

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. 06 | June 2024 | Price ₹ 150 | Pages 52

5G TECHNOLOGY: Transforming Security with Speed and Precision

Staying Safe on Public Wi-Fi:
Tips & Best Practices for Secure Browsing

Why Next-Gen Data Intelligence Platforms
are a Game Changer for Businesses?

Next-Gen Fire Detection Systems:
Advancements & Applications

Differentiating Between Facial Authentication
and Facial Recognition



BEST SECURITY INDUSTRY PUBLICATION



**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.**

HIKVISION®

See Far, Go Further

REDEFINE SECURITY STANDARDS WITH HIKVISION

HIKVISION

Step into the future of security with Hikvision, where we redefine the standards through state-of-the-art technology, superior quality, and unwavering commitment to safeguarding what matters to you the most.

 /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



5G TECHNOLOGY'S APPLICATION IN SECURITY

COVER
STORY

16

5G technology has seen a rapid roll out all over India in the last few years. For an average cellular telephony user 5G can offer low latency of under 5 milliseconds! Lower latency brings advancements in other areas, such as high-speed internet and faster download speeds. Users have been watching high definition movies smoothly on Netflix on their mobile phones, just because the 5G tech is in place. This technology is impacting physical security systems significantly. Read on to see how...

WISE THOUGHTS 8

The Evolving Role of Access Control in Healthcare

Daniel May, Director at Consort, highlights the importance of access control systems in healthcare for managing security challenges like high foot traffic and protecting sensitive data. Modern systems, including electronic credentials and biometric scanners, enhance patient safety and comply with regulations. Decision-makers must ensure these systems are scalable and adaptable to evolving needs, requiring careful implementation and collaboration. As technology advances, healthcare facilities must stay informed to maintain security and efficiency.



10 INDUSTRY UPDATE

22 CASE STUDIES

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.

26 SU GYAN



Surveying and Designing Physical Access Control Systems

This article highlights the importance of Physical Access Control Systems (PACS) in securing business assets. It stresses the need for thorough site surveys and planning to understand current systems and identify security needs.

30 TECH TALK



Staying Safe on Public Wi-Fi: Tips and Best Practices for Secure Browsing

This article outlines essential tips for staying safe on public Wi-Fi, which is vulnerable to threats like fake networks, man-in-the-middle attacks, eavesdropping, and malware. It also stresses the importance of educating employees on these practices to ensure secure remote work.

36 PRODUCTS UPDATE

50 EVENTS CALENDAR

28 BIZ BUZZ

- Why Next-Gen Data Intelligence Platforms are a Game Changer for Businesses?
- Differentiating Between Facial Authentication & Facial Recognition

32 FIRE CHAT



Next-Gen Fire Detection Systems: Advancements and Applications

This article discusses the advancements in next-gen fire detection systems, including improved sensors, IoT integration, and real-time analytics. It highlights how these technologies enhance accuracy, reduce false alarms, and provide proactive fire risk management across various industries, emphasizing their role in improving overall fire safety.

- Why Employees Need Fire Safety Training At The Workplace

44 INDUSTRY SPOTLIGHT



In The New World, Access Control Takes a Whole New Meaning

Explore the evolving landscape of access control, its integration with IT and cybersecurity through advanced technologies like IAM, MFA, and zero trust. Understand how modern access control practices are crucial for managing security risks and meeting regulatory requirements.

EDITOR'S NOTE



Dear Reader,

Many times we have all seen a hype being created about a technology or a product by marketing teams by creating compelling content which makes us believe them to be the right fit for us. We start believing in those technologies and products as if they are the panacea for all our security risks and problems. For any Security Systems Designer / Consultant / Systems Integrator, choosing the right technologies is critical to the success of any project and in the interest of the end user. It's not just about selecting the newest or buzzworthy tools and gizmos; rather, it's about ensuring that the technical stack aligns with the project's as well as with the overall business goals of your clients and scales with them.

Assessing the risk and then the technical requirements to plug that with tech for your project is an important step when choosing the right technologies. Remember to consider the core functionalities and features that you require carefully. This involves breaking down the product or technology and understanding its components, both in terms of functional and non-functional requirements.

Another critical consideration is scalability. Most security system projects require an easily scalable technical stack that allows for expansion while avoiding the need for substantial development rework, excessive complexity or skyrocketing costs. By evaluating performance, costs and latency requirements before selecting

technologies, you narrow your options down to the ones that best fit the present and future technology goals.


Overall, taking the time to assess technical requirements beyond the common denominators saves significant costs long-term. Greenfield security projects can harness feedback gained from users, competitors and emerging trends and translate them into actionable practical developments, hence entrenching the culture of seeing scalability not as an eventuality but as a channel or marker of success.

Researching and shortlisting technologies are essential when evaluating technology options. Exploring different products available in the market is recommended, alongside assessing compatibility with your development team's expertise to be able to customise it to your needs. You should also evaluate the ease of integration with existing systems, availability of APIs and developer resources.

In order to make informed decisions, have a solid understanding of the requirements and available options and align them in line with project and business goals, the selection process becomes easier.


In this issue's cover story we have featured 5G technology and examined its pros and cons, and In our next issue of SECURITY UPDATE we shall discuss key criteria for evaluating and making informed decisions when opting to purchase for new technologies.

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


G B Singh
Group Editor

 gbsingh@1stasset.org

 [@gbsingh9](https://www.linkedin.com/in/gbsingh9)

 [@EditorGB](https://twitter.com/EditorGB)

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

Printed, published and edited by G B Singh on behalf of 1st Academy of Security Science Education & Training Pvt. Ltd. Printed at Ask Advertising Aids Pvt. Ltd. 88 DSIDC Sheds, Okhla Indl. Area Ph-I, New Delhi 110020 Published at "Security House", 24-B, Udyog Vihar-V, Gurugram 122016, Haryana, INDIA.

info@1stasset.org

POWER UP YOUR SECURITY BRAND OUTREACH



SECURITY SOLUTIONS FOR ALL

- Commercial Establishments
- Defence & Homeland Security
- Industrial Security
- City Surveillance
- Public Infrastructure
- Banking & Finance
- Travel & Hospitality Sector
- Transportation Sector
- Retail Establishments
- Education Establishments
- Healthcare Sector
- Home Security

MUST ATTEND FOR BELOW PROFILES

- CSOs, Procurement, Purchase, Admin, Facilities, IT, Consultants
- Heads or Managers Responsible for Plant, Operation, Floor
- Channel Community – Dealers, Distributors, Retailers, Resellers, System Integrators, Solution Providers, Installers

VISITOR REGISTRATION



Premier Plus Partners



BOOK YOUR SPACE



Premier Partners



Exhibit Partners



Knowledge Partner



Supporting Associations



Media Partners



Media Partner



CONTACTS:- PROJECT HEAD: Rajeev Jain | M: +91 99877 90776 | E: rajeev.jain@informa.com
 NEW DELHI: Sanjay Khandelwal | M: +91 98117 64515 | E: sanjay.khandelwal@informa.com
 NEW DELHI: Nivedita Adhikary | M: +91 99537 03803 | E: nivedita.adhikary@informa.com
 BENGALURU: Vaishali Jain | M: +91 99838 71404 | E: vaishali.jain@informa.com
FOR SPEAKER OPPORTUNITIES: ADEESH SHARMA | M: +91 98103 07335 | E: adeesh.sharma@informa.com
FOR MARKETING & ALLIANCES: DEEKSHA SHARMA | M: +91 92057 41641 | E: deeksha.sharma@informa.com

The Evolving Role Of Access Control In Healthcare



Daniel May

Daniel May is the Director of Consort, a manufacturer and supplier of architectural hardware to the construction industry. He reviews the integration of access control systems in healthcare settings, outlining the benefits and key considerations decision-makers must make throughout product specifications.

From patient safety and traversal to the protection of sensitive data and pharmaceuticals, healthcare environments are faced with several operational challenges. And where security remains at the forefront of decision-making, modern access control systems may often hold the answers.

Hospitals in particular have developed into multi-faceted spaces that house hundreds to thousands of patients, staff and visitors at any one time. In England for example, research has found in the three months leading to June 2023, an average of 44,626 people visited major hospital A&E departments each day, with over 16 million attendances typically recorded over the course of a year-

not to mention an additional nine million logged at other minor units.

For any building, this level of sustained footfall can invite severe security tests. With that, the need to deploy effective physical security systems in healthcare is clear. And so, as access control continues to become more readily adopted and new products enter the market, decision-makers are reminded to consider the requirements of their building, ensuring they select the solutions most suited to their settings and budget.

Patient safety will always remain the top priority in healthcare settings, and where matters of health and social care come into question, a diverse set of



professional regulatory bodies are tasked with setting and maintaining high standards. When it comes to healthcare premises specifically, patient security and perimeter security often come hand in hand and are amongst the most pressing of challenges that decision-makers must face.

To help address operational planning and potential design concerns in the NHS, the Health Building Note (HBN), provides general design guidance for healthcare buildings under HBN 00-01-citing the use of access control measures as a way of maintaining security and protecting the safety of patients, staff and visitors.

Hospital buildings, for example, must control varied levels of access for a number of operational and security purposes. Routine scenarios exist where vulnerable patients are under monitoring and thus refrained from exiting the premises for their own safety, while at the same time, permitted staff must be able to reach their patients and medicines when required.

For this, the use of access control is key. Equally, access credentials can also help management teams keep track of those who may be entering or exiting rooms with equipment and pharmaceutical supplies, deterring any unwanted visitors and opportunists in the process.

On a similar note, regulations have set a minimum standard for how personal data should be stored and managed in healthcare environments, giving decision-makers an added responsibility to regulate staff-controlled areas with patient medical records. While instances of personal data breaches are rare, healthcare facilities and professionals are at legal risk should confidential data be found misused or missing.

As such, the incorporation of access control systems has become essential in keeping data storage areas secure, with intuitive online systems capable of permitting access to staff with the correct credentials while simultaneously tracking who has requested clearance at digital entry points.

To function effectively, healthcare facilities must always be perceived as safe places by the people who reside within them, and as HBN guidance implies, a unified physical security system can help address key safety and security concerns while enhancing patient and staff experience. Opportunely, access control systems are more accessible and adaptable than ever and combine several technologies such as mechanical locks and automatic doors with electronic access credentials in the form of smartphone apps, badge readers and biometric scanners.

By integrating these systems into the building's existing infrastructure, healthcare professionals are better equipped to control the sheer volume of people entering and exiting the premises without impairing the general flow of movement and coordination around the facility.

Despite the clear benefits offered to healthcare facilities, there are a number of considerations to be mindful of when choosing an access control solution. Poorly implemented systems can have an adverse effect on security and functionality - quickly costing healthcare organisations time and budget to rectify and replace the inadequate products that don't meet the building's requirements.

For that reason, decision-makers and design teams are reminded that there is no single solution that fits all healthcare buildings. As such, it's crucial for decision-makers to understand the systems that are being put in place throughout each of the touchpoints in their facility. Clear collaboration is required during periods of specification, where together, teams can ensure the selected product works on all angles, from meeting fire safety and sustainability standards to aesthetics and scalability.

Frequently overlooked, scalability is a key area that decision-makers must review when selecting access control systems. Such is their diverse nature; healthcare facilities can often change and develop as years go by, and by selecting a system that facilitates growth, such as a cloud-based solution-security and efficiency is long-established.

While modern access control products are known for seamless integration, there are some systems that may restrict the ability to use different vendors throughout the remainder of the building's infrastructure. This, in effect, causes a monopolisation of products throughout the estate, which can have an adverse effect on growth by increasing costs and reducing the levels of service associated with the security system already in place.

A scalable and reliable access control system will continue to improve security and safety by adapting to a building's new requirements-and all while having minimal impact on its operational network.

And so, while technology will no doubt continue to influence and transform the access control market, healthcare facilities and their professionals must continue to remain educated on their own systems, ensuring they have the best options in place to keep their patients, staff and visitors safe and secure for years to come. ■

OPTEX celebrates 45th anniversary of continued sensing innovation

Pioneering sensor manufacturer OPTEX celebrates its 45th anniversary, recognized for its commitment to intelligent sensing and detection technologies. Founded on 25 May 1979 in Kyoto, Japan, by Toru Kobayashi and colleagues, OPTEX has grown into a global leader with nearly 2,000 employees across 42 companies worldwide. Its EMEA headquarters are in the UK and the Netherlands, with offices in over 15 countries.

OPTEX introduced the world's first far infrared automatic door sensor and the first wireless outdoor security sensors. Its REDSCAN sensors revolutionized intrusion detection using LiDAR technology.

“OPTEX never stands still and continues to anticipate and innovate to meet the ever-changing needs of the market and our customers,” says CEO Toru Kamimura.



He credits the company's success to its employees, partners, and customers, emphasizing the ongoing focus on quality, reliability, and investment in R&D. “The journey continues as we explore new technologies and the power of sensor data to create a safe, secure, and comfortable society.”

Joe Levy Appointed CEO of Sophos



Sophos, a global leader of innovative security solutions for defeating cyberattacks, has announced that Joe Levy is now chief executive officer (CEO) of the company. To drive a critical role in the execution of his strategy to shape the future of Sophos, Levy has named Jim

Dildine Sophos' new chief financial officer (CFO) and a member of his senior management team.

Levy is a nearly 30-year veteran of innovating and leading cybersecurity product development, services and companies. During his nine-year tenure at Sophos, Levy drove the transformation of Sophos from a product-only vendor into the global cybersecurity giant it is today, including an incident response team and managed detection and response (MDR) service that defends more than 21,000 organisations worldwide.

As CEO, Levy plans to expand Sophos' already strong customer base in the midmarket, which includes nearly 600,000 customers worldwide and generates more than \$1.2 billion in annual revenue. As a leading provider of cybersecurity solutions for the midmarket, Sophos has a unique ability to further scale its business and the business of its partners by helping organisations in dire need of basic and expanded defences against opportunistic and targeted cyberattacks.

These organisations include the critical substrate, small- to mid-sized organisations that comprise the machines of the world's economy and are just as

susceptible to cyberattacks as major corporations. In fact, the critical substrate, including smaller organisations within the classic 16 critical infrastructure verticals, are prime attacker targets, as evidenced by Sophos' Active Adversary report and 2024 Threat Report. Both intelligence reports reveal how attackers are repeatedly abusing exposed Remote Desktop Protocol (RDP) access at mid market organisations, as well as going after them for data theft, spying, ransomware payoffs, or supply chain attacks to gain entry to bigger prey.

“When midmarket organisations – the global critical substrate – are paralyzed due to ransomware or other cyberattacks, business activities linked in our supply chains also stagnate, slowing our economy down. Operations of all sizes and shapes suffer collateral damage when dependencies in their supply chains are attacked. This can be devastating in often unpredictable ways because of the increasing complexity of how the modern industrialised global economy works,” said Levy.

“Our goal is to help more organisations in the midmarket – the estimated 99% of organisations that are below the cybersecurity poverty line – be better at detecting and disrupting inevitable cyberattacks. Our envisioned approach to achieving this is to work with MSPs and channel partners that can scale alongside us with our innovative critical cross domain technologies – endpoint, network, email, and cloud security – and managed services that they can resell and co-deliver. Cyberattacks against the midmarket could severely impact the world's ability to function; they are relatively under-protected compared to the 1%, and Sophos is on a mission to change that.”



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.

IDEMIA Secure Transactions partners with IIT Hyderabad on post-quantum cryptography

IDEMIA Secure Transactions (IST), a division of IDEMIA Group, announces a strategic research partnership with the Indian Institute of Technology, Hyderabad (IIT Hyderabad) on Post Quantum Cryptography.

The objective of the partnership will be to strengthen privacy frameworks against quantum threats, with a specific focus on designing post-quantum schemes based on lattices and to create post-quantum cryptography solutions that ultimately ensure the long-term security of products. As part of this partnership project, IST will sponsor PhD scholars over a four-year period.

IST's active involvement in advancing post-quantum cryptography efforts in India includes collaborations with key industry and government bodies. The company actively contributes to standardisation bodies and organisations in India, including TSDSI, TEC, and CDOT, showcasing its commitment to advancing cryptographic research in the region.

IDEMIA Secure Transactions is committed to fostering innovation globally, having established

multiple post-quantum research partnerships with European universities. These collaborations aim to invest in the future and further technological advancements in cryptographic research.

"We are excited to embark on this journey with IDEMIA in advancing post-quantum research. IDEMIA



Secure Transactions' unparalleled expertise and commitment to innovation align seamlessly with our vision. Together, we look forward to pioneering groundbreaking solutions that will shape the future of cryptographic systems and safeguard transactions worldwide," said Dr. Mudrika Khandelwal, Dean, Alumni and Corporate Relations, at IIT Hyderabad."

"We are very excited to launch this academic partnership with IIT Hyderabad. At IDEMIA

Secure Transactions, we are committed to advancing technology and safeguarding information in the post-quantum era. By nurturing the next generation of scholars and engineers and fostering collaborations with esteemed institutions like IIT Hyderabad, we're spearheading the evolution towards a secure digital future," said Paul Dischamp, Cryptography & Security Lab Director R&D at IDEMIA Secure Transactions.

AddSecure Wins European Inspiring Workplace Award

Addsecure, a leading European provider of secure IoT connectivity, has been named one of the top 25 winners of the Inspiring Workplaces Europe 2024 award. The company also received special recognition for "Inspiring Wellbeing" and "Inspiring Employee Experience."

The Inspiring Workplace Awards require entrants to demonstrate their investment in six key categories: Culture and Purpose, Leadership, Wellbeing, Inclusion, Employee Voice, and Employee Experience. Judges praised Addsecure's flexible working options and focus on employee wellbeing.

"Being named an Inspiring Workplaces winner once again is truly humbling. This award, along with the special recognitions, is a testament to our investment in our employees and our dedication to making Addsecure a great place to work," said Liljana Vall, Chief People &

Culture Officer at Addsecure.

Matt Manners, Founder of The Inspiring Workplaces Group, congratulated Addsecure and the other top winners, emphasizing the importance of a people-first approach: "Focusing on personal development and caring for employees will drive performance and protect their wellbeing, leading to higher performing teams and a competitive edge. Being people-first isn't a nice to have, it's a business imperative!"



acre security rebrands products to acre Intrusion

acre security, a global provider of state-of-the-art security systems, has announced an initiative as part of its ongoing effort to unify and simplify its product offerings.

According to the company, the rebranding of the SPC intruder detection system to acre Intrusion marks a strategic alignment within the company's streamlined branding framework. This approach also includes the acre Access Control and acre Visitor Management solutions, bringing a cohesive identity to the entire portfolio.

"Since its inception, acre has been dedicated to transforming security from a complex challenge into a seamless aspect of our clients' daily lives. The transition to acre Intrusion highlights our commitment to a more modern branding structure that mirrors this mission," says Mark Roberts, CMO, acre security. "This strategic

effort also supports the broader acre security solutions portfolio and ensures that we continue to meet the high expectations of performance and reliability that our customers rely on. Also, it is important to reinforce



that this initiative is strictly about the branding and positioning of our intrusion portfolio. We continue to offer the same comprehensive intrusion portfolio, now unified under the acre banner."

acre Security emphasises the move to a new name better reflects its holistic approach to security,

underscoring the strength and centralization of the company's entire portfolio. The naming strategy to acre Intrusion the company asserts, highlights that acre solutions are both robust and adaptable, tailored to meet the specific needs of customers while offering peace of mind through acre's demonstrated expertise and experience.

Additionally, the company suggests that in a market that prizes simplicity and trust, acre Intrusion is designed to be user-friendly and straightforward. The new naming convention reflects this, simplifying the identification of acre's solutions and demonstrating a commitment to ease of use. From the acre Intrusion Gen1 and EVO series panels to acre Intrusion Connect, each component is crafted for seamless integration while maintaining the features and functionality that these technologies were originally built upon.

BSIA appoints new Association Chair in the UK



The BSIA has appointed Martin Watson as its new Chair at the Association's Spring Forum and Annual General Meeting. With 40 years of experience in fire, security, and engineering, Martin is currently Industry Liaison Director for Mitie Fire & Security Systems and Chair of the Fire Industry Association. He takes over from Simon Banks, the BSIA's longest-serving Chairman,

who led significant changes over six years.

Mike Reddington, BSIA Chief Executive, thanked Simon Banks for his leadership: "Simon's guidance helped us establish the BSIA as the recognized voice of the professional security industry. We look forward to working with Martin Watson to build on these strong foundations."

Simon Banks reflected on his tenure: "I'm proud of our achievements, including the Special Project Fund investing £400k into member projects. Skills for Security has transformed from a loss to a profitable enterprise with 85 staff and 1,000 apprentices. I wish the BSIA continued success."

Martin Watson said, "I'm delighted to take over as Chair. Thanks to Simon, the BSIA team, the Board, and our members for their hard work. We have much to do in this ever-changing industry, and I look forward to addressing both opportunities and challenges."

Sparsh CCTV invests Rs 300 crores for Capacity expansion



Sparsh CCTV, a leading manufacturer of video surveillance and security solutions, announced a strategic investment of Rs. 300 crores over the next five years to enhance capacity for tapping new opportunities emerging from the Government of India's push to use 'Made in India' surveillance equipment. This investment will allow Sparsh CCTV to scale up their operations, along with strengthening their position as a market leader.

Recently, the Ministry of Electronics and Information Technology has implied Essential Requirements for CCTV procurement mandating Cyber security certification and trusted value chain (defined as per Land Border clause of GFR) thus enabling preference to domestic manufacturers in government procurements.

This will ensure restrictions to the Chinese CCTV companies that have

been dominating the Indian market. Sparsh CCTV has been aggressively working on raising awareness on cybersecure video surveillance and on market strategies to capture major market share over the next two-three years.

Sanjeev Sehgal, Managing Director, Sparsh CCTV said "We are setting up an anchor unit in the Electronic Manufacturing Cluster 2.0 in Kashipur, Uttarakhand with a production capacity of 1 million units per month. This facility will be fully backward integrated with in-house capabilities of tool room, plastic moulding, die-casting, sheet metal workshop and cable connectors manufacturing. In Haridwar last year, we opened up a new manufacturing facility upgrading our production capacity to 2.5 million units per year from 1 million units previously. We aim to be the Factory for the World in the surveillance space."

Recently, the company's equipment were installed in tunnels between, Baramulla Rail link project, Banihal-Sangaldan Railway line in Jammu and Kashmir, Ayodhya Dham railway station, Tunnels (T-6, T-9, T[1]10, T-11 & T-12) between KM 39 to 61 on Katra-Dharam section of Udhampur-Srinagar and has bagged All Zonal Railway and Divisional Headquarters. Sparsh CCTV has been at the technological forefront and has introduced new features in the global video surveillance arena with a presence in 10 countries.

Honeywell closes Carrier deal, readies market push in cloud access control

Honeywell has completed its \$4.9 billion acquisition of Carrier Global Corporation's Global Access Solutions (GAS) business, adding 1,200 employees and positioning itself as a leading provider of security solutions. This acquisition aligns with Honeywell's focus on automation and cloud-based services.

In October, Honeywell integrated three brands—LenelS2, Onity, and Supra—into its portfolio to enhance its software capabilities. GAS is expected to bolster Honeywell's Building Automation business, offering high-value products critical for buildings and generating over \$1 billion in annual sales when combined with Honeywell's existing security portfolio.

Honeywell CEO Vimal Kapur stated, "As the world's security needs evolve from a focus on protecting people to protecting both people and critical assets, we see strong growth prospects for our Access Solutions acquisition." He emphasized that the acquisition would accelerate growth and margin expansion.

Kumar Sokka, President and General Manager of LenelS2, noted during PSA TEC 2024 that Honeywell's \$25 billion investment aims to drive growth in building automation, energy efficiency, and aerospace. Sokka highlighted the potential for leveraging data from combined systems in buildings, such as fire, lighting, HVAC, and access control, to solve various problems and enhance sustainability and efficiency.

We'd Love to Hear From You!

Share your 'Security' insights with us! Email your articles, case studies, or press releases in an MS Word file, along with images. We look forward to featuring your work!

Submit your work at- info@1stasset.org



DOES SECURITY REALLY MATTER?

OUR PAN-INDIA SUBSCRIBERS SAY

YES IT DOES!

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



5G Technology's Application In Security

5G technology has seen a rapid roll out all over India in the last few years. For an average cellular telephony user 5G can offer low latency of under 5 milliseconds! Lower latency brings advancements in other areas, such as high-speed internet and faster download speeds. Users have been watching high definition movies smoothly on Netflix on their mobile phones, just because the 5G tech is in place. This technology is impacting physical security systems significantly. Read on to see how...

The advent of 5G technology continues to revolutionise security and safety systems by providing faster, more reliable, and low-latency communication. Enhanced connectivity enables real-time surveillance, rapid response to threats, and integration of advanced technologies like AI and IoT in security infrastructure. It supports the deployment of smart cities, where interconnected sensors and devices can efficiently monitor and manage public safety. However, 5G also introduces new cybersecurity challenges, and

other issues necessitating a careful evaluation of its adoption. Overall, 5G's impact on security systems is transformative, promising greater efficiency and effectiveness while demanding heightened vigilance in cybersecurity.

While older 3G and 4G networks are still in use, they could not support operations that depended on large volumes of data moving back and forth across networks. In physical security, that often means high-definition video and large data sets collected by Internet of Things



(IoT) sensors. 5G technology promises to enhance physical security operations by providing the network transfer speeds required to support sophisticated modern 5G security applications.

While discussing 5G technology we often speak of latency and bandwidth, let's examine what they actually are:

Latency refers to the time it takes for data to travel from its source to its destination across a network. Think of it as the maximum safe speed limit on a highway. In security systems, lower latency means minimising the time between detecting a security event and receiving the alert, allowing quicker response to potential threats or incidents.

On the other hand, bandwidth is the maximum rate at which data can be transferred over a network within a given amount of time, usually measured in megabits per second (Mbps) or gigabits per second (Gbps). Higher bandwidth allows more data to flow across a network. In our highway metaphor, greater bandwidth would mean more lanes open for traffic. For security systems, higher bandwidth means supporting high-definition video streams, large volumes of sensor data, and other information-intensive tasks without network bottlenecks or delays.

Now let's look at some key benefits of 5G for physical security:

Speed: With greater bandwidth and lower latency, 5G's most significant advantage is its ability to deliver data instantly. For security systems, this means quicker alerts and notifications, enabling security personnel to respond rapidly to routine events and emergencies.

Connectivity: 5G's ability to connect a wide array of devices within a network enhances various security measures, such as perimeter security and access control. This interconnectedness ensures a comprehensive coverage area, minimising blind spots and strengthening an organisation's overall readiness.

Real-time Analytics: Leveraging AI and machine learning, real-time video analytics can identify potential security threats from large data sets, like transaction logs of asset and visitor management systems or video surveillance feeds. 5G's low latency and higher bandwidth make it possible to analyse new events as your different physical security systems capture them. Your personnel get actionable intelligence faster and can make decisions faster.

Remote monitoring: With 5G, security professionals

can monitor multiple locations from a centralised command centre in real time. This capability ensures swift responses to incidents, even when you don't have boots on the ground.

Integrating your security systems with 5G technology can significantly enhance your team's data collection abilities. The key to harnessing the full potential of connecting vast networks of sensors lies in adopting open architecture standards where all 5G security applications can communicate seamlessly. Such a platform centralises data from diverse sensor types and systems into one unified solution.

For example, initially, you might integrate your video surveillance, access control, and intrusion detection systems into a single platform. This consolidation offers your security team a more comprehensive view of your environment, facilitating swift responses to threats or incidents. Then, as a second stage, you might incorporate additional systems like intercoms, building management, point-of-sale systems, or automatic number plate recognition (ANPR) through your surveillance network to enrich the data pool. This integrated approach enhances your team's situational awareness and enables greater automation through event-triggered actions and reporting.

Built-in analytics tools and the emergence of a new generation of artificial intelligence (AI)- driven capabilities herald new frontiers for connected physical security. These new possibilities only exist because of the foundation laid by 5G connectivity. AI tools can perform tasks ranging from motion detection and traffic flow analysis to people counting and crowd density estimation.

An asset management system might trigger alerts when devices report a faulty code and automatically dispatch technicians to retrieve the device. Meanwhile, the local system can lock down the faulty stored device so it doesn't accidentally end up back in circulation. These offer valuable insights into both security and business operations.

Beyond merely alerting potential issues, these advanced AI capabilities also help filter out false alarms, allowing your team to concentrate on critical situations. Furthermore, based on the scenario, an AI-enhanced platform can provide step-by-step guidance from initial response to resolution, empowering your team to manage any situation confidently. This approach streamlines security operations and leverages data to drive informed business decisions.

Challenges of 5G in Physical Security Systems

While the transition to 5G offers numerous benefits, it also presents a few challenges that organisations looking to deploy new wireless systems should be aware of.



Cybersecurity risks: More connectivity creates more attack surfaces for hackers. The increased digital infrastructure deployed to make 5G security applications work raises concerns about the potential for cyberattacks.

Protecting 5G-connected devices against unauthorised access and data breaches requires physical security teams to work more closely with their network security counterparts to ensure proper protections are in place. This is called security convergence. While the concept has been around for decades, 5G networks and IoT deployments have brought them in the cross hairs of many security teams.

Infrastructure upgrades: Adopting 5G technology necessitates upgrading existing security infrastructure to be 5G compatible, which can involve significant investment. External 5G infrastructure may still be rare in some rural parts. Depending on where your work sites are located, you may be able to deploy 5G internally, but you will still be restricted to lower cellular network speeds externally.

While 5G applications to physical security may sound good, Jim McHale, managing director of the Stockholm-based market research firm Memoori feels everything may not be as hunky dory as this may

sound. He opines:

“In the physical security sector, 5G is being hailed as a significant change for video surveillance and other security applications. However, our latest research suggests that 5G might not be the disruptive physical security technology that many suggest,” he says.

“Many analysts and industry observers contend that the proliferation of 5G will have a major impact on the video security market, arguing that in the years to come, we will see the proliferation of large networks of wireless cameras streaming ultra-high-definition video in real-time,” he said.

“Back in 2019, Gartner predicted that outdoor surveillance cameras would become the largest market for 5G IoT solutions by 2022, with 11.2 million units installed. At Memoori, we do not share this view. In fact, as of 2022, we see very little momentum or market appetite from either camera manufacturers, integrators, or end users for the deployment of 5G wireless surveillance at scale,” said McHale.

As the 5G hype around video surveillance suggests, all this makes 5G much better than 4G for wireless connectivity, but that doesn't necessarily make it better than wired solutions in the majority of physical security scenarios.

The upstep in data transmission speeds provided by 5G is often overplayed but significant nonetheless, approximately 1,000 times faster than 4G based on realistic projections. Latency is also expected to improve, falling from around 50-100 milliseconds with current 4G technology, to a near-instantaneous 1-4 milliseconds with 5G. And, 5G also has a much greater capacity than the previous generations of the technology, able to accommodate thousands more IoT devices per square mile.

As the 5G hype around video surveillance suggests, all this makes 5G much better than 4G for wireless connectivity, but that doesn't necessarily make it better than wired solutions in the majority of physical security scenarios.

It is a fact that most areas that require high-definition video surveillance are already well serviced by the fundamental wired communications infrastructure required to enable UHD video streaming from surveillance cameras. The 5G technology may be able

to support wireless transmission of 4k Video, but would it really be cost-effective to do this? There is a cost attached to 5G.

Although prices are rationalising 5G bandwidth is still relatively expensive as compared to wired forms of data transmission, and UHD video is extremely data hungry. With multiple cameras installed, the costs would rack up rapidly, and additional spending on 5G routers would be required to support such deployments. Therefore, we see end-users willing or able to justify the additional cost implications of running their video security solutions wirelessly over 5G.

Coaxial, optical, and twisted pair cables all present a better business case for video surveillance connectivity than 5G when you factor in cost at scale. Furthermore, 5G signals consume significantly more power than 4G signals, which could have severe knock-on effects on battery life and the thermal management of the device, as well as its overall lifespan. The IoT market has typically demanded progressively smaller and lower-power devices and it seems very unlikely that the market would reverse these trends to accommodate 5G considering the practicality of wired alternatives in the vast majority of use cases.

“Wireless bandwidth is now more than sufficient for most surveillance applications, and prices have dropped significantly over the last decade. Wired high-speed broadband has improved and is available in many video surveillance locations. These improvements

should have boosted wireless growth, but they haven’t really,” explains McHale.

Power over Ethernet (PoE) networks have become a cost-effective and practical alternative to many use cases where wireless may have seen adoption, negating many of the benefits listed above. Despite offering new applications and a more robust solution, wireless is only slowly increasing its Video Surveillance market share.”

The wireless video market for home security applications has grown rapidly in recent years, and much of the technology designed for the home could be rebranded for the commercial building market or repurposed by commercial building managers, but that isn’t really happening either.

In the short to medium term, 5G-enabled video surveillance seems more likely to only succeed in specific niches such as large cities. The installation of surveillance equipment in remote or hazardous locations, for example, in these less profitable remote areas 5G is likely to be rolled out last.

Surveillance systems in smart cities may also find significant advantages from 5G for traffic or crowd management, for example, but most of these scenarios will also offer wired or wearable alternatives. The temporary installation of 5G devices on construction sites is showing more promise, however, and most longer-term visions of smart cities served by intelligent drone networks also depend on 5G and 6G connectivity.

5G Cameras Explained

5G security cameras harness the high-speed and low-latency capabilities of advanced network technology, offering unparalleled surveillance efficiency and quality. But do you know what 5G security cameras are? Are they the next generation of 4G cellular security cameras?

The misconception surrounding 5G security cameras often arises from the assumption that they rely on 5G cellular signals. In actuality, these cameras predominantly utilise 5GHz Wi-Fi signals rather than cellular 5G networks. They are not cellular security cameras, but fall under the category of Wi-Fi cameras, leveraging the higher frequency band of 5GHz for data transmission, which offers faster speeds and reduced interference

compared to the 2.4GHz band commonly used by Wi-Fi devices.

This misunderstanding might stem from the terminology, as 5G refers to both the fifth generation of cellular technology and the 5GHz frequency band used in Wi-Fi communication. The confusion is exacerbated by the widespread anticipation and hype surrounding 5G cellular networks and their potential for enhancing connectivity across various devices.



5G cameras predominantly utilise 5GHz Wi-Fi signals rather than cellular 5G networks. They are not cellular security cameras, but fall under the category of Wi-Fi cameras, leveraging the higher frequency band of 5GHz for data transmission, which offers faster speeds and reduced interference compared to the 2.4GHz band commonly used by Wi-Fi devices.

5GHz vs. 2.4GHz Wi-Fi: Understanding the Differences

Wi-Fi networks operate on two primary frequency bands: 5GHz and 2.4GHz, each offering distinct characteristics that can significantly impact the performance of devices, including surveillance cameras. Understanding the differences between these two frequencies is crucial for optimising the functionality and efficiency of Wi-Fi-enabled security systems. Here are the details you should know about the differences.

Speed and Bandwidth

5GHz offers faster speeds and wider bandwidth, ideal for high-definition video streaming. It supports faster data rates but has a shorter range compared to 2.4GHz, whereas 2.4GHz provides greater coverage but at slower speeds. Its longer wavelengths enable better penetration through walls and obstructions but with lower data rates.

Interference and Congestion

5GHz experiences less interference from other devices due to a wider range of available channels, resulting in fewer connectivity issues in

crowded areas, whereas 2.4GHz is more susceptible to interference from common household devices like microwaves and cordless phones due to its narrower channel range.

Range and Penetration

5GHz offers a shorter range but delivers better performance in close proximity, making it suitable for high-bandwidth applications like video streaming, whereas 2.4GHz covers a longer distance and penetrates obstacles more effectively, making it better for devices located farther from the router.

For cameras, the 5GHz frequency often ensures smoother video streaming and faster data transfer, ideal for high-definition surveillance footage. It is one of the most important reasons that you need to choose 5G cellular security cameras.

Dual-Band vs. Single-Band Security Cameras: Which is Better?

Dual-band Wi-Fi cameras offer several advantages over single-band counterparts, primarily in signal strength, range, and compatibility. ■



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



I want to subscribe to

SECURITY Update
THE SECURITY & FIRE SAFETY TECHNOLOGY MAGAZINE

Signature _____

Date _____

This subscription 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

HID Mobile Access elevates safety and convenience in George Mason University

Overview:

George Mason University (Mason), the largest public research university in Virginia and named one of Money magazine's Best Colleges in America 2023, has seen rapid growth and increased enrollment. With over 40,000 students from 50 states and 130 countries, Mason emphasizes diversity and innovation, particularly in STEM fields, and holds top rankings for its cybersecurity and engineering programs.

Challenges:

As Mason expanded, maintaining a safe and secure campus environment while ensuring ease of access became a critical challenge. The need for a balance between public access to services and the convenience of contactless entry was essential, especially given the open nature of the campus. Daniel W. Anthes, Director of Technology Services, stated, "We have a very open campus. Most of our doors are unlocked from 7 AM until 11 PM... we need to make sure access control isn't in the way."

Solution:

To address these challenges, Mason turned to HID Global and Atrium for an innovative solution. Already using a card-based access control system with HID Seos credentialing technology, OMNIKEY chips, Asure ID card printing software, FARGO printers, and Signo card readers, Mason transitioned to HID Mobile Access® with Seos as the credential technology. This allowed any compatible mobile device to



function as a credential for accessing doors, gates, networks, and more. Anthes explained, "This would make it easier for staff and students to get where they needed to be without having to fumble with a set of keys."

Implementation:

The deployment of HID Mobile Access was straightforward due to the existing Signo readers, requiring only a simple upgrade. The versatile Signo readers support various credential technologies, enabling a seamless transition for users who preferred to continue using physical ID cards. "The seamlessness of the mobile credential and how quickly they can get where they need to be with their phone or wearable is cool to see in action," said Anthes.

Impact:

The implementation of HID Mobile Access significantly increased convenience and operational efficiency without compromising security. More than 50,000 students, faculty, and staff can now use mobile credentials to access approximately 7,000 doors, campus cash registers, printers, copy machines, and recreational facilities. Mobile access also facilitated express check-in for residence halls, reducing wait times and improving the overall student experience. Anthes highlighted, "The police department also absolutely

loves the wearables from a public safety standpoint, because they can get through the doors a whole lot faster than they could with the traditional cards or when they had to fumble with keys."

Future Plans:

Mason plans to expand mobile access to shuttle buses, enabling tracking of utilization data and special event access. Anthes expressed optimism about the ongoing benefits, stating, "We are only two months in, so there are a lot of benefits we have yet to see with Mason Mobile ID, but I'm excited about what we've already started noticing in terms of students engaging faster with their peers and community."

Conclusion:

The partnership with HID and Atrium has provided Mason with a comprehensive and seamless solution for modernizing campus access control. "New technology like mobile access is how Mason improves operations, so if there is an opportunity, I will certainly push to have HID involved," said Anthes. The successful implementation of HID Mobile Access has set a new standard for campus safety and convenience, positioning Mason as a leader in embracing technological innovations in higher education.

Paragraph Freedom Square Hotel deploys Vingcard Allure locks

Overview:

Paragraph Freedom Square Hotel, a Luxury Collection Hotel in Tbilisi, Georgia, has adopted Vingcard Allure door locks, provided by Vingcard, an ASSA ABLOY company known for its advanced hospitality technologies. This marks the first Marriott franchised Luxury Collection hotel in Eastern Europe to feature these innovative door locks, ensuring enhanced safety and a superior guest experience for its 220 guestrooms.

Challenges:

Situated in the heart of Tbilisi's city center, the hotel is part of an extensive construction plan that includes two additional Marriott franchised properties. A key challenge was to ensure the highest level of guest safety and security while maintaining a modern and welcoming environment. The hotel needed a solution that not only provided state-of-the-art security but also complemented its luxurious design and guest experience standards.

Solution:

To address these challenges, Paragraph Freedom Square Hotel selected Vingcard Allure door locks, known for their advanced credential encryption capabilities such as MIFARE Ultralight AES. The locks feature a fully LED-lit panel installed adjacent to the guestroom door, which can be customized to match the hotel's style and branding. The panel includes the hotel's colors and logo, guestroom numbers, and can even serve as a doorbell.

Irina Adeishvili, Head of PR and Marketing Director at the hotel, explained, "When we set out to create a guest stay experience that's truly exceptional, we knew that the check-in and room entry process plays an important part in creating a welcoming and safe environment, so we aimed to adopt the best solution that the industry has to offer."

Impact:

The adoption of Vingcard Allure locks has significantly enhanced the safety and convenience for

guests at Paragraph Freedom Square Hotel. The locks' customizable LED-lit panels have not only improved the aesthetic appeal but also the functionality, providing an exceptional guest experience from the moment they check-in. Additionally, the ability to electronically post do-not-disturb and make-up-room requests via an interior guestroom-facing panel adds to guest privacy and convenience.

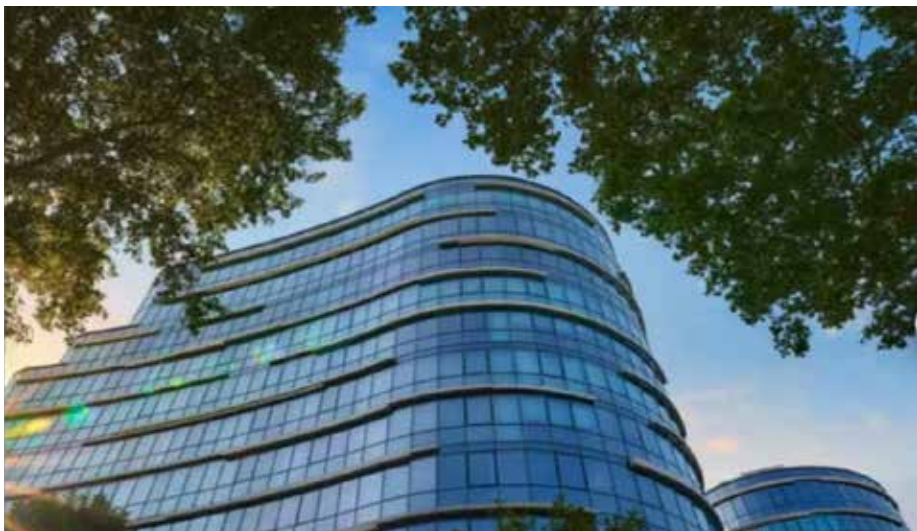
Future Prospects:

Vingcard Allure also offers Mobile Access compatibility, allowing hotels to provide digital guestroom keys through personal devices without the need for hardware replacements. This feature positions the hotel to easily adopt future technological advancements, further enhancing guest convenience and operational efficiency.

Adeishvili highlighted the solution's impact, stating, "Vingcard Allure with its instantly appealing and brightly lit design along with its added convenience capabilities ensure that our guests experience a heightened level of service that they will always remember."

Future Prospects:

The integration of Vingcard Allure door locks at Paragraph Freedom Square Hotel demonstrates a successful blend of advanced security technology and luxury hospitality. The hotel has not only heightened its safety standards but also enriched the guest experience, setting a new benchmark for hospitality in the region.



Texas State University boosts security to keep pace with rapid growth and expansion

Overview:

Texas State University, founded as the Southwest Texas State Normal School in 1899, has grown from a single building into a major multi-purpose university. Its original San Marcos campus now spans 485 acres with 267 buildings, supplemented by an additional 5,038 acres of recreational, instructional, farm, and ranch land. The university has also added a second campus in Round Rock, expanding from 15 temporary buildings to a 101-acre campus with state-of-the-art facilities. With a student population that surged from 303 in 1903 to over 35,546 in 2013, Texas State has experienced 16 consecutive years of enrollment growth.

Challenges:

As Texas State University anticipated continued growth, it recognized the need for improved security policies, particularly regarding key management. With over 5,000 new freshmen enrolled in 2013, the university faced the challenge of managing access for a growing number of on-campus residents and maintenance staff. Traditional key management practices were inefficient and posed a high-security risk, with maintenance staff often struggling to locate keys that were already checked out.

Solution:

To address these challenges, Texas State's University Police Department and other stakeholders conducted an extensive review of key management systems, considering various options through research, customer discussions, and on-site presentations. Ultimately, they chose KeyWatcher Touch from Morse Watchmans for its robust feature set, competitive pricing, and responsiveness to specific needs, such as implementing a six-digit user ID. The system's domestic production and the company's 130-year history also contributed to the decision.

Implementation:

The majority of the KeyWatcher systems were deployed within Texas State's Department of Housing and Residential Life, which serves around 7,000 residents across 25 facilities. The department, which includes 110 full-time employees and 170 building paraprofessionals,

found the enterprise management capability and robust reporting features of KeyWatcher Touch particularly valuable. The system's network capabilities allowed all deployed units to connect to the university's network, interfacing seamlessly with the card access and email systems.

Results:

The implementation of KeyWatcher Touch significantly improved key management efficiency and security at Texas State. By having keys available in each residence hall, the maintenance staff no longer needed to carry multiple master keys across campus, reducing liability and increasing efficiency. The system's ability to generate logs of key usage established better employee accountability, with alarms for keys checked out beyond set durations, eliminating unnecessary key unavailability.

Kyle Estes, Associate Director of Housing Facilities Services, stated, "We've been especially happy with the KeyWatcher's access and reporting capabilities, and the system's reporting tools make reviewing events and issues incredibly simple."

Impact:

The success of the initial deployment within the Housing and Facilities Department led to ongoing expansion, with Texas State University planning to implement up to 85 KeyWatcher systems. The ease of use and centralised management features streamlined the process of generating reports and reviewing incidents, with the ability to access the system from anywhere further enhancing its effectiveness.

"Because the system automatically generates a log of who has each key, we've been able to establish much better employee accountability for key usage," said Estes. "The ability to set a maximum duration that each key can be checked out and to receive alarms when that limit is exceeded has eliminated the problem of having keys unnecessarily checked out and as a result inaccessible when someone needs them."

Conclusion:

Texas State University's implementation of KeyWatcher Touch has significantly enhanced security, efficiency, and accountability in key management, supporting the university's continuous growth.

Mitigating cybersecurity risks in industrial control systems with Honeywell

Overview:

A global pharmaceutical company recognized potential vulnerabilities in its partner ecosystem that could impact its industrial control systems (ICS). To proactively address these risks, the company enlisted Honeywell's expertise to conduct a comprehensive assessment of its suppliers' operational technology (OT) cybersecurity gaps.

Solution:

Honeywell's OT cybersecurity experts undertook a meticulous process to understand the pharmaceutical company's operations across more than 100 global sites. Leveraging their deep knowledge and experience in OT, Honeywell provided tailored assessments to meet the customer's unique needs. Unlike many competitors, Honeywell's focus on OT, rather than just IT, made them the preferred choice for the pharmaceutical company.

Assessment Process:

The project was extensive, encompassing a global two to three-phase approach. The initial assessment was carried out at the company's site in India, with subsequent assessments planned for other locations. Honeywell's team conducted a thorough Cybersecurity Vulnerability Assessment, analyzing the customer's ICS infrastructure, processes, procedures, and safeguards to identify and mitigate potential risks.

Detailed Evaluation:

Honeywell's experts performed a physical site review to identify security compliance issues, such as unlocked control room doors and visible passwords. They also evaluated the customer's network equipment, including switches, routers, and firewalls, as well as infrastructure configurations and installation processes. The findings,



including all identified vulnerabilities, severity levels, and remediation details, were compiled into a comprehensive report.

Results:

The Cybersecurity Vulnerability Assessment report provided detailed best practices and site-specific recommendations to help the pharmaceutical company prioritize and mitigate identified threats. Honeywell's team, adept in IEC 62443 standards and other industry-specific guidelines, delivered a holistic assessment that considered the entirety of the customer's ICS environment, including people, processes, and technical issues.

Impact:

Despite challenges such as the pandemic-related shutdown in India, Honeywell exceeded the customer's expectations by remaining diligent and adaptable. The inclusion of an OT cybersecurity expert with real-life experience in the pharmaceutical industry further tailored the assessment and recommendations to the customer's specific needs.

Challenges:

Honeywell faced several challenges during the project, including the global scale of the assessment and the need to navigate pandemic-related disruptions. However, their expertise and commitment to excellence ensured that the assessments were thorough and actionable.

Conclusion:

Honeywell's proactive and comprehensive approach to assessing and improving the pharmaceutical company's OT cybersecurity posture has significantly enhanced the company's ability to protect its ICS from internal and external threats. The project's success underscores Honeywell's unparalleled expertise in OT cybersecurity and their dedication to exceeding customer expectations.

"We've found that expanding these systems is straightforward and doesn't delay key management for sensitive areas," concluded Kyle Estes, Associate Director of Housing Facilities Services, Texas State. "The system has been reliable, and the support staff is responsive and readily available to resolve any minor issues." ■

Surveying and Designing Physical Access Control Systems



Physical Access Control Systems (PACS) form the backbone of every security plan. When it comes to protecting business assets, physical security plays just as vital a role as cybersecurity. A full site survey helps you identify the type and status of each component in your current PACS architecture as well as other important factors.

Whether you manage a small business or a large organisation, you need strategies for controlling who has access to certain parts of your building. An access control system uses technology solutions that interface with your physical infrastructure to prevent unauthorised access to your building and keep track of who enters sensitive areas.

A robust access control system can protect your organisation's assets from theft and tampering and help create a safer environment for workers and guests. It can also provide an accurate record of authorised access to identify busy areas and traffic flow problems during specific times of the work day. However, you may find it challenging to implement an access control system if the system's requirements exceed current infrastructure.

To build physical security from the ground up, you need to create an access control plan that is aligned with the organisation's business goals and security requirements. Even if you're upgrading your access cards from an old frequency, considering a move to a more secure platform, or moving to Mobile Access you'll need to start with a complete understanding of your current system. A thorough site survey can generate the kind of understanding that will help you move ahead confidently.

Whether you have one system in one building or many

systems over hundreds of facilities the main considerations in a complete site survey include:

- The physical infrastructure of the technology
- Building construction around readers and other components
- Technical Infrastructure
- Current identification (card, biometric, mobile access) credential technology

Start with the Planning

Planning is crucial when designing physical access control systems because it ensures that security measures align with an organisation's specific needs and vulnerabilities. Proper planning helps in identifying critical access points, determining the appropriate level of security for each area, and integrating various security technologies effectively.

It also allows for the consideration of future scalability, ensuring that the system can adapt to evolving threats and organisational growth. Moreover, thorough planning helps in allocating resources efficiently, minimising costs, and avoiding potential security gaps. Overall, a well-planned access control system enhances security, operational efficiency, and user convenience.

An access control plan is the blueprint for your access control system. It takes into account your organisation's unique security requirements and lays out a comprehensive strategy for addressing them. Your plan might specify the areas you need to secure, the type of verification required, the type of access control hardware you plan to use, the location of the equipment, and who will monitor and manage the system after installation.

Know the environment

You must be aware of the site conditions, culture of

the staff, the organisation's security policies and the willingness of the top management in implementing a good PACS. Some businesses hold employees to strict standards, while others conduct business in a more open manner. There's nothing wrong with having a relaxed work culture, but you should keep this attitude from extending to security where it matters.

To see what training and culture changes might factor into your access control plan, observe the behaviour of employees on a normal day. Security concerns occur when employees do things like: holding the door for others without verifying employment status, prop open locked doors for convenience, and allow visitors to easily bypass the reception desk.

Physically surveying the site/s

After planning an access control system, you will have a clear understanding of your security risks. You will also understand how to implement an access control system that meets your needs. Now is the time to take a physical tour of the facility. Conducting a site survey to install a new system or upgrade the existing one is a crucial step in the preparation process. A successful site survey will provide you with the answers you need so you can successfully plan and execute security solutions. But a poor site survey can lead to great frustration for you and your clients alike.

Starting with the floor plans

Before you move any further into the process, the first step is to secure a floorplan of the site you'll be surveying. Facility floor plans will be the most accurate representation of actual dimensions and may reveal hidden features or obstacles that your team wouldn't notice on a site visit.

The site visit

A site visit helps verify that what you have on paper matches the reality you see in the building and helps you start designing. Walk through the site with your customer or stakeholder, collaborating with them on where each device should go. Involving them in this step of the process helps gain their buy-in and trust. Plus, there should be fewer revisions later in the process if they are involved from the beginning. In some cases, when you conduct the site walk, you'll be gathering what is already in place.

Get your answers before you leave:

When conducting a site survey for the purpose of planning and implementing a security system, make sure you learn what every space is used for. Blueprints

and site visits are crucial tools, but they leave many usage-oriented questions unanswered.

Some spaces (restrooms, offices, residence halls) seem straightforward enough in terms of use case. But asking more questions and making fewer assumptions is the right way. Only once you know what each space in an office building or a manufacturing plant is used for can you formulate a comprehensive and truly effective physical security system. Questions such as:

- No. of Doors to be Electronically Controlled
- No. of Entry & Exit Readers Required. Their locations
- No. of Users and their access privileges. Reader Preference - Contactless Proximity / Smart Cards, Biometric or Mobile Credentials.
- Integration with Intrusion / Fire Alarm / Video Surveillance System
- Software - On premise / Cloud
- Type of Reports required
- Future scalability

Record and document existing infrastructure

If you're upgrading or outfitting an existing system with new or updated security measures, you typically won't be starting from scratch. Some of the existing infrastructure may remain. Be sure to document anything electronic that already exists, Access controllers, Readers, locks and everything else that will be integrated with your new installation. Even if you're not going to be using anything electronic that's part of the old or previous system, you'll still want to note any physical infrastructure that could be reused. Existing cable runs, mounting points, conduits, power connections, network equipment, and more could save time and money — but only if you know they're there.

Ensure Compliance With Codes and Regulations

Your new access control system must comply with all applicable building codes and regulations, such as the Indian Standards (IS) and the National Building Code (NBC). Keep regulatory requirements in mind as you create your access control plan.

Thorough planning helps in allocating resources efficiently, minimising costs, and avoiding potential security gaps. Overall, a well-planned access control system minimises risk, enhances security, operational efficiency, and user convenience. ■

Why **Next-Gen Data Intelligence** Platforms are a **Game Changer** for Businesses?

BY **Siddharth Deshmukh**

Chief Operating Officer, Clover Infotech



In today's competitive business landscape, making informed decisions and managing resources efficiently is more critical than ever. However, many businesses face challenges with data silos and the complex integration of diverse technologies for data management and analytics. This is where data intelligence platforms come into play. They enable businesses to transcend traditional data and analytics applications, providing insights tailored to users' roles and workflows.

Here's why such platforms are a game changer:

They enhance data integration and management— Next-gen data intelligence platforms integrate data from a variety of sources, both structured and unstructured, including IoT devices, social media, and external databases, offering a comprehensive view of business operations. By helping businesses understand how their data relates to different processes and goals, these platforms provide a holistic perspective on various aspects such as customers, products, accounts, suppliers, and employees. This enables businesses to make quick, informed decisions.

They leverage predictive and prescriptive AI/ML models— Through predictive and prescriptive AI models, these platforms can predict trends, customer behaviour, and potential disruptions, allowing businesses to proactively address issues. Further to prediction, these platforms can suggest actions to optimise performance, enabling enterprises to improve efficiency and reduce costs.

They facilitate improved decision-making— With advanced analytics and real-time data, decision makers have access to accurate and up-to-date information. Further, virtualization tools help in interpreting complex data sets, making it easier for stakeholders to understand insights and take suitable actions.

They automate processes and boost efficiency— These platforms can automate routine tasks and processes, reducing manual effort and minimising human errors. By streamlining processes and providing actionable insights, these platforms help in optimising resources and improving operational efficiency.

They offer scalability and flexibility— Next-gen data intelligence platforms are built to scale with the business, accommodating growth and changing business needs. They also offer flexibility in deployment options (cloud, on-premise, hybrid), and can adapt to various business models and processes.

They augment user experience— Since such platforms offer customised experience to users based on their roles and preferences, they improve usability and satisfaction. With cloud-based solutions, users can access data and receive actionable insights from anywhere. This facilitates seamless cohesion and collaboration.

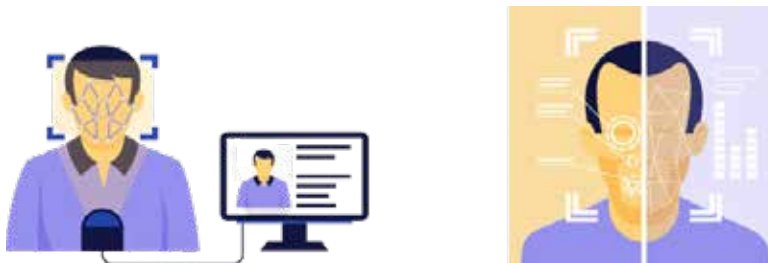
Many technology leaders such as

Microsoft, Oracle, Google have their own data intelligence platforms combining data integration, analytics, AI models, and intelligent applications to enable customers to achieve better outcomes. Oracle's Fusion Data Intelligence Platform delivers businesses data-as-a-service with automated data pipelines, 360-degree data models, rich interactive analytics, AI/ML models, and intelligent applications.

It would be correct to say, next-gen data intelligence platforms empower the existing systems and processes with advanced capabilities that drive smarter, faster, and more strategic business operations. By leveraging real-time data, advanced analytics, and automation, businesses can enhance their decision-making processes, optimise operations, and maintain a competitive edge in an increasingly data-driven world. ■



Differentiating Between Facial Authentication & Facial Recognition



Facial authentication and facial recognition are often conflated, but they serve distinct purposes and carry different implications for security and privacy. The experts at Alcatraz AI suggest that understanding the nuances between these two technologies is crucial, especially in an era where biometric identification methods are increasingly prevalent in various aspects of daily life. Here they explain the definitions and differences of the two technologies and explain why it is so important.

Facial authentication, as the name suggests, involves the process of confirming or verifying the identity of a known individual based on their facial features. This verification process is typically employed for granting access to systems, buildings, or devices, where security is paramount.

The fundamental principle underlying facial authentication is the comparison of the facial characteristics of the person seeking access with those stored in a database of authorised users' biometric profiles, who have opted into using facial authentication. By matching these features, the system can ascertain the identity of the individual and grant or deny access accordingly. The primary objective of facial authentication is to ensure secure access while minimising the risk of unauthorised entry, thereby enhancing overall security measures.

In contrast, facial recognition

operates on a broader scope, aiming to identify unknown individuals by analysing and matching their facial features with those stored in a database of known faces, most often, according to Alcatraz AI, without the knowledge or consent of the individual. This technology is commonly deployed in various domains, including city surveillance, law enforcement, and marketing.

While facial recognition offers undeniable benefits in terms of crime prevention, public safety, and targeted advertising, its widespread adoption has sparked significant concerns regarding privacy, civil liberties, and potential misuse. Critics argue that indiscriminate facial recognition systems can lead to mass surveillance, erosion of privacy rights, and the tracking of individuals without their consent or knowledge. Furthermore, there are concerns about the accuracy and reliability of facial recognition algorithms, particularly regarding their potential for bias and misidentification, which could have serious consequences, especially in law enforcement and criminal justice contexts.

The experts at Alcatraz AI are careful to highlight that they recognise the importance of prioritising facial authentication over facial recognition, particularly in environments where security and privacy are paramount. The company's facial authentication solutions are meticulously designed

to offer enhanced security features while safeguarding user privacy rights.

By focusing on authenticating the identities of known individuals, who choose to opt-into using facial authentication, rather than indiscriminately recognising faces, the company strives to strike a delicate balance between security and privacy concerns, and, with a commitment to privacy-centric design principles to ensure that individuals can access the resources they need without compromising their personal data or privacy.

While facial authentication and facial recognition are often used interchangeably, they serve distinct purposes and have different implications for security and privacy. By understanding these differences and implementing appropriate measures, organisations can leverage biometric technologies effectively while upholding the rights and privacy of individuals. At Alcatraz AI maintains a steadfast commitment to providing secure and privacy-respecting facial authentication solutions that meet the evolving needs of its clients.

Facial authentication represents a revolutionary approach to identity verification, leveraging the power of biometrics and AI to provide secure and convenient access control. By prioritising security, convenience, and privacy, facial authentication offers a compelling alternative to traditional authentication methods. ■

Staying Safe on Public Wi-Fi: Tips and Best Practices for Secure Browsing



In our increasingly mobile world, remote work has become the norm for many employees. Whether you're traveling on a train, working from a coffee shop, or connecting from an airport lounge, public Wi-Fi can be a convenient way to stay productive on the go. However, the convenience of public Wi-Fi comes with significant security risks. Understanding these risks and knowing how to protect yourself is crucial to safeguarding sensitive information.

The Risks of Public Wi-Fi

Public Wi-Fi networks are often unsecured, making them prime targets for cybercriminals. Some of the most common threats include:

1. Fake Wi-Fi Networks: Cybercriminals can set up rogue Wi-Fi hotspots that appear legitimate but are designed to capture any information you enter while connected. These networks can mimic the names of popular Wi-Fi networks, making it easy to mistake them for the real thing.

2. Man-in-the-Middle Attacks: On unsecured networks, attackers can intercept data traveling between your device and the internet. This can include login credentials, credit card numbers, and other sensitive information.

3. Eavesdropping: Without encryption, any data sent over a public Wi-Fi network can be intercepted and read by others. This includes emails, instant messages, and any files you transfer.

4. Malware Distribution: Cybercriminals can exploit vulnerabilities in your device to install malware over an unsecured Wi-Fi connection. This malware can then be used to steal data, monitor your activities, or take control of your device.

Tips for Safe Public Wi-Fi Usage

1. Verify the Network: Before connecting, confirm the network name with an employee at the establishment. Avoid connecting to networks that

appear suspicious or have generic names like “Free Wi-Fi.”

2. Use a VPN: A Virtual Private Network (VPN) encrypts your internet connection, making it difficult for hackers to intercept your data. Always use a VPN when connecting to public Wi-Fi.

3. Enable Two-Factor Authentication (2FA): Wherever possible, enable 2FA on your accounts. This adds an extra layer of security by requiring a second form of verification in addition to your password.

4. Avoid Sensitive Transactions: Refrain from accessing sensitive information, such as online banking or entering credit card details, while on public Wi-Fi. Save these activities for when you are on a secure, private network.

5. Use HTTPS: Ensure the websites you visit use HTTPS encryption. Look for “https://” in the URL and a padlock icon in the browser’s address bar, indicating the connection is secure.

6. Keep Software Updated: Regularly update your operating system, browser, and other software to protect against the latest security vulnerabilities.

7. Turn Off Sharing: Disable file sharing, printer sharing, and other network sharing settings when connected to public Wi-Fi. This reduces the risk of unauthorized access to your device.

8. Use Antivirus Software: Install and maintain reputable antivirus software to detect and protect

against malware and other threats.

9. Log Out After Use: Always log out of accounts and websites when you are finished using them, especially on public Wi-Fi.

10. Forget the Network: After using public Wi-Fi, forget the network in your device settings. This prevents your device from automatically connecting to the network in the future.

Educating Employees

Employees who frequently work remotely need to be aware of these risks and best practices. Regular training sessions can help increase awareness and minimize the risk of security breaches. Topics should include:

- Identifying legitimate Wi-Fi networks
- The importance of using VPNs
- Recognizing signs of potential scams
- Safe browsing habits
- Steps to take if they suspect their data has been compromised

By implementing these strategies and educating employees, companies can significantly reduce the risks associated with using public Wi-Fi. The convenience of staying connected on the move does not have to come at the expense of security. With the right precautions, employees can work remotely with confidence, knowing their information is protected. ■



Next-Gen Fire Detection Systems: Advancements & Applications

BY IVY COSCA,
Contributing Editor at Marcus Media

In the field of fire safety, detection systems have made significant advances, moving beyond old-fashioned methods to adopt new technologies. This article explores the latest improvements in fire detection systems – including better sensors, IoT integration, real-time analytics, and how they are used in different industries.

Old fire detection systems relied on basic sensors and manual checks. But now, new technologies are being developed to make detecting fires more accurate and faster.

According to a report by MarketsandMarkets, the global market for fire detection and suppression systems is expected to reach £59.9 billion by 2027, driven by innovations in sensor technology and IoT integration.

Advanced Sensors: Improving Detection Accuracy

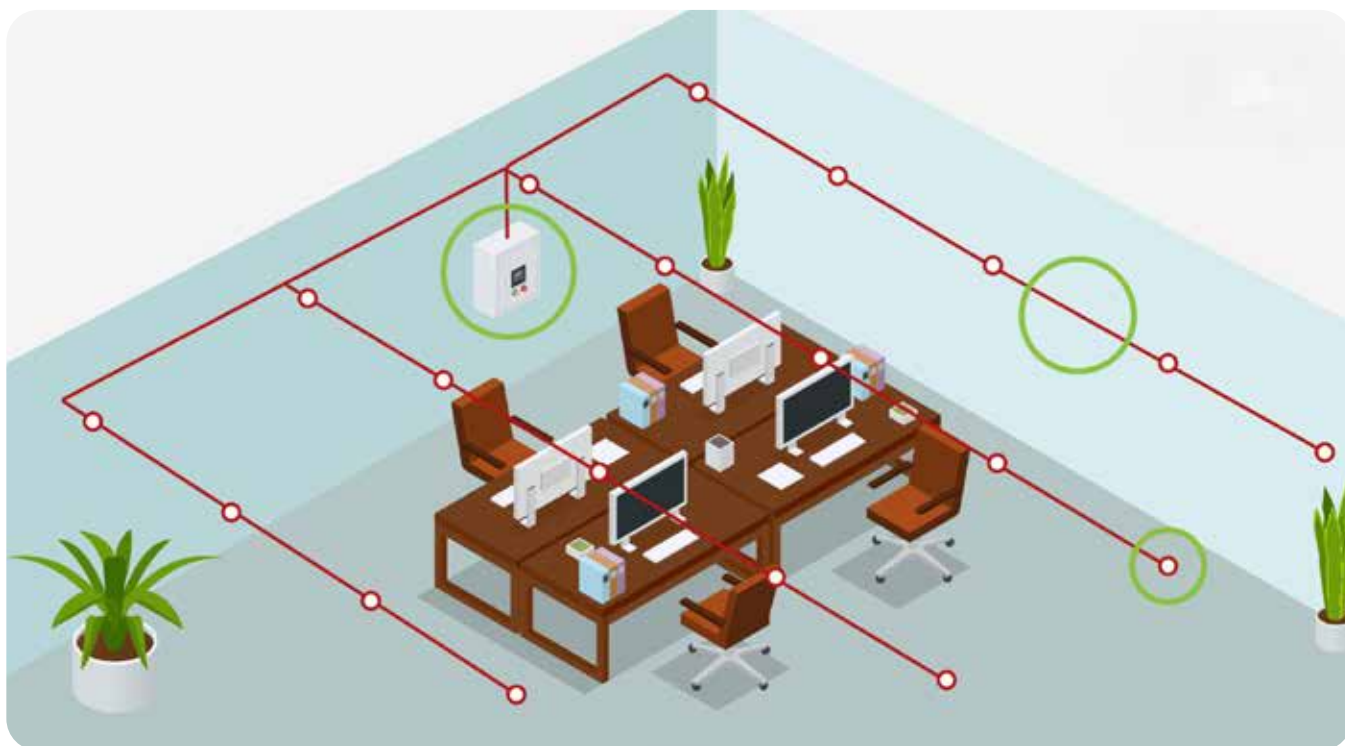
One of the key improvements in next-gen fire detection systems is advanced sensors.

Optical sensors, for example, use light to detect smoke particles more accurately than older types of sensors. Thermal sensors can spot changes in heat, while multispectral sensors can detect different types of fires, like slow-burning fires, which older detectors might miss.

Research from the Fire Protection Research Foundation shows that these advanced sensors reduce false alarms and make it easier to spot fires early. This not only makes places safer but also reduces disruption in places where it's important to keep things running smoothly.

IoT Integration in Fire Detection Systems

The use of Internet of Things (IoT) technology



has revolutionised fire safety by allowing devices to connect and share information – IoT-enabled fire detection systems can send data in real-time to monitoring centres, so they can respond quickly and do maintenance work before a fire starts. In places like offices and hospitals, IoT sensors can keep an eye on things like temperature and air quality. This means they can warn people about fire risks before they become serious.

Real-time Analytics: Using Data to Improve Safety

Real-time analytics are important for making fire detection systems more proactive.

By looking at data from sensors and IoT devices, these systems can find patterns that show when there might be a fire risk. This means they can take action to stop problems before they get worse.

A study in Fire Technology showed that using real-time analytics with fire detection systems can make response times up to 30% faster. This is a big help for places like offices and factories where safety is very important.

This is a big help for places like offices and factories where safety is very important.

Applications Across Industries

Next-gen fire detection systems are used in many different industries, each with its own safety needs and challenges. In hospitals, for example, these systems can spot fires early and help get patients out quickly and safely.

Buildings like offices benefit from smart systems

The Global Market for Fire Detection and Suppression Systems is expected to reach £59.9 Billion by 2027.

that not only find fires but also help manage buildings better and keep people safe. In factories and warehouses, where there are higher risks, strong fire detection systems are needed that can work in tough conditions and fit in with safety rules.

Regulatory Compliance and Standards

As new technologies come out, rules and standards are made to make sure fire detection systems are safe and work well.

Companies that make these systems have to follow rules set by organisations like the National Fire Protection Association (NFPA) and the European Committee for Standardisation (CEN). Following these rules makes sure fire detection systems do their job right and make people feel safe about using them.

Challenges and Future Trends

Even with all their benefits, next-gen fire detection systems have some challenges – things like making sure different systems can work together and keeping data safe from cyber-attacks are important. But work is being done to fix these problems, so new ideas can keep coming.

New trends like using AI to look at data and make better decisions, and using systems that can work on their own, show promise for making fire detection systems even better in the future.

Making Fire Safety Better with New Ideas

New fire detection systems are a big step forward in keeping people and places safe from fires.

By using better sensors, IoT connections, and real-time analytics, these systems find fires more easily and stop them from getting worse.

People in different industries should use these new technologies to make safety better. As more people want good fire detection systems, the way we keep fires away from people and places will get better too. ■



Why Employees Need Fire Safety Training At The Workplace



Globally, less than 50% of occupants in buildings are confident that they know what to do and where to evacuate in the event of an emergency. Because so many offices lack the training and knowledge of what to do in a fire, it can lead to more fire damage and even loss of life.

One of the biggest benefits of employee fire safety training is that it teaches your employees about common fire hazards in your workplace. Understanding potential risks and threats in your workplace can help teach your employees how to prevent fires.

For example, if your employees know that damaged power cords are a common fire hazard, they can recognise these as an issue and can do something to prevent a fire, such as notify an office administrator to get it taken care of.

Helps Prevent Fires

Not only does training for fire safety in the workplace teach your employees about common fire hazards in your industry, but it can also help them prevent fires. This is one of the most important parts of fire safety courses, as it is much easier to prevent a fire than it is to put one out. If employees in each part of your building know how to prevent fires, you will protect your business from fire damage and can even save the lives of your employees.

Teaches Proper Response

In an emergency like a fire, it can be easy to lose focus and panic. However, with fire safety training, you can teach your employees how to properly respond to this type of emergency.

Have your employees practice their training during a fire drill by going through your fire safety plan, using your emergency exits, and more. This will make it more likely that they will remember the proper response if a real fire were ever to happen.

Identifies Emergency Exits

A vital part of fire safety is having a fire evacuation plan for your employees. Not only do you need to have a plan, but you want each of your employees to be familiar with this plan.

With fire safety training, you can identify emergency routes and exits. Physically showing your employees where each emergency exit is will make them more likely to be able to find it, even in the chaos that comes with a fire in the building.

Having your emergency exits clearly marked and free from any obstacles is vital to having a safe way to get out of the building. Make sure that you do not store anything near emergency exits as they may be necessary to use for yourself and for first responders that come to your aid in a fire.



Trains Employees to Use Fire Fighting Equipment

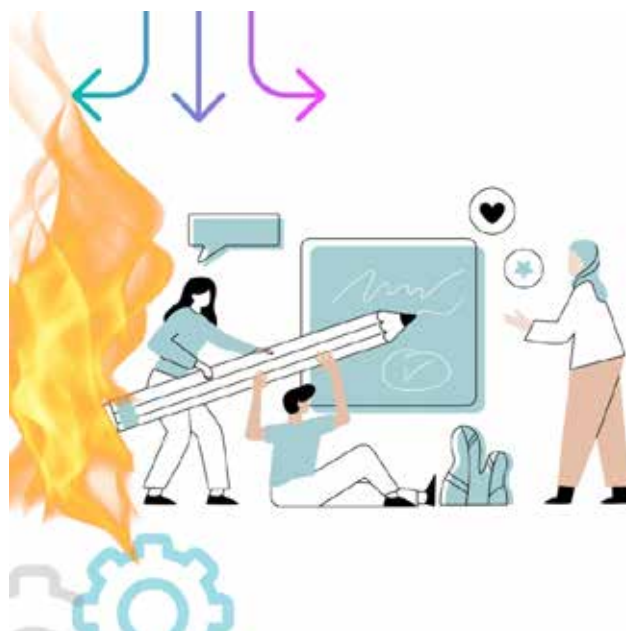
Another huge benefit of fire safety training is that it allows a professional fire safety specialist to train your employees to use fire fighting equipment. Most employees don't even realise that there are different types of fire extinguishers that are used for different classes of fires. Because so many people are not confident in using any type of fire fighting equipment, this training can help them learn how to use this equipment in an emergency.



Creates a Communication Plan

Finally, utilising fire safety training is vital because it helps you create a communication plan. In an emergency, it is important that you know how you can communicate with your employees and other people on the premises of your building. Having a method of communication during an emergency makes it easier to confirm that everyone makes it out of the building safely and that each of your employees is safe. It can also help you find ways to quickly and effectively tell others about the emergency to get the fastest response possible.

Fire safety training is an essential tool that can help you and your employees stay safe in the event of a fire and even prevent fires from happening in your workplace. By teaching your employees how to use fire fighting equipment and fire hazards in the workplace, you can potentially save their lives. ■



Hikvision elevates security with VCA 3.0 upgrade for HeatPro Bi-Spectrum Thermal Cameras

Hikvision, a world-pioneering manufacturer and supplier of security products and solutions that deliver the ideal combination of high performance and extreme value, announces a significant upgrade to its HeatPro Bi-Spectrum Thermal cameras with the integration of VCA 3.0.

This improvement introduces a range of advanced features designed to enhance performance, detection, and accuracy, further solidifying Hikvision's commitment to providing innovative security solutions.

"Hikvision's new VCA 3.0 update for our HeatPro Bi-Spectrum Thermal Cameras sets a new standard in security technology. By integrating intelligent deep learning algorithms and advanced analytics, we deliver unparalleled accuracy and efficiency in threat detection, ensuring our customers have the most reliable protection available," said John Xiao, Vice President of Marketing, Hikvision USA. "The addition of VCA 3.0's self-learning calibration and distillation model further enhances our cameras' performance, leaving more time for true fire prevention and other critical security measures."

The VCA 3.0 upgrade brings enhanced algorithms that significantly improve processing power and efficiency, allowing for greater accuracy in detecting and analysing potential threats. VCA 3.0 ensures that the cameras can operate effectively in all weather conditions, providing reliable performance regardless of environmental challenges.

The intelligent VCA setup has been simplified, making the configuration process more straightforward and user-friendly. This allows users to quickly and easily set up their systems to maximise the benefits of the advanced features.

Accurate alarms are now more precise, reducing false positives and ensuring that genuine threats are promptly identified and addressed. The distillation



model introduced in VCA 3.0 offers advanced filtering capabilities, ensuring that the most relevant data is highlighted for security personnel.

The self-learning calibration feature allows the system to adapt and improve over time, continuously enhancing its performance. Combined event alarms integrate multiple event triggers, offering a cohesive and comprehensive alert system that ensures no critical event goes unnoticed.

Hikvision's Bi-Spectrum HeatPro Thermal Bi-Spectrum Cameras debunk common myths for thermal technology, bringing cost-effective innovation to the market with several key features:

- **Discover Hidden Objects:** Thermal technology is not limited by smoke, fog, darkness, or strong backlight, illuminating the unseen for maximum protection.
- **Early Detection and Warning:** Monitors temperature changes and triggers alarms before a fire occurs for rapid response and asset protection.
- **Accurate Target Focus:** Using deep learning algorithms, HeatPro cameras accurately identify humans and vehicles, no matter the environment, for improved alarm efficiency.
- **Cost-Effective Technology:** Intelligent thermal perimeter protection, early temperature anomaly detection, and asset protection are all available at a competitive market price.

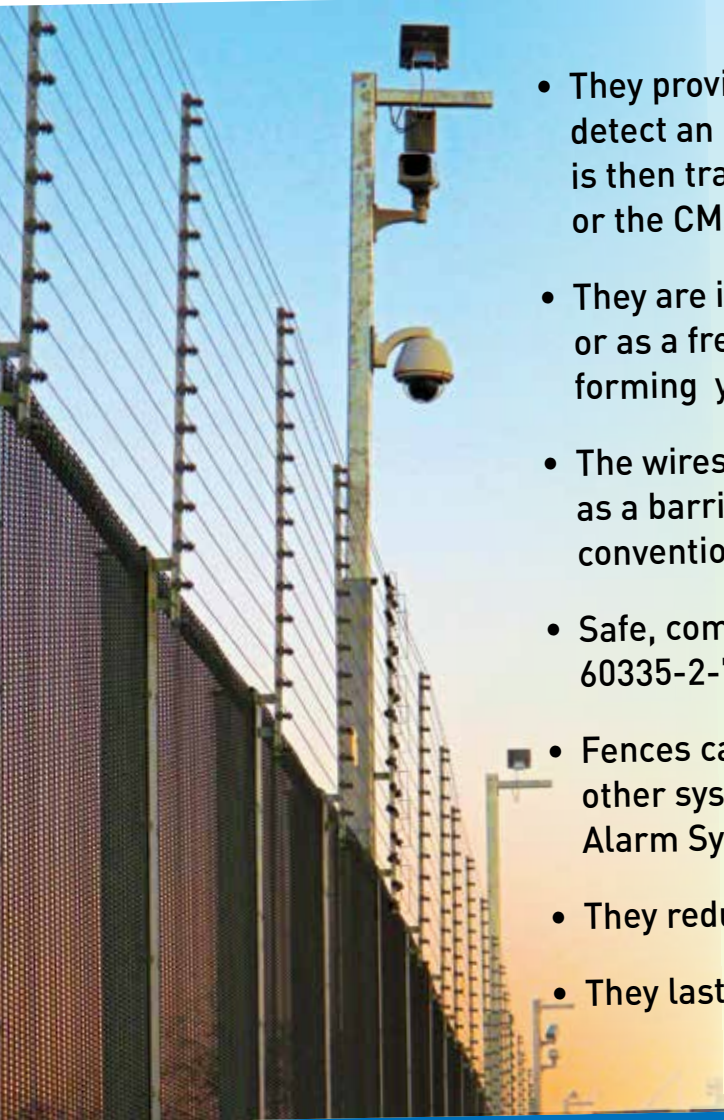
YOUR SECURITY BEGINS WITH YOUR PERIMETER

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...



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



Theia's MY23F lens

The MY23F lens offers a 1.8–3mm focal range, 120° horizontal field of view, and ruggedisation to withstand 50 mph impacts, capturing high-resolution, undistorted vehicle crash images.



Reolink's Argus 4 Pro

The Argus 4 Pro redefines surveillance with its 4K UHD 180° blindspot-free view and day/night color vision, using proprietary technology and user-centric features for home and business security.

Hanwha Vision's AI TNV-C8011RW



The TNV-C8011RW is a 5MP AI IR wall mount camera with a 180° panoramic lens and adjustable tilt, providing clear, eye-level facial views and infrared imaging up to 15 meters.

3xlogic's Powerful HD Cameras



- 10MP Dual-Imager IP camera: two adjustable 5MP cameras in one housing for high-definition coverage.
- 20MP Varifocal IP camera: four adjustable 5MP imagers with infrared, pan/tilt, and remote zoom.

3xlogic's Powerful HD Cameras

3xlogic is expanding its portfolio with two powerful cameras, offering multi-directional HD viewing in challenging lighting conditions.

The first is the 3xlogic 10MP Fixed Dual-Imager (2x5MP) IP camera, which combines two adjustable 5MP cameras in one housing. It supports Edge-Based Deep Learning analytics for interior or perimeter protection and integrates with the Vigil Video Management System (VMS). Features include 60' IR, Audio and Alarm, IP67 and IK10 ratings, and ONVIF Profile

S, making it ideal for hallway or corner installations.

The second addition is the 3xLogic Varifocal 20MP (4x 5MP) Surround-view IP camera, which has four independently adjustable imagers for pan/tilt and remote zoom. Challenging corner mount applications can be solved by positioning one of the imagers in the centre of the unit by facing it down. This multi-sensor camera is perfect for large areas like retail, education (cafeteria, auditorium), large commercial, warehousing, parking lots, and data centres.

Theia's MY23F lens

Theia's ML183M and MY23F lenses are key in vehicle crash testing, offering rugged, high-resolution, wide-angle views with minimal distortion. The ML183M lens, used in over 3000 tests, features a 1.8-3mm focal range, 120° HFOV, 5+ MP resolution, and patented Linear Optical Technology for rectilinear images. The MY23F lens enhances these features with ruggedisation, surviving impacts at 50 mph. These lenses, distributed by RMA Electronics, are integrated with high-speed cameras like Vision Research's Phantom Miro C210J, providing crucial imagery for detailed crash analysis.

Key Features include:

- Ultra-wide, no barrel distortion ...



Smiths- X-ray Diffraction Scanner

X-ray Diffraction (XRD) accurately identifies materials by analyzing molecular structure, ideal for detecting evolving compounds like explosives or narcotics in various forms, even with similar densities.

...

- 1.8-3mm focal range, up to 120° HFOV
- 5+ MP resolution
- Near IR corrected
- Slip ring for easy positioning
- Minimal re-focus with EasyZoom™
- Compatible with 1/2.3” sensors or smaller

Reolink’s Argus 4 Pro

The Argus 4 Pro, with dual 4mm lenses, offers a 4K UHD 180° blindspot-free view and all-day color vision, redefines surveillance. Reolink’s ColorX technology delivers vivid nighttime images without infrared lights, conserving 30% more battery life. Enhanced by Wi-Fi 6, it ensures smooth 4K streaming and robust privacy protections with end-to-end encryption.

Key Features include:

- 4K UHD 180° view

Hanwha Vision’s AI TNV-C8011RW

Hanwha Vision’s TNV-C8011RW is a 5MP AI IR wall mount camera designed for entrances, exits, and retail areas. Installed at eye level, it provides clear face views and nearly 180-degree coverage with adjustable tilt (±25 degrees). It features AI detection, Wisestream III compression, and IR functionality up to 15 meters. Business intelligence tools like people counting and queue management enhance efficiency. Its compact, anti-ligature design allows

discrete, flexible mounting options.

Key Features:

- 5MP resolution
- Nearly 180-degree field of view
- Adjustable tilt lens (±25 degrees)
- IR functionality up to 15 metres
- AI detection and classification
- Wisestream III compression
- Business intelligence features
- Anti-ligature, compact design
- Flexible mounting options

Smiths- X-ray Diffraction Scanner

Smiths Detection has launched the SDX 10060 XDI, an advanced X-ray scanner utilizing X-ray Diffraction (XRD) technology for precise material discrimination and substance identification. Designed to meet ECAC Standard 3.1/3.2 and TSA 7.2, the scanner automates

explosive detection, enhancing security and operational efficiency in high-volume screening environments. It integrates seamlessly with existing baggage systems, supporting customs agencies in detecting narcotics and contraband effectively.

- All-day color vision
- 30% more battery life
- Wi-Fi 6 for smooth streaming
- Easy installation
- Smart detection alerts
- 128GB SD card & Reolink Home Hub support
- Remote access
- 24-hour battery with 10-min charge

“The Argus 4 Pro represents the next evolution in smart home security,” said Fabrice Klohou, Marketing Manager at Reolink.

New Mercury MP Controller line provides a fully functional hardware and firmware infrastructure for new builds and legacy upgrades



Mercury Security, the globally renowned manufacturer of OEM technology, and HID, a worldwide pioneer in trusted identity and access control solutions, announce the next-generation Mercury MP Controllers, designed to deliver enhanced flexibility and security for businesses of all sizes. As technology advances, access control systems require robust encryption and advanced threat detection.

The new Mercury MP Controllers empower access control software providers and integrators to seamlessly combine a wide range of access control technologies, elevator control, building automation, IoT applications, and third-party solutions into a unified, centralised and fully robust infrastructure.

This open approach provides the freedom to choose the right solution for specific customer requirements. Taking this commitment a step further, the new intelligent controllers were designed with advanced security features to safeguard sensitive data and to help protect against evolving cyber threats.

A robust cryptographic engine supported by a secure boot CPU, crypto chip and data encryption aim to provide proactive protection against unauthorised access and attacks.

The Mercury MP Controllers provide partners and end users with:

- **Flexibility:** The freedom to design and upgrade systems without limiting software and hardware choices, and seamlessly integrate the latest technologies with no costly rip-and-replace projects. This flexibility extends to OEMs, allowing them to seamlessly integrate the controllers with both on-premises and cloud-based access control environments.
- **Scalability:** The ability to meet system architecture from a single door to an entire enterprise.
- **Heightened Security:** The support for physical and cybersecurity features to help keep networks and data safe.
- **Reliability:** The peace of mind of having invested in reliable and trusted hardware in the business

The Mercury MP Controllers deliver powerful new features such as a dual-footprint circuit design with alternate components for business continuity, a future-ready app development environment for expanded integrations and the adoption of enhanced cybersecurity best practices, like ARM TrustZone, to protect systems.

Cliq upgrade boosts security and user convenience

The Cliq intelligent key-based access management system from Assa Abloy allows users to flexibly manage access, and to secure almost any opening with electronic cylinders or padlocks and programmable smart keys. Now, a new upgrade in the programming device family simultaneously enhances this security and convenience.

Requiring regular credential updates is one of the simplest, most effective methods for keeping premises secure. Assa Abloy's new Cliq Wall Programming Device (PD) helps to update keys' access rights faster without involving the system administrator. This cuts the risk of unauthorised keys circulating.

Cliq is built around precision-engineered locking cylinders and high-end microelectronics. A standard battery, lasting approximately 10 years with typical use, inside each programmable smart key powers the cylinder or padlock — and encrypts data transfer between lock, key and system. Robust, durable Cliq cylinder locks secure lifts, machines, mailboxes, cabinets and more with the same control as sensitive doors. A range of programming devices transfer and update access rights for keys. The

Cliq Wall PD, available as an indoor and outdoor variant, has now been redesigned to make this updating process faster and easier than ever.

The upgraded Cliq Wall PD protects users against mis-steps, confusion or false positives during key programming: Intuitive LED lighting instantly confirms when their key is updated in both the indoor and outdoor product variants. The Cliq Outdoor Wall PD is the ideal solution for demanding environments as it is protected against weather and vandalism.

With the new Cliq Wall PDs, keyholders and facility managers do not need to worry about data privacy. Enhanced encryption via Ethernet ensures every issued Cliq key is protected with robust security. The upgraded device now supports the 802.1x protocol for enhanced security.

And with rapid installation — using the existing wiring and backplate — it is simple to switch existing wall programmers for new devices to keep a site and staff safer. Total compatibility with existing and future Cliq keys ensures that replacing old programmers with the new Cliq Wall PD is hassle-free and future-proof.



Iris ID and Uclockit partner to humanise workforce management



Iris ID, a global leader in iris recognition technology and Uclockit, a provider of a cutting-edge cloud-based platform for HR management, have partnered to “humanise” the approach that organisations have towards administering workforce management.

Iris ID and Uclockit recognise that a high-quality workforce management user experience and organisational efficiency are not mutually exclusive. Together these two companies will deliver a level of service and customisation that modernises how people are managed and time and attendance solutions are implemented.

The Uclockit software solution is a complete human resources and time and attendance tool. With its intelligent digital assistant concept and adaptable modular approach, Uclockit.pt empowers users with a robust suite of tools to streamline time and attendance, manage vacations, schedules, shifts, productivity across cost centres, and more.

Together the multimodal IT100 and the Uclockit.pt software aim to help organisations build the solution they need, reduce payroll and administrative costs, eliminate time fraud with the use of biometrics and create a more informed and productive workforce. According to the two companies, this is a win-win scenario for all.

“This collaboration is based on mutual values of technological resourcefulness and a shared belief in prioritising people above all,” said David Barnabé,

founder and CEO, Uclockit. “With both teams sharing a rich history of collaboration with major breakthroughs in the early 2000s, and a deep understanding of the importance of user-centric solutions, this partnership thrives on trust in the expertise of the teams and the unparalleled support provided.”

The Uclockit.pt software is easily paired with the Iristime Timeclock for the Modern Workforce, also known as the IT100. This advanced security multimodal iris and facial recognition device is the only solution on the market that allows ISV (Independent Software Vendors) using REST API web-based applications to create custom software solutions to meet the specific needs of any organisation. Iris ID also offers an Android SDK which allows apps to be developed and installed on the IT100. The flexibility of the device was a key selling point to cement the partnership as we continue to grow the Iristime IT100 App ecosystem.

The benefits of Iris ID’s IT100 biometric solution are far reaching, including that the device is suitable for any work environment, is fast, accurate and that identification takes less than a second. The iris face fusion mode is another customisation feature that companies can use to suit their needs.

The alliance between Uclockit and Iris ID is timely as the global time and attendance software market was valued at \$2.7 billion in 2022. The market is projected to reach \$8.3 billion by 2032, growing at a CAGR of 12.1% from 2023 to 2032. This is according to the Global Opportunity Analysis and Industry Forecast, 2023-2032.

EZVIZ revolutionises Security Surveillance system with the launch of H8C 4G Camera Range

EZVIZ, a global smart home security company, has strengthened its outdoor security camera portfolio with the launch of revolutionary EZVIZ H8C 4G camera range, setting a new standard for seamless protection in areas with limited Wi-Fi access. The H8C 4G camera offers unparalleled features, including 2K resolution, 360-degree coverage, AI-powered detection, and more, ensuring uninterrupted security regardless of Wi-Fi limitations.

The EZVIZ H8C 4G is a cutting-edge security camera system designed to provide unparalleled convenience. With its integrated connectivity, this camera offers flexibility and reliability, allowing users to monitor their property remotely without the need for a Wi-Fi connection.

This feature makes it ideal for areas with limited or unreliable internet access, ensuring continuous surveillance even in remote locations. Additionally, it comprises advanced motion detection capabilities and real-time alerts, enabling users to stay informed of any suspicious activity around their property. Its compact and weatherproof design further enhances convenience, allowing for easy installation both indoors and outdoors.

Experience peace-of-mind with the H8C 4G

camera's advanced detection, real-time alerts, and two-way communication. Speak to visitors via smartphone, enhancing security with pre-recorded messages. Rest assured with impressive night vision, offering three modes for clear visibility day and night. Choose from full colour, black and white, or smart night vision to suit any need. Save footage locally on a microSD card of up to 512 GB, or subscribe to EZVIZ Cloud Play for encrypted cloud storage, ensuring your recordings are always accessible.

The EZVIZ H8C 4G camera is designed to meet the needs of users in areas with limited Wi-Fi access. With its innovative 4G network connectivity, users can enjoy real-time alerts, two-way communication, and remote access via the user-friendly app, eliminating connectivity frustrations and offering a solution with dual connectivity options, allowing users to access the network via 4G SIM cards or a cable through the RJ45 Ethernet port.

The camera range can be easily managed via the EZVIZ App with easy integration and hands-free control for added convenience. It comes with a detachable mount plate that simplifies the installation process. By detaching the mounting base from the camera body, installation becomes hassle-free, eliminating the need to hold the entire camera in place while finding the optimal installation spot.



In The New World, **Access Control** Takes A Whole New Meaning

While access control in physical security is a widely understood and recognised facet of security, in current times with IT rapidly taking over the centrestage, access control has taken an altogether newer and more crucial form.

The overlap between IT access control and physical access control occurs in various areas, including the use of access cards, biometric authentication, and identity management databases, which ensure consistent user authentication and authorization across both physical and digital domains. Additionally, Physical Security Information Management (PSIM) systems integrate physical and IT security systems, enabling unified monitoring and response to security incidents, further highlighting the convergence of physical and IT access

control for enhanced security.

Access control is a crucial component of information technology (IT) and cybersecurity. It is a mechanism that regulates who or what can view, use, or access a particular resource in a computing environment. The primary goal is to minimize security risks by ensuring only authorized users, systems, or services have access to the resources they need.

Access control is not just about allowing or denying access. It involves identifying an individual or system, authenticating their identity, authorizing them to access the resource, and auditing their access patterns. This process minimizes the risk of unauthorized access, protecting sensitive information and systems.



Modern IT infrastructure and work patterns are creating new access control challenges. Trends like the use of cloud computing, the growing use of mobile devices in the workplace, and the transition to remote work, mean that the number of access points to an organization is growing exponentially. New technologies like identity and access management (IAM) and approaches like zero trust are helping manage this complexity and prevent unauthorized access.

Cybercriminals are becoming more sophisticated, utilizing advanced techniques to breach security systems and gain unauthorized access to resources. Access control is a proactive security measure that helps deter, detect, and prevent unauthorized access. By controlling who or what has access to a resource, it ensures that only those with the necessary permissions can access the data or service. This significantly reduces the risk of a security breach, both from external attackers and insider threats.

Moreover, access control in security is crucial for compliance with various regulatory requirements. Regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) require organizations to implement stringent access control measures to protect personal data. Non-compliance can result in severe penalties and reputational damage.

How Does Access Control Work? 5 Key Components

Here is the general process involved in securing access and managing access control within an organization.

1. Authentication

Authentication is the first step in access control. It involves verifying the identity of the user or system requesting access. This is usually done by matching the provided credentials with the stored information. Authentication methods include password-based, biometric-based, and certificate-based authentication.

2. Authorization

Authorization follows successful authentication. It involves granting or denying access based on the user's or system's privileges. The privileges are predefined and dictate what resources the user or system can access and to what extent. Authorization helps in maintaining the principle of least privilege, ensuring users and systems have only the access they need.

3. Access

Access refers to the actual use or interaction with a resource. This could involve viewing, modifying, or deleting data, or using a service. The extent of access is dictated by the authorization process. Access is monitored and controlled to prevent unauthorized activities.

4. Manage

Management of access control involves maintaining and updating the access control system. This includes defining and updating access policies, managing user credentials, onboarding and offboarding users, and maintaining the access control hardware and software. Effective management ensures the access control system remains robust and up-to-date.

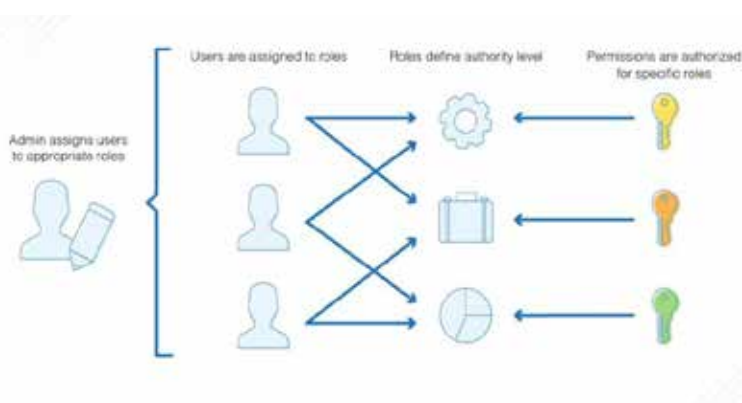
5. Audit

Auditing is an essential component of access control. It involves monitoring and recording access patterns and activities. Auditing helps in identifying any unusual or suspicious activities and aids in forensic investigations. Regular audits can reveal security vulnerabilities and help improve the access control system.

There are several technical approaches to managing access control. Here are the main ones:

Role-Based Access Control (RBAC)

Role-Based Access Control, or RBAC, is an access control framework that assigns system access rights and permissions to users based on their roles within an organization. For instance, a financial analyst in a company might have access to sensitive financial data but would not have the same access to the company's HR records. RBAC is widely adopted due to its simplicity and ease of administration.



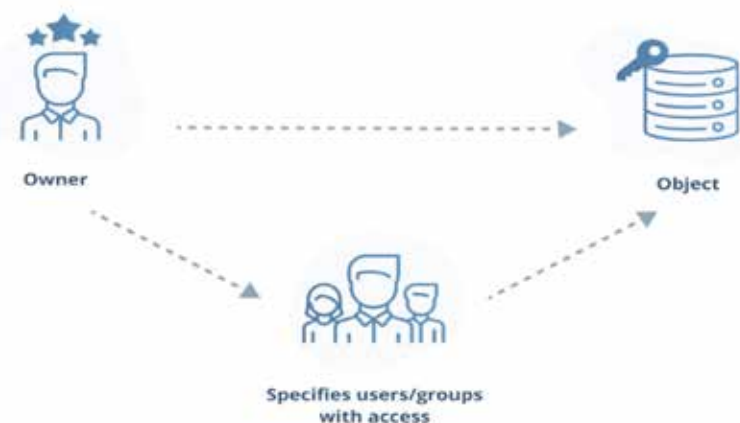
Attribute-Based Access Control (ABAC)

Attribute-Based Access Control, abbreviated as ABAC, is a security framework that uses a set of policies to grant or deny access to resources. These policies are based on attributes, which can include user attributes (like role or location), resource attributes (like the type of information), and environment conditions (like time or network location). ABAC is dynamic and flexible, making it suitable for complex environments where access decisions need to consider a multitude of factors.



Discretionary Access Control (DAC)

Discretionary Access Control (DAC) is a method that grants access rights based on rules specified by users. In DAC, the owner of the information or resource decides who can access specific resources. This model provides flexibility and individual control, but it also comes with risks as users might inadvertently grant access to those who should not have it.



Mandatory Access Control (MAC)

Mandatory Access Control, or MAC, is an approach where access is granted or denied based on the information's classification and the user's security clearance level. It is widely used in organizations handling highly classified



and sensitive data, like military institutions or government agencies. MAC is rigid and highly secure, but it can be complex to implement and manage.

Policy-Based Access Control (PBAC)

Policy-Based Access Control, or PBAC, is an access control model that determines access based on a set of policies that define allowable actions within a system. PBAC policies are often complex, involving a combination of rules, roles, attributes, and environmental factors. This model allows for fine-grained access control, enabling administrators to manage access based on the specific needs of the organization and the context of the access request. While PBAC is fairly similar to ABAC, it is easier to implement and requires less IT and development resources.

Challenges of Access Control in Cybersecurity

Distributed IT Environments and the Adoption of Cloud Computing

The proliferation of distributed IT environments and the widespread adoption of cloud computing have significantly impacted access control in cybersecurity. In a distributed IT environment, resources are spread across multiple locations, including on-premises data centers and various cloud services. This dispersion of resources creates a complex network of access points, each requiring robust access control mechanisms.

With cloud computing, organizations rely on external providers for infrastructure, platforms, or software services. This reliance introduces external access points

that must be secured, making the enforcement of consistent access control policies across different environments challenging.

Effective access control in such scenarios requires a comprehensive understanding of the cloud service models (IaaS, PaaS, SaaS) and the specific security responsibilities assigned to the provider and the organization. Additionally, the use of cloud access security brokers (CASBs) and robust identity and access management (IAM) solutions can help enforce uniform access control policies across distributed and cloud environments.

The rise of mobility and remote work has introduced new challenges in access control. With an increasing number of employees working remotely, often using their own devices (BYOD), the traditional perimeter-based security model becomes less effective. Remote workers need to access corporate resources from various locations and devices, expanding the potential attack surface.

To address these challenges, organizations are adopting technologies like virtual private networks (VPNs), which secure remote connections, and employing endpoint security solutions to protect individual devices. Another critical aspect is the implementation of context-aware access control, where access decisions are based not only on user identity but also on factors such as device security posture, location, and time of access.

The concept of password fatigue refers to the challenge users experience when they have to remember multiple passwords for different applications. This is a significant issue for access control in security.

Password fatigue can lead to users adopting poor password practices, such as using weak passwords or reusing the same password across multiple applications. This can significantly weaken an organization's security posture and make it easier for attackers to gain unauthorized access to sensitive resources. Moreover, password fatigue can also lead to increased help desk calls for password resets, which can be a drain on IT resources.

In many organizations, different departments or systems may maintain their own user databases, leading to disparate identity silos. This fragmentation makes it difficult to manage user identities and access rights consistently across the organization. It also complicates the process of onboarding and offboarding employees, as changes in one system might not be reflected in others.

To overcome these challenges, organizations are increasingly adopting centralized identity management solutions. These solutions provide a unified view of user identities and access rights across all systems and applications. Centralized identity management not only simplifies administration but

also enhances security by ensuring consistent enforcement of access policies and reducing the risk of orphaned accounts or inconsistent access rights.

Data governance refers to the overall management of the availability, usability, integrity, and security of the data employed in an enterprise. A crucial component of this is access control.

However, achieving effective data governance can be challenging. It requires consistent reporting to provide visibility into who has access to what data, when they accessed it, and what they did with it. This can be a complex and time-consuming task, particularly in large or complex environments.

Software as a Service (SaaS) applications are becoming increasingly prevalent in business environments. While they offer many benefits, such as scalability and cost savings, they also present unique challenges when it comes to access control in security.

One of these challenges is managing multi-tenancy. Multi-tenancy refers to a situation where multiple users or groups share the same application instance, each with their own separate and secure access.

In addition, SaaS applications often have complex permission structures that can be difficult to manage and understand. This can make it easy to accidentally grant more access than intended, potentially exposing sensitive data to unauthorized users.

Identity and Access Management (IAM) plays a key role in modern access control strategies within organizations. IAM systems are designed to identify, authenticate, and authorize individuals or groups of people to have access to applications, systems, or networks by associating user rights and restrictions with established identities.

IAM plays a few important roles in securing access control within modern organizations:

- **Centralization of identity management:** IAM centralizes and simplifies the management of user identities. It provides a framework for managing digital identities and access rights, ensuring that only authorized individuals can access the right resources at the right times for the right reasons.
- **Facilitating user management lifecycle:** IAM facilitates the entire user management lifecycle, from provisioning (creating accounts and assigning access), through to the ongoing management of user access and eventually deprovisioning (removing access and deleting accounts).
- **Enabling advanced authentication and authorization techniques:** IAM systems incorporate advanced authentication and authorization techniques, such as multi-factor authentication

(MFA), role-based access control (RBAC), and attribute-based access control (ABAC), to provide additional layers of security for access control.

- Improving user experience and productivity: Beyond security, IAM solutions also enhance user experience and productivity. Single Sign-On (SSO) capabilities, for instance, allow users to access multiple applications with a single set of credentials, reducing password fatigue and streamlining the login process.

Here are some important best practices that can make access control more secure.

Implementing multi-factor authentication

Multi-factor authentication (MFA) requires users to provide two or more verification factors to gain access to a resource. This could be something they know (like a password), something they have (like a smart card), or something they are (like a fingerprint).

By implementing MFA, you add an extra layer of security. Even if a malicious actor manages to get hold of one factor, they will still be unable to gain access without the other factors. MFA is especially useful in protecting against phishing attacks, where attackers trick users into revealing their passwords.

Implement Strong Password Policies and Consider Going Passwordless

Passwords are often the first line of defense in security. However, weak passwords can easily be guessed or cracked by attackers. Implementing strong password policies is a must. These policies should enforce the use of long, complex passwords and regular password changes.

But even strong passwords have their limitations. They can be forgotten, stolen, or even guessed. That's why many organizations are now considering going passwordless. Passwordless authentication methods, such as social login, magic links, and biometrics, eliminate the need for passwords altogether, reducing the risk of password-related breaches.

No Shared Accounts

Shared accounts, which are used by multiple individuals or systems, are often a major security risk. They make it difficult to track user activities and hold individuals accountable for their actions. If an incident occurs, it's almost impossible to determine who was responsible.

Instead of shared accounts, consider implementing individual user accounts. These accounts should be tied to a specific individual, making it easier to track activity and identify any potential issues. This also helps in fostering

a sense of responsibility among users, as they know their activities can be traced back to them.

Even in situations where shared accounts seem inevitable, there are other ways to manage this. For instance, you could use privileged access management solutions that allow for session monitoring and logging. Such solutions give you improved visibility into who did what, and make it possible to investigate and respond to suspicious activity.

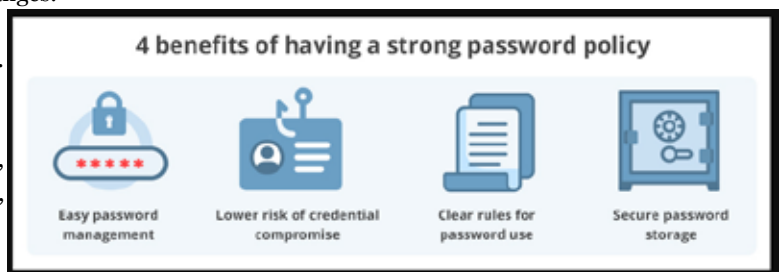
Implement the Principle of Least Privilege

The principle of least privilege (PoLP) is a computer security concept where a user is given the minimum levels of access necessary to complete his job functions. This approach minimizes the risk of malicious activities, as the access to sensitive information and systems is restricted.

The implementation of least privilege is a continuous process. It begins with a comprehensive audit of users and their access rights. Once the audit is complete, unnecessary privileges are revoked. This is followed by regular reviews and updates to ensure that the privileges remain aligned with the employees' roles and responsibilities.

It's not enough to just implement the principle of least privilege. You must also monitor for privilege creep, which occurs when users accumulate more access privileges over time, often exceeding what they need to perform their jobs. Regular audits and proactive management can help prevent this from happening.

Zero trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.



The zero trust model operates on the principle of “never trust, always verify.” This means that every access request is thoroughly vetted, regardless of where it comes from or what resource it accesses.

Implementing zero trust requires a shift in mindset. It requires letting go of the old assumption that everything inside the network is safe. However, with the right approach and tools, it can significantly enhance your organization's security posture. ■

Advertise here with us and reach your potential customers @ ₹.4200/- per month

AD Size
92mm x 120mm

Job Postings

Post your job opening here!

This space can be yours.
Contact us for more information
about this space

Tender Notices

Post about your tender notices here!

This space can be yours.
Contact us for more information
about this space

Education & Training Course

Post about your education & training here!

This space can be yours.
Contact us for more information
about this space

Security Equipments Rentals

Post about your security equipments rentals here!

This space can be yours.
Contact us for more information
about this space

Products & Services Offered by MSME's

Post about your products & services here!

This space can be yours.
Contact us for more information
about this space

Repair & Maintenance Services

Post about your repair & maintenance services here!

This space can be yours.
Contact us for more information
about this space



Grow Your Business With Us!
Your Connect to Channel Markets

- The premier security and fire safety technology focused channel magazine.
- Comprehensive coverage of physical and IT security products and issues that matter most to decision makers
- It features the latest technology and educative updates, news, articles and more
- Vital information that helps formulate strategy and make business decisions
- It reaches even the smallest installer in the remotest part of India
- Available as a Print and Online version



EVENTS CALENDAR

 **INDIA**
04-05 July, 2024
International Police Expo 2024
Pragati Maidan
New Delhi
www.internationalpoliceexpo.com

 **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**
04-05 July, 2024
8th India Homeland Security Expo
Pragati Maidan
New Delhi
www.homelandsecurityexpo.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

 **INDIA**
05-06 July, 2024
SAFE South India
Chennai Trade Centre
Chennai
www.safeindiaexpo.com/

 **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/

 **HONG KONG**
10-12 July 2024
Fire Asia 2024
Hong Kong Convention Centre & Exhibition Centre
<https://fireasia2024.com/en/index.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


 **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

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

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



PAST SUPPORTING PARTNERS

SECURING THE CITIES FOSTERING GROWTH

Safety of public defines the character of the city.
PRAMA Safe City solution assures safety of public for
a better growth and development.

PEOPLE MANAGEMENT

- Facial Recognition
- Behavioral Analysis
- Crowd Density Analysis

VEHICLE MANAGEMENT

- Traffic Enforcement
- Traffic Flow Management

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