONDAL | M: +880 17613 69456 | E: avijit.istation@gmail.com

www.ifsecbangladesh.com

Media Partner

Security Update

Proactive Security: The Future Of Perimeter Defence

Tom Galvin
The writer Tom Galvin is the CEO, Evolon

The days of being reactive are over. That's right, we as an industry, can no longer afford to be reactive. As threats evolve, the need for proactive security is critical. While traditional methods, including physical barriers and security personnel, are still necessary, the future of our approach is built on the backs of emerging technologies.

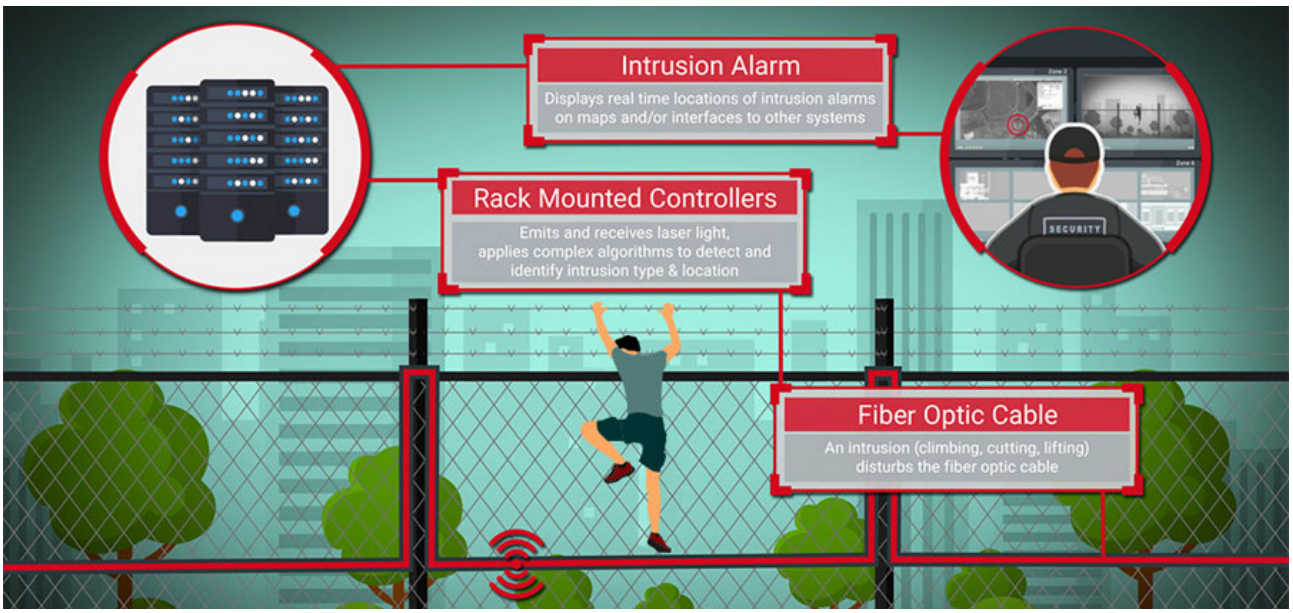
As an industry, we've operated reactively for decades, it has been common for security teams to address threats only after they occur. The growing risk landscape proves that this approach has significant limitations. Human oversight, delayed responses, and the inability to monitor large areas have exposed substantial vulnerabilities.

Times are changing though and it's largely due to the emergence of AI. AI is revolutionising the security landscape by making technology smarter. It enables real-time monitoring, advanced data analysis, and more accurate risk detection. This ensures a higher level of security and safety, minimising potential incidents' impact while enhancing overall safety.

AI's ability to process vast amounts of data quickly and accurately is, quite frankly, a game-changer. It can identify patterns and anomalies that can provide stakeholders with critical insights to respond in a more prepared manner.

By automating routine tasks and highlighting potential issues, AI also allows operators to focus on more complex and strategic aspects of security management, rather than responding to false alarms.

The future of security lies in AI. The Security Industry



> An initial investment in AI technology can result in substantial long-term savings (and ROI) by reducing the need for physical infrastructure and on-site security personnel.

Association (SIA) has recognised AI as one of the top security megatrends in 2024. However, the challenge is not adopting AI, it is about effectively using it to enhance security.

AI systems can easily integrate with existing infrastructures, providing a layered defence that combines traditional methods with more modern technology. For example, AI can enhance video surveillance by improving object detection, reducing false alarms, and enabling real-time, informed responses. This ensures that security measures are adaptive, scalable, and capable of addressing the evolving risk landscape.

One of AI's most significant benefits is its ability to provide proactive insights. AI can predict potential breaches by analysing behaviour patterns and detecting anomalies allowing security pioneers to do something before an event happens. This shift, from reactive to anticipatory measures, marks a significant advancement in asset protection and risk management.

AI systems can also continuously analyse data and distinguish between everyday events and real-world threats. It's AI's continuous learning capabilities that mean the systems can adapt and improve over time to become more accurate and efficient in threat detection and response.

Contrary to common belief, adopting AI technologies will not put a security department over budget. It may be surprising, but these solutions offer cost-effective and scalable alternatives to traditional security measures.

An initial investment in AI technology can result in substantial long-term savings (and ROI) by reducing the need for physical infrastructure and on-site security personnel.

AI systems are also inherently scalable and can be tailored to meet the specific needs of different environments. This ensures the system can evolve with emerging threats and technological advancements without requiring a complete system overhaul.

The ability to scale and customise AI solutions makes them a practical and efficient choice for enhancing perimeter defence. How's that for staying within budget?

Integrating AI into perimeter security is the future of proactive and intelligent security. As these technologies continue to evolve, we can expect even more refined solutions that are predictive, autonomous, and capable of directly addressing new and emerging threats.

We're experiencing an exhilarating transformation as AI becomes more trusted, precise, and advanced on multiple levels. This evolution is bigger than pilots and small, low-profile deployments.

For instance, France is preparing to deploy AI-powered video surveillance as it gears up to host the 2024 Olympics, part of its efforts to detect sudden crowd movements, abandoned objects, and suspicious activities. Think about the sheer scale of that project.

We're finally moving forward, and staying one step ahead must be our priority. But this shift requires a significant change in mindset. Are you ready to make the change? ■

Rising Woman Power: Rakhi Deepak to be the New National President (Elect) of FSAI in 2024-26

The Fire & Security Association of India (FSAI), a premier trade association of the fire safety and security domains has announced the appointment of Ms. Rakhi Deepak, as the association's new incoming president (elect) for the years 2024-2026. She will be the first woman president in the association's history! Congratulations Rakhi Deepak!

Founder & CEO of SagTaur, Rakhi is a distinguished entrepreneur and industry expert with a remarkable career in fire safety, building management systems, and security systems.

Over the years Ms. Rakhi has successfully served more than 300 esteemed clients across diverse sectors, including metro rails, airports, hotels, resorts, IT parks, warehouses, industries, and hospitals.

She has earned a post-graduate degree in physics and has completed the entrepreneurship development programme from the Indian School of Business, Hyderabad, as a Goldman Sachs Scholar. Additionally Ms. Rakhi is a NABET accredited Auditor in Administration. Beyond Professional achievements She is actively involved in various social initiatives, and is a member of other esteemed organisations such as, NFPA, CIC, Ascent & Rotary. Rakhi has a passion for the arts, especially music, dance & drama, and believes in cultivating a balanced life.

Hikvision India Showcases Latest AIoT Video Security Solutions at Security and Fire Expo (SAFE) South

Hikvision India has participated in the Security & Fire Expo Security and Fire Expo (SAFE) South India in Chennai recently. The elaborate display of innovative AIoT technology enabled products and solutions at the expo attracted a large number of security professionals. The SAFE South India has brought together internationally renowned exhibitors, consultants, industry experts and visitors from the public sector onto a single platform. Hikvision India had premiered its advanced security products and solutions at the show. The latest trending technologies such as Artificial Intelligence (AI), Robotics and IoT Security Tech were on the display at the event.

While commenting about being at the SAFE South India expo, Mr. Ashish P. Dhakan, MD & CEO, Prama Hikvision India Private Limited said, "We are elated to be part of the SAFE, South India. It is a good platform to connect with the esteemed end-users and valuable partners. We introduced 4G Solar Camera, eNVR, Smart Hybrid camera and PT Solutions. We had welcomed the security industry focused visitors to get an overview of Hikvision's latest product offerings."

He further added, "Hikvision India is showcasing latest technological innovations in Artificial Intelligence (AI) and Robotics Technologies. We unveiled the latest products and solutions in the Video Security, Access Control, Intrusion Alarm, Inspection and Perimeter Security segments. We have also introduced Mobile Robot Products, Machine Vision Products and Logistic Vision Solutions."

The key highlights of the technologies and solutions were on display at Hikvision India booth, it included AI Cameras, Smart Hybrid Camera, ColorVu, Thermal and AcuSense Cameras, Audio Sensor, eDVR and eNVR. The myriad product categories on display were Access Control, Command and Control Systems, Hikcentral, Intelligent Traffic Management System (ITMS), Video Door Phone (VDP) and Security Inspection Products. The other products included AX-PRO, AX-Hybrid PRO Series Alarm System, Energy Solutions, Thermal Solutions, Commercial Display, Professional Transmission Solution, and Smart Storage Solutions.

SAFE South India also hosted a two-day technical seminar. On the first day Hikvision has partnered and supported a session based on the theme 'Make-in-India' 2.0 -The Next Level. It was followed by a panel discussion on the theme 'Managing security across locations globally – Risks & Challenges', Sidharth SB, National Manager, Prama Hikvision shared invaluable insights in the discussion.

Hikvision India, apart from displaying advanced security solutions across product categories, had also conducted various fringe programs, including quiz contests to engage the visitors.

IS THIS HOW YOU GO INTO THE MARKET LOOKING FOR CUSTOMERS?

Let your customers find you @ SECURITY UPDATE

Advertise in SECURITY UPDATE and exhibit your product/service line for meaningful business.

SECURITY UPDATE is the best read channel publication brought exclusively to you by the most read and followed magazine in the Industry - **SECURITY TODAY**.

If you are a Security & Fire Systems Manufacturer, Distributor, Dealer, Integrator, Installer, IT Systems Integrator or VAR, then **SECURITY UPDATE** is just the right medium to advertise in and augment your business via our print and digital publications and web portal.

Why wait?

Contact us today @ 9811549545
or info@1stasset.org

Note: To subscribe to our print and digital editions log on to https://www.securityupdate.in or Scan this QR Code and choose your tenure and mode of delivery, fill your contact details make your payment on our secure gateway using your credit/debit card. Alternatively, you may even tear and physically fill the subscription form available in this magazine, and courier it to us along with your payment.

Milestone Systems merges with Arcules effective July 2024

Global video technology company Milestone Systems has announced that effective July, 2024, they will merge with the cloud-based video surveillance solutions provider, Arcules.

The merger brings together Milestone and Arcules' best-in-class capabilities within video management software (VMS), video analytics and video surveillance as a service (VSaaS), providing a complete video technology offering.

The VSaaS market is predicted to experience exponential growth within the following years and at the same time Artificial Intelligence (AI) is creating new possibilities that were not possible just a year ago. By adding Arcules to Milestone's product line, the company is optimally positioned to lead the video technology software industry.

This merger represents a transformative leap, combining robust video management with the agility and scalability of the cloud and the promise of leveraging AI. Combining forces is a bold step towards pioneering advancements in the rapidly growing VSaaS market.

With the rise of AI, they have the potential to derive insights from video data and support decision intelligence. The merger offers unparallelled ability to exploit the rapidly changing AI landscape from on-prem to cloud and both Milestone and Arcules are advanced in working with video analytics. The combination of these strengths will provide significant market advantages.

Based in Irvine, California, Arcules was spun out from Milestone in 2017. The decision to reunite the companies is driven by a shared vision to deliver intelligent, data-driven video technology that empowers customers to make better decisions and optimise their operations.

Thomas Jensen, CEO of Milestone Systems, said: "Milestone and Arcules have a strong existing partnership and a common DNA. By uniting and working as one, we can provide a world-class offering that suits many different needs and gives customers greater freedom of choice. As one company, we will shape the future of open-platform video technology."

Andreas Pettersson, CEO of Arcules, said: "We are excited to rejoin Milestone, a global pioneer and trusted partner. This merger will accelerate our growth and innovation, delivering greater value to our customers and partners. Together, we are committed to realising our vision of empowering people, businesses, and societies through intelligent video solutions." The merger is scheduled to be finalised by the end of the year.

Paxton wins company of the year award

Paxton has been recognised as Company of the Year at the Security Buyer Awards 2024.

The Security Buyer Company of the Year Award is presented annually to the company that consistently demonstrates outstanding performance in the security industry.

This award honours not only product quality and innovation but also commendable business growth and significant contributions that benefit the entire industry.

Paxton designs and manufactures access control systems, Net2 and Paxton10, Entry, the plug-and-play video door entry system, and Paxlock, smart wireless door handle. The company innovates to offer world-class products and customer service to its installers, through free product training, free technical support, and a 5-year guarantee on its portfolio of products.

Idis scores a quartet at Secure Campus Awards

Idis has scored four wins in the latest annual Secure Campus Awards, with judges singling out the 4MP Edge AI PTZ and the 2MP Video Intercom for recognition. The gold and platinum awards honour the outstanding achievements of security industry manufacturers whose products are considered particularly noteworthy in their ability to improve campus security. Idis won the top awards in the NDAA compliant cameras category, and in entry security intercoms, underlining the benefits of its end-to-end solutions for universities, colleges and schools, hospitals, and corporate campuses.

The new, best-in-class 2MP Video Intercom from Idis is the first NEMA 4X, IK10, and IP66 rated product of its kind offered by any video surveillance vendor. The vandal-resistant and waterproof DC-I6212WRX gives users a host of performance benefits, including advanced functions and unmatched durability in harsh conditions.

Housed in a toughened casing with a choice of flush and surface mount options, the DC-I6212WRX can withstand extreme temperatures and humidity up to 90%, and features intelligent trigger events including active tampering, motion detection, and trip zones. With a robust built-in speaker, it is easy to integrate with Idis's choice of VMS, including the totally cost- and licence-free Idis

Center, as well as third-party systems, including access control systems and electromagnetic door locks.

Access control and visitor management are further boosted with two-way VoIP (SIP) audio, enhanced by echo cancelling and noise reduction. The DC-I6212WRX provides a clear foreground focus and sharp image capture of the scene behind thanks to superior 2MP (1920x1080) image capture with a 180-degree fisheye view, true 120dB wide dynamic range (WDR) and an IR LED nighttime range of 16 feet.

The 4MP Edge AI PTZ camera includes a "first-of-a-kind" AI-powered auto-tracking functionality designed to make it easier to track, monitor, and record the movements of target individuals in high-definition, without error or distraction. With options for manual or automatic target selection, it ensures unbroken surveillance even during the highest pressure moments.

The camera's highly accurate, user friendly AI functionality is invaluable for all settings where it's important to monitor events in real time - to support rapid responses; to assist responder coordination; and to enable efficient incident investigations.

"Idis video technology is playing an increasingly important role protecting campuses and educational settings, keeping students and staff safe and helping them to feel safe," says Mike Rose, Senior Vice President of Sales, Idis Americas. "With two of our latest innovations we are honoured to be among the leading manufacturers singled out for praise in the 2024 Secure Campus Awards."

Advancis enters into a new partnership in Sweden

Advancis has entered into a new partnership with Enaco Sverige AB, as the company becomes the new Advancis System Partner for Sweden.

This collaboration aims to enhance Enaco's security and safety management solutions and represents an important milestone in providing comprehensive and integrated security offerings across multiple sectors.

Enaco, a leading critical infrastructure company, will now utilise Advancis' advanced, vendor-neutral software solutions, such as Winguard, to improve the efficiency and security of its customers.

"We are very pleased about this partnership with Advancis. Their expertise in the field of security and building management systems is a perfect complement to our own. Together, we can now offer our customers even more comprehensive and integrated solutions," says Mikael Berggren, CEO of Enaco.

"We are looking forward to the partnership with Enaco and to contributing our open software platforms Aim and Winguard, our experience and our know-how. I am confident that Enaco's current and future customers will strengthen their security infrastructure with our high-quality and reliable solutions," says Christoffer Lindblom, Sales Director, Advancis Sweden.

Stid accelerates growth plans with €20 million capital injection

Stid, a leading European provider of contactless identification solutions (Radio Frequency Identification (RFID), Bluetooth (BLE), and Near Field Communication (NFC)), has successfully achieved a €20 million funding round from investment firm Capital Croissance.

The funding will enable Stid to pursue its ambitious growth plan while maintaining its independence. The operation was decided to accelerate Stid's innovation in the field of secure access control, particularly internationally, thus ensuring its market lead.

Vincent Dupart, Stid CEO, comments: "With the support of Capital Croissance, Stid is accelerating its development and making investments that are in line with the actions taken over the past five years. We will intensify our international development, particularly in the USA, Canada, Europe, the Middle East, and in Asia, while improving the quality of our services in our historical markets. In addition, we will continue to invest in the development of trusted technologies that have made our success: certified and interoperable solutions such as Systems Security Certified Practitioner (SSCP)."

According to the company, it is driven by strong growth dynamics, both in France and globally, thanks to a strong close relationship with its partners. The company has seen its turnover grow by 100% over the last 3 years, reaching €29 million in 2023.

In 2022 and 2023, STid made two strategic acquisitions (Springcard and Unicacces) resulting in significant growth. Stid also stands out for its Architect range, the most rewarded in the world and a true bestseller on the market, as well as for the user experience of its software platform Stid Mobile ID (SMID), offering intuitive and centralised access management.

Stid has updated its growth plan by integrating new perspectives following the group's expansion. It is strengthening its investments to guarantee the availability and support of its offer to its new network of partners. This fundraising is part of an ambitious development logic. It will allow Stid to accelerate its research and development investments to support its innovation policy and defend its status as one of the most awarded brands in the sector, while strengthening the sales and support teams.

To achieve its objectives, this year Stid plans to expand its teams by integrating 18 new employees in addition to deploying new training programs and initiatives dedicated to quality of life at work.

For sustainable growth and international expansion Stid has won the trust of the Capital Croissance investment fund, with a shared alignment in entrepreneurial values. This minority interest allows Stid to maintain an independent strategy while upholding sustainable development. This partnership will allow the company to consolidate a leading position in Europe and pursue its market share gains internationally by relying on the expertise and network of Capital Croissance.

In addition to its commercial expansion, Stid is developing a strategy with a strong societal and environmental impact. The enterprise has recently created a Corporate Social Responsibility Department and distinguishes itself through its initiatives in sustainable performance.

"Our objective is to develop our strategy and our societal and environmental impact by integrating these values into the heart of our solutions and our operations," adds Vincent Dupart.

Dallmeier Achieves ISO 27001 Certification for Information Security

Video technology manufacturer Dallmeier has been awarded ISO 27001 certification for its Information Security Management System (ISMS). This international standard confirms that Dallmeier meets the highest standards of data protection and security.

As IoT components, surveillance cameras, software, and recording systems are vulnerable to cyber threats, selecting a trustworthy manufacturer is crucial. The ISO 27001 certification assures Dallmeier customers that their data and systems are well-protected, with effective processes in place to minimize risks and continuously improve information security.

This certification is particularly significant for operators of critical infrastructure systems, helping them fulfill NIS-2 requirements for a secure supply chain. Additionally, Dallmeier ensures compliance with GDPR and the NDAA, vital for international customers relying on secure data processing.

Armin Biersack, CSO at Dallmeier electronic, states, "The ISO 27001 certification is an important milestone for Dallmeier electronic and underlines our commitment to the highest security standards and the protection of our customers' sensitive data. Combined with our existing NDAA and GDPR compliance, our customers can be assured that they are working with a trusted partner that understands their security and privacy needs and meets current and future regulatory requirements."

DOES SECURITY REALLY MATTER?

INDIA'S #1 SECURITY MAGAZINE

For Subscriptions, Advertising and other Brand Building opportunities email us at:
info@1stasset.org

https://www.securitytoday.in

CITIES/TOWNS LISTED ARE ACTUAL SUBSCRIBER LOCATIONS

Security Systems Project Handover Essentials

In today's business climate, the importance of implementing a comprehensive security system cannot be overstated. A properly designed and installed security system can provide the end user with a number of important advantages, including deterring crime, protecting assets, and providing peace of mind.

Managing large physical security system integration projects professionally, such as critical infrastructure, airports and power plants is a complex process that requires careful planning, coordination, and execution. However, one of the most critical aspects of these projects, often understated, is the handover phase. This phase marks the transition of the system from the Systems Integrator (SI) to the End-User (client), signifying the culmination of the project. A successful handover ensures that the system functions as intended and that the client is fully capable of operating and maintaining it. This article explores the intricacies of managing such projects, with a special focus on the importance of a well-executed handover. We hope the End Users as well as Consultants and Systems Integrators will find it useful. Your feedback is welcome at *info@1stasset.org*

The transfer of ownership of the project from the systems integrator to the client or end user can have an effect on security and safety, reliability, standards of operation, maintenance and operational cost efficiencies to the client. The transfer/handover period can be a very stressful time for systems integrators as well as the client security teams as spaces become occupied and operation of the facility starts. The commissioning and fine tuning operations during handover can also impact heavily on the core business of the client if not managed in a structured manner.

This article attempts to detail the requirements and actions required to be undertaken during any protection systems project handover. The whole process should be driven by the project manager in conjunction with the SI and subcontractors, if any.

Pre Project Handover Site Meeting

Projects will require a dedicated project meeting to discuss the project handover process and to agree on requirements and outcomes. The meeting should be held at least four weeks prior to the proposed project completion date. This meeting will lend clarity as to what information and actions are required at the time of the final project handover.

Introduction and purpose of the meeting.

CAD information: Provide hard and soft copies of all site maps and drawings.

As-fitted drawings: Include system and subsystem connection diagrams and single-line wiring schematics. The system should have been installed and configured in accordance with the system design proposal. Any deviations from the system design proposal should be agreed, in writing, with the client

Device and equipment details: Document the location (siting) and purpose of all devices, including control units. Provide information on the functionality of each device, their purpose, and the areas or objects they protect. Camera views should be documented through drawings, printouts, or video recordings.

System record: State the make and model number of all equipment. The system record, reflecting the "as installed" setup, should be agreed upon with the client and a copy provided to them.

Manufacturer's documentation: Include operational settings and controls, along with full instructions for correct system use, routine testing procedures, and maintenance requirements.

Additional operational guides: Provide any other detailed documentation and videos.

Maintenance manuals: Include strategies, recommendations, and service schedules.

Licences and certificates: Include software licences and any other necessary certificates.

Commissioning test records: Ensure thorough testing and commissioning of the system. Provide a record of any test results related to the commissioning of the installed equipment.

Safety and health measures: Include prescribed essential safety features and maintenance guidelines for the defects liability period (DLP).

Defects management: Outline procedures for managing defects and after-hours callouts.

Trouble ticket procedure: Provide a procedure for registering trouble tickets along with an after-sales support escalation matrix, draft maintenance contracts and SLAs. Include contact information for future support, maintenance, and upgrades.

Penetration Testing and Security Audits: Ensure the security system's robustness and identify potential vulnerabilities before handover. A summary of any penetration testing or security audits performed on the integrated system (cyber and physical) prior to handover should be prepared. These tests are designed to simulate potential security breaches, identify vulnerabilities, and ensure that the system is resilient against unauthorised access or attacks.

Systems operational and maintenance training: Include plans for training and support to the end-user, including, system operation and maintenance, troubleshooting and fault resolution, building operations such as evacuations.

Warranties and guarantees : Provide a comprehensive overview of the warranties and guarantees associated with all installed equipment, components, and software. This should include the duration of coverage for each item, specifying what is covered under the warranty (e.g., parts, labour, technical support) and any exclusions or limitations.

Regulatory Compliance: Ensure that the system adheres to all relevant local, national, and industry-specific regulations and standards. Include documentation demonstrating compliance with these regulations, as well as any necessary certifications and approvals.

Recording media: Outline procedures for the operation, storage, and cycling of recording media.

Control Room operations: Include operations and management procedures for the Control Room.

Test Period: Following the handing over of the security system it is recommended that the system is tested by the client for an agreed time period. During this period the system should be operated normally.

System Acceptance: Following the successful completion of the test period the client should be prepared to sign an acceptance certificate stating the security system has been installed in accordance with the as-fitted document and operates accordingly and that, and sufficient instruction and training has been provided to ensure the proper operation of the system. Prepare and discuss the format of the formal acceptance of the project from the client.

The project manager should arrange this meeting with all stakeholders (architects, consultants, key system integration team members, site security team, IT team, FM team, and any other stakeholders connected with the success of the perceived security system outcomes).

All the documents listed above and including any other information related to the protection systems project should be bound together in a logical sequence and be made a part of the Site Security Manual.

Proper documentation is essential as it serves as a reference for the client's personnel, ensuring they have the necessary information to operate the system correctly. It also helps in troubleshooting and maintenance, reducing downtime and ensuring the system remains functional over time.

Mr. Deepak Chaturvedi, Chairperson of the Physical Security Community of ASIS International, speaking to SECURITY UPDATE said:

Training the client's security team before the handover of an integrated security system is not just important—it is essential for the system's success and longevity. The effectiveness of any security system depends on the ability of the end-users to operate, manage, and troubleshoot the system effectively. Without proper training, even the most advanced and well-integrated security solutions can fall short of their potential, leaving gaps in security and increasing the risk of operational failures.

One of the key reasons training is so crucial is that modern security systems are highly sophisticated, often comprising multiple technologies - such as surveillance cameras, access control, intrusion detection, and sometimes even advanced analytics and cybersecurity measures. These components must work seamlessly together to create a cohesive security posture. If the client's security team does not fully understand how these systems interact, they may struggle with daily operations, potentially leading to mistakes that could compromise security.

Training ensures that the security team is not only familiar with the system's functionality but also comfortable with its operation. This familiarity is particularly important in high-pressure situations, where quick and decisive action is required. A well-trained team can confidently manage the system, responding appropriately to alerts and incidents, and making informed decisions that enhance overall security.

Moreover, training provides the security team with the skills necessary to maintain the system over time. This includes routine tasks such as updating software, managing user access, and performing basic troubleshooting. Proper maintenance is critical to ensuring that the system remains effective and continues to protect the facility as intended. When a team is well-trained, they can handle these responsibilities in-house, reducing downtime and minimising the need for external support.
Another aspect that cannot be overlooked is the ability of a trained team to adapt to future changes and upgrades. As security threats evolve, so too must the security systems that protect against them. A team that has been thoroughly trained from the outset will be better positioned to embrace new technologies and integrate additional features without requiring extensive re-education.

Finally, the training process develops a sense of ownership among the client's security team. When team members are actively involved in learning about the system, they become more invested in its success. This ownership translates to better day-to-day management and a greater commitment to maintaining the integrity of the security environment.

The Importance of Handover in Security System Integration

A well organised, efficient and effective transfer of information from the SI team to the Client is essential. The handover phase is perhaps the most critical aspect of the entire project lifecycle. It marks the point at which responsibility for the security system is transferred from the integrator to the client. A well-executed handover ensures that the client is equipped to operate and maintain the system effectively, thereby maximising the system's utility and lifespan.

Training

Without doubt, a key component of the handover

Supported by:

ASIS INTERNATIONAL Stronger Together
All India Chapters

PSP PUNE SECURITY PROFESSIONALS

INDIAN POLICE FOUNDATION

Knowledge Partner:

1st ASSET Academy of Security Science Education & Training Pvt. Ltd.

Media Partner:

SECURITY TODAY The Magazine that Best Sums up the Indian Protection Industry!

SECURITY update

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

For details, visit our website:
https://securitytoday.in/knowledgesummit/ | E-mail: events@1stasset.org

process is providing comprehensive documentation. However, the other most important aspect of the project handover is the training which is to be imparted by the systems integration team to the client site security team. Training is a critical element of the handover process. The integrator must provide thorough training to the client's staff, covering all aspects of system operation, maintenance, and troubleshooting. This training should be tailored to the client's specific needs and should ensure that the staff is comfortable with using the system. Hands-on training sessions, supported by instructional materials, are often the most effective way to achieve this.

Only qualified and competent trainers are to be used. These could be people like the manufacturer's representatives or others duly trained by the manufacturers who are knowledgeable about the installations/systems.

The training need not be delegated to the last days, as the client's team may require time to understand the installed systems, their operation and maintenance. Adequate and effective training must be arranged for early, partial or staged handovers. These early handovers must be reviewed and reinforced during final project handover training program development.

Post Handover Support

Even after the formal handover is complete, the integrator's role does not necessarily end. Many projects include a post-handover support phase, where the integrator provides ongoing assistance for a specified period, also called down-stream monitoring of the installed systems. Many adjustments and calibrations may be required during this phase. For example, if there is an occurrence of false alarms from the perimeter fence, the sensitivity of the sensors may need to be adjusted. This support can include regular system checks, software updates, and troubleshooting assistance. Offering post-handover support is beneficial as it helps maintain the client relationship and ensures the long-term success of the security system. A satisfied client often results in positive referrals and increased business.

Despite its importance, the handover phase is often fraught with challenges. One common issue is the lack of thorough documentation, which can leave the client's staff ill-prepared to manage the system. Another challenge is inadequate training, which can result in operational inefficiencies or even system failures. To avoid these issues, it is essential for the integrator to invest the necessary time and resources into the handover process, ensuring that all aspects are covered comprehensively.

Best Practices for a Successful Handover

To ensure a successful handover, integrators should adhere to several best practices. First, planning for the handover should begin early in the project, with clear milestones and deliverables. This proactive approach ensures that there are no last-minute surprises and that the client is well-prepared to take over the system.

Second, communication is key throughout the project. The integrator should maintain regular contact with the client, providing updates on progress and addressing any concerns promptly. This helps build trust and ensures that the client's expectations are met.

Third, thorough testing and quality assurance are essential before the handover. Any issues identified during testing should be resolved before the system is handed over, ensuring that the client receives a fully functional system.

Finally, the integrator should provide ongoing support even after the handover is complete. This could include regular follow-ups, maintenance services, and updates to ensure the system continues to perform optimally.

Final Acceptance and Sign-Off

The final acceptance of the system is a formal process that involves the client verifying that the system meets all agreed-upon specifications and is fully operational. This step often includes a final walkthrough, where the integrator demonstrates the system's capabilities and addresses any last-minute concerns or questions from the client. Once the client is satisfied, they provide a formal sign-off, marking the official completion of the project.

By considering these key aspects, Systems Integrators can ensure a smooth handover, customer satisfaction, and a well-documented project completion. ■

Want to Unlock Expert Insights and Cutting-Edge Technology Updates Every Month?

Subscribe to SECURITY UPDATE & Know The Latest:

- Industry Trends
- Technology & Products
- Industry Expert Interviews
- Insider knowledge

& More....

INDIA'S LEADING PUBLICATION ON SECURITY & FIRE SAFETY TECHNOLOGY

ORDER FORM

YES!

I want to subscribe to Security Update

THE SECURITY & FIRE SAFETY TECHNOLOGY MAGAZINE

Signature _____ Date _____

This subscrition is for ◯ personal / ◯ office use _____

Complete your details PLEASE USE CAPITAL LETTERS TO FILL THE FORM

Name (Mr./Mrs./Ms.) _____

Job Title _____ Organisation _____

Address _____

Town _____ District/State _____ Country _____

PIN/Zip/Postal Code _____ Tel/Mobile _____ Email _____

SIMPLE STEPS TO SUBSCRIBE NOW:

1 Fill up the form above 2 Click a picture of the form 3 WhatsApp it to our team at: +91 98115 49545

CASE STUDY

Hikvision IP Cameras Enhance Security at South Africa's Shopping Malls

Overview:

The scenic splendour of South Africa's Western Cape Province, particularly Cape Town, attracts millions of tourists and business visitors alike. The town of Somerset West, situated on the outskirts of Cape Town, boasts the region's third-largest shopping centre, Somerset Mall. Opened in 1993 and strategically located on the N2 Freeway, the mall has continually attracted a growing number of visitors.

With two expansion phases increasing its size to over 1.3 km of storefronts, 204 stores, an Adventure Arena, and extensive parking facilities, Somerset Mall now welcomes an average of 200,000 visitors per week. However, the CCTV security system had not kept pace with this growth, prompting the mall's management to seek an enhanced security solution.

Challenge:

The expansion of Somerset Mall and the increase in visitor numbers stretched the existing analogue CCTV system to its limits. Enhancing surveillance in pedestrian areas and extensive car parks was a priority. The mall's management realized that the existing system could not meet the current security needs or support further expansion.

Solution:

Systems-integrator SSC Infrasek was tasked with implementing a comprehensive CCTV system to maintain security throughout the complex. According to Mario Groenewald, Technical Manager at SSC Infrasek, simply supplementing

the existing analogue system was not viable. The decision was made to replace it with a fully IP CCTV system using Hikvision network cameras.

Implementation:

SSC Infrasek selected 130 Hikvision network cameras, supplied by local distributor Sensor Limited, for the new system. The choice of Hikvision technology was based on several factors, including the wide range of available cameras, their robust and reliable nature, and the high-quality images they deliver. Hikvision's support from system design through to implementation also played a key role.

Interior Surveillance: For the mall's interior, SSC Infrasek installed 100 DS-2CD7153-E network mini dome cameras. These cameras are ideal for areas like Somerset Mall due to their high image quality and robust build. Key features include:

- 2 megapixel HD resolution (1600 x 1200 pixels)
- Dual real-time video streams up to 720p
- Multiple video compression options (H.264, MPEG4, MJPEG)
- Vandal-proof IP66 rated housing
- Day/night automatic switching
- Motion detection and other alarm triggers
- PoE capability for versatile placement

Exterior Surveillance: To cover the mall's exterior and 3,800 outdoor parking spaces, 30 Hikvision DS-2DF1-518 PTZ network high-speed dome cameras were installed. These cameras offer:

- 36x optical zoom and 16x digital zoom
- 1/4" Sony Super HAD CCD image sensor
- Tough, weatherproof IP66 housing
- 3D intelligent positioning and powerful PTZ control
- Day/night operation down to 0.02 lux in black & white

Results:

The new IP CCTV system significantly enhanced security at Somerset Mall, supporting current needs and future growth.

Mario Groenewald, Technical Manager at SSC Infrasek, stated, "The successful implementation of this IP surveillance solution demonstrates our expertise and Hikvision's commitment to advanced technology, paving the way for more IP projects."

Conclusion:

Hikvision's comprehensive IP CCTV system has future-proofed Somerset Mall's security, ensuring a safe environment for its visitors. This project underscores the value of advanced technology and expert integration in addressing complex security challenges.

Heathrow Airport Transforms Security with Genetec Solutions

Overview:

Heathrow Airport, Europe's busiest airport, handles approximately 80 million passengers and 14 million tons of goods annually. With over 76,000 employees working across its 1,227-hectare site, the airport's operations are vast and complex, including maintaining passenger flow, securing premises, and managing over 1,300 daily take-offs and landings for 89 different airlines.

Challenges:

Heathrow needed a comprehensive and unified security solution to manage its large-scale operations effectively. The airport's existing systems were fragmented, making it challenging to maintain security, ensure data privacy, and comply with cybersecurity regulations. The goal was to enhance operational efficiency and improve the passenger experience.

Solution:

Heathrow partnered with Genetec Inc., a leading provider of unified security, public safety, operations, and business intelligence solutions. The airport initially deployed Genetec Security Centre to unify all its IP security systems into a single platform. What started as a 2,000-camera deployment in 2016 has since grown significantly, incorporating video, access control, LIDAR, analytics, automatic licence plate recognition (ALPR), and more.

Implementation:

The implementation of Genetec solutions at Heathrow involved several key components:

- *Unified Security Platform:* Genetec Security Centre unified various IP security systems, providing a single platform for video surveillance, access control, and analytics.
- *Comprehensive Coverage:* The system now includes over 8,000 cameras, monitoring passenger flow, securing premises, and managing vehicle access.
- *Advanced Monitoring:* Genetec solutions monitor over 150 km of baggage belts and facilitate the daily entry and exit of over 150,000 vehicles.
- *Customised Dashboards:* These enable 90 different stakeholder groups across 110 control rooms to focus on specific tasks, such as monitoring passenger flow or ensuring system health.

Results:

The deployment of Genetec solutions has significantly transformed Heathrow's operations:

- *Efficiency:* Streamlined security and operational workflows.
- *Enhanced Security:* Improved surveillance and control over the airport's expansive infrastructure.
- *Custom Solutions:* Adapted to new requirements and operational realities, ensuring continuous improvement.

Danny Long, IT Product Owner for physical security products at Heathrow, noted, "We're essentially running a small city operation that happens to be called Heathrow. Alongside traditional airport security functions, we're responsible for monitoring roads, retail space, train stations, a bus terminal, offices, a church, fuel stores, a high voltage electrical network, and all the other associated infrastructure that maintains passenger flow."

Simon Barnes, Director of Business Development at Genetec, Inc., added, "The joy of working with London Heathrow is that the team is constantly striving to put our system through its paces and identify new areas where it can add value. While our software is configured to their requirements at the time, once in the field, new requirements emerge, and we have to adjust to their reality."

Conclusion:

Heathrow Airport's partnership with Genetec has significantly enhanced its security and operational capabilities. The unified platform and scalable solutions provided by Genetec enable Heathrow to maintain high standards of efficiency, security, and passenger experience while remaining adaptable to future needs.

Dahua Cameras Secure Tripoli Stadium in Libya

Overview:

Built in 1970, Tripoli Stadium is Libya's largest Olympic stadium with a capacity of 50,000 spectators. Recently renovated to meet FIFA's safety and security standards, the stadium needed advanced surveillance to ensure the safety of spectators and smooth management of events.

Challenges:

On match days, controlling the large crowds and ensuring safety with limited police and security staff posed significant challenges. The stadium also needed to stream match action to large screens inside and outside for fan engagement and advertising purposes.

Solution:

Dahua Technology provided a comprehensive solution by installing a mix of Hubble Panoramic and PTZ cameras, alongside more than 180 WizMind 5 series cameras.

Hubble Panoramic Cameras:

- *Placement:* Positioned high in the stadium for a panoramic overview.
- *Coverage:* Offered 180°, 270°, or 360° coverage with Ultra HD resolution up to 24MP.
- *Features:* Included crowd number and density detection, vehicle counting, density monitoring, and augmented reality mapping.
- *Tracking:* Integrated dome cameras for zooming and tracking specific incidents.

WizMind 5 Series Cameras:

- *Technology:* Utilized Starlight and deep learning algorithms.
- *Intelligent Functions:* Included face recognition, perimeter protection, and people counting.
- *Durability:* Available in dust-proof, waterproof, and vandal-proof versions.

Implementation:

The installation included eight Hubble Panoramic cameras and over 180 WizMind 5 series cameras strategically placed throughout the stadium to enhance situational awareness for managers and security teams. The system provided:

- *High-Resolution Coverage:* Ultra HD panoramic views for overall monitoring and incident tracking.
- *Intelligent Recognition:* Enabled identification and tracking of blocklisted suspects and validation of authorized ticket holders.
- *Crowd Management:* Automatic heat mapping to anticipate overcrowding and congestion points.
- *Perimeter Protection:* Detected and tracked abnormal intrusions

Additionally, giant 15m x 9m LED screens were installed to display live match footage and advertisements. All equipment was managed via Dahua's DSS video management software from a central control room.

Results:

The deployment of Dahua's advanced surveillance system significantly enhanced the stadium's security and operational efficiency. Key benefits included:

- *Improved Safety:* Enhanced situational awareness and crowd control.
- *Efficient Access Control:* Streamlined with face recognition technology.
- *Enhanced Fan Engagement:* Live streaming of match action and advertisements on large screens.
- *Proactive Incident Management:* Enabled quick response to potential incidents with intelligent tracking and perimeter protection.

Testimonial:

A stadium representative stated, "The installation of Dahua equipment has provided our staff and security personnel with a high degree of situational awareness, allowing us to control access, anticipate overcrowding, and effectively manage security throughout the venue."

Conclusion:

Dahua Technology's comprehensive surveillance solution has transformed security and operations at Tripoli Stadium, ensuring a safer and more enjoyable experience for spectators while meeting modern international standards.

Enhancing Security for County Offices with Konica Minolta and MOBOTIX S16 Cameras

Overview:

A county office responsible for issuing new or renewing car tags faced several security and operational challenges with their existing video surveillance system. The county required a solution that provided comprehensive oversight of transactions, secure access control, and improved image quality for verification purposes.

Challenges:

The existing surveillance system presented multiple disadvantages:

1. *No Audio Recording:* The absence of audio meant that crucial parts of the transaction conversations were not documented.

2. *Disparate Cameras:* Each camera operated independently without a unified platform, complicating the security team's tasks.

3. *Lack of Real-Time Viewing:* The independent cameras did not offer a convenient dashboard for simultaneous viewing of all locations.

4. *Poor Image Quality:* The existing cameras failed to provide clear images, making transaction verification difficult.

5. *Lack of Access Control:* There was no secure entry control system for employees.

Solution:

The county partnered with Konica Minolta Intelligent Security Services to implement a robust solution. They chose the MOBOTIX S16 camera for its dual sensor flexibility, high-quality video and audio recording capabilities, and the unified platform provided by the Mx Cloud interface. This solution was designed to enhance their multi-location operational oversight.

Implementation:

The MOBOTIX S16 camera was selected for its ability to:

- *Dual Sensors:* One sensor focused on documents and currency, and the other on the customer and employee, ensuring the entire transaction was recorded with a single camera.
- *High-Resolution Images:* The cameras provided high-resolution images with no loss of detail, crucial for transaction verification.
- *Unified Platform:* The Mx Cloud interface offered a single, intelligent video network that allowed easy verification of any transaction across multiple locations.

To complete the security solution, the county added the Genetec access control system, ensuring secure access points for county employees.

Results:

The implementation of MOBOTIX S16 cameras and the Genetec access control system resulted in several significant improvements:

- *Enhanced Oversight:* The county now had a unified, intelligent video network that provided comprehensive oversight of transactions.
- *Improved Verification:* High-resolution video and audio recordings enabled accurate verification of transactions.
- *Increased Security:* The Genetec access control system provided secure entry points for employees, enhancing overall security.
- *Operational Clarity:* The new system offered greater clarity on business operations with high-quality video images and audio reflecting actual transactions.

A county representative stated, "With the new intelligent video security solution in place, we now have greater clarity on our business operations and high-quality video images and audio reflecting the actual transactions. The MOBOTIX S16 cameras and Genetec access control system have significantly improved our ability to ensure secure and efficient operations."

Conclusion:

By partnering with Konica Minolta Intelligent Security Services and implementing MOBOTIX S16 cameras, the county office successfully addressed their security challenges, improved transaction verification, and ensured secure access control. This case study highlights the effectiveness of integrating advanced video surveillance and access control solutions to enhance operational security and oversight. ■

Revolutionising Door Security with Electric Strikes

Electric Door Strikes are a vital component in modern access control systems, although we see more Electromagnetic Locks (EM Locks) installed out in the field. In our March 2024 edition of SECURITY UPDATE we had covered EM Locks and also said that, "There are many system integrators and installers of security systems for whom the electromagnetic lock is their first choice, usually because these individuals are not familiar with other electromechanical and electrical locking hardware, and they consider an electromagnetic lock as a quick fix for the majority of applications."

As such, our editorial team trains its sights on Electric Door Strikes in this issue.

An Electric Strike offers a secure and efficient way to manage entry to buildings and restricted areas. It is an access control device used for doors. It replaces a standard strike mounted on or in the door frame and operates with an electric current, hence the name 'electric strike'. The purpose of an electric strike is to release the latch when an access control system sends an electrical signal.

These devices are installed in the door frame and work in conjunction with electronic locks and access control systems to control whether a door remains locked or can be opened. Unlike traditional mechanical door strikes, electric door strikes allow for remote access control, providing the flexibility to grant or deny entry based on credentials such as keycards, PIN codes, or biometric data.

The primary advantage of electric door strikes lies in their ability to integrate seamlessly with security systems, allowing for real-time monitoring and control. When integrated with a building's security network, electric strikes can be configured to lock or unlock doors during emergencies, restrict access to sensitive areas, or even log entry attempts for audit purposes. This makes them an essential tool for maintaining security in various environments, from office buildings and schools to hospitals and government facilities.

An electric strike is used for door frames. To understand

the electric strike, one first must understand the term "strike." In the context of door hardware, "strike" means a metal plate or assembly that is installed into or onto a door frame on the lock side to receive a latch or bolt and hold it securely. It replaces the fixed strike faceplate often used with a latch (also known as a keeper). Like a fixed strike plate, it normally presents a ramped or bevelled surface to the locking latch allowing the door to close and latch just like a fixed strike would. This is a movable cavity into which the latch projects when the door is closed. However, an electric strike's ramped surface can, upon command, pivot out of the way when the lock on the door is in the locked position and the door is opened, allowing a user to pull/push the door to open it without operating the mechanical lock or using a mechanical key. After the door is opened past the keeper, the keeper returns to its standard position and re-locks when power is removed or applied, depending upon the strike's configuration.

The 'Faceplate' has mounting holes in it through which screws are inserted to fasten the electric strike to the door frame. The 'Lip' bridges the gap between the faceplate and the edge of the door frame and provides a path for the latch to enter or exit the electric strike, and the 'Body' contains the internal electrical and mechanical parts of the electric strike.

Electric strikes are generally available in two configurations: Fail Secure and Fail Safe.

Fail-secure

Also called fail-locked or non-fail safe. In this configuration, applying electric current to the strike will cause it to unlock. In this configuration, the strike would remain locked in a power failure, but typically the mechanical lock can still be used to open the door from the inside for egress from the secure side. These units can be powered by alternating current, which will cause the unit to buzz, or DC power, which offers silent operation, except for a "click" while the unit is powered.

Hold-open: In this configuration, an electric current is applied to the strike, causing it to unlock and remain unlocked until it is used. As soon as the strike has been used, it goes back to standard locked position. This is used in many residential, commercial and industrial applications, the Hold-open function eases usage because the powering of the strike and the opening of the strike do not need to be exactly synchronised.

Fail-safe

Also called fail-open. In this configuration, applying electric current to the strike will cause it to lock. It operates the same as an electromagnetic lock would. If there is a power failure, the door opens merely by being pushed or pulled.

A new trend is a strike that is quickly reversible from fail safe to fail secure (and back again if needed). This adaptability makes them suitable for a wide range of applications, ensuring that security requirements are met in different scenarios.

Some manufacturers require the opening of the solenoids, but others allow the reversing of the function within seconds (usually take less than 10 seconds) with only the movement of two external screws or a mechanical unlocking accessory which is directly accessible when the door is open. This is exactly the same principle as a child safety door lock which is installed on car doors.

Electric strikes on AC allow someone outside the door to hear when the door is open. The buzzing noise is typically made by applying alternating current (AC) to the strike instead of direct current (DC). When using a DC powered strike, the sound is almost imperceptible.

There are many manufacturers of electric strikes, and there are many things that have to be considered when buying one, i.e., type of jamb, type of locking hardware, whether one requires fail-secure, fail-safe or hold-open function, length of the latch, depth of jamb, voltage requirements and the length of the faceplate. Only in fail-safe situations, it is also a good option to choose a magnetic lock.

Many solutions on the market are promoted as "high-security" but not all of them live up to this claim. It's important to select a lock based on the accreditations and certifications of the brand that manufactures them. The true measure of a high-security lock is the extent to which it is difficult to manipulate and the degree to which it can prevent forced entry. It is also critical to have the right type of lock for the right application. One must also check the applicable local fire laws and compliance requirements with respect to the fire code as the electric strikes you may install must comply with the fire code. ■

Productivity Vs Security: How CIOs and CISOs Can See Eye to Eye

When it comes to cybersecurity, organisations often tread a fine line. Of course, they want the most robust defence possible. But at the same time, they don't want the solutions to over-burden employees with intrusive security requirements that slow productivity.

A perfect example is multi-factor authentication, or MFA. While it's been proven to be a strong deterrent against the rising number of identity-based attacks, many organisations have been slow to adopt the common-sense security protocol because employees hate the extra steps required to log in to regularly-used systems.

It's often up to the CIO and the CISO to manage the delicate balance between safety and efficiency. And as cybersecurity increasingly becomes an enterprise-wide risk, amplified by the new risks that might be introduced by the anticipated growth of AI within most businesses, the CIO and CISO must work closer than ever to ensure their company's IT assets are protected — with the least interruption possible for end users.

For many years, organisations often viewed cybersecurity as a "check the box" function. Businesses may have done the bare minimum to comply with standards like those from the National Institute of Standards and Technology (NIST). But amid a surge in both the cadence and type of incidents, organisations are now realising the potential financial and reputational risks of a cyberattack.

And in the same way the Enron scandal two decades ago launched a new generation of compliance requirements for businesses, elevating the role of chief financial officer to greater prominence within the C-Suite, the growing frequency and intensity of cyberattacks is today putting a bigger spotlight on the CISO.

And yet, as many CISOs take on more risk and compliance responsibilities, it's imperative that security professionals learn how to work more closely with the CIO, whose team owns operationalizing many security practices and procedures.

While CISOs spend their days worrying about detecting and recovering from a cyberattack they

know will inevitably happen, CIOs might be spread too thin to fully absorb those risks. Instead, their mind is racing with thoughts on how to modernise their company's infrastructure and ensure the workforce is more productive. And increasingly, CIOs are being tasked with managing the organisation's AI strategy.

As a result, it's not uncommon for the two roles to be in conflict. CIOs are usually inundated with complaints from employees about any additional step (like MFA) that separates them from the work they need to do. At the same time, the CIO needs to understand how changes that might enhance productivity could create severe security risks.

For example, if several employees on a video conference call are all recording the session, there are now multiple files, possibly stored in different locations, that contain potentially sensitive information. Considering the number of video calls that likely occur across a large enterprise on a given day, it's easy to see how the resulting security vulnerabilities could become a big concern for the CISO.

In order for the CIO-CISO relationship to work, businesses also need to understand the type of skill set they require in a CISO right now — and the type of expertise that will be needed to push the organisation forward.

For example, even most mid-size organisations might not be prioritising cybersecurity yet. Of course, they understand the severity of the threat landscape. But their risk management committees might be focused on other issues, like diversifying the supply chain to ensure future manufacturing capabilities, rather than thinking much about IT security.

In this instance, it would be wise for the organisation to hire a CISO who would bring new focus to the technical aspects of defending the company's IT environment and developing a recovery plan in response to the inevitable attack. However, when the business reaches a certain size, investors will start demanding that cybersecurity be treated as an enterprise risk, raising it to a boardroom-level issue. And that's when the company should consider hiring a CISO who has a more compliance-related background.

Once the right candidate is in the organisation, the CIO should also make sure the CISO is set up for success. If the CISO's top mandate is tilted more towards corporate risk management, for example, then the business should hire a deputy chief information security officer (we call it a "lowercase ciso") — someone who is tasked solely with managing the technical side of the defence operation.

That way, the CISO can instead spend more time aligning with the CIO on the broader cybersecurity strategy and communicating those plans to other leaders, including the board of directors. Meanwhile, the "ciso" can handle the day-to-day work, perhaps even doing some coding themselves.

The CISO can be a difficult position. The typical mandate – to protect what are increasingly complex and widely-dispersed IT environments – is incredibly broad. At the same time, CISOs have little domain control. They must work across the entire enterprise and get buy-in from several key stakeholders to implement the necessary procedures and policies.

Often, CISOs face stiff resistance from the business, especially if the security chief wants to implement measures that would impact how business-unit leaders and their teams are used to working. It's why the CIO must make sure the CISO has a direct line of contact to the appropriate leaders, whether that's the CMO, the CFO, the global head of sales or any other function with a corresponding executive leader.

And while the CISO won't have final authority, those divisional leaders should take the security chief's recommendations seriously. The CIO can aid this effort by aligning with the CISO so they are in agreement on what should be implemented.

When it comes to basic operational issues, like a cloud storage centre going down, the CIO should take the lead. However, when a cyber incident occurs, the CISO should have the authority to execute the established response plan to ensure a timely and thorough recovery, with minimal downtime and data loss.

But CISOs also must understand where their authority ends. For example, in the event of a ransomware attack, the decision to pay would ultimately come down to other leaders in the business, like the board of directors and the CEO.

The rise of AI and the push towards becoming a digitally-connected business is putting fresh attention on the debate between enhanced productivity and increased security risks. Tilting too far in one direction could open the business up to more attacks or significantly hinder employees' ability to do their jobs. In both cases, the company ultimately suffers.

The divisions between IT and security are quickly disappearing; so should the organisational barriers within the business. And as technology drives more-and-more of a company's core functions, it's up to CIOs and CISOs to learn how to keep level the proverbial IT see-saw. ■

Credits: Venturebeat

Senstar Offers 5 Step Guide On Eliminating False Alarms

The team at Senstar has investigated the common causes of nuisance alarms generated by outdoor perimeter intrusion detection sensors with a particular focus on those generated by fence sensors and intrusion-detection video analytics.

After deeper analysis, they came up with a five step set of general recommendations aimed at reducing or even defeating nuisance alarms once and for all, here we look at a summary of their findings.

1. Maintain your perimeter

A well-maintained perimeter is the first step in eliminating nuisance alarms. Perform a perimeter survey and identify potential security issues and risks, for example, the condition of the fence, the position of the surrounding buildings and trees, and if used, ensure the coverage of the cameras is complete and unobstructed.

2. Work with industry experts

Before deciding on any specific technology, look for system integrators, consultants and vendors with proven track records. When deployed in the real-world, security systems need to contend with a wide variety of potential nuisance alarm sources. Experienced security professionals in your particular domain can help as they should understand the requirements. Ensure the installers, vendors and operators are certified and trained on the right systems. A poorly installed system will almost certainly generate a far higher number of nuisance alarms.

3. Select appropriate technology

While there are many types of sensor technologies that protect perimeters, some are niche solutions while others have a general appeal. The factors to consider when selecting a system should include, probability of detection – look for speed, reliability and accuracy; nuisance alarm rate – high rates of nuisance alarms can result in response complacency; ease of installation and can it be configured remotely; integration options - consider other technology that you might want to integrate with it such as VMS and cameras; consider the alarm communication methods, and ensure it includes things like mapping, precise alarm location - and other situational awareness tools.

4. Conduct periodic site audits

An often-overlooked part of reducing nuisance alarms is periodic site audits. Over time, new site characteristics may be introduced that negatively affect the overall performance of the on-site systems. For example, almost all the points in step one should be regularly checked, fence condition, surrounding vegetation, new buildings, and new vehicle routes etc.

5. Eliminate common causes

During the testing or lifespan of any system, problems may arise. For systems to remain operating at maximum performance, they need to include the features and tools necessary for operators and technicians to quickly locate and resolve issues.

For intrusion sensors, several features are critical to address the causes of nuisance alarms, the first being covered in step 3, precise location reporting. However, the system should also be able to deal with environmental disaggregation such as heavy winds, for example.

Ranging sensors like the Senstar Fiberpatrol, Flexzone, and the Senstar LM100 are able to recognise these disturbances as non-intrusions and so do not trigger an alarm. According to Senstar, Sensors should also include intelligent signal processing that recognises disturbances generated by environmental forces, sudden changes in lighting, and high-activity sources (e.g. traffic, trains, etc) and reject them accordingly.

For sites that suffer from frequent nuisance alarms or require the highest probability of detection possible, the Senstar team recommends its new Sensor Fusion Engine (part of the Senstar Symphony Common Operating Platform), a so-called breakthrough technology that synthesises data from separate systems to generate actionable information. More than just a simple Boolean logic integration, the sensor fusion engine accesses low level data from both fence sensors and video analytics to intelligently characterise potential risks. This data synthesis enables the system to achieve a level of performance that exceeds those of the individual sensors while defeating nuisance alarms once and for all.

Is Right to access CCTV as per DPDP Act allowed?

BY **DIVYA JAIN**
Founder- HRD & Data Privacy Law Consultant

The recent case study highlighting the incomplete response to a subject access request for CCTV footage in an educational institution rings alarming bells in the context of India's newly implemented Digital Personal Data Protection Act (DPDP Act). This case throws light on the importance of data privacy and access rights, particularly for victims of crime seeking evidence through CCTV recordings.

Under the DPDP Act, complying with subject access requests is paramount. The right to access personal data, enshrined in Article 15, empowers individuals to know what information organisations hold about them and how it is processed. This right extends to CCTV footage capturing an individual's image, especially in situations involving alleged criminal activity.

The case study points to several crucial aspects impacted by the DPDP Act:

Timely Response: Article 13(3) of the DPDP Act stipulates a maximum response time of 30 days for data controllers (organisations) to respond to subject access requests. This case, where the response was incomplete and delayed, constitutes a violation of the Act.

Complete and Accurate Data: The Act mandates providing all personal data, not just excerpts deemed "significant" by the controller. In the case study, denying access to footage from two camera angles and offering incomplete stills violate this principle.

Data Storage and Retention: Organisations cannot claim their recording cycle automatically deletes footage as a reason for non-compliance. The DPDP Act requires data fiduciaries (individuals responsible for data processing) to retain personal data for as long as necessary for the designated purpose or until the data subject withdraws consent.

Consequences of Non-compliance: The DPDP Act empowers the Data Protection Board to impose significant penalties for non-compliance, including fines up to 50 crore rupees. Failure to provide complete and timely access to CCTV footage, as in this case, falls under this purview.

In light of these provisions, the DPDP Act has significant implications for CCTV usage:

Mandatory Functionality: Organisations cannot rely on malfunctioning CCTV as an excuse for non-compliance. Ensuring proper maintenance and functionality of CCTV systems becomes crucial for upholding data access rights.

Clear Data Retention Policies: Establishing and adhering to clear data retention policies for different types of CCTV footage becomes essential. This ensures timely availability of footage in case of access requests.

Streamlined Response Procedures: Organisations must develop clear internal procedures for handling subject access requests related to CCTV footage, ensuring timely and complete responses.

The DPDP Act provides a much-needed legal framework for data privacy and access in India. By understanding its application to CCTV footage, organisations can improve their data management practices and ensure compliance. This, in turn, empowers individuals, especially victims of crime, to exercise their right to access valuable evidence.

Remember, upholding data privacy and access rights is not just a legal obligation, but also a fundamental right under the DPDP Act. By ensuring proper procedures and compliance, organisations can foster trust and empower individuals in the data-driven era. ■

Pet Fire Safety Day Urges Preparedness From Pet Owners In Case Of A House Fire

The 15th of July is a day for pet owners to think about how their furry friends can be impacted by house fires. In honour of Pet Fire Safety Day, local leaders are reminding you to make an emergency plan that involves your four-legged family members. According to the National Fire Protection Association, pets accidentally start nearly 1,000 home fires each year.

The Eau Claire Fire Department recommends people take preventative actions, such as removing cords that pets could chew on and keeping hot items out of reach so they don't get knocked over. They also suggest isolating your home by shutting doors while you sleep to prevent the spread of a house fire and so you know where your pet is located so they can be rescued faster.

"Anything that you can do to keep them safe in the same manner you would do for a small child, kind of keep that in mind. You know, don't leave them in a hot vehicle on a day where it's really hot," said Bob Haller, the Deputy Chief for the Eau Claire Fire Department. "You've got to think about the well-being and safety of your pet, too."

Here are a few tips to keep your pets safe and prevent fire hazards:

• Wagging tails and curious cats can potentially knock over candles and other open flames. Consider flameless candles for a light source during power outages.

• Store leashes and collars near the entrance of your home in case you need to leave quickly due to an emergency.

• When away, keep your pets in the main living area or rooms near the entrance to make a rescue in an emergency easier.

• Use monitored smoke detectors to add an extra layer of protection beyond battery-operated smoke alarms.

• Pet-proof your home. Look for areas that may be hazardous causing pets to start a fire inadvertently, such as loose wires, unsecured flammable chemicals, or low stove knobs.

ROCKWOOL® Launches Whitepaper To Support Fire Safety Of Multifunctional Roofs

New whitepaper explores how to identify and mitigate fire risks for flat roofs functioning as additional social or practical spaces of a building, including for solar installations. Today's flat roofs are increasingly used as multifunctional spaces for social and practical applications, including solar energy installations. This expanding remit, particularly in crowded urban areas, brings multifaceted challenges to specification and building design.

The role of the roof in modern building design has expanded significantly in recent years

Now ROCKWOOL has published a whitepaper aimed at helping specifiers and roof contractors to consider and plan for possible fire risks arising from flat roofs being used as multifunctional spaces for a variety of social and practical applications, highlighting, for example, the increasing number of solar energy installations.

'Flat roofs: The functional fifth façade paper' explores the fire safety implications of modern multifunctional roofs and discusses best practices for identifying and mitigating the risks. It also explains the role of the guidance provided in approved documents, including Approved Document B (ADB) for fire safety, and examines potential limitations of such advice for non-standard flat roof circumstances and scenarios.

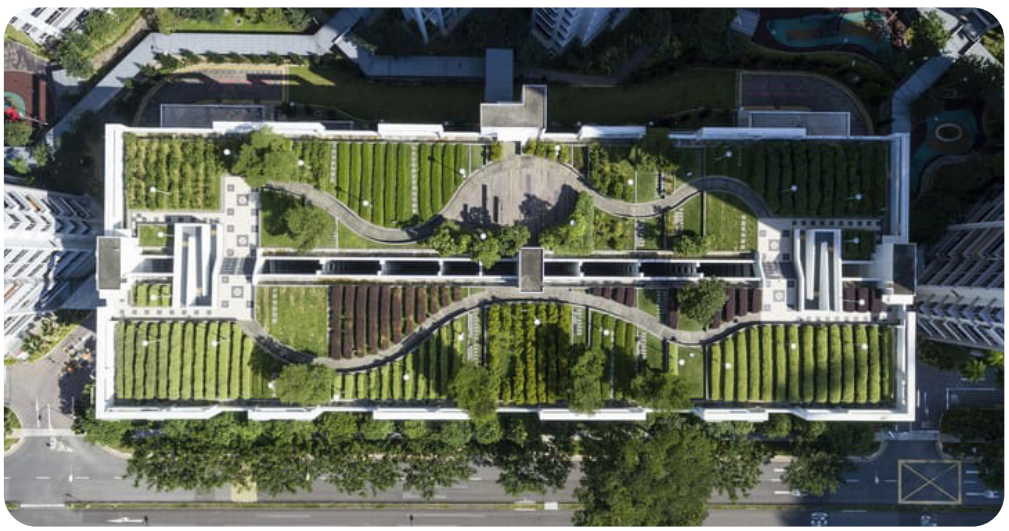
"While the use of flat roofs as functional spaces is not a new concept, the practice has become more and more popular in recent years, especially in increasingly crowded urban areas," explains Lisa Stephens, Product Manager – Building Envelope, ROCKWOOL UK.

"Now, flat roofs don't just house plant and building services but energy efficiency infrastructure and social spaces too."

The whitepaper explores how to balance sustainability with fire safety on flat roofs. With the increasing complexity of the flat roof space in mind, this whitepaper addresses the risks associated with social and commercial uses of flat roofs, considering implications such as greater footfall and the impact of penetrations from building services and cabling on compartmentation and fire resistance.

With the market for solar energy growing rapidly in the UK and Europe, 'Flat roofs: The functional fifth façade' also places a specific focus on the lack of dedicated guidance for solar panels despite evidence that their presence may increase fire risk.

"The information in the whitepaper will help those involved in the design and installation of flat roofs to make responsible choices when selecting materials to enable a modern flat roof to be multifunctional, safe and long-lasting," says Lisa Stephens. "It offers practical advice to simplify specification whilst going above and beyond legislative requirements."



Protecting Against LIB Fires in Recycling Facilities

BY **AMY MARSLAND**

Amy Marsland is a forensics investigator at Jensen Hughes. She is an expert in fire and explosion investigations, hazardous materials, and failure analysis and has conducted numerous investigations within commercial and residential settings.

Lithium-ion batteries (LIBs) are the powerhouses found in our most-loved everyday electronic gadgets and devices, from disposable vapes to electric vehicles (EVs).

LIB technology has historically been the power cell of choice for smartphones and a wide range of other portable gadgets too. However, modern smartphones now are increasingly featuring lithium-polymer (Li-poly) batteries, a suitable alternative for a wide variety of consumer electronic gadgets.

However, improper disposal of LIBs in household waste can pose serious risks due to their reactive nature, with the potential to catch fire or even explode during waste collection and processing.

Additionally, the toxic substances within the battery can pose a risk to life, contaminating soil and water and causing long-term environmental damage. Preventing catastrophic LIB fires in recycling facilities requires consumers, local authorities and facility management to work together to reduce LIBs in the waste stream and implement appropriate protective measures.

The best way to safely dispose of LIBs once they reach the end of their life is to transport them to specialised facilities. There, they can be completely discharged and dismantled, and valuable metals such as lithium, nickel and manganese can be extracted. Instead, many consumers mistakenly throw LIBs and devices—mostly portable electronics like laptops, cell phones and vapes into municipal waste or single-stream recycling collection programs.

The problem is that the impacts of sun exposure, compaction, tipping and sorting during material collection and processing can damage or crush battery cells, triggering thermal runaway and igniting the battery electrolyte. Thermal runaway can result in the production of heat and gases that can lead to fires and explosions.

During the normal operation (discharge and charge) of a LIB cell, heat is produced and dissipates into the environment. Thermal runaway occurs when the heat generated by “abnormal” chemical reactions inside the cell reaches a level where it cannot be dispersed. The additional heat generated causes further exothermic reactions, releasing more heat and toxic gases. This becomes a self-sustaining reaction, which continues until the reaction material is consumed.

Venting gases produce hissing or popping noises from the battery, along with black smoke or a white vapour cloud. Under certain conditions, the flammable gases in the cloud can ignite, producing rocket-like flames. Delayed ignition of flammable gases can result in an extremely dangerous and sudden vapour cloud explosion, which may impact other nearby battery cells or ignite combustible materials.

Disposing LIBs into general household waste significantly elevates the risk of fires in recycling centres. As the use of LIBs continues to grow, the risk will likely continue to rise, leading to higher costs for everyone.

A report from Eunomia Research and Consulting, published with the assistance of the Environmental Services Association (ESA), revealed that an estimated 201 waste fires are caused by LIBs every year in the United Kingdom, costing the country over 100 million pounds sterling ($129.6 million) per year.

Another risk of LIBs in household waste processing is environmental pollution resulting from the long-term accumulation of battery scrap. The hazards produced during a thermal runaway event also can significantly contaminate the surrounding environment. The release of chemicals pollutes the atmosphere while the runoff from the vast quantities of water required to extinguish LIB fires can contaminate the soil and groundwater. Events like these require recycling centres to have pollution response strategies.

The first line of defence against LIB fires is the employees, who should be trained to identify and remove such batteries from the waste stream and respond to fires. Collections and facility staff should have the authority to deal with improperly discarded materials by declining to collect them and providing educational resources. They should also be aware of fire risks, management practices to limit the potential for fire spread and emergency response procedures.

For example, disposable vapes have become a more prevalent concern with their recent rise in popularity. It is estimated that around five million vapes are thrown away in the United Kingdom every week. While most disposable vapes are labelled as recyclable, dealing with the single LIB contained within results in additional costs to the household recycling centre.

To address this growing problem, Aberdeenshire in the United Kingdom has introduced a new procedure for vape and e-cigarette disposal at household recycling centres. The devices are put into drums containing vermiculite to reduce the risk of fire, which allows them to be transported to a specialised facility to extract valuable materials from the battery cells.

Additionally, incident preplanning, with input from the local fire department, can reveal any deficiencies in current fire protection measures and enhance the efficiency of incident responses. This includes providing the fire department with specialised training and personal protective equipment (PPE) to manage the toxic vapour clouds produced by thermal runaway from LIBs.

While the fire industry is working hard to develop suitable and safe portable devices for immediate incident response, a silver bullet solution for controlling LIB fires has yet to be discovered. Portable devices currently available to control fires, such as extinguishers and blankets, can put a person in close proximity to fire and explosion hazards, potentially without the necessary training and protective equipment needed to keep them safe.

Appropriate fire suppression systems and equipment tailored to LIB fires also play an important role in reducing the impact of LIB fires on recycling and waste management centres. These include surveillance monitoring, on-site private water supply, high-powered fire nozzles, sprinkler systems and specially designed flame, smoke and mist detectors, as well as passive fire management practices and active systems designed to mitigate fire growth in surrounding combustible materials.

The future of LIB recycling requires a collaborative effort. As the usage and disposal of LIBs continues to rise, industries and consumers need to work together to create a sustainable battery recycling infrastructure to prevent environmental harm and mitigate the risk of fire. This includes local authorities and facilities implementing regulations and policies that encourage proper disposal and recycling and establishing procedures to comply with disposal regulations. We must also support research and development in battery technologies and raise awareness among consumers about the importance of recycling and the risks associated with LIBs. ■

> "The best way to safely dispose of Lithium Ion batteries once they reach the end of their life is to transport them to specialized facilities. There, they can be completely discharged and dismantled, and valuable metals such as lithium, nickel and manganese can be extracted."

Hikvision India Introduces Traffic Cameras Featuring DarkFighterX To Combat Urban Light Pollution

Hikvision India has introduced traffic cameras featuring DarkFighterX to combat urban light pollution. Traffic cameras fitted with DarkFighterX, Hikvision's ultra-low-light video imaging technology, combine these three approaches to combat light pollution effectively. They are designed to sense both visible and invisible light, reducing the need for blinding flashes. This scales down the number of LEDs used in the flash—merely four LED beads suffice where once many were needed. What's more, incorporating an LED lattice significantly diminishes stray light, so that the intensity that escapes beyond the camera's focus is effectively eliminated.

In addition, DarkFighterX technology uses deep learning to improve image quality in Hikvision cameras, correcting color bias and eliminating headlight halo effects. This enhances traffic violation enforcement while reducing the need for high ambient light.

"Hikvision's innovative traffic cameras have already been successfully implemented in many countries and these cameras are helpful in the Indian environment too," says Mr. Ashish P. Dhakan, MD & CEO, Prama Hikvision India Private Limited. "Given the increasing global emphasis on sustainable living, mitigating urban light pollution through advanced technology like Hikvision's traffic cameras is not only an immediate solution but also a future trend."

Managing the urban environment has always been about making progress and then dealing with the new that it inevitably creates. One of the latest challenges is the glare which is created by the guardians of our intersections, traffic cameras. Although they help detect violations and ensure road safety, this unintended glare also poses risks to drivers and residents.

Bright flashes from traffic cameras, meant to enhance safety, can sometimes do the opposite. According to the NHTSA, glare contributed to about 2.8% of road accidents in 2020, as sudden bursts of light can impair drivers' vision, especially at night. For city residents, these flashes can disrupt sleep and reduce quality of life.

In order to combat light pollution, progressive cities such as Barcelona, London, Oslo, and San Diego, are adopting smart streetlights that dim when not needed. Motion sensors are employed to provide light only when necessary and shielded lighting is being implemented to focus light where it's required, minimising spillage into surrounding areas.

But what about the traffic cameras that need to operate around the clock? Engineers and urban designers have been working on developing cameras that emit less light while still capturing clear images. Here are a few approaches they are taking:

One method involves installing shields around traffic cameras and using directed lighting techniques. This helps to focus the light only on the required areas while minimising light pollution in other directions. The problem with this approach, however, is that these modifications require significant up-front investment and ongoing maintenance, which, understandably, is causing many urban areas to hesitate.

Another approach involves the use of invisible light sensors, which significantly reduce the reliance on blinding flashes for successful imaging. Traffic cameras with this technology can operate within the non-visible spectrum. They effectively capture images without the intense bursts of light that pierce the night. This approach is particularly effective in areas with high levels of light pollution, where it is important to minimise the additional impact of traffic camera lights.

New camera technologies combine AI algorithms with image signal processing (AI-ISP) to correct color inconsistencies and capture high-definition images in low light. This reduces the need for bright flashes, enhancing traffic camera efficiency while minimizing environmental impact.

Given the increasing global emphasis on sustainable living, mitigating urban light pollution through advanced technology like Hikvision's traffic cameras is not only an immediate solution but also a future trend.

YOUR SECURITY BEGINS WITH YOUR PERIMETER

NEMTEK
Electric Fencing Products

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

ECONOMICAL. RELIABLE. EFFECTIVE.

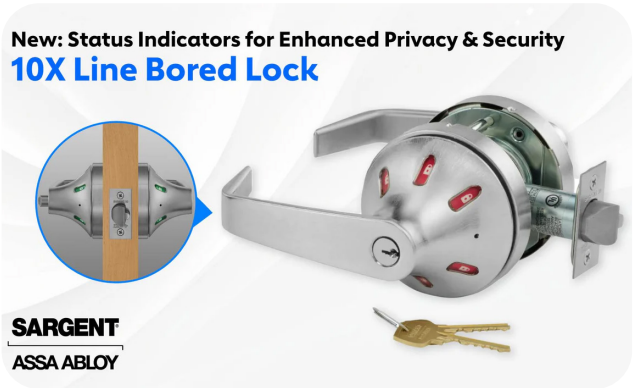
- They provide a higher level of detection capability to detect an intrusion attempt and set off the alarm which is then transmitted to the security personnel, police or the CMS.
- They are installed easily on existing walls or fences, or as a free standing secure energy perimeter fence, forming your 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...

KAWACH
PROTECTION SYSTEMS
Technology on Guard

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

New SARGENT 10X locks by ASSA ABLOY Enhance Security



SARGENT, an ASSA ABLOY brand, introduces the updated 10X Line bored locks featuring visual status indicators for enhanced security and convenience. These locks provide clear, instant confirmation of a door's locked or unlocked status, improving safety across various applications such as classrooms, restrooms, and entryways.

Key Features:

• Instant Status Recognition: Highly visible indicators show the door's status at a glance.

• Versatile Installation: Suitable for new constructions and retrofits across different door types.

• Proven Durability: Exceeds industry standards for strength and longevity.

• Optimal Visibility: Indicator windows can be placed inside, outside, or on both sides of the door.

• Sleek Design: Modern aesthetics complement any architectural style.

The new SARGENT 10X Line locks combine security, privacy, and durability in a user-friendly design.

Allegion US launches Von Duprin 70 Series exit devices

Allegion US introduces the Von Duprin 70 Series Exit Devices, combining trusted quality with a medium price point, ideal for various applications such as warehouses, offices, and retail spaces.

Key Features:

• High Standards: ANSI/BHMA Grade 1 certified for top-tier quality.

• Versatile Options: Available in panic and fire-rated models, with wide (78 series) and narrow (75 series) stile options, plus rim, surface, and concealed vertical rod configurations.

• Quiet Operation: Quiet Electric Latch Retraction (QEL) option for low-noise environments.

• Modern Design: Sleek aesthetics with harder lines, matching the Von Duprin portfolio.

• Quick Shipping: Fast delivery for time-sensitive projects.

• Comprehensive Support: Expert advice, compliance assistance, and training available.

The 70 Series offers a reliable, aesthetically pleasing solution at a competitive price point.

Evolon announces Insites 2.0 Video Surveillance Solution

Evolon Technology, Inc., a developer of intelligent software technology that turns surveillance video into real-time actionable information, has launched Insites 2.0, the latest version of its proactive video surveillance and monitoring platform. This upgrade introduces powerful new features for mobile apps, web platforms, and edge plugins, alongside AI-driven security enhancements for better risk management.

Key Features:

• Mobile Enhancements: Includes an "SOS" emergency dispatch feature, mobile live view for Axis and Hanwha cameras, and AI-powered forensic searching with talk-to-search functionality.

• Web Platform Upgrades: Simplified multi-customer management, pro-monitoring account tools, and enhanced live view and forensic search for rapid video analysis.

"Insites 2.0 redefines video monitoring, offering businesses a seamless, all-in-one platform with unmatched versatility and power," says Tom Galvin, CEO of Evolon.

i-PRO's new AI-enabled Corner Camera for high-security use

i-PRO Co., Ltd., a global pioneer in professional security solutions for surveillance and public safety, announced its new AI-enabled Corner Camera. Built in Japan for the rigours of high-security facilities, this exceptionally compact and robust stainless steel camera represents the smallest form factor, which is IK11 compliant. Its ability to withstand a 70 Joule (70J) impact far exceeds the common IK10 (20J) impact ratings of similar devices.

"The i-PRO Corner Camera represents a new standard for high-security environments, providing unmatched reliability and advanced AI-powered analytics all within the most compact form factor," said Gerard Figols, Chief Product Officer at i-PRO, adding "With its IK11+ 70J rating, it is clearly the most shock-resistant corner mount surveillance camera in the industry today."

The camera's wide-angle view (131° horizontal, 95° vertical) limits blind spots, providing full room coverage. The sensor provides a ±5° yaw adjustment and a ±5° tilt to further conform to installation requirements.

An invisible IR-LED illuminates up to 15 metres using a 940nm wavelength. While the stainless steel body exceeds an equivalent IK11+ impact rating, any attempt to tamper with the camera, from impacts to opening the case, instantly sends an alarm to operators.

The i-PRO Corner Camera measures just 197x139x126 mm (7.76x5.47x4.96 inches). With a dynamic range of 132 dB, images remain clear in a variety of lighting conditions. "The engineers at i-PRO have done it again. When you factor in the additional licence-free AI applications, it's truly an industry-renowned camera," said Gerard Figols.

The camera's all-important anti-ligature design prevents self-harm incidents, while minimising any attempt to remove the camera by force. The corner camera supports up to three free i-PRO AI applications simultaneously, such as AI Video Motion Detection, Privacy Guard, and People Detection.

To protect privacy, i-PRO's AI Privacy Guard feature can automatically blur faces or entire bodies, creating a redacted stream. A built-in microphone facilitates AI-based sound detection of loud noise, screaming, glass breaks, and more. For enhanced cybersecurity, the vandal-proof camera includes a secure boot feature and complies with the FIPS 140-2 level 3 standard.

Centrios launches complete access control product line

Centrios, a new brand created within ASSA ABLOY to serve the small business market, has announced its first shipment of hardware products to SECLOCK.

Centrios is a cloud-based access control solution developed to radically simplify the needs of small and growing businesses. By connecting the Centrios mobile app with Centrios smart readers and locks, owners and managers can quickly and easily manage access for all employees and visitors in one place.

Other solutions within the Centrios product line include the Smart Reader that enables users to unlock virtually any door with electrified hardware from the perimeter to the core of a small business. The Smart Reader is an access control solution for storefronts, employee entrances, storerooms, gates, offices, automatic doors, and access control retrofits.

The company notes that dealers can pair the Smart Reader with other electronic access control systems, features Bluetooth mobile access and PIN code management which can be managed with the Centrios mobile app, and the Smart Reader is designed to install and operate easily. The new Centrios Smart Reader is IP65 weather resistant, FCC/IC certified, ADA compliant, and operates in temperatures ranging from -40° to 140° F (-40° to 60° C).

Continuing to outline the Centrios product line, the brand offers bundled kits to make purchasing convenient and

...

Interface Systems launches Wobot AI for QSR and retail

Interface Systems, a renowned managed service provider of business security, actionable insights, and purpose-built networks for multi-location businesses, has launched Wobot, an AI-powered video analytics solution tailored for quick-service restaurants (QSRs) and retail. This innovative tool leverages existing security cameras to provide real-time insights, streamlining operations and safeguarding assets.

Key features include AI-enabled checklists, no-code workflow configurations, and real-time notifications via email and Microsoft Teams. Wobot helps QSRs enhance dine-in and drive-thru experiences by identifying service gaps, optimizing shift planning, and ensuring health and safety compliance. For retailers, it offers real-time visibility into customer demand, service speed, and security. Interface Systems also provides turnkey implementation and maintenance services for Wobot, ensuring seamless deployment across locations.

hassle-free for small business owners. Each bundle includes a Smart Reader and various access control components depending on the type of hardware required. Examples of what can be selected include electric strikes from HES and Adams Rite, power supply from Securitron, no touch request to exit switch from Alarm Controls, and Securitron DPS.

position sensor, and an LED for lock events and alarms.

The Centrios cylindrical lock typically operates for an entire year on four AA batteries and includes exterior emergency 9-volt DC power backup and a configurable auto relock. Small businesses can choose from one of four lever designs and five finishes, including the very popular black

Elaborating on the technology the product line utilises, the company says the products feature several new patents. The Centrios cylindrical lock is said to offer high performance, installation convenience, and a simple user interface. The cylindrical lock facilitates access via an optional mechanical key or Bluetooth mobile access, features privacy mode with an included door

suede, satin chrome, bronze, bright brass, and satin nickel.

Centrios also emphasises the cylindrical lock is ANSI/BHMA A156.2 Grade 1 compliant; it features a UL10C 3-hour fire rating, it is IP57 weather resistant, FCC/IC certified, ADA compliant, and it operates in temperatures ranging from -40 degrees to 140 degrees F (-40° to 60° C).

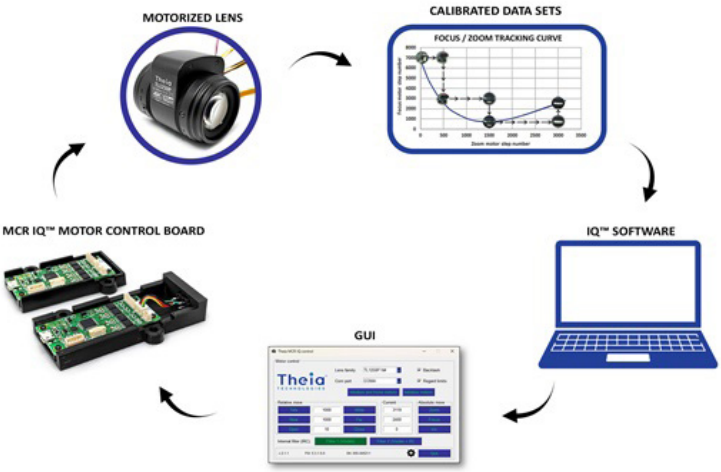
Theia introduces new IQ Lens system

Theia Technologies is launching the company's new IQ Lens System which includes a motorised lens, motor control board, average calibration data, and software with graphical user interface (GUI).

Theia's motorised lenses and motor control board are designed for integration into vision systems for automation, robotics and intelligent traffic systems and use stepper motors to operate the zoom, focus, iris, and filter of the lens. Until recently, using them together required the user to develop software to translate desired engineering parameters into motor steps and motor steps into lens commands. With Theia's new IQ Lens System, enhancements to both allow for quick and easy integration into the imaging system.

Theia's new IQ Lens line provides an average measured zoom/focus tracking curve and lens focal length, plus design data for distortion, aperture and relative illumination for the family. Knowing the relationship of focal length to zoom motor step position allows accurate field of view setup; best focus step to focal length position

allows best focus location with minimal focus adjustment. The IQ Lens line includes software and graphical user interface (GUI) that translates engineering units like FOV or F/# into motor steps without requiring the user to look up which motor step correlates to what FOV, or which iris step equates to what F/#. The new IQ Lens System also works with Theia's fully calibrated lenses.



Theia has also launched the MCR IQ Motor Control Board with software and GUI to convert motor steps into machine commands that move the lens to desired positions. The board communicates via USB, UART or I2C protocols. Calibration data and applications are available including a royalty free license with IQ Lens and MCR IQ purchase.

OnSight Technology Unveils OWL, a Cutting-Edge Fire and Smoke Detection System

Fire incidents pose significant risks, particularly in facilities with extensive solar infrastructure. Research indicates that fire durations exceeding five minutes can increase damage by 3.6 times and harm by 1.5 times. OWL addresses these concerns by providing real-time alerts for fire, smoke, and abnormal heat signatures, ensuring rapid response and minimising potential damage.

OnSight Technology, a leader in advanced monitoring solutions, has announced the launch of its latest product, OWL, an innovative rooftop and field fire and smoke detection system. With its state-of-the-art AI capabilities and swift response times, OWL is set to revolutionise fire safety in various facilities, especially those housing solar installations.

Key Features of OWL:

- AI at the Edge: OWL utilises advanced AI algorithms to process data locally, ensuring rapid detection and response.
- Comprehensive Monitoring: Equipped with high-resolution cameras and a robust detection system, OWL offers millisecond response times and can detect people, animals, and potential fire hazards.
- Easy Installation and Independent Operation: The system is designed for fast and straightforward installation on a 25ft non-penetrative pole and operates independently with 4G/LTE connectivity.
- Versatile Power Options: OWL supports 120VAC power with battery and solar options, ensuring uninterrupted operation.
- Extended Range: The OWL V2 model features four 16MP cameras with a 100-degree field of view, covering up to 500 meters (200 acres).

Advanced Detection Methodology:

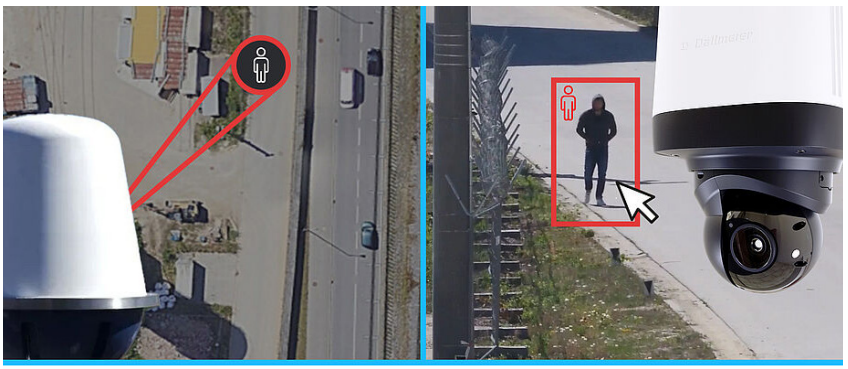
- Comprehensive Datasets: OWL's detection algorithms are trained on diverse datasets, covering both urban and rural environments.
- High Sensitivity: The system employs transient analysis and ensemble models to ensure high sensitivity and redundancy.
- Real-Time Monitoring and Custom Alerts: Users can access real-time monitoring through a dedicated dashboard and receive custom alerts via SMS and email.

"OWL represents a significant advancement in fire safety technology," said Derek Chase, CEO of OnSight Technology. "Our goal is to provide a reliable, efficient, and easy-to-install solution that enhances safety and reduces risks for facilities across North America."

OnSight Technology is a leading provider of advanced monitoring solutions, dedicated to improving safety and efficiency through innovative technology. The company's team, comprising experts in robotics, AI, and engineering, brings decades of experience in developing cutting-edge solutions for various industries.

In addition to OWL, OnSight Technology is renowned for its robotic inspection services, which offer unparalleled precision and reliability in inspecting critical infrastructure. These services have earned the company numerous accolades, including the prestigious Tech Innovator Award and recognition as one of the Top 50 Technology Companies to Watch.

Technological partnership brings improved airside surveillance



By combining innovative radar, camera and software technologies, Navtech and Dallmeier electronics now offer an integrated solution for optimised airside security at airports. By integrating the two systems, airport operators can achieve a very high level of objective security against a wide range of threat scenarios at low total cost of ownership.

Airside violations are a major security problem in air traffic. The scenario of possible threats ranges from disruptions of flight operations by activists to serious threats from terrorist activities. By integrating the innovative Navtech radar systems into Dallmeier's Hemisphere software suite, airport operators can now implement an optimal solution to improve airside security.

Navtech Advanceguard high-resolution sensors automate critical airside tasks such as general Perimeter Protection, Critical Part (CP) Line Monitoring, runway incursion detection, Surface Movement Radar (SMR) and Foreign Object Debris (FOD) detection. Advanceguard provides Hemisphere users with the ability to create multiple virtual zones and alerts operators in advance, enabling proactive threat management. A "friend or foe" integration distinguishes between legitimate and non-legitimate activities, reducing false alarms and increasing operator confidence. The long-range 360° sensors cover large areas with minimal infrastructure, ensuring cost efficiency and effective deployment.

If one or more intruders are detected by the Navtech radar system, the system automatically controls connected Dallmeier or third-party cameras responsible for the area. Hemisphere users can now conduct visual verification of the event and track the intruded persons or objects. Thanks to the bi-directional integration into the Dallmeier Hemisphere software suite, users benefit from an extremely powerful workflow for handling alarms triggered by the Navtech system. Incidents can be managed from either of the systems.

The integrated solution of Navtech Advanceguard and the Dallmeier Hemisphere software suite minimises the risk of human error and increases objective security by combining two superior technologies that complement each other perfectly. End users can rely on many years of experience of both companies providing solutions in airport security. With the high level of user-friendliness, excellent overview and high degree of automation, the integrated solution also requires comparatively low personnel costs. Both manufacturers follow the "Privacy and Security by Design" principles set out in the GDPR and are NDAA-compliant, ensuring maximum security against cyber-threats and compliance towards existing and upcoming legal regulations.

Bosch introduces latest additions to Praesensa line

Bosch has unveiled the latest additions to the Praesensa ecosystem, the PRA-WCP wall control panel and version 2.0 of the Praesensa Public Address and Voice Alarm (PA/VA) system software.

The hardware and software solutions are aimed at enhancing the efficiency and user-friendliness of sound system management for system designers, systems integrators, and professional users. The launches mark a significant step forward in simplifying sound system setup and control.

The Bosch PRA-WCP wall control panel has been designed with user convenience in mind. This compact,

IP-networked wall control panel boasts a 4.5 cm (1.77”) colour TFT display and a single-knob rotary/push encoder. This intuitive design allows personnel to effortlessly adjust the volume of background music and select the audio source for a specific zone.

System designers can configure minimum and maximum volume settings to tailor the sound levels according to the needs of each zone. Furthermore, the support for Unicode characters enables the display of zone names and music channels in various local languages, ensuring a seamless and inclusive user experience.

The PRA-WCP panel simplifies the installation process with its PoE (Power over Ethernet) capability, making it a straightforward addition to both EU and US standard wall-mount boxes. It also comes with interchangeable front covers in white and black, allowing it to seamlessly integrate into a variety of room aesthetics.

For larger installations or areas requiring multiple control points, several PRA-WCP panels can operate within a single zone while maintaining synchronised control settings across each of the TFT displays. Enhanced security is provided through PIN-based access, ensuring that only authorised personnel can control the background music settings.

The introduction of the PRA-WCP wall control panel offers a cost-effective solution for managing background music in both small setups and large-scale projects requiring numerous control panels. This flexibility and efficiency underscore Bosch’s commitment to delivering versatile, high-quality sound system solutions. ■

Bespoke Technologies To Safeguard The Perimeter

Perimeter security or perimeter protection are security solutions that utilise physical and software technology systems to protect from unauthorised access and intrusion, aiming to safeguard people, places, and property.

Perimeter security can include video analytics, video management, access control, fence sensors, buried sensors, above-ground sensors, security management, and physical security measures such as fences, gates, lighting, and barriers. The deployment of a customised perimeter security strategy will depend on the asset(s) to be protected and the type of intrusion risk.

Critical infrastructure facilities, military facilities, and high-risk infrastructures like airports, cell towers, and gas lines have historically employed perimeter security solutions. Today, perimeter security solutions have expanded to residential and commercial industries, including retail, manufacturing, and transportation.

Providing perimeter security for buildings is challenging, and especially so for complex settings such as airports and factories. In this article we look at the various challenges and solutions that can and should be considered to help strengthen your perimeter.

Ensuring the security of your organisation or property's perimeter is important to prevent unauthorised entries and avoid trouble. However, it can be hard to deal with security issues quickly and efficiently. Sometimes, warnings can be missed; at other times, alarms go off when they shouldn't because it is hard to tell if someone's trying to get in or if it's just something harmless.

That's why you need an advanced perimeter protection system that is tailor-made to suit your needs. Using cutting-edge technologies like artificial intelligence (AI) and multi-dimensional sensors, a system that watches over your property like a sharp-eyed guardian! One, which is always alert and ready to catch any potential threats quickly and accurately. With such a system in place, you can know your organisation or property is well-protected from security risks related to perimeter breaches.

Perimeter protection is a 4-stage process

An effective perimeter security system is like a well-coordinated team working together to guard your space from potential threats. This team detects dangers, raises alarms, responds quickly, and gathers evidence, ensuring your environment stays safe.

Detection:

Spotting potential trouble timely and accurately helps. The first and most crucial step in perimeter protection is detection. A reliable system needs to spot threats accurately without sending too many false alarms. With the help of AI advancements, the system has become even more capable of distinguishing between a person, a vehicle, or an animal. This sharp eye for detail ensures the system knows of what it perceives as a real threat or just a harmless occurrence, such as a passer-by. This sets the stage for what happens next.

Alarm:

When something suspicious is detected, people need to be alerted. Accurate detection ensures that alarms are only triggered by real threats. The more precise the detection, the more reliable the alarm.

Response:

When an alarm rings out, a rapid response is needed. A good protection system can automatically kick in right away, like lights flashing or sounds blaring to scare off intruders. Meanwhile, security personnel assess the situation using video camera feeds to decide if more help is needed, such as speaking through two-way audio or sending someone to the spot.

Evidence:

After the incident settles, it's time to review what happened. Video recordings and traceable evidence play crucial roles in post-incident analysis. They help figure out what went wrong, identify any weak spots, and improve safety measures to prevent future incidents.

Technologies to safeguard your perimeter

In this article we limit our discussion to some intelligent video, radar and fibre optic based solutions: To appreciate how intelligent modern solutions have become, imagine a security watchtower that not only sees intrusions but can understand what is happening and act proactively. Traditional video systems often miss incidents until it's too late or have trouble dealing with lots of false alarms.

Hikvision, a global leader in video solutions, applies large model algorithms to see the difference between real threats and harmless events, allowing faster and more effective responses. With DarkFighterS technology, cameras capture clear images even in low light. AcuSense technology enables cameras to proactively light up or sound an alarm to scare away intruders, while a network speaker allows for direct conversations to prevent break-ins. The AI-powered NVR makes it easy to review footage by swiftly identifying human or vehicle targets.

Thermal imaging solutions:

Imagine having night-vision glasses that can see in the dark, fog, or rain; and, because these glasses sense heat, they even work in poor weather and light conditions. Thermal imaging solution provides additional benefits due to its advanced Video Content Analysis (VCA) technology, which has been further improved by the distillation model. This model trains a large model to guide a smaller one in accurately distinguishing between real threats and false alarms. When it spots danger, it can trigger warnings or play recorded messages through speakers to dissuade intruders. Paired with an AI-powered NVR, thermal imaging not only boosts security but also provides clear evidence when needed. It offers comprehensive protection day and night, making it perfectly suited for places such as solar farms, airports, and oil fields.

Radar solutions:

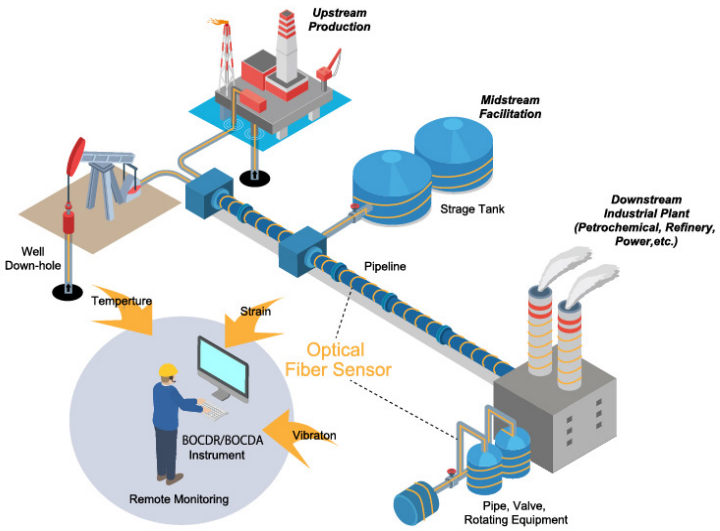
Like thermal imaging, a radar "sees" through darkness, rain, or fog. It can pinpoint an object's exact location, speed, and distance, even without any light visibility. In addition, it offers 3D protection over wide spaces, which is ideal for large, open locations such as open-air mines. Hikvision's radar solution has taken this protection a step further.

By seamlessly combining radar with PTZ cameras, you can build systems that detect threats, trigger alarms, and record key events. With the power of advanced AI, such systems identify intrusions with high levels of accuracy and know exactly what type of target they are dealing with. They operate like a smart, tireless guard standing watch over crucial spaces.

Fibre-optic vibration sensing solutions:

Fibre-optic vibration sensing solutions use Distributed Acoustic Sensing (DAS) technology to precisely detect and respond to environmental changes. These optical fibres cover ultra-long distances, even in harsh or hard-to-reach locations such as underground, fenced, or off-grid areas.

What's more, they are immune to fire, weather, and electromagnetic interference, making them a reliable 24/7 perimeter protection tool. Hikvision pairs this



technology with video systems and network speakers. This creates a powerful system that sends accurate alarms and provides clear visual evidence. This seamless integration ensures that every potential threat is seen and recorded, making perimeter protection more thorough and efficient.

LIDAR based sensing solutions:

LiDAR is an acronym for Light Detection and Ranging. In LiDAR, laser light is sent from a source (transmitter) and reflected from objects in the scene. The reflected light is detected by the system receiver and the time of flight (TOF) is used to develop a distance map of the objects in the scene. This is increasingly being used in perimeter security systems due to its ability to provide highly accurate, real-time 3D mapping and detection capabilities.

REDSCAN Pro Series is a highly accurate outdoor and indoor security sensor using LiDAR technology with advanced detection performance, long-range customisable detection and environment resistance. It provides 50 x 100 m, 190 degree detection allowing it to protect wide areas, with just one sensor. The detection area can be divided in up to 8 independent zones, and for each of them the object target size, sensitivity and output can be customised. It gives great flexibility to adapt the settings depending on the zone's location and level of threat. For instance one detection zone can be set to detect people, while another is set to detect vehicles, or one zone can be set as pre-warning and another as immediate security alert. The REDSCAN Pro's detection range and versatility enables it to achieve what is usually done by multiple sensors. In addition the sensor has a built-in camera which can record on the device, alarm events and save both logs and pre-post event photos and videos, to be used as additional support to review what triggered the alarm and make any adjustments necessary to the settings.

How to choose the right solution

The combination of these different technologies and techniques creates a robust shield around any complex site. However, because every situation and every site is different, choosing the right tools means understanding your specific needs and environment. Imagine, for example, a vast, expansive mining operation stretching out under the cover of night.

Here, advanced radar silently sweeps the area, detecting any movements, no matter how small. Suddenly, it picks up something unusual. In an instant, powerful AI cameras present a visual image, easily identifying potential intruders.

At this point, these smart cameras kick into action, sounding alarms and recording every detail. They don't just capture images; they respond, ensuring the situation is assessed in real-time. This system might even feature speakers that issue warnings, or perhaps engage in conversation to scare off anyone who shouldn't be there.

All the while, security personnel will be watching from a remote location, getting instant alerts and ready to act if necessary. In this particular example, each element of the system—radar, cameras, and speakers—plays a unique role. They work together seamlessly to detect dangers, sound alarms, respond quickly, and record everything that happens. The high-definition video ensures clear visuals but is sensitive to environmental changes. On the other hand, thermal imaging, although lower in definition, excels at target detection in poor lighting or weather conditions, such as at night. Radar and fibre-optic vibration sensing may not provide a visual image, but they are highly reliable for long-range target detection and location under any weather condition or time.

The Benefits of Perimeter Protection

Perimeter is the first line of defence. Perimeter protection acts as a shield, guarding your physical assets against

intrusion and potentially disastrous impacts. It's not just about fencing or surveillance cameras—it's about an all-encompassing, holistic approach to security that integrates advanced technological solutions and vigilant human oversight.

Preemptive Measures: Detect, Deter, Delay

The true strength of perimeter protection lies in its preemptive nature. It aims to detect potential threats, deter would-be intruders, and delay unauthorised attempts to breach the boundaries. This triad of detection, deterrence, and delay can provide precious time, allowing for a swift and effective response to potential intrusions.

Boosted Operational Continuity

Perimeter protection reinforces operational continuity. By thwarting disruptions at the perimeter level, your core operations remain untouched, ensuring the rhythm of your activities continues unaffected. This continuity is critical in maintaining trust with your stakeholders, upholding your reputation, and safeguarding your bottom line.

Enhanced Peace of Mind

An often overlooked advantage of perimeter protection is the peace of mind it brings. The knowledge that your physical assets are well protected from external threats brings a sense of assurance. This peace of mind can foster a safer, more focused work environment conducive to productivity and innovation.

The importance of perimeter protection extends beyond mere security—it shapes the resilience of your operations, your stakeholders' trust, and your employees' well-being. Consider it a defensive measure and a proactive strategy for managing potential risks. ■

With Inputs from Hikvision India, Senstar and Optex

YOUR OPINION MATTERS

At SECURITY UPDATE, we are dedicated to ensuring our content is consistently **Informative**, **Engaging**, and **Captivating**.

We welcome your thoughts, feedback and suggestions.
Write to us at: **info@1stasset.org**

EVENTS CALENDAR

USA
14-16 August 2024
IAFC Fire-Rescue International
Kay Bailey Hutchison Convention Center, Dallas
www.iafc.org/fri

Philippines
25-27 September 2024
ADAS 2024
World Trade Center Metro Manila
www.adas.ph

CANADA
23-24 October 2024
Security Canada Central
Toronto Congress Centre
Toronto
https://securitycanada.com/attend/central

INDIA
22-24 August 2024
FSIE 2024
JIO World Convention Centre, Mumbai
http://www.fsie.in/

Saudi Arabia
01-03 October 2024
Intersec Saudi Arabia
Jeddah Center for Forums & Events
Riyadh
intersec-ksa.ae.messefrankfurt.com/ksa/en.html

Singapore
4-5 November 2024
ASIS Asia Pacific Conference
Singapore Marriott Tang Plaza Hotel
https://asis-singapore.org.sg/asis-asia-pacific-conference-2024/

BANGLADESH
12-14 September 2024
IFSEC Bangladesh
Hall 4 (Naboratri), ICCB
Dhaka
https://ifsecindia.com/bangladesh/

INDIA
05-07 October 2024
India International Security Expo (IISE)
Pragati Maidan,
New Delhi
https://www.indiatradefair.com/

INDIA
14 November 2024
SECURITY TODAY Knowledge Summit
Grand Hyatt- Gurgaon
Delhi NCR
https://knowledgesummit.securitytoday.in/

GERMANY
17-20 September 2024
Security Essen 2024
Messe Essen, Norbertstrasse 2
Essen
www.security-essen.de/impetus_provider/

Bosnia & Herzegovina
09-10 October 2024
ADRIA Security Summit
Convention Centre Hills
Sarajevo
www.adriasecuritysummit.com

USA
19-21 November 2024
ISC East
Javits Center
New York City
https://www.discoverisc.com/east/en-us.html

USA
23-25 September 2024
Global Security Exchange (GSX)
Orange County Convention Center
Orlando
Florida
www.gsx.org

Turkey
9-12 October 2024
ISAF 2024
Istanbul Expo Centre
Istanbul
www.isaffuari.com/en/

Egypt
26-28 November 2024
Egypt Energy 2024
Egypt International Exhibition Centre
Nasr City, Cairo
https://www.egypt-energy.com/en/home.html

UK
24-25 September 2024
International Security Expo 2024
Olympia
London
www.internationalsecurityexpo.com

UK
17 October 2024
Consec 2024
Hilton Hotel, Terminal 5
Heathrow
www.securityconsultants.org.uk/events/consec

UK
2-4 December 2024
IFSEC International
ExCeL London
https://www.ifsecglobal.com/ifsec-international-security-event/

SECURITY TODAY®

SECURITY Update
CREATING BUSINESS OPPORTUNITIES

PRESENT

TOP INDIAN WOMEN INFLUENCERS IN SECURITY

Stay Tuned

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

In order to recognise and honour the accomplishments, value and contributions of women in this vital sector of the economy, SECURITY TODAY & SECURITY UPDATE in association with Infosec Girls and WISECRA announce the "Top Indian Women Influencers in Security" recognition for the year 2024.

In 2020, this accolade was developed to help recognise women in security in India who made significant contributions in shaping the industry and shaped the path for future generations of professionals. 20 torch bearers were recognised from 272 nominations received in a virtual ceremony by the nation's 1st, most famous & iconic lady IPS officer, Her Excellency, Dr. Kiran Bedi, the then Hon'ble Lieutenant Governor of Puducherry. Distinguished senior people from different sectors were carefully chosen as 'members of the jury' for this event.

Visit: https://tiwiis.securitytoday.in

PAST SPONSORS

SIS Group Enterprises · PRAMA MADE FOR INDIA · MADE BY INDIA · MADE IN INDIA · genpact

PAST SUPPORTING PARTNERS

InfosecGirls · WISECRA WOMEN IN SECURITY & RESILIENCE ALLIANCE · ASIS INTERNATIONAL Stronger Together Ahmedabad, Bangalore, Chennai, Hyderabad, Mumbai, New Delhi & Pune Chapters · IISSM · PSP PUNE SECURITY PROFESSIONALS · ISRM INSTITUTE OF STRATEGIC RISK MANAGEMENT · WiCyS women in cybersecurity

SECURITY UPDATE Postal Registration No. GRG/32/2024-26
Published on 28th day of every month

SECURITY UPDATE is registered with
The Registrar of Newspapers for India, No. HARENG/2011/39714

PRAMA®
MADE FOR INDIA - MADE BY INDIA - MADE IN INDIA

MAKING EVERY JOURNEY SAFER & CONVENIENT

PRAMA Intelligent traffic solution offers dedicated, high-performance cameras for event capture, reliable video terminals for event recording and a centralized video management platform – unifying all the ITS devices and deliver service-extensible applications.

/PramaIndiaOfficial

भारत में बना, भारत का अपना सर्वेलेंस ब्रांड

/PramaIndiaOfficial

PRAMA INDIA PRIVATE LIMITED
Office No. 103, F. P. No. 765, Fly Edge,
TPS III Junction of S. V. Road,
Near Kora Kendra, Borivali West,
Mumbai - 400 092, Maharashtra, India.
Board No.: +91-22-6896 5500
Web: www.pramaindia.in

Sales: +91 22-6896 5533 | **E mail:** sales@pramaindia.in
Toll Free: 18002091234
Tech Support: +91 22-6896 5555 | **Whatsapp:** +91 9076305555 | **E mail:** techsupport@pramaindia.in
Repair Service: +91 22-6896 5544 | **Whatsapp:** +91 9076005544 | **E mail:** service@pramaindia.in