VOLUME 23 | MARCH 2026 | ISSUE 1 | 17 €

79 824

GIT SECURITY INTL

MAGAZINE FOR SAFETY AND SECURITY – WORLDWIDE

Cover Story page 8:

25 Years One Jump Ahead

Salto Systems: From a Bold Idea to a Global Access Ecosystem

BEST-OF EXCERPT

More news, case studies & tech reports on www.GIT-SECURITY.com

WILEY

WILEY

REGISTER NOW

CLOSING DATE
MARCH 31st

Conditions of Participation on:

www.security-award.com

BHE | TÜV HESSEN | VDMA | ZVEI: Automation | ZVEI: Sicherheitssysteme | WILEY

A New **Story** Begins

As we enter 2026, one reality is clear: Rapidly advancing AI and rising geopolitical tensions are rewriting traditional threat models creating uneven levels of protection and shifting the responsibility of security leaders from safeguarding systems to safeguarding people.

Security today is not merely a technological discipline. It is about protecting lives, environments and the continuity of communities in a world that is transforming faster than the structures designed to secure it. It is in this climate that we open the first issue of the year.

This edition begins with a milestone worth pausing for: Salto's 25th anniversary. On page 8, we look at how a wire-free idea grew into a global access ecosystem that helped shape the modern language of secure movement. Their story is more than a retrospective; it is a reminder that trust, innovation and user-centric design can scale together, and a hint of where digital identity and access are headed next.

On page 14, Lufthansa Group's Daniel Lehner offers a candid look into personal protection in corporate environments, where abstract threats quickly become real, and where preparedness, training and clear structures determine whether organizations are able to act in the critical minutes before help arrives. His insights show what duty of care truly requires in a time of hybrid, unpred

The theme of preparedness continues in education. Schools and universities are no longer dealing with simple facility logistics; they are managing hybrid digital–physical vulnerabilities. Our article on page 24 explains why outdated keys or isolated systems can no longer meet this responsibility, and how modern credentials, cloud management and real-time oversight build the foundations for safer, smarter campuses. Three case studies illustrate what this looks like in practice.

Looking ahead, we turn to the technologies shaping the coming year. Genetec (p.36) cuts through industry hype to identify what will matter most in 2026: flexible cloud strategies, responsible AI, and unified system architectures that allow organizations to derive real operational value from their security investments. And Axis (p.38)

Cinzia Adorno

extends this view with a forward-looking analysis of ecosystems, edge AI and mobile video, showing that the future of security will be defined not by isolated devices, but by the intelligence and connectivity that bind them.

Before we close, a word to all creators, developers and security thinkers: This year's GIT SECURITY Award is your chance to stand alongside a community that's redefining best practices and building what comes next. If you've developed something that deserves the spotlight, we invite you to share it with us and take part in the 2026 competition. Entries remain open until March 31.

Have a good read,

Cinzia Adorno

Cover Story

25 Years One Jump Ahead

Salto Systems: From a Bold Idea to a Global Access Ecosystem

page 8

Dennis-Kenji Kipker

Marc Gomez

Daniel Lehner

Hanna Bjuke

Martin Reguero


Nima Hooshyar and Suraj Parmar

Gaelle Ramu

Comfortably read your e-Issue of GIT SECURITY on your sofa: Register here

INDEX

QUICK-FINDER

ORGANISATIONS, INSTITUTIONS AND COMPANIES IN THIS ISSUE


© Cyberintelligence institute

RISK MANAGEMENT

Between War and Peace

Hybrid Attacks and the Impact on Critical Infrastructure

Drone overflights at airports and Bundeswehr sites, digital espionage, covert influence operations and "disposable agents": traditional military conflicts are increasingly being replaced by subtle, multilayered forms of threat. Since the beginning of Russia's war of aggression against Ukraine, Germany has been confronted with a growing number of such incidents. Companies and operators of Critical Infrastructure now face the challenge of fundamentally transforming their security architectures. GIT SECURITY International spoke with Prof. Dennis-Kenji Kipker, founder and Research Director of the Cyberintelligence Institute.

GIT SECURITY International: Professor Kipker, in recent times we often hear that the boundaries between peace and war are becoming increasingly blurred. What is your view on this?

Dennis Kenji Kipker: It describes the growing dissolution of traditional distinctions between clearly defined military conflicts and periods of formal peace. What is meant is that states and non-state actors deploy measures that are conflict oriented but deliberately remain below the threshold of an openly declared military attack. This includes covert, asymmetric, digital and psychologically effective methods that can be flexibly combined. This approach creates a grey zone in which civilian and military spheres overlap, exposing those affected to a permanent state of latent threat.

There have recently been several worrying cases of drone deployments – for example at the airports in Copenhagen and Munich. Could you give us a situational overview?

Dennis Kenji Kipker: Since the beginning of the Russian war of aggression against Ukraine, Germany has seen a clear increase in unauthorized drone overflights. The documented figures already exceed several hundred incidents, with more than 440 overflights recorded above Bundeswehr sites alone in 2023.

The range spans from large, high performance military drones that are presumably controlled from greater distances – such as from ships in the North or Baltic Sea – to commercially available quadcopters operated at close range by individuals. What exactly are hybrid attacks?

Dennis Kenji Kipker: Hybrid attacks describe the strategic combination of various physical, digital, intelligence based and psychological tools aimed at destabilizing states, societies or companies, without triggering an open military escalation. These attacks include acts of sabotage, cyber operations, traditional espionage as well as information and influence operations. The combination of different attack vectors makes it difficult to identify the perpetrator and complicates appropriate political or international law responses. Proxy groups, cover identities or non state organizations are often used for concealment. Due to their multidimensionality, hybrid attacks simultaneously affect operational, structural and psychological levels, creating an environment of persistent uncertainty.

Since the attack on Ukraine, Russian diplomats have repeatedly been expelled. With intelligence officers lacking on the ground, "disposable agents" are now being hired. How exactly does that work?

Dennis-Kenji Kipker: Following the mass expulsion of Russian intelligence officers across Europe, the FSB and GRU have increasingly shifted to a model of short-term, digitally recruited "disposable agents." These individuals are often contacted via social media, receive instructions exclusively through encrypted messenger applications, and act primarily in exchange for payment. Many have a criminal background or a high willingness to take risks, or simply lack awareness of what they are getting involved in. They are used for sabotage operations, explosive attacks or simple espionage tasks.

The link between handlers and agents remains largely anonymous, minimizing the risk for Russian intelligence. Recruitment mechanisms are based on financial incentives, ideological messaging, psychological manipulation or - more rarely - blackmail. Operational control is divided across several intermediaries and layered communication channels. This approach complicates detection and attribution while deliberately amplifying psychological effects such as uncertainty and intimidation.

How well prepared are German companies and Critical Infrastructures for all this?

Dennis Kenji Kipker: The preparedness of German companies and Critical Infrastructure operators is currently undergoing major transformation processes. The

planned KRITIS Umbrella Act and the European requirements of the NIS2 Directive will create a comprehensive framework intended to harmonize security requirements and significantly raise the level of protection. Many organizations have already begun implementing expanded risk management, reporting and security requirements. Nevertheless, gaps remain in many areas, particularly in physical protection, defense against human attack vectors, and the integration of hybrid threat scenarios into security architectures.

The maturity level varies considerably depending on industry, resource access and the established security culture.

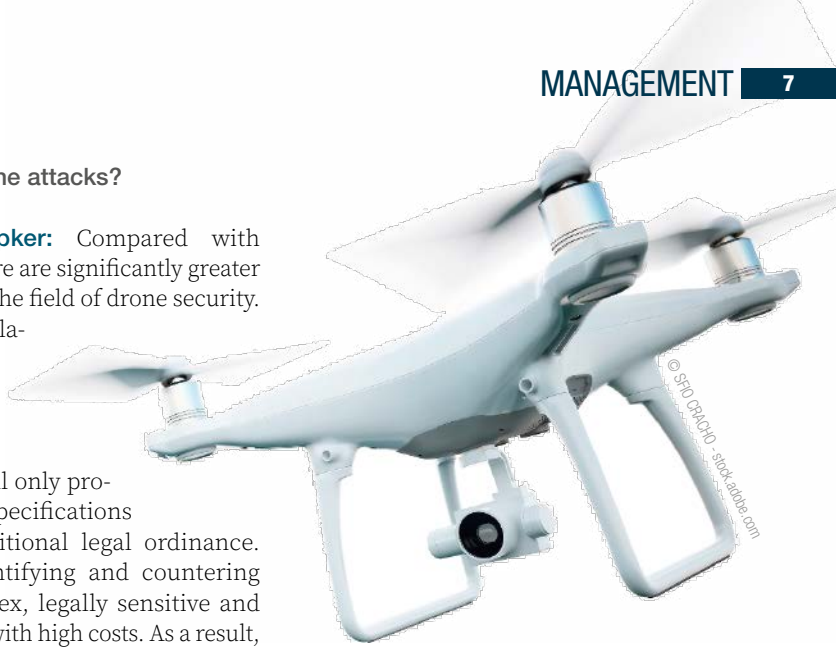
It is now widely accepted that one must prepare for cyberattacks, correct?

Dennis Kenji Kipker: The need for action in the field of cybersecurity is widely recognized in the corporate sector. That said, the threat landscape remains dynamic and requires constant adaptation. The NIS2 Directive obliges affected organizations to introduce and continually develop comprehensive technical, organizational and procedural protective measures. This includes, among other things, risk management and reporting obligations.

In many industries, corresponding standards have become established, and especially NIS2 affected entities, such as large companies and Critical Infrastructure operators, already possess relatively well developed cyber defense structures. However, SMEs, municipal administrations or educational institutions often still have catching up to do given the scale of the threats.

What about drone attacks?

Dennis Kenji Kipker: Compared with cyberattacks, there are significantly greater uncertainties in the field of drone security. A uniform regulatory framework is still lacking, and the planned KRITIS Umbrella Act will only provide concrete specifications through an additional legal ordinance. Technically identifying and countering drones is complex, legally sensitive and often associated with high costs. As a result, many companies and Critical Infrastructures currently possess only limited capabilities to systematically detect, classify or effectively prevent drone activities. The gap between the threat situation and available protective measures is particularly pronounced in this area.



What can companies and Critical Infrastructure operators ideally do? What would an optimal setup look like – and what can they achieve if they do everything right?

Dennis-Kenji Kipker: An ideal security posture is based on an integrated, multi-layered approach that combines technical, organizational and personnel measures. Key components include a systematic understanding of the threat landscape at leadership level, regular awareness and training programs for employees, and a comprehensive risk analysis that incorporates hybrid attack vectors. Building on this, holistic security concepts should be established, incorporating robust early-warning mechanisms, clear reporting chains, defined response procedures and recurring exercises. Organizations that implement this consistently achieve significantly higher responsiveness in crisis situations and reduce the effectiveness of the psychological impact associated with hybrid attacks. They can minimize operational disruptions, reduce attack surfaces and, ideally, identify vulnerabilities before they can be exploited. GIT

Cyberintelligence Institute
www.cyberintelligence.institute

COVER STORY

25 Years One Jump Ahead

Salto Systems: From a Bold Idea to a Global Access Ecosystem

For 25 years, Salto has been quietly redefining how the world secures spaces, identities, and movement. Founded in 2000 with a bold idea – bringing smart, networked access to any door without complex wiring – the company has grown from a small Spanish startup into a global leader in electronic locking, identity management, and cloud-based access solutions. Today, as organizations rethink security, flexibility, and digital identity, Salto's quarter-century journey offers a blueprint for how user-centric design, technological foresight, and trust can scale together.

Salto's early innovations, including RFID-based credentials, the Salto Virtual Network (SVN), wireless online systems, and later cloud-based mobile access, redefined what access control could be. Instead of viewing doors as isolated endpoints, Salto introduced a unified platform with one language and one seamless user experience.

Wire-free installations meant faster deployment with minimal disruption. Wireless networking enabled remote updates and management. A single ID-based credential allowed users to move seamlessly across entire facilities. Simplicity, security, and usability were no longer trade-offs; they became the foundation. This philosophy shaped Salto's DNA and positioned the company as an industry pioneer rather than a trend follower.

Marc Gomez,
CEO of Salto Wecosystem

Scaling Secure Access Worldwide

Over the past 25 years, Salto's solutions have expanded far beyond their original scope. Today, Salto technologies power more than 10 million access points, secure over 40 million daily users, and support over 100,000 projects across 40 countries.With more than 40 offices worldwide and a workforce of over 1,850 employees, the company serves diverse industries including education, healthcare, hospitality, residential, workplaces, and critical infrastructure.

Salto's position as one of the top three electronic lock manufacturers globally reflects its role in accelerating the worldwide shift from mechanical keys to digital and cloud-based access.

More Than Technology: People, Partners, and Culture

Behind every product and project are the people who believed in Salto from its earliest days, when the company operated from a modest apartment in northern Spain. Over time, these individuals connected teams, cultures, and countries, transforming a startup into a global organization. For Salto, success has never been just about technology. It has been about collaboration, partnerships, and a shared belief that secure access should empower people rather than restrict them. Every challenge solved and every relationship built has unlocked new opportunities for innovation.

The Salto Wecosystem Today

Salto is now part of the Salto Wecosystem, uniting Salto, Gantner, and Vintia under a shared mission: empowering access to places, experiences, and opportunities.

The ecosystem combines smart access, ticketing, digital identity, and electronic locking technologies into a connected platform that supports modern security and identity needs across industries.

Sustainability is also a core focus. Salto has achieved carbon neutrality through emissions reductions across product design, manufacturing, and energy use, including 100% certified green electricity.

Looking Ahead: The Future of Secure Digital Access

As Salto marks its 25th anniversary, the company continues to invest in AI, biometrics, cloud infrastructure, and digital identity platforms, technologies that will define the next era of access control.

"Our anniversary is both a celebration of the journey so far and a declaration of our future," says Marc Gomez, CEO of Salto Wecosystem. "We will continue advancing smart access to create safer, smarter experiences worldwide."

In an era where security, identity, and usability must work together seamlessly, Salto's next leap is already underway. GIT

Salto Systems
www.saltosystems.com

From a wire-free locking idea developed in northern Spain to a global smart-access ecosystem securing millions of identities, Salto celebrates 25 years of innovation and looks ahead to the future of digital trust; Salto Systems' headquarters in Oiartzun, Spain

PHYSICAL SECURITY

Trendy Topics For 2026

A Comparison of Today's Technology for Physical Security Applications

When predicting hot topics for 2026, no list would be complete without addressing the impact of artificial intelligence (AI) on the physical security sector. However, there are other technologies and trends that will likely shape and define the next 12 months. Andreas Beerbaum, VP of global sales and services, physical security, for Hexagon's Safety, Infrastructure & Geospatial division, discusses some options for the choice of security technology in 2026, starting with VSaaS.

Andreas Beerbaum, VP Global Sales & Service, Physical Security at Hexagon Safety, Infrastructure & Geospatial

Deploying bandwidth-hungry AI-powered video solutions relies on having the right foundation in place. Historically, video management systems (VMS) have been installed on-premises, requiring significant investment in infrastructure, maintenance, and upgrades. However, cloud-based VMS solutions (otherwise known as VSaaS – video-surveillance-as-a-service) are becoming increasingly popular with organizations operating across multiple sites. A VSaaS platform provides better access for these organizations and allows users to view, manage, and control video feeds from IP cameras (often from multiple vendors) from anywhere. Combined with powerful generative AI capabilities, a VSaaS platform can enhance situational awareness, improve response times and streamline post-incident investigations.

A 'traditional' CCTV system relies on human operators either monitoring live video feeds or reviewing recorded footage. This can be difficult given that the number of cameras will inevitably outnumber personnel, in some cases by 100 or 1,000 to one. This is where generative AI (video analytics) steps in, offering a second set of 'eyes' that work tirelessly in the background, analyzing video feeds in real-time to detect potential threats and alert teams before incidents escalate.

An added benefit of a cloud-first video management strategy is the reduction of

on-site hardware. Cloud-based systems lower energy consumption and carbon footprints – a priority for many European organizations striving to meet environmental goals.

Lidar switches from a buzzword to business case

At the start of 2025 Lidar was hailed as the 'next big thing' in physical security. The buzz has continued as Lidar took center stage in new security projects. For example, energy company EGD (part of the EON group) has deployed Lidar to improve the safety and security of electricity substations across its network. The demand for Lidar in perimeter security continues to grow: analysts value the global market at USD 1.38 billion in 2025, rising to USD 4.07 billion in the next eight years. Expect to hear more in 2026 about the use of 3D Lidar detection systems in a wide range of sectors, notably critical infrastructure, aviation and rail, data centers, correctional facilities, warehouses, and logistics operations.

Better sharing of video evidence

In the past five years, almost every UK police force has either deployed, or is in the process of rolling out, digital evidence management technology. One of the main drivers: making it quicker and easier to electronically request and receive CCTV and other video footage from businesses, particularly those in the retail sector.

The Crime and Policing Bill currently progressing through the UK parliament would repeal the 'immunity' afforded to shoplifters stealing goods valued at £200 or less. Furthermore, the British Retail Consortium (BRC) now recommends that retailers report every crime, assuring a forthcoming increase in the volume of video evidence to be shared in 2026. In addition, the National Police Chiefs Council Retail Crime Action Plan states that ".. retailers should send CCTV footage of the whole incident and an image of the shoplifter via the digital evidence management system as quickly as possible after an offense has been committed."

Retailers are investing heavily and the BRC estimates the cost of crime prevention at £1.8 billion per year, a 52% increase from 2022/23. Given these changes, the VSaaS model is an attractive proposition for a growing number of retailers. This shift to a cloud-first strategy will support the work being done by police forces. It will also mean that larger chains with centralized control rooms can retrieve and submit footage from individual stores faster, while smaller retailers will be able to share footage more efficiently, without the need to save it to a USB drive or disc.

The latest VMS solutions also support the integration of body-worn video, which is being widely adopted by retailers (particularly larger businesses in the UK) both for in-store and for delivery staff.

Riding the regulatory rollercoaster

The coming year promises major changes in the regulatory landscape for the physical security industry. In addition to the Crime and Policing Bill, other relevant legislation includes the UK's Terrorism (Protection of Premises) Act 2025 (Martyn's Law), the KRITIS-Dachgesetz, which impacts critical infrastructure operations in Germany, and the EU AI Act, which is currently being amended by the European Commission.

The next 12 months promises to be a year of innovation, investment and improvement in physical security. For organizations large and small, there will be access to highly advanced technology and deployment models that were either unaffordable or inconceivable just a few years ago. GIT

Hexagon
hxgnsecurity.com

© Image: Hexagon

POST-SHOW REPORT

Intersec 2026

A Global Benchmark for the Security Industry

With over 1,400 exhibitors and more than 50,000 trade visitors, Intersec 2026 at the Dubai World Trade Center confirmed its role as a global benchmark for the security industry. It clearly demonstrated how physical security, cyber-security and AI-driven intelligence are converging into integrated security architectures.

Under the patronage of His Highness Sheikh Mansoor bin Mohammed bin Rashid Al Maktoum, the exhibition, organized by Messe Frankfurt Middle East, placed a strong emphasis on resilience, command-and-control technology, and cyber-physical protection solutions for critical infrastructure, smart cities, and public spaces.

Messe Frankfurt Middle East underlined that Intersec has evolved from a classic product showcase into a strategic platform where global security challenges and solutions are discussed at an operational and policy level. A key message emerging from Intersec 2026 was the definitive shift towards integrated, multi-layered security systems. Physical security technologies such as access control, perimeter protection and video surveillance are increasingly embedded into digital ecosystems, supported by AI-based analytics, cloud architectures and cyber-resilience frameworks. According to Messe Frankfurt's official communications, this convergence reflects real-world requirements, where threats are no longer isolated, but hybrid in nature.

Artificial Intelligence

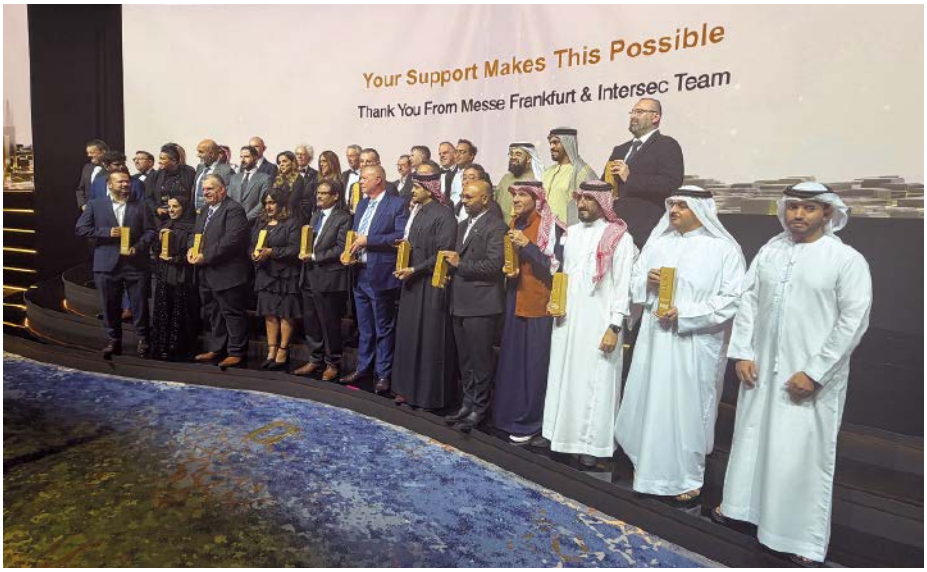
A dominant theme at Intersec 2026 was the application of deep learning models to large-scale video environments. Multiple manufacturers demonstrated analytics engines running parallel algorithms for facial and object recognition, vehicle and license plate identification, crowd density analysis, and perimeter intrusion detection. Warmly greeted were the advances highlighted by industry experts in the significant reduction of false alarms. Context-aware analytics can now distinguish between harmless deviations and genuine threats, delivering prioritized, actionable alerts to security operators. This capability is especially welcome in critical infrastructure environments. Another strong message from Intersec 2026 was the full integration of video analytics into unified security management systems. Video data is increasingly fused with access control, perimeter detection, radar, drone surveillance and cyber-security inputs, delivering a single operational picture that combines physical and digital security layers.

Artificial intelligence was one of the most dominant technology themes across the exhibition halls. Numerous exhibitors presented AI-supported video analytics, behavioral detection, object recognition and predictive security solutions. The focus was not merely on automation, but on improving situational awareness and decision-making speed in security operations centers.

Control Rooms

The Control Room Innovation Theater highlighted the changing role of security operations centers. Modern SOCs are

increasingly designed as intelligent command-and-control hubs, capable of orchestrating physical response, digital countermeasures and emergency coordination simultaneously. Discussions centered on cognitive control rooms, AI-assisted incident management and the integration of public safety, private security and critical infrastructure protection within unified platforms.Integrated solutions combining perimeter protection, intelligent video, intrusion detection and cyber-security were positioned as standard requirements for critical infrastructure protection, rather than premium options. Urban security and smart city protection concepts showed how digital twins, AI-based traffic and crowd analysis, and predictive risk modeling are increasingly shaping metropolitan security strategies.



Prizewinners at Intersec 2026

Future Priorities

Intersec 2026 demonstrated that security has become a permanently convergent discipline, where physical protection, cyber defense and intelligent data processing form a single operational reality. The exhibition provided not only a comprehensive overview of current technologies but also a clear outlook on future priorities: AI-supported situational awareness, cyber-physical resilience and integrated command structures. Intersec's 28th edition takes place January 11–13 2027 at the Dubai World Trade Center – co-located with Light + Intelligent Building Middle East. Yet another good reason to attend! GIT

Messe Frankfurt Middle East
www.messefrankfurt.com

Keenfinity Group acquires Avonic

From left to right: Murat Keskinkilinc and Pawandeep Singh (Keenfinity Group), Martijn van Bodegom (Avonic), as well as Walter Harrewijn (CEO of Avonic) and Lars van den Heuvel (Keenfinity Group), at the signing ceremony of the acquisition agreement.

Keenfinity Group's Audio Business has signed an acquisition agreement with Avonic, a provider of AI-driven cameras and voice-tracking technologies for the AV conferencing market. The move strengthens its audio portfolio with integrated, state-of-the-art video solutions, giving system integrators a seamless, one-stop offering. Both companies serve mission-critical environments such as government, institutions, education and corporate settings, where video has become essential for hybrid meetings. By combining Avonic's AI-enabled video with reliable audio, Keenfinity delivers an intuitive, future-proof experience for on-site and remote users. CEO David Hunter said the acquisition expands leadership in conferencing and supports fully integrated customer solutions. Bosch-branded conference products, now under Keenfinity, continue their legacy of quality and reliability, with Avonic's PTZ cameras and software driving further innovation and integration.

www.keenfinity-group.com

PERSONAL PROTECTION

Safety and Security in an Emergency

How companies take responsibility with strategic personal protection and amok prevention

Daniel Lehner is the head of a specialized personal protection team at the Lufthansa Group, previously worked for over a decade with a special task force and advises on protection concepts, operational security structures, measures and behavior in extreme situations. In his article for GIT SECURITY International, he explores the question of how companies can prepare for attacks, rampages and direct threats to employees.

The idea that there could be a targeted or indiscriminate attack on a company, a rampage or a direct threat to a manager or employee still seems remote to many (security) managers or decision-makers – almost theoretical, but at least very abstract. People generally think that the police will come – or „We're not relevant, something like that won't happen here…".

But this assumption is dangerous. Because actual incidents don't happen in theory, but in everyday life: at public events, in office buildings, on business trips on trains or in parking garages.

From my time as a police officer and now head of a specialized personal protection team in the corporate environment, I know that the dynamics of such threat situations are fast, complex – and above all unpredictable. If you only react when it is already too late, you have no options for action.

This article is intended to raise awareness and show how modern companies should position themselves today in the area of personal protection and crisis management – not with martial measures, but with strategic foresight, integrative security concepts and practical preparation with real-life scenarios. Because real security does not begin with planned access, but with understanding.

© Lufthansa Group / Oliver Roesler

Real Threats, Real Responsibility

In July 2025, a 21-year-old employee attacked several colleagues with a knife on the premises of a public utility company. One woman was killed and two others were seriously injured. Only the courageous intervention of employees was able to prevent further deaths or injuries. The pre-existing mental illness could have prompted preventative measures under certain circumstances.

The incident shows possible gaps or weaknesses in internal communication or early detection. Lessons can be learned: companies need low-threshold structures for the early detection of mental health crises, clear escalation paths and employees who know how to act in an emergency.

Incidents Involving Mentally Disturbed or Violent Persons

Not every incident ends fatally – but every incident has the potential to do so. An employee of a furniture store in the north threatened a colleague by telephone after being dismissed and announced that he would return to the store armed – a dismissal is an everyday situation for any company. The police were on the scene very quickly with special forces and were able to search for and apprehend the perpetrator.

Such situations are highly dynamic, very difficult to assess and, depending on how quickly information is provided, the perpetrator may already be on site. This requires well-prepared employees who can act in a de-escalating but decisive manner and quickly convey factual information to the right people, such as the emergency services.

Dealing with such scenarios requires specific first responder training, clearly defined communication channels and prepared response plans – this is the only way to save time, which is very valuable in such scenarios. The difference between professionals and beginners is the extent to which they shorten the response time and intervene or react with clear options for action.

Potential Scenarios in the Group Environment

Many threat scenarios are not made public for understandable reasons. Whether it is threats against managers, escalated dismissals or external threats – large corporations in particular often symbolize industries, actions or past events and are increasingly exposed to specific risks.

The conclusion from this is that the protection of exposed persons and particularly vulnerable areas of the company should not be a taboo subject – it should be part of every organization's security strategy.

Training, Equipment and Mindset

Skills and quick reactions are not a question of instinct, but of preparation and targeted training. Personal protection teams must train mental stability, stress resistance, clear priorities (e.g. level-headed approach, no „hunting fever", self-protection before intervention) and tactical thinking under stressful conditions more than once! A „freeze" must not be an option in an emergency.

A well thought-out personal protection concept including an „amok component" includes Means of communication (radio, silent alarm (visual)), emergency call systems, evacuation and retreat plans (including alternative routes such as roofs etc.), first aid equipment focused on the „stop the bleeding concept", surveillance areas, recognizability for the police and clear coding.

The training or scenarios must go far beyond mere theory and include the following in particular: Behaviour in the event of a rampage, evacuation, shielding or intervention, first aid measures under self-protection (assessing and prioritizing multiple casualties) and communication with the following emergency services.

Waiting is Not a Safety Concept

In many companies, the principle persists: „We wait for the police – we don't do a shootout here." This attitude may seem prudent at first glance, but in an emergency it is not only wrong, but also very dangerous.

The police rarely arrive at the scene before the first critical minutes (7 to 10 minutes) have passed. Anyone who fails to act in this first phase – whether through evacuation, lockdown measures, protective measures or first aid – not only risks human life in this phase, but also capitulates to violence with a lack of concept. During this critical period, the responsibility lies with those who are already in the building: The personal security team, plant security and trained personnel.

Professional security forces and personal protection teams know that it is not about catching the perpetrator: It is not about fighting the perpetrator, but about protecting lives, slowing down the violent acts or distracting from the victims and gaining time until special forces, such as police SEKs, take over the situation.

Companies that employ armed security personnel in particular have a responsibility. Security does not mean violence – it means being prepared, acting responsibly and with an acceptable level of risk. Professional protection concepts do not rely on confrontation, but on active, graduated action: Evacuation, shielding, medical first aid or communication with the arriving emergency services. This also includes shielding endangered persons or controlled retreat. Inaction under the guise of de-escalation is not a strategy – it is the opposite of protection.

Assumption of Responsibility and Ability to Act

It is important in this context: No one expects a company or organizational unit to take on the role of the police – especially not the role of a SEK. But anyone who has an armed personal protection team – internal or external – bears responsibility.

Anyone who instead remains passive and simply waits for the authorities risks human life and, in an emergency, breaches their own duty of care and sense of responsibility.

Security does not mean violence – but certainly the ability to act. A prepared response team can save lives in an emergency. Not through „shootouts", but through control, clarity and consistent action.

A strong and resilient security network is based on cooperation – not only internally, but also with external partners:

- Police and emergency services need a clear briefing, a clear summary of the situation, rapid familiarization with the location and evacuation aids.
- Personnel management, communication and legal must be involved in the event of threats from the inner circle.
- Managers must be able to fulfill their role during and, above all, after a crisis (evacuation responsibility, communication and follow-up).
- Emergency plans and crisis teams: clear communication, response and, in particular, aftercare for all employees – we don't send anyone home without a face-to-face meeting.

Please turn page ▶


© Lufthansa Group, Alex Tino Friedel ATF Pictures

© Lufthansa Group

Processing Phase

The processing phase begins immediately after an incident: crisis intervention teams, pastoral care, psychosocial support, availability of talks for those affected and first responders, training for managers in dealing with traumatized employees.

Professional follow-up always includes a debriefing, a short „hot debrief" at the end of the operation and a detailed one after an appropriate period of time with the following focal points:

- Tactical follow-up: Was the procedure as trained and expected by everyone? An honest analysis of weaknesses – what didn't work? Because we always learn best from mistakes. Clear documentation for improvement and a memory log.
- Long-term measures include training for new employees, integration into the company health management system and internal communication that is open, honest and solution-oriented.

Conclusion

Threats of violence in the corporate environment have long ceased to be an abstract danger – they are real and have already occurred on several occasions, as recent cases show. Anyone in a position of responsibility today – whether in management or on the board of directors, in corporate security or human resources (HR)—must understand that Security is not a one-time measure, but a continuous process that is and must be constantly changed or adapted in light of current events.

Modern protection concepts combine adequate risk awareness, tactical preparation, interdisciplinary cooperation, and a commitment to duty of care. The decisive factor is not whether something happens, but whether you are prepared. GIT

Lufthansa Group
www.lufthansagroup.com

Securitas CFO Announces Departure

Securitas' focus remains on becoming the leading intelligent security solutions partner for our clients by combining our extensive presence with connected technology and intelligent use of data. Andreas Lindback, CFO, has decided to step down from his position at Securitas to spend more time with his family. This change is effective from the second quarter of 2026. All other Group Management members continue in their current roles. „Thank you for your hard work and tireless dedication to Securitas in all the roles you have held over the last 15 years. Your integrity and commitment are second to none and have been essential to our delivery of very ambitious targets. I have personally truly appreciated our partnership and wish you all the best for your next chapter", says Magnus Ahlqvist, President and CEO. **www.securitas.com**

Building on 40 Years of Trust: Introducing TDSi by Hirsch

Integrated access control and security manufacturer TDSi today announced that from 1st January 2026, it operates under the new name: TDSi by Hirsch. The change follows the global transformation of its parent company, Vitaprotech, into the Hirsch Group, unifying its security brands worldwide under one trusted name. As TDSi moves into this next chapter as TDSi by Hirsch, its commitment to its customers, partners, and the wider security community remains unchanged. All existing products, services, support channels, and points of contact will continue as normal, ensuring complete continuity throughout the transition.

Customers can expect to see the TDSi by Hirsch Logo begin to roll out from early next year, marking the start of a gradual evolution rather than an overnight change. With the strength of the Hirsch Group behind it, TDSi is poised to deliver even greater value while continuing to operate with the same reliability, expertise, and customer-first approach that have defined the business for over four decades. **www.tdsi.co.uk**

Integrated intelligent monitoring and early-warning analytics enable SafeStore Auto to detect gradual interference and strengthen overall security resilience.

HIGH VALUE STORAGE

Silent Threats

Enhancing Detection and Response in High Value Storage Environments

Threats rarely present themselves in a single, predictable way. While some are immediate and overt, others develop gradually and remain unnoticed until their impact is felt. They vary in speed, scale and direction, which makes reliance on any one security measure insufficient. Effective security responses, says Hanna Bjuke, Sales Director for High Security Solutions, Gunnebo Safe Storage in Europe depends on a layered approach, where different elements work together to address different types of risk and ensure the right level of protection is in place at every point.

Changing Characteristics of Physical Threat

Before 1985, only individual components such as doors could be certified, not the security architecture, leaving many older vaults with an inherent and often unseen vulnerability. As a result, their true level of resistance is difficult to determine with confidence.

Recent events have reinforced how adept organised criminal groups are at assessing systems in their entirety, identifying points of weakness and exploiting them. Where the overall architecture has never been certified, such weakness may be far more accessible than anticipated. Construction methods material properties environmental conditions and operational routines are studied to enable slow controlled progress that avoids attention. Rather than breaching access points attackers may target structural boundaries that sit outside traditional access focused security models.

Planned criminal activity is timed to coincide with predictable reductions in oversight such as weekends, holidays extended closures or periods of reduced staffing. Under these conditions interference can continue unnoticed for long durations particularly when detection systems are configured to respond only to sudden change. Gradual drilling cutting or manipulation produces low level vibration acoustic emission and minor structural movement. Similar signals may be generated by benign sources including building services maintenance activity or nearby works. When viewed in isolation these indicators could be easily dismissed. Risk accumulates when indicators are not interpreted over time. Security strategies benefit from contextual analysis, particularly where threats develop gradually and remain low visibility.

Detection and Interpretation Over Time

Effective protection depends on the ability to correlate information rather than react to single events. Vibration acoustic structural and environmental data provide greater value when assessed collectively across extended periods. Patterns trends and repetition often provide stronger indicators of interference than any individual signal. Establishing reliable baselines is critical, especially where background conditions vary significantly between facilities and over time. This baseline, supported by a modern and reliable intrusion alarm system

SafeStore Auto eliminates direct human access through a fully automated vault design, raising physical protection to a higher level.

and clear internal procedures designed to reduce the risk of fraud, creates a stronger and more resilient overall security foundation. Intelligent systems support interpretation by distinguishing cumulative anomalies from routine background activity. Their value lies in supporting informed decision making grounded in context.

Response as a Risk Control

The purpose of physical protection is to introduce delay, slowing an intrusion for long enough to allow an effective response. Higher-grade vaults are designed to withstand attack for longer periods, which is particularly relevant given that many older vaults were never formally certified. In those cases, resistance times can be extremely limited, increasing the likelihood intruders have already left the site before the police arrive. Monitoring needs to always be continuous rather than periodic and remotely available by authorised personnel. Centralised oversight supports this requirement particularly during periods when on site presence is limited. Real time visibility allows emerging risks to be assessed before routine inspections would otherwise occur. Clear escalation structures allow for single events to be highlighted alongside indicators observed over a longer period. Decision-making is then shaped by accumulated evidence, enabling more informed responses, reducing the likelihood of errors and ensuring operational interventions are proportionate and timely.

Operational Routines and Residual Exposure

Operational routines influence exposure within high-value storage environments in ways that are not always immediately visible. Inspection frequency, periodic checks, and reliance on certified construction can affect how emerging issues are identified and addressed over time. Secure facilities should be understood as dynamic systems, with risk profiles that evolve in response to changes in usage, maintenance practices, staffing structures and the surrounding environment. Safe storage environments are built around layered protection and continuous assurance. Continuous monitoring, regular servicing and periodic reassessment of threat assumptions ensure alignment between physical protection and detection capability. For private investors the implications may not be immediately visible. Assets placed in secure storage frequently hold long term financial legal or personal importance. Prolonged undetected access can therefore result in consequences that extend well beyond direct financial loss.

Confidence Trust and Institutional Impact

Confidence in safe storage depends on visible control as much as physical strength. When incidents reveal prolonged undetected interference attention quickly shifts from construction standards to oversight effectiveness. Banks and private storage providers face increased scrutiny following such events particularly where multiple customers are affected. Questions focus on whether warning signs were present and how they were assessed rather than whether structures met certification requirements. Rebuilding confidence depends on demonstrable improvement in integrated detection monitoring, visual verification capabilities and response rather than reassurance alone. Institutions that can evidence continuous oversight and informed escalation are better positioned to maintain trust.

Regulatory and Standards Context

Regulatory frameworks and industry standards increasingly reflect an integrated view of physical security. Resistance ratings are complemented by expectations around detection response and ongoing management. European and international guidance emphasises the relationship between structural protection monitoring capability and operational control. Compliance assessments increasingly consider whether ongoing interference can be identified and addressed rather than relying solely on certified resistance performance.Operational context plays a central role in this assessment. Facility layout staffing models asset types and local threat conditions all influence residual risk. Controls that are not adapted to these variables may leave exposure unaddressed despite formal compliance.

Looking Ahead

As threat methods continue to evolve, institutions that regularly review and adapt their security assumptions are best positioned to sustain resilience over time. High value storage environments are often designed with long service lives in mind. Construction decisions made decades earlier may still define the protective envelope today. While certified resistance does not expire operational reality around those structures changes continuously. Older structures may not be as resilient as assumed, particularly as tools, techniques and the value of stored assets change. Staffing models shift as institutions pursue efficiency and automation, while the rapid growth of digital systems makes robust authorisation, strong digital protection and clear access procedures increasingly essential. Each of these factors influences how interference signals appear and how easily they can be recognised. Ongoing service and maintenance allow detection strategies to adapt to changing operational and environmental conditions.

Compliance to Latest Security Standards

Banks and private investors encounter both governance and technical considerations in security management. Decisions are often shared across property management, security operations, compliance and executive leadership. When responsibilities are well-coordinated and embedded into operational foundations, risk assessment can be more proactive and continuous. Strengthening visibility and collaboration helps address potential gaps before they are exploited. Insurance considerations

increasingly reflect expectations around monitoring and preventative controls. Prolonged undetected activity can lead to disputes over whether reasonable protective measures were in place particularly where losses span multiple accounts or clients. Documentation of monitoring oversight and response processes therefore becomes as important as construction certification. For private investors and family, offices reliance on third party storage providers introduces additional dependency. Due diligence focuses on physical specifications location and reputation. Transparent governance and demonstrable monitoring practices provide an important basis for confidence. From a regulatory perspective physical security, supervisory attention increasingly considers whether institutions can evidence control over risk throughout the lifecycle of an asset or facility. Detection and response capability form part of this expectation even where explicit prescriptive requirements are limited. Standards bodies have begun to reflect this shift by emphasising the relationship between resistance detection and response rather than treating them as independent domains. Compliance is moving toward a performance based assessment of resilience rather than a binary evaluation of construction features. Institutions that continue to treat physical protection as a one-time investment may find themselves exposed despite formal compliance. Those adopting a systems-based view, inclusive of initial design, specification, maintenance and monitoring are better positioned to adapt as threat methods change.

In summary, as regulations, market pressures and risk factors continue to evolve,

Hanna Bjuke, Sales Director for High Security Solutions, Gunnebo Safe Storage in Europe

innovation must be introduced, aligned with latest developments in integrated security technology, Ai and machine learning, inclusive of connectivity and cloud-based platforms. Balancing these forces requires informed leadership and a willingness to revisit assumptions, based on the definition of safe storage.

Gunnebo Safe Storage continues to engage with financial institutions regulators and standards bodies to contribute to this ongoing reassessment of physical security. Solutions such as SafeStore Auto incorporating Planar Protection reflect an approach where structural resistance, intelligent monitoring and operational oversight function as a unified system. In an SafeStore Auto, no individual has direct access to the vault interior, which elevates the level of physical protection well beyond traditional safe deposit lockers.

Within this integrated framework, early awareness, informed response and alignment with evolving regulatory expectations become attainable objectives, delivering ongoing and trusted peace of mind. GIT

Gunnebo Safe Storage
www.gunnebosafestorage.com

Altronix Partners with Hanwha Vision

Altronix has partnered with Hanwha Vision to support the launch of Hanwha's new OnCafe access control platform. As part of the collaboration, Altronix's Trove Access and Power Integration products become the preferred power option, enabling seamless system design and reducing installation time and labor costs. According to Altronix President Alan Forman, the partnership reflects a joint commitment to high performance, cost-efficiency and reliable protection for customers. Hanwha Vision Product Manager William Vallera highlighted Altronix's proactive product development, strong technical support and engineering collaboration as key reasons for the partnership, calling the company a true innovation ally. He emphasized that Altronix solutions are known for their flexibility, U.S.-based design and manufacturing, and a lifetime warranty, reinforcing trust and long-term reliability.

www.solutions.altronix.com

Primion Belgian Subsidiary Renamed

As part of its strategy to consolidate and align internationally, Primion has announced the completion of the legal renaming of its Belgian subsidiary: GET NV is now Primion Technology NV.

The legal renaming of the Belgian subsidiary of Primion GET NV to Primion Technology NV is purely an administrative step and does not change day-to-day operations. Continuity is ensured for customers and partners, existing business relationships remain unchanged, all contracts retain full legal effect, established points of contact stay the same, and the Belgian VAT/tax number also remains unchanged.

Primion Technology's converged security solutions and workforce management solutions continue to be available as before, with the new legal name now appearing on contracts, invoices, and other official documents. **primion.io**

Now

Register for our free Newsletter

Your **Number 1** for over 20 years

e-Issue included!

News for Decision-makers and Managers in Safety & Security Matters

www.GIT-SICHERHEIT.de/de/newsletter/register

WILEY

LEADERSHIP

Introducing Martin Reguero

Strengthening Optex's Presence in Iberia

Martin Reguero has recently joined Optex as Key Account Manager, based in Madrid. With over 30 years' experience in the security industry, Martin brings a wealth of expertise in intrusion systems, access control, CCTV and fire detection. His career combines practical knowledge of installations with extensive experience in commercial and customer service roles.

Martin has spent much of his career working closely with installers, distributors and end users, supporting them through training, system demonstrations and practical solutions to real-world problems. In his new role at Optex, he will be responsible for developing and supporting key accounts, working closely with customers to create long-term value and collaborating with Nikitas to combine a commercial approach with solid technical expertise, strengthening Optex's local presence and customer support.

Optex Europe: Can you tell us a little about your background and your journey in the security industry?

Martin Reguero: I started my career over 30 years ago in the security industry, and since then it has been a journey of learning and growth. I started out working directly in the installation of intrusion systems, which gave me a solid understanding of how security technologies work in real-world conditions. Over time, I moved into commercial and customer service roles, working closely with installers, distributors and end users to provide training, demonstrations and practical solutions. This combination of technical and commercial experience has been incredibly rewarding and continues to shape the way I approach my work today.

What initially attracted you to joining OPTEX?

Martin Reguero: Optex has a very strong reputation in the security industry, and being part of a company with a recognised and trusted brand was an important factor for me. I was also attracted by the opportunity to contribute to Optex's expansion in the Iberian market and to work with a team that values both technical expertise and excellent customer support.

What do you enjoy most about your role?

Martin Reguero: What I enjoy most is interacting with our customers, understanding their challenges and helping them find the right solutions. It is incredibly satisfying to be able to support them in a way that generates real and lasting value, strengthening our relationships. Being able to combine technical knowledge with a commercial approach makes the job interesting and rewarding every day.

What is your favourite Optex product and why?

Martin Reguero: It's hard to choose just one, but I would say that Optex's outdoor detectors really stand out. They are incredibly reliable and versatile, making them a key component in many security solutions. Knowing that these products can help protect people and property gives me a real sense of pride in what we offer.

And finally, how do you relax and unwind outside of work?

Martin Reguero: Outside of work, I enjoy spending time with my family and enjoying outdoor activities. Whether it's going for a walk, exploring nature, or simply spending quality time at home, this helps me recharge and stay focused. GIT

Optex Europe Ltd
www.optex-europe.com

BIOMETRICS

Trust, Not Surveillance

How Facial Recognition Can Be Used Responsibly in Democratic Societies

Facial recognition is among the most controversial topics in modern video analytics. On one hand, there are concerns about intrusions into privacy, excessive surveillance, and potential biases in algorithms. On the other hand, the technology offers opportunities for solving serious crimes. Given its high risks and high potential, facial recognition requires responsible use. How can we balance technological progress with responsible application? Thomas Jensen, CEO of Milestone Systems, explores this question in his contribution to GIT SECURITY International.

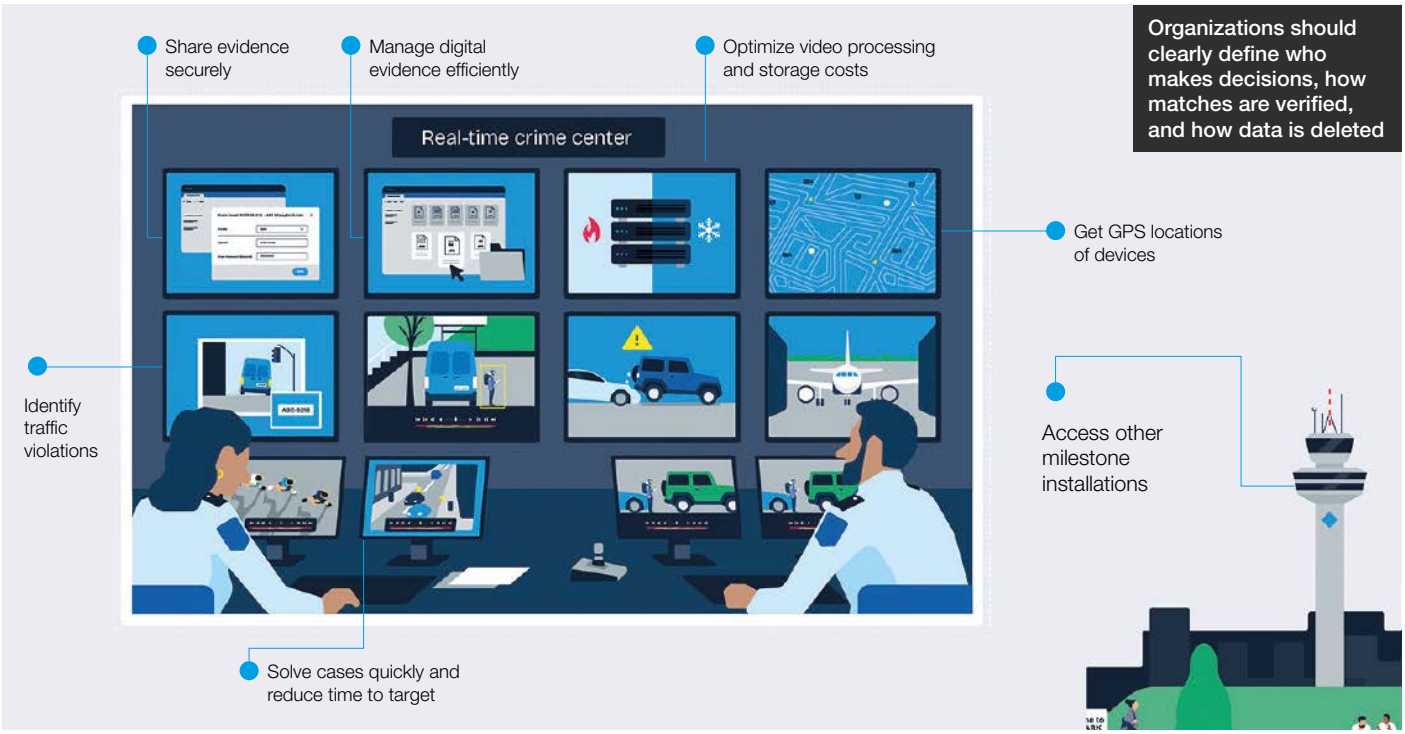
Many people fear that facial recognition could be misused as a tool for blanket surveillance. The idea of being recorded at all times conflicts with fundamental democratic values and represents a deep intrusion into personal privacy. For this reason, facial recognition should only be used in clearly justified situations. These include comparisons with well-defined, legally authorized databases such as Europol or Interpol watchlists. Its use can also make sense when searching for missing persons, provided that family members give their consent.

Using photos from social networks without explicit and informed consent would be highly problematic. Personal pictures were never published with the intention of ending up in surveillance systems. Moreover, if databases were filled without strict purpose limitation, every person would become a potential match.

A positive example of a privacy-friendly application is facial recognition at automated border control gates in airports. There, the live image of a traveler is compared solely with the biometric photo stored in their passport. The data is processed locally and only for the duration of the check. Another important aspect concerns the security of biometric data. Modern systems do not store raw images. Instead, a digital signature is generated from a face, one that is largely useless to other systems and cannot be reverse-engineered. Even so, high security standards remain essential, including strong encryption, access controls, and strict rules for data minimization.

Algorithmic Bias

Critics rightly point out that facial recognition can misidentify people. Groups that are underrepresented in training data are



particularly affected. Studies by the MIT Media Lab and the U.S. National Institute of Standards and Technology have shown accuracy differences for women, older people, and individuals with darker skin tones.

This makes it even more important to systematically detect and reduce bias. Developers should build fairness-testing methods directly into their processes. Systems should also be regularly tested with diverse datasets that reflect the real population. Transparency around accuracy rates for different demographic groups is a fundamental requirement.

Facial recognition is among the most controversial aspects of modern video analytics

Clear Procedures and Legal Boundaries

Facial recognition belongs in areas involving serious crimes or acute threats. Normalizing its everyday use would gradually erode civil liberties.

Regulation plays a crucial role. The European Union's AI Act sets clear boundaries. It largely prohibits real-time facial recognition in public spaces. Exceptions apply only in special cases such as searching for missing persons, responding to an imminent terrorist threat, or identifying suspects in serious crimes. Retrospective analysis of recordings is possible, but only under strict judicial oversight.

Real-time recognition is often seen as particularly invasive. However, such systems immediately discard data that is not needed, whereas retrospective analysis relies on stored footage. What matters, therefore, is not the method itself but the context and purpose of its use. Real-time systems must be restricted to narrowly defined watchlists.

In addition to legal requirements, clear internal guidelines are essential. Organizations should define who makes decisions, how matches are validated, and how data is deleted. The four-eyes principle is recommended: any match should be verified by at least two qualified individuals. Logging, documentation, and clear retention periods are also necessary. A storage duration of 30 days appears reasonable unless an active investigation is ongoing.

Unified standards would support responsible use across countries. Facial recognition is a tool designed to support fast decision-making, it does not replace human judgment.

Shared Responsibility

Public authorities establish the legal framework, but technology companies share responsibility as well. They should define clear codes of conduct, communicate openly about system limitations, and train their customers. They must also be prepared to decline business opportunities that fail to meet their ethical standards, even if such use might be legally permitted.

Moreover, it is important for companies to actively collaborate with policymakers. Only then can regulatory frameworks emerge that realistically address both the opportunities and risks of emerging technologies.

Facial recognition should remain a carefully regulated tool. It belongs in scenarios where significant risks or dangers exist. With clear rules and responsible application, it is possible to strike a balance between technological development and the protection of privacy. GIT

Milestone Systems
www.milestonesys.com

Dallmeier Goes Logimat 2026: Panomera V8 in Focus

– From March 24 to 26, 2026, Dallmeier experts will showcase how companies can make their logistics and security processes more efficient, transparent, and secure with state-of-the-art video technology "Made in Germany". At the joint booth of the Mobility & Logistics Cluster at Logimat 2026 (hall 4, booth 4D53), the spotlight will be on the new Panomera V8 – a high-performance camera solution for expansive logistics areas. With just a single system, it provides seamless 180° coverage with no blind spot, enabling uninterrupted monitoring, rapid incident analysis, and the optimization of operational workflows. A special highlight this year is the new Panomera V8. With a single camera, it delivers 180° panoramic coverage of large traffic, loading, and transshipment zones. This allows for reliable monitoring of vehicle movements, loading operations, and security-relevant events – all without blind spot. Combined with intelligent video analytics, the system enables accurate counting, optimization of operational workflows, and rapid incident analysis – contributing to increased efficiency, security, and transparency across the entire site. **www.dallmeier.com**

ACCESS

School's Out – And In

Digitizing to Manage Access Control in an Educational Environment

Across Europe, the Middle East and beyond, schools, colleges and universities are looking to modernize security while preserving openness. Their duty of care extends to protecting people, property and data, yet education sites must also enable the free movement of staff, students, and visitors. At the same time, budgets are tight and expectations of user experience are high. The right access management strategy must reconcile safety, efficiency and cost-effectiveness – and when implemented effectively, it can greatly benefit daily operations.

Education sites always host multiple user-groups with different access needs, as have schedules that are constantly shifting. Staff, students, contractors, and other external users share the same spaces at different times of day. Management may be complex and time-consuming at sites where they still rely on mechanical keys, often across large campuses. Lost or duplicated physical keys can expose entire premises to risk and require expensive re-keying. Manually updating permissions for thousands of users is inefficient. Outdated systems and protocols may make it difficult to monitor who is on site or to coordinate a rapid lockdown in an emergency.

Facilities teams are frequently looking for intelligent access solutions that provide real-time visibility, centralized control, and reduced maintenance. An increasingly digital-native user-group, especially the students themselves, expects the convenience of digital solutions such as mobile keys stored on their personal smartphone.

Recent data underlines the urgency of a more connected approach to access. UK universities, for example, are at high risk of a cyber breach, with perhaps millions of stolen credentials circulating on the dark web. Such weaknesses illustrate a growing hybrid threat. If a single credential can both open doors and provide access to in-house networks, its compromise endangers the institution's operations and reputation. To mitigate these risks, mobile digital credentials – instantly revocable, amend-

able, and traceable – can help education facilities teams to close this gap. Reliable, digital physical security and access is now a fundamental building-block of the modern education institution.

The Solution is Access Digitization

Digitization offers a coherent way forward. Assa Abloy has extensive experience in digitizing access management for educational buildings, helping these institutions to create a secure, safe and convenient environment for students, teachers and visitors. A vast range of Assa Abloy digital solutions can protect people and valuable assets from the perimeter right into the heart of a building, all the way to intelligent locks for server racks that integrate seamlessly with almost any access management software. Schools and universities can choose to manage access rights on-site, via a secure cloud, or with a choice of Software as a Service packages.

For security staff and facilities managers, programmable locks and credentials boost the responsiveness and efficiency of access management. Lost or stolen cards can be deactivated with a click, preventing unauthorized entry without the expense and hassle of having to replace hardware. Rights are issued, amended, or withdrawn remotely, backed by a full audit trail. Digital access also enhances flexibility: smartphone or smart-card credentials can be configured for specific areas and time windows, supporting after-hours study or revenue-generating rentals while maintaining control, for example. Facilities managers gain oversight across multiple buildings and can administer access off-site through intuitive software. The outcome is safer, more adaptable premises and a significant reduction in administrative effort – and therefore costs. For staff and students, the convenience and security of a digital credential gives them the peace of mind to move about the premises in safety and comfort.

European standards and regulation also support this digital shift. EN/IEC 60839 sets functional and interoperability requirements for digital access systems, while EN 179 and EN 1125 specify safe egress for emergency exits. The GDPR ensures personal and credential data are handled transparently, and biometric use is governed by national consent laws such as France's CNIL or the UK Protection of Freedoms Act. In addition, the EU's NIS2 Directive is bringing many academic research locations under its scope, obliging them to strengthen both digital and physical protection in line with the directive's "all-hazards" approach to connected security. Institutions that fail to comply risk financial penalties; another clear incentive to modernize access infrastructure. In this regulatory environment, investment to meet these evolving challenges is building. The European school and campus security market was valued at around EUR 0.92 billion in 2025, and continues to expand as educational facilities modernize and further digitalize access.

Learn From Real-World Case Studies

Firstly, For The Camp, a business-education provider based near Aix-en-Provence, France, realized that security had to match its culture of innovation. Their site has offices, event areas, kitchens, and on-site accommodation operating around the clock. Safety for a constantly changing population of residents and visitors required an access system able to adapt in real time.

Assa Abloy Aperio wireless devices are now integrated with TIL Technologies' platform to simplify management of access to the entire campus from a single interface. Permissions are updated instantly as staff, students and guests arrive or depart. Lost credentials are canceled and reissued on demand. Defined profiles segment access to areas such as meeting or server rooms, keeping valuable assets secure even during busy events. Wireless devices also align with The Camp's sustainability goals. Battery-powered operation reduces energy consumption compared with hard-wired systems and preserves the site's architectural aesthetic. Security, flexibility and environmental responsibility work together.

Secondly, at Vejle Friskole in Denmark, maintaining mechanical keys used to consume several hours each week. Lost keys caused disruption, and tracking who had access to which rooms was an onerous task. The school installed a SMARTair wireless digital access system, an out-of-the-box solution managed with straightforward software. Each teacher and student carries a programmed fob with individual permissions. When a credential goes missing, administrators simply update digital rights, instead of changing cylinders – saving money and time.

This simple change has transformed daily administration. Security management now takes minutes rather than hours, freeing security staff time for other responsibilities. The system also supports flexible building use outside school hours, allowing safe access for events without adding to the workload or risk. For smaller schools without dedicated security staff, SMARTair provides an accessible, easily scalable route to digitization.

Thirdly, in Villiers-le-Bel near Paris, the financial impact of lost keys could run to thousands of euros per incident. Staff at the Municipal Technical Center used to carry multiple keys for different sites; when one went missing, entire suites of locks required replacement. Administrators digitalized with Cliq electromechanical locking cylinders and programmable keys. Using the Cliq Web Manager software, lost keys are now canceled immediately and new permissions issued remotely. Each programmable key stores the user's specific access rights, replacing dozens of physical keys with one secure, flexible credential.

The new system has reduced both cost and complexity. Staff no longer collect keys from a central office, and administrators monitor access across schools and other municipal buildings via a standard web browser. This enhances protection for sensitive sites while keeping the solution scalable and within budget.

Towards Smarter, Safer Campuses

The education sector's digital transition is accelerating, in both learning delivery and facilities management. Rapid change in access control is being driven by a need for operational efficiency, national and regional regulations and compliance, and the fast-evolving risk landscape. NIS2 adds further urgency specifically at universities where sensitive research is conducted. Whether in a small primary school or a multi-site university, wireless and intelligent-key technologies enable cost-effective control across every opening. Hybrid cyber–physical threats highlight the importance of secure credential management, for example. Microsoft estimate that more than 40% of UK universities face attack on a weekly basis. Mobile digital credentials, quickly and remotely canceled if lost or compromised, are one powerful defense. Integrated, standards-based digital access at schools and universities across the EMEIA region can not only underpin compliance, but also the trust and flexibility essential to delivering education's mission. GIT

Assa Abloy Opening Solutions EMEIA
www.assaabloy.com

© EWN

SWITCHES

Smart Grid Security

How redundant OT communication, hardware and UPS solutions from Connect Com and Slat make the energy supply future-proof

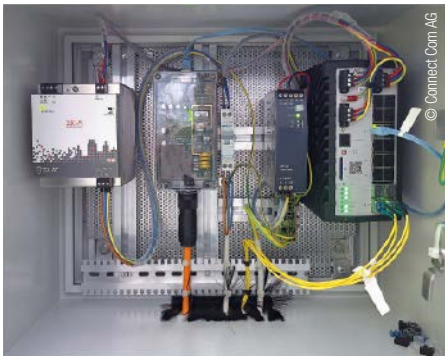
The Nidwalden cantonal electricity utility in central Switzerland (EWN) was faced with the challenging task of replacing at least 80% of its electricity meters with smart meters in line with the Swiss Energy Strategy 2025 – a project of considerable scope, as it involved over 20,000 meters. This involved modernizing the entire OT communication infrastructure to meet the high requirements for availability, reliability and future viability.

In times of increasing digital networking, a stable network infrastructure is the basic prerequisite for a reliable energy supply. Any interruption can lead to considerable disruption. The aim was therefore to build a flexible and scalable network that supports future intelligent requirements in the smart grid. A key requirement was to ensure that both the switches and the connected end devices remain continuously supplied even in the event of outages or power fluctuations.

By using a PLC smart meter solution that communicates via Aginode switches with redundant power supply through Slat DC UPSs from the SDC series, the energy supplier found a strong partner for current and future requirements in Connect Com AG Switzerland.

Backbone of OT communication

The systems offer a highly available network architecture that ensures redundancy at all levels. With Aginode switches, which use a bumpless redundancy protocol, dual communication paths are available. If one path fails, the data is forwarded seamlessly and without interruption as it is sent in parallel via both paths. This ensures maximum availability of critical control and protection systems.


© Connect Com AG

Protection of OT hardware through multi-level power supply

- A 48 V power supply unit ensures a stable primary supply for the switches.
- A first 48 V micro-UPS from Slat's SDC series secures the supply to the Aginode switches, protects against failures and voltage fluctuations and enables uninterrupted communication.
- A second 48 V SDC supplies the connected end devices separately so that they can also continue to run reliably in the event of power failures.

In addition to high availability, the two micro-UPSs also offer extensive monitoring and diagnostic functions via RS-485/Modbus and enable proactive maintenance and remote monitoring.

The advantages at a glance

- Maximum operational reliability: Redundant data and power paths reliably protect communication and control devices from failures.
- Seamless switchover: Power failures are intercepted immediately; interruptions to data communication are ruled out.
- Real-time monitoring: Remote monitoring of the power supply enables a rapid response to faults and reduces downtimes.
- Modular and scalable infrastructure: Easy expansion for smart grid applications or the integration of additional IoT devices
- Sustainability and longevity: High-quality components and intelligent control maximize the service life of the systems and minimize maintenance costs.

With the integrated solution from Connect Com Switzerland, "Kantonale Elektrizitätswerk Nidwalden" (EWN) now operates a robust, highly available and digitally controlled OT communication infrastructure that confidently meets the high demands of modern Swiss energy supply.

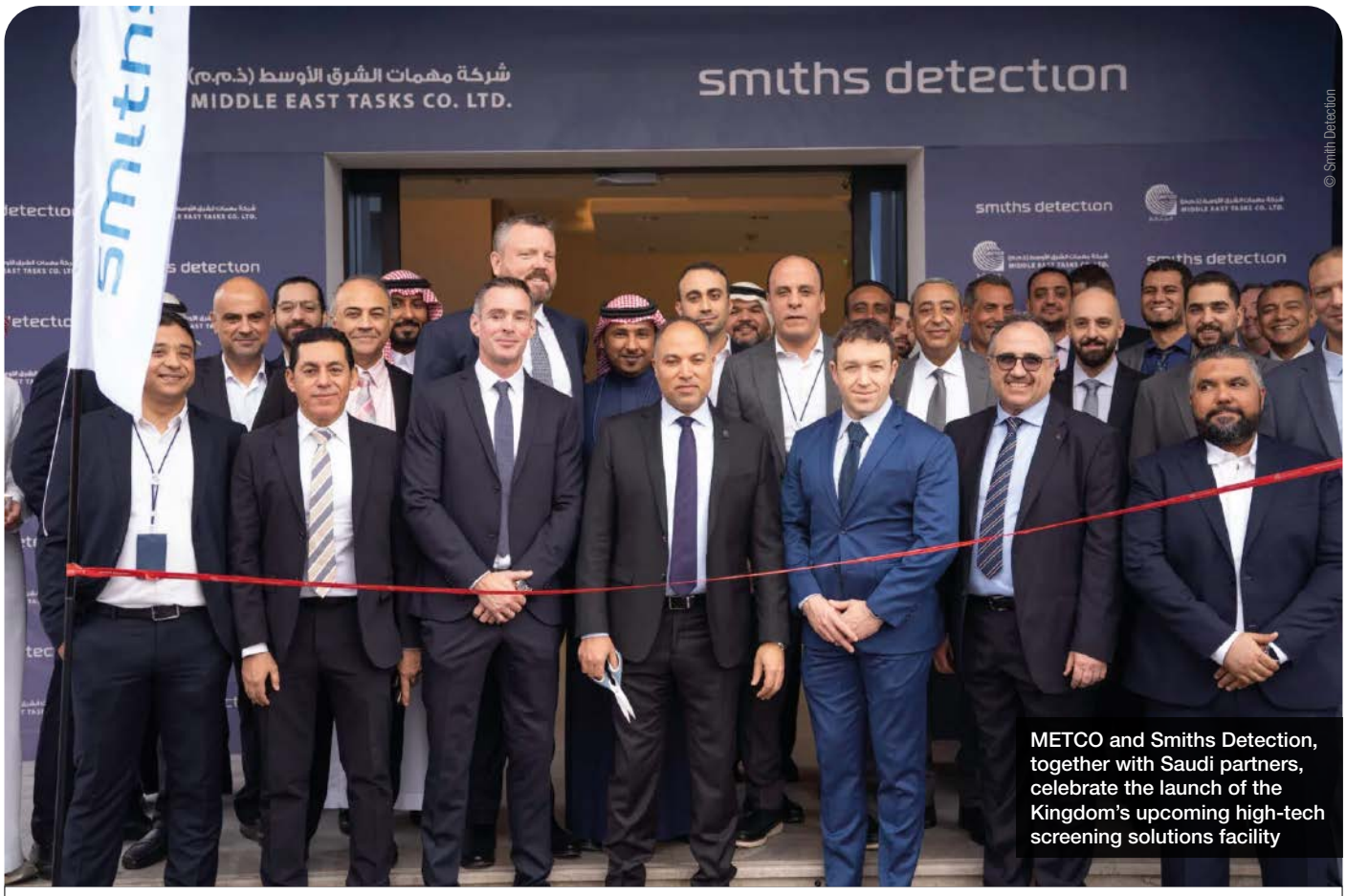
Author:
Frauke Petzold

Slat GmbH
www.slat.com

BUSINESS

Building Tech Strength

METCO and Smiths Detection Announce Opening of New Assembly and Manufacturing Facility in Saudi Arabia Aligned with Vision 2030



METCO and Smiths Detection, together with Saudi partners, celebrate the launch of the Kingdom's upcoming high-tech screening solutions facility

METCO, with partner Smiths Detection, today announce that the opening of its new Assembly and Manufacturing Facility, designed to assemble, commission and manufacture advanced screening solutions (including Smiths Detection's industry-leading X-ray screening products) is scheduled for Q1 2026.

The new facility will not only serve as an assembly and commissioning hub but also feature a dedicated showroom where clients can explore the full range of METCO and Smiths Detection's screening solutions and products. In addition, the centre will include a comprehensive training facility, providing hands-on experience and professional development for security personnel and operators.

The initiative aligns with Saudi Arabia's Vision 2030 and beyond, supporting the Kingdom's goals of technological advancement, workforce development, and local capability building in high-tech sectors. Importantly, the facility is expected to create a significant number of jobs for Saudi nationals and allow them to gain valuable experience at a national level, contributing to both career growth and the Kingdom's broader development objectives. By collaborating with leading technology partners, METCO is ensuring that the facility upholds the highest standards of quality, safety, and innovation.

"We are excited to expand our capabilities with this new Facility," said Osama Shasha, CEO of METCO. "It enables us to provide end-to-end support for our clients, from product assembly, commissioning, manufacturing to training and demonstrations, all under one roof, while contributing to the Kingdom's broader vision for innovation, local industry development, and workforce skill-building. The facility is expected to begin operations in Q1 2026, offering an integrated platform for showcasing and supporting cutting-edge screening technologies."

"We are proud to partner with METCO in Saudi Arabia," said Matt Clark, VP Commercial at Smiths Detection. "Our mission is to make the world a safer place and together with METCO, we are committed to deploying industry-leading security screening solutions in KSA as well as training security operators to deliver the best possible security and passenger experience outcomes for airports." GIT

Smith Detection
www.smithdetection.com

THREAT DETECTION

Eyes Beyond Sight

Khon Kaen Airport Enhances Airside Security with Navtech Advance Guard

Khon Kaen Airport, a key regional hub in northeastern Thailand, plays a crucial role in supporting the area's industrial, commercial and logistics activity. Handling around 1.5 million passengers per year, the airport's growing operations required a more robust approach to monitoring airside movements and ensuring uninterrupted safety across expansive open areas.

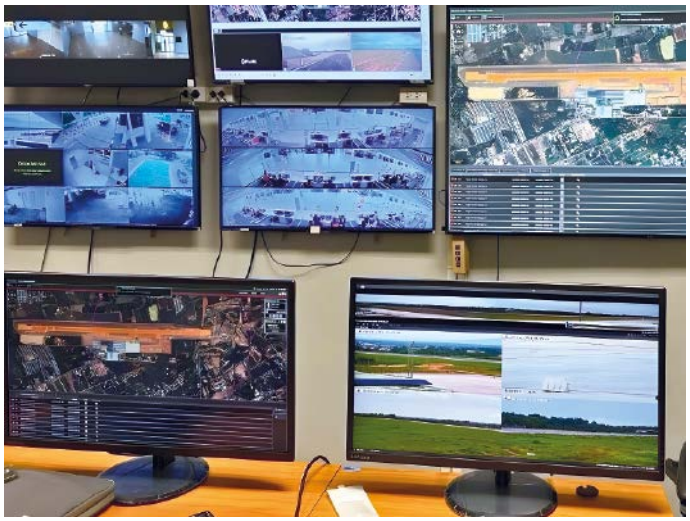
For years, security teams had to contend with rapidly changing weather conditions, reduced visibility and the operational limitations of traditional camera-based systems. These systems often struggle in rain, fog or low light, creating blind spots and making it difficult to maintain continuous situational awareness. As airside activity increased, the need for technology that could deliver dependable, all-weather detection became more urgent.

The Challenge: Reliable Detection in All Conditions

Khon Kaen Airport needed a future-proof security solution capable of detecting and tracking unlimited targets simultaneously across large distances, without performance degradation during adverse weather. Maintaining high operational resilience was essential, as even brief monitoring interruptions could slow responses to unauthorised access or runway incursions. To meet these requirements, the airport partnered with Navtech Radar and local technology consultant Chotipon Bunyarat. Together, they identified radar as the most effective approach for ensuring continuous, precise and scalable surveillance. The result was the adoption of Navtech's AdvanceGuard system; an intelligent radar-based solution that delivers real-time situational awareness and supports security teams with consistent, reliable data regardless of conditions.

The Solution: Integrated Airside Security

Working collaboratively, Navtech Radar and consultant Chotipon Bunyarat



Dallmeier Panomera multi-focal sensors and Hikvision cameras are integrated to enable real-time visual verification, giving operators complete awareness and a faster, coordinated response to alerts.

A detailed site study helped define detection zones and optimize radar placement for full coverage, ensuring no blind spots across the active airside area.

Specialists review terrain, visibility challenges and infrastructure layouts to validate the AdvanceGuard surveillance design.

One of the newly installed HDR311 high definition radar units integrated with Navtech's AdvanceGuard software platform. The system delivers real time wide area monitoring, automatic rule based alerts, and seamless camera cuing for rapid airside incident verification.

developed an integrated solution based on Navtech's Advance Guard wide-area surveillance system. The installation uses two HDR311 sensors, each providing 1,250 metres of coverage, ensuring full airside visibility and early detection of unauthorised movement.

The radars were configured to focus detection within the airside, avoiding unnecessary alarms from activity outside the perimeter. This enables security teams to act quickly and confidently when real incursions occur. From the Advance Guard interface, operators can view all airside movement in real time, giving them complete situational awareness from a single screen.

The system is fully integrated with on-site Hikvision cameras, automatically directing them for visual verification when radar detects an object of interest. This seamless interaction between radar and cameras provides immediate visual confirmation and enables a fast, coordinated response.

The installation process included a detailed site study, commissioning, and performance tuning, ensuring the system achieved optimal coverage and consistent performance. The partnership between Navtech and Chotipon Bunyarat was central to the project's success, combining local knowledge with global radar expertise.

> For the cost, compared to the performance, Navtech Radar Solution can overwhelmingly win over other solutions
>
> **Chotipon Bunyarat,** Local Technology Consultant

Summary

Navtech's radar-based airside security solution at Khon Kaen Airport demonstrates the value of close collaboration and thoughtful system design. By combining Navtech's high-definition radar technology with local expertise, the airport now benefits from a fully integrated, future-ready solution that enhances security and operational efficiency.

Advance Guard gives operators a clear, reliable view of all airside movement in every weather and light condition. Integrated with Hikvision cameras, the system automatically directs them for visual verification, enabling faster assessment and coordinated response.

Through partnership and continuous improvement, Navtech and Chotipon Bunyarat have delivered a solution that not only meets today's airside security needs but continues to adapt as Thailand's aviation sector evolves. GIT

Navtech Radar Ltd
www.navtechradar.com

Powered by Nvidia: Milestone launches Vision Language Model (VLM)

Milestone Systems launched an advanced Vision Language Model (VLM) powered by Nvidia Cosmos Reason to improve real-world and traffic video understanding. The model drives two solutions: a Video Summarization tool for XProtect and Hafnia VLM as a Service (VLMaaS). The summarization plug-in converts video clips into quick, structured text summaries, helping reduce manual review and cutting false-alarm fatigue by up to 30%. Users can search content, filter events and integrate summaries with existing rules. VLMaaS gives developers API access to production-ready video intelligence, reducing the effort of building custom AI systems by up to 70 times. **www.milestonesys.com**

Planning locking systems is a complex process that Dom simplifies and accelerates with its digital platforms.

Nima Hooshyar, Product Manager cylinder systems, Web Tools & Loyalty Program Coordinator at Dom

Suraj Parmar, Group IT-Manager at Dom UK

ACCESS

Mastering Key Systems

How a Digital Platform Simplifies Complex Locking Systems

Dom Security's digital platforms aim to transform how locksmiths and security professionals interact with Dom products. Group IT Manager Suraj Parmar and Nima Hooshyar, Product Manager for Cylinder Systems and Web Tools at Dom, explain how in this interview.

GIT SECURITY International: Mr. Parmar, Mr. Hooshyar, for everyone who doesn't know eNet and the Master Key Planner: What are they?

Suraj Parmar: eNet is our digital platform that serves as the central touchpoint for customers. It is modular and can be adapted to specific market requirements. The Master Key Planner (MKS Planner) supports customers in planning and ordering complex master key systems.

Nima Hooshyar: The Master Key Planner simplifies the ordering process. It automates many tasks, optimizes workflows, and minimizes errors. Previously, planning data had to be sent via email or on paper. Now customers enter everything directly into the Planner, and the order goes straight into production.

And this works across national borders…

Nima Hooshyar: Eighty-five percent of our customers are already registered. They appreciate the easy handling and the central management.

Suraj Parmar: Each country has its own version, tailored to local needs, while the core system stays the same.

How did the development of the Master Key Planner come about?

Nima Hooshyar: Customers wanted an online tool instead of the Excel plan. With the Planner, they can place orders at any time, even on weekends.
Suraj Parmar: The Planner gives customers more control. It displays the configuration and pricing directly and speeds up all processes.

Is the Master Key Planner easy to use for people without technical expertise?

Suraj Parmar: Yes. It's designed for anyone who plans locking systems without needing to be an IT expert.
Nima Hooshyar: The design is modern and simple. Users can switch between the classic view and the new interface.

What does the ordering process look like?

Nima Hooshyar: Customers set up projects, choose key profiles, and add cylinders. The system guides them step by step and shows the price instantly.

Cylinders and Key Systems by Dom

Suraj Parmar: Orders are transmitted directly to production. Fast-lane orders are delivered within five days in Germany.

Is the Master Key Planner integrated into the fast-lane service?

Suraj Parmar: Yes, orders that meet the criteria are automatically flagged and processed immediately.
Nima Hooshyar: Customers instantly see which items are available and when they will be delivered.

What's next on the roadmap?

Nima Hooshyar: We want to make it possible to extend existing master key systems and order replacement cylinders through the Dom Master Key Planner as well.
Suraj Parmar: We're planning to launch the Planner in additional countries, automate key orders, and integrate Tapkey licenses. GIT

Dom Security
www.dom-security.com

Light + Building 2026 Frankfurt

From 8 to 13 March 2026, Frankfurt will once again become the global meeting point for innovation in lighting and building services technology. Light + Building, the world's leading trade fair in this sector, invites professionals and visionaries to experience the future of smart buildings and lighting design under the inspiring motto "Be Electrified – Electrifying Places. Illuminating Spaces."

Under the motto "Be Electrified – Electrifying Places. Illuminating Spaces.", Light + Building will showcase how electrification and intelligent connectivity are shaping the future of urban spaces and architecture. The fair focuses on three major themes: sustainable transformation, smart connectivity, and living light. These topics are highly relevant for security experts, as they highlight the growing role of integrated systems and digital technologies in creating safe and efficient environments. Visitors can expect a comprehensive program featuring trend talks, award ceremonies, and guided tours. Highlights include the Design Plaza, the prestigious IALD Awards, and dedicated areas for young talent and future-forward concepts. For security professionals, the event offers valuable insights into how lighting and building technologies intersect with access control, surveillance, and smart infrastructure. **www.messefrankfurt.com**

Motorola Solutions Expands AI-Powered Security Platform

At Intersec 2026 in Dubai, Motorola Solutions presented its latest AI-driven technologies for safety and security, highlighting how organizations can move from reactive incident detection to proactive response. A centerpiece of the showcase was Avigilon Visual Alerts, an on-premise generative AI solution that allowed security teams to create custom visual alerts and detect site-specific safety, compliance, and logistical risks across large camera networks. The system addressed the needs of key Middle Eastern sectors such as oil and gas and healthcare by providing real-time detection of hazards, patient falls, and restricted-area breaches. Motorola Solutions also demonstrated long-range cameras suited for extreme environments and operational resilience software designed to help enterprises better anticipate and manage events across their operations. **www.motorolasolutions.com**

ACCESS

Smarter Locking

Unified Online and Offline Access Control Management

Comelit-PAC has expanded its access control portfolio with the launch of PAC Lock, a fully integrated offline locking solution that enables customers to manage wired and wireless doors within the same Access Central platform.

PAC Lock extends Access Central with OSS-based offline locking, enabling unified management of wired and wireless doors.

PAC OPS credentials store permissions and events, allowing PAC Lock devices to verify access locally and maintain system integrity.

PAC Lock brings the benefits of Open Security Standard (OSS) offline technology to the PAC ecosystem. The result is a practical and scalable way to extend access control to areas where cabling or constant connectivity may not be possible or cost-effective.

David Hughes, Head of Product Management at Comelit-PAC, said: "PAC Lock represents a significant step forward in the evolution of Access Central. It gives our partners and customers the flexibility to secure more doors without compromising on system integrity or user experience. By adopting the OSS protocol and using our OPS credential across both online and offline environments, we're providing a unified approach that simplifies configuration and day-to-day management."

With PAC Lock, access permissions are written to the secure PAC OPS credential, which stores user permissions, event data, revalidation periods and other key information. When the credential is presented to a PAC Lock device such as an electronic cylinder, handle set or cabinet lock, the lock verifies the access permissions locally and writes the event to the OPS credential.

The credential is seen by the Access Central updating device and access permissions are updated, where events are collected and seen in the events screen or viewed as part of a standard report. This allows both online and offline doors to be administered through the same interface, ensuring consistency for installers, administrators and end users. PAC Lock integrates directly into the Access Central workflow, with offline locks configured and managed using the same process as wired doors. It includes defining access groups, assigning credentials and managing revalidation schedules. Installers benefit from a familiar setup procedure, reducing training requirements and simplifying deployment across mixed installations.

David Hughes concluded: "The introduction of PAC Lock means Access Central can now manage more doors, more efficiently, and in more environments. It's a powerful addition to the PAC range that strengthens our position as a trusted technology partner for installers and end users seeking flexible, future-ready access control." PAC Lock supports an extensive range of locking formats, including electronic cylinders, handle sets, padlocks and cabinet locks. This allows integrators to specify solutions tailored to different door types and usage patterns from main entrances requiring live online monitoring to interior areas where standalone control is sufficient. GIT

Comelit-PAC Ltd.
comelit-pac.co.uk

VIDEO

Intelligence-First Video Security

IQSIGHT Introduces a New Approach to Video Analytics

Accelerating into a new era of intelligence-first security, IQSIGHT is the evolution of Bosch Video Systems, delivering a synergy of trusted engineering and real-time visual intelligence. Empowering organizations to see clearly, act confidently, and improve outcomes in environments where every second matters.

Sabrina Stainburn, CEO of IQSIGHT – Formerly Bosch Video Systems

Accelerating into a new era of intelligence-first security, IQSIGHT is the evolution of Bosch Video Systems, delivering the perfect synergy of trusted engineering and real-time visual intelligence, empowering organizations to see clearly, act confidently, and improve outcomes in environments where every second matters.

According to a press release of the company, IQSIGHT is expanding AI-enabled video capabilities designed to eliminate blind spots and enable faster, data-driven decision making. While the brand has progressed, its foundation remains unchanged—more than 60 years of engineering excellence, reliability, and an unwavering commitment to innovation in video security.

"As security environments become more dynamic and complex, customers need intelligence they can trust," said CEO Sabrina Stainburn. "IQSIGHT delivers accurate and reliable alerts and insights that give teams foresight into events and patterns, helping them make fast, appropriate decisions. Our solutions have a strong legacy of proven performance even in challenging environments, and we are building on that portfolio to address the ever-changing threats our customers face."

Intelligence that works in the real world

IQSIGHT moves beyond traditional video surveillance by transforming video data into practical, actionable intelligence. Intelligence is delivered at the edge and within existing video management system (VMS) environments, with cloud capabilities applied only where they add value, ensuring reliable performance without unnecessary complexity or overhead. This intelligence-first approach enables solutions-driven outcomes across industries where safety, business continuity, and operational performance are deeply interconnected.

At ISC West, March 25-27 in Las Vegas, IQSIGHT will showcase AI-led offerings designed to perform under operational pressure, providing practical, reliable intelligence for education, government, critical infrastructure, transportation, and smart city environments. Highlights include:

1.Advanced analytics software delivering insights on object classification, counting, and attribute detection, including vehicle models and individuals' clothing colors, helping customers to shift from reactive response to proactive improvement

2.GenAI-driven scene understanding that interprets complex environments and identifies what is happening without requiring training on specific behaviors

3.IQSIGHT's new intelligence-first platform, powering the latest generation of cameras, including the Flexidome dual 7100i IR, Autodome 7100i IR, and Dinion 7100s series

4.Scalable, evidence-based outcomes delivered in collaboration with leading VMS partners, Genetec and Milestone

IQSIGHT
www.iqsight.com/en/

VIDEO

Large Areas, Smart Analytics

A New Generation of Intelligent Video Surveillance

The Panomera V8 brings together cutting-edge multifocal sensor technology and artificial intelligence in one device, delivering a seamless 180° field of view without blind spots and highly precise analytics, even across expansive areas.

Panomera V8: The new generation of intelligent video surveillance combines seamless 180° coverage with maximum range for smart solutions

Dallmeier's new Panomera V8 achieves a 180-degree field of view and uses eight lenses, eight sensors, and eight AI chips to capture a very large area with just one camera. A sophisticated process merges the eight systems into one large overview image and logically links the neural networks. This significantly increases the efficiency, precision and reliability of both human operators and AI-assisted systems. In this way, a wide range of environments - from public squares and logistics facilities to airport aprons – can be monitored and analyzed.

Business-Intelligence Applications

According to the company, a key differentiator of the Panomera V8 is its seamless 180° field of view with no blind spots, combined with the ability to logically connect the neural networks of the eight integrated AI chips. This eliminates one of the biggest weaknesses of many video analytics systems: incomplete, inconsistent, or duplicate image data.

This unique feature provides the ideal foundation for extensive analytical capabilities, both with Dallmeier's own AI analysis apps and with solutions from technology partners. The system's complete scene capture enables in-depth evaluations, whether for incident analysis, movement patterns, or the tracking of complex workflows. As a result, the Panomera V8 becomes the basis for a wide variety of security and business-intelligence applications.

AI That Delivers Real Added Value

The combination of a continuous image, high detail depth, and tightly integrated intelligent analytics creates extensive opportunities for users. People and objects can be located within seconds based on external attributes such as clothing or bags. Personnel or vehicle flows can be recorded with high precision, and large areas can be protected against unauthorized access with far fewer false alarms. Whether for queue management, effective crowd control, or improving parking operations, the system's advanced analytical capabilities not only enhance security but also help optimize operational processes sustainably.

AI Made in Germany

Like all Dallmeier products, the Panomera V8 is "Made in Germany" and meets the

highest standards for quality, reliability, and cybersecurity.

This also applies to the artificial intelligence: the manufacturer relies on self-trained neural networks, maintaining complete control over the training data. With this approach, the company aims to improve accuracy and reliability and establish a foundation for trust in the technology.

From Security to Efficiency

Whether in smart cities, airports, stadiums, logistics centers, or retail, the system enables operators to combine security with economic efficiency. Thanks to precise analytics, workflows can be improved, resources deployed more strategically, and costs reduced.

"With the Panomera V8, the camera becomes an essential data source," says Christian Linthaler, Chief Sales Officer at Dallmeier. "Our customers benefit not only from maximum security but also from valuable insights into their processes; a dual advantage that goes far beyond traditional CCTV."

The new Panomera V8 delivers a 180° view with no blind spots

Cost Efficiency Through Reduced Infrastructure

As with all Panomera models, the V8 series offers another crucial economic benefit: thanks to its extensive area coverage, significantly fewer cameras, poles, and cables are required compared to conventional systems. This greatly reduces the total cost of ownership (TCO) while increasing user convenience.

The system is suitable for smart-city applications (urban security and traffic-flow analysis), airports (passenger management, perimeter protection, and parking optimization), stadiums and events (crowd management and real-time security), logistics centers and ports (area surveillance and process optimization), as well as industrial sites and critical infrastructure (protection of sensitive zones and occupational safety). GIT

Dallmeier
www.dallmeier.com
www.panomera.com

Asis Europe 2026 Unveils Fourth Set of Leadership Track Speakers

The Asis Europe Conference 2026, taking place from 23–25 March in Antwerp, is further shaping its program with the announcement of its fourth set of Leadership Track sessions. The newly added topics highlight some of the most urgent challenges in modern security leadership, from AI-driven preparedness to human-centric resilience.

Sessions include an exploration of AI-powered digital-twin simulations for crisis readiness, presented by Massimo Pani, offering insight into how rehearsal intelligence can strengthen organizational response capabilities. A panel led by Dr. Karin von Hippel, Lucy Stone and Jacob Painter examines whether intelligence is merely a buzzword or a practical, dependable capability in security operations. Dr. Jose Marquez presents doctoral research demonstrating how Enterprise Security Risk Management (ESRM) enhances resilience in listed companies.

Dr. Johan J. de Wit emphasizes the need for co-innovation to keep pace with rapidly evolving security technologies, urging leaders to collaborate or risk falling behind. Finally, Thomas Michael Pedersen highlights the essential role of people, showing how workforce engagement and training can make employees the strongest link in an organization's security posture.

www.asisinternational.org

PHYSICAL SECURITY

What's Next

Genetec on the Future of the Physical Security Industry in 2026

According to security software provider Genetec, organizations will focus on flexibility, responsible AI, and unified, connected systems to strengthen security and enhance operational performance.

Cloud Deployment: A More Mature Discussion

In 2026, Genetec expects the conversation around cloud adoption to continue maturing. Companies will prioritize solutions that offer flexibility and scalability in deployment. Rather than committing to a single deployment model, they will evaluate each workload based on performance needs, cost, and data residency requirements. They will then choose the environment that best supports their operational goals; whether on premises, in the cloud, or a hybrid approach.

Open architecture solutions allow end users to select the devices and applications that best support their workflows. This approach extends the lifespan of existing infrastructure and allows teams to deploy cloud services where they deliver the most value. Providers offering comprehensive deployment options and strong interoperability across environments will be best positioned to meet these expectations. In contrast to proprietary systems that limit choice and lock customers into specific vendors, open solutions provide a more adaptable path that ensures long term flexibility and control.

AI: From Hype to Intelligent Automation

The conversation, Genetec predicts, will shift from the hype around AI and LLMs to practical, results driven solutions that enable intelligent automation (IA). IA will streamline workflows, increase accuracy, and enable faster, more informed decision making. It will automate repetitive tasks, improve monitoring accuracy, support predictive maintenance, and extract meaningful insights from growing volumes of data.

Instead of adopting technology for its own sake, users will focus on features that genuinely enhance daily operations, such as intelligent search to speed up investigations, reducing false alarms, and improving situational awareness. By optimizing response times and reducing manual effort, IA allows users to concentrate their time and expertise on critical tasks and decisions that require human judgment.

As the market matures, expectations for transparency and responsible implementation will rise. Users will demand clarity on how AI is applied, how systems are built, and how data is collected, processed, and protected. They will also expect providers to prioritize cybersecurity and ensure that AI features are deployed in a controlled, secure, and responsible manner. Organizations will move away from innovation for innovation's sake and instead focus on delivering measurable, trustworthy, and meaningful outcomes enabled by intelligent automation.

Modernizing Access Control

Genetec forecasts that access control will remain a high priority as companies modernize outdated systems and seek to maximize their return on investment. The value of access control goes far beyond locking and unlocking doors: it delivers measurable business benefits through improved energy efficiency, occupancy management, and operational insights.

Adoption of Access Control as a Service (ACaaS) will accelerate as companies seek simpler maintenance, greater scalability, and predictable operating costs. Organizations will favor hybrid deployments that combine on premises and cloud based

capabilities. By unifying ACaaS with Video Management as a Service (VSaaS), transparency will improve further and management across multiple sites will become more efficient.

Connected Systems

In the coming year, the number of connected devices will continue to grow as organizations integrate IoT sensors, building systems, and smart devices into unified security and operational platforms. Consolidating this information in one place gives teams a clearer picture of what is happening in their facilities and enables faster, safer responses.

The convergence of IT, operational technology, and physical security will accelerate, enabling real time data sharing and smarter decision making across all sites. End users will expect open, scalable platforms that securely connect diverse devices and deliver both operational and security related value.

As the landscape becomes increasingly complex, companies will look for guidance on how to select and manage the right technologies effectively. Leaders in the field will be those who can securely unify diverse devices, offer cloud native and hybrid options, and integrate cybersecurity and data residency requirements into their system design. GIT

Genetec
www.genetec.de

Hirsch Secure and Quanergy Partner to Deliver LiDAR-Based Perimeter Security and Intrusion Detection Across DACH Markets

Hirsch Secure GmbH, a trusted provider of access control, intrusion detection, and integrated security solutions across Germany, Austria, and Switzerland, and Quanergy Solutions, Inc., a leading provider of 3D LiDAR-based perception solutions for perimeter security and real-time tracking, today announced a strategic technology and commercial partnership.

Through this partnership, Hirsch Secure will integrate Quanergy's Q-TRACK LiDAR-based perimeter intrusion detection and tracking solutions into its security portfolio, enabling customers to achieve greater situational awareness, earlier threat detection, and more reliable perimeter protection across complex and high-security environments.

Hirsch Secure GmbH is recognized across the DACH region for delivering enterprise-grade security systems that combine access control, video, and intrusion technologies into unified platforms. By incorporating Quanergy's 3D LiDAR technology, Hirsch Secure expands its ability to protect large outdoor perimeters, critical infrastructure, and mission-critical facilities.

Hirsch Secure is also planning to open a dedicated demonstration center at its headquarters and in Northern Germany, providing customers and partners with hands-on access to LiDAR-based perimeter security and real-time tracking solutions.

Michael Schreiber, General Manager at Hirsch Secure GmbH, and Heiko Viehweger, Senior Sales Consultant PIDS, are excited about the new partnership: 'It is our commitment to provide our customers with first-class, high security solutions that meet the highest standards in every component. The addition of Quanergy's Q-TRACK technology complements our security portfolio and allows us to deliver another layer of security, reduce false alarms and to offer a technology for applications where other sensor technologies face accuracy and reliability limitations.'

Heiko Viehweger, Senior Sales Consultant PIDS and Michael Schreiber, General Manager at Hirsch Secure GmbH

www.hirschsecure.com

PHYSICAL SECURITY

Innovation Through Dialogue

Technology Trends for the Security Sector

Axis Communications has once again identified several technology trends this year that will shape the security sector in the coming year.

In 2026, Axis is focusing primarily on technological developments that represent an evolution of trends already observed: artificial intelligence, advances in imaging, improved data-processing capabilities on end devices ("on the edge"), and optimized communication technologies. Even technologies that may initially seem far off, such as quantum computers, could potentially have noticeable effects on industries that prepare for them early. Another key driver, in the context of increasing connectivity and digitalization, is the growing involvement of IT departments and experts in the field of physical security, which strongly influences purchasing decisions in this area.

"The technology trends we have identified for 2026 clearly show how significantly the security sector is evolving and diversifying. The influence of IT on strategic decisions is growing rapidly, and with it the need to understand security solutions as an integral part of a larger digital ecosystem that incorporates cybersecurity," says Tobias Metsch, Regional Director Middle Europe at Axis Communications. "At the same time, at Axis we think far beyond the coming year: innovation does not emerge in isolation, but in dialogue. That is why we listen closely to our customers and partners, understand their challenges, and develop solutions together that sustainably improve security, operational efficiency, and business intelligence."

Axis Communications has identified four key trends:

1. "Ecosystem First" becomes a central guiding principle for decision-making

The "Ecosystem First" principle is increasingly shaping decision-making processes in security technology and reflects the growing influence of IT departments and experts on these processes. Instead of selecting isolated security solutions, companies are increasingly opting for integrated end-to-end systems that seamlessly connect devices, sensors, and analytics functions.

This approach enables more efficient configuration and management, strengthens long-term support throughout the entire product lifecycle, and ensures faster and more scalable deployment of solutions. As a result, modern security strategies and investments increasingly prioritize the ecosystem approach.

2. Continuous evolution of hybrid architectures

Hybrid architectures are becoming more widespread as technological advances in edge and cloud computing make purely on-premise solutions less attractive. Modern AI-powered network cameras now offer significantly higher computing performance and image quality, enabling the generation of higher-quality metadata. In addition, more and more analytics tasks can be performed directly on the device ("on the edge"), while cloud resources provide the analytical power needed to comprehensively evaluate ever-growing volumes of data and derive business-relevant insights, tasks that were previously reserved for local servers.

Although on-premise components such as network video recorders continue to play an important role and will remain prevalent for the foreseeable future, the greatest added value increasingly lies in combining edge devices with cloud resources, as this delivers higher performance levels while ensuring reliable data integrity.

3. The growing importance of edge computing

Edge computing continues to gain importance, directly linked to the evolution of hybrid architectures. As long as hybrid systems relied on a combination of edge, cloud, and server resources, the potential of edge AI was not always fully realized, as local servers took over many tasks and slowed the shift toward the edge. This is now changing fundamentally: improved AI capabilities directly on devices allow companies to make more conscious and targeted decisions about where to deploy AI and which analyses should take place at the edge versus in the cloud. Modern cameras and a growing variety of edge-AI-enabled sensors increase both efficiency and effectiveness.

Edge-based data processing provides immediately usable business and metadata about objects and scenes. This information forms the basis for scalable functions such as intelligent video search or system-wide analytics. Each additional edge component increases the available computing power, allowing the overall system performance to grow particularly efficiently with every new device.

Furthermore, earlier reservations about edge computing are increasingly losing relevance. Today's edge devices feature robust integrated cybersecurity functions such as secure boot or signed operating systems, actively contributing to strengthening overall system security.

4. Mobile video security experiences strong growth

Mobile video security solutions are currently experiencing rapid growth, driven by technological and commercial factors that significantly expand their application possibilities. Improved connectivity, remote access, and edge AI enable the flexible use of modern network cameras in mobile scenarios, from public spaces to construction sites to large events.

Technological advances in energy management significantly reduce device power consumption without compromising performance, making the use of battery storage and renewable energy sources feasible in such scenarios. In addition, official permits for mobile video security solutions are often easier to obtain than those for fixed installations. This enables comprehensive security even in locations where deploying security personnel is difficult. GIT

Axis Communications
www.axis.com

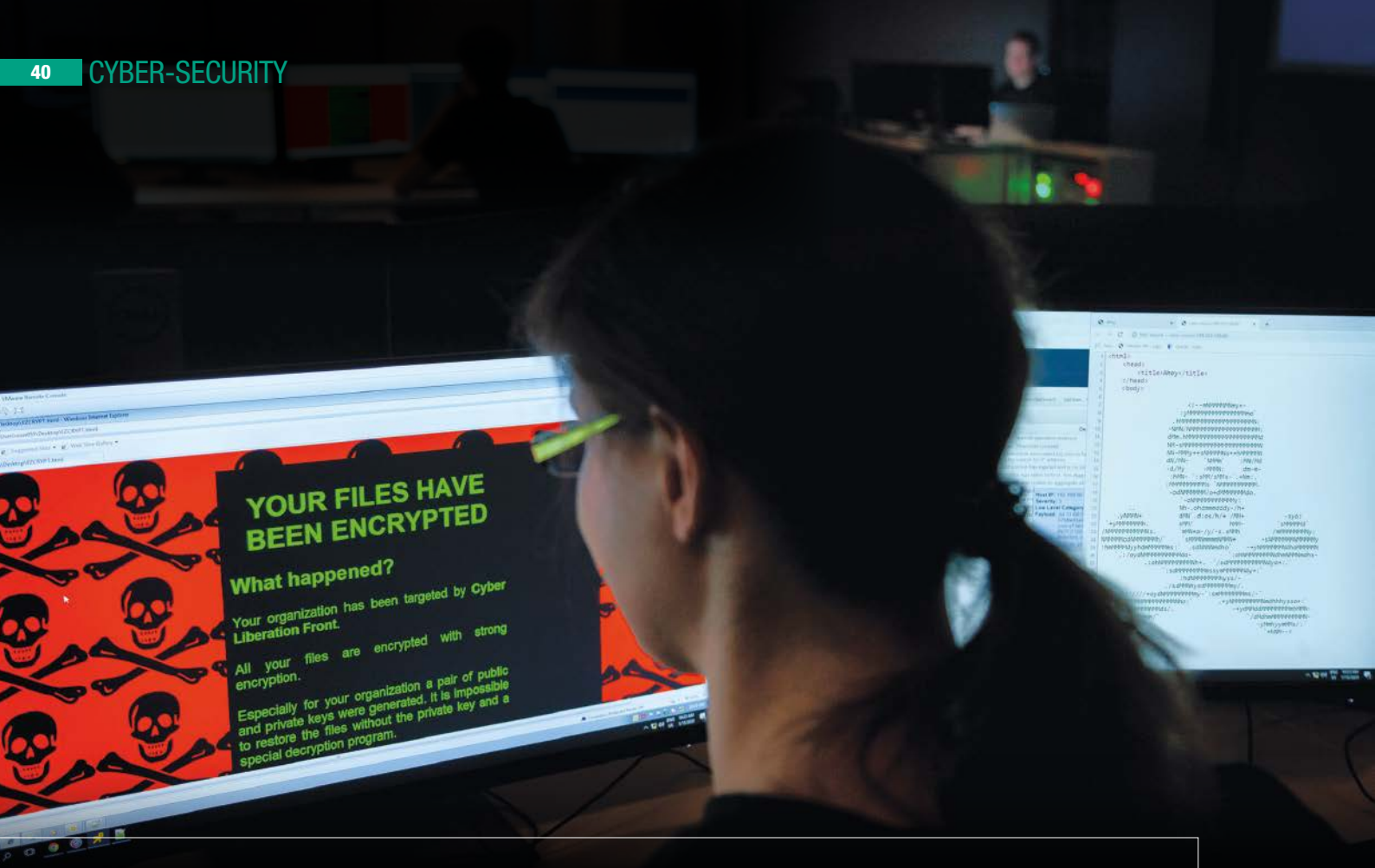
SMARTair® digital access
Your out-of-the-box solution

ASSA ABLOY
Opening Solutions

Switching to digital access has never been simpler.
SMARTair has everything you need: battery-powered devices,
versatile digital credentials, and intuitive,
robust software. With SMARTair, you're ready to go!

Scan the QR code and discover what's inside a SMARTair box

Experience a safer
and more open world



TRAINING

Training at Fraunhofer SIT

Strengthening Resilience Against Cyber Attacks

Rapid technological progress, an increasing attack surface, cyber criminals are arming themselves. These risks can no longer be countered with technology alone. People with specialist knowledge are needed. But knowledge in cyber security is evolving faster than in almost any other technical field; knowledge on which a great deal can depend. This is why continuous training in cyber security is important. An article by Dr. Markus Schneider, Deputy Director & Head of Cybersecurity Training at Fraunhofer SIT & National Research Center for Applied Cybersecurity Athene.

The Federal Office for Information Security (BSI) describes the cyber security situation in Germany as tense. For companies and authorities, the question of attacks is less a question of if and more a question of when. For some years now, cyber attacks have been considered the greatest business risk, impacting competitiveness and even the very existence of a company.

The digital transformation is constantly leading to new applications and functions; technological progress brings many advantages, e.g. efficiency gains. However, this also increases the attack surface and poses major challenges in terms of protection.

Arming includes technical measures for protection, processes and knowledge. Due to its scope, cyber security is becoming an issue that affects more and more different levels in organizations and roles, from operational tasks in IT administration to strategic issues at management level. The fast pace of technological development inevitably leads to the rapid further development of relevant cyber security knowledge, and relevant new legal acts demand a response.

In view of the immense professionalization of cybercrime and the resulting threat, it is important to keep the relevant knowledge in organizations up to date at all times. However, even very good training can no longer cover the required knowledge over longer periods of time; further training is essential, especially due to the immense shortage of cyber security specialists. Due to the cross-sectional nature of cyber security, further training is becoming increasingly differentiated.

Cybersecurity Knowledge – Why So Special?

The framework conditions for cyber security knowledge differ significantly from other areas. While market requirements and new functions are the evolutionary

drivers in other ICT areas, the threat situation is the driving force in cyber security. Predictability is usually much lower here than in other areas. Cybersecurity knowledge becomes outdated and is replaced by new findings. The half-life of tactical knowledge is a few months, in other ICT areas a few years; in strategic knowledge, a few years compare to many years

The required response times can be very short, while longer periods are accepted in other ICT areas. Obsolescence is also pronounced differently: abrupt abandonment in cyber security versus gradual transitions in other ICT areas. Furthermore, due to the need to act at short notice, documentation relating to cyber security is often incomplete, whereas in other ICT areas it tends to be more comprehensive and structured.

Today, cyber security is one of the fastest evolving fields in ICT technology. This has huge implications for what organizations need to know in cyber security and how they keep this knowledge up to date. What was right yesterday may be obsolete tomorrow. These discrepancies in knowledge in cyber security and other ICT areas result from various influencing factors: Shortage of specialists, overload, technological complexity, enlargement of the attack surface, asymmetry between attacker and defender side, new attack methods, new regulatory requirements, differentiation of various roles and tasks, application orientation versus fundamentals.

In addition to long-term knowledge (e.g. basic principles, cryptographic primitives), medium-term (e.g. threats from new application technologies, tools) and short-term knowledge (e.g. new vulnerabilities, patches) also play an important role in cyber security. Short-term knowledge can become relevant on an ad hoc basis, but can also quickly become outdated again. Solid medium and long-term knowledge helps with the independent classification of current reports.

It is often challenging for universities to keep pace with their curricula. In addition, it takes time for students to enter the labor market as skilled workers. In order to protect themselves better, companies need to focus on further training in cyber

Dr. Markus Schneider, Deputy Director & Head of Cybersecurity Training, Fraunhofer SIT & National Research Center for Applied Cybersecurity Athene

security, preferably on an ongoing basis. Last but not least, they also help the management to prove that it is responsible for risk prevention.

Obligations for Organizations

To protect their own interests, organizations must do what is necessary to stay up to date with cyber security. If they do not do this and do not take the necessary measures, there is a risk of organizational failure. This becomes transparent at the latest after attacks have occurred.

Further training in cyber security, e.g. in the form of courses or training, is mandatory for organizations under various legal acts. This applies to organizations either directly (e.g. GDPR, IT Security Act) or indirectly in accordance with the due diligence obligations for board members or management (e.g. AktG, GmbHG). They are also responsible for providing the necessary resources (e.g. time, finances).

Needs

The shortage of cyber security specialists is not limited to Germany. Companies and authorities around the world are looking for suitable specialists whose expertise meets the application-oriented requirements. This requires good training and appropriate further training. A study conducted in the USA a few years ago found that even Ivy League university graduates no longer met the content requirements of organizations. As the lack of specialists and content deficits were seen as a national security problem on the government side, the National Initiative for Cybersecurity Education (NICE) was launched; it has developed a competence framework for training and further education. Other countries, such as China, also see education and training in cybersecurity as a pillar of their national security. In line with NICE, Europe has responded with the EU Cybersecurity Skills Framework (ECSF).

Companies need further training that can be easily integrated into the practical world of work in terms of content and process. Practical components in knowledge transfer are expected to lead to faster and more effective learning success. Important new findings must be incorporated into training curricula without delay.

Knowledge Over Short Distances

Fraunhofer SIT is a contributor to the National Research Center for Applied Cybersecurity Athene, the largest research center for cybersecurity in Europe. In addition to R&D, Fraunhofer SIT has an extensive range of training programs. The proximity to applied research is very valuable, as new findings are quickly adopted:

- **TISP:** The content covers practically relevant knowledge on technical, organizational, legal, and economic topics, which is based on national and international standards.
- **Athene Cyber Range:** Here you can train the detection and defense of real cyber-attacks.
- **Cyber Security Learning Lab:** Content is taught using practical exercises and compact theory. The practical application of newly acquired knowledge leads to better learning success.

To protect against cyberattacks, organizations must enable their employees to continuously learn about cybersecurity. Lifelong learning is important, as cyber security is evolving rapidly. Because content and offerings vary greatly, it is crucial to select the training and courses that are relevant to your own needs. GIT

Frauenhofer SIT
www.sit.fraunhofer.de/en

BIOMETRICS

When Knowledge Is Not Disclosed

Zero-Knowledge Biometrics as a New Authentication Logic

Digital identities have long evolved into a central security asset for modern organizations. Employees, customers, and partners access numerous systems and applications daily, distributed across cloud platforms, mobile devices, and hybrid IT environments. However, with this increasing connectivity, controlling access securely and reliably is becoming ever more complex.

Henning Dittmer, Regional Vice President DACH at Ping Identity

Classic authentication methods such as passwords or one-time codes are increasingly regarded as weak points. They are vulnerable to phishing, social engineering, and automated attacks, often serving as a gateway for security incidents. While biometric methods promise greater security and convenience, they have for years been caught in a tension between technical effectiveness, data privacy requirements, and user acceptance.

Zero-knowledge biometric authentication now offers an approach that resolves this tension. By utilizing cryptographic methods, identities can be verified without biometric data having to be disclosed or centrally stored. This allows high security standards to be combined with consistent data privacy and user-friendly authentication.

Why Traditional Biometrics Reach Their Limits

Biometric authentication has established itself primarily in the consumer sector, for example, in the form of fingerprint or facial recognition on smartphones. Technically, these methods can be roughly divided into local, central, and decentralized models. Local biometrics implemented in operating systems are considered comparatively privacy-friendly since biometric traits do not leave the end device. However, this approach is of limited use to companies as it allows for hardly any control, transparency, or cross-platform usage. Centralized biometric systems store and compare biometric templates server-side, which solves the control issue. However, this creates a massive risk: central databases containing biometric information are an attractive target for attackers. Unlike passwords, biometric traits cannot simply be changed. A successful attack thus has potentially lifelong consequences for those affected.

Decentralized architectures attempt to mitigate this risk by fragmenting biometric data or processing it in a distributed manner. Yet, a residual risk remains here as well, as individual fragments or metadata may potentially allow conclusions to be drawn about identities. The central question, therefore, is: How can biometric authentication be realized without disclosing biometric data?

Zero-Knowledge as a Principle: Trust Without Disclosure

The answer is provided by a concept from cryptography: the Zero-Knowledge Proof. This involves proving that a statement is true without revealing any additional information. Applied to biometric authentication, this means a system can confirm that a person is authorized without having to access their biometric feature or being able to reconstruct it.

Zero-Knowledge Biometric Authentication combines biometric recognition with advanced cryptographic methods. During onboarding, a biometric feature – such as a facial image - is captured locally and immediately converted into a mathematically irreversible representation. From this, a cryptographic proof is generated which serves as a reference. Neither raw data nor reconstructible templates are stored. During a subsequent login, the system generates a new zero-knowledge proof from the current biometric input. The server checks exclusively this proof and can thus determine whether there is a match without ever seeing or storing biometric data. Authentication typically takes place within a few hundred milliseconds, making it suitable even for high-frequency login scenarios.

Balancing Data Privacy, Security, and User Comfort

This approach opens up new possibilities for companies. Since biometric data is neither stored centrally nor processed, the risk of serious data breaches is significantly reduced. At the same time, compliance with regulatory requirements, such as the GDPR, is significantly facilitated, as highly sensitive personal data is virtually non-existent in the system.

From the user's perspective, zero-knowledge biometrics also offer advantages. Authentication is passwordless, fast, and intuitive, requiring no additional hardware or complex multi-factor mechanisms. Simultaneously, the methods are robust against modern threats such as AI-supported deepfakes or replay attacks, as cryptographic proofs are not reproducible.

Market Development and Technological Maturity

The growing importance of this technology is also evident at a strategic level. For instance, Ping Identity recently announced the acquisition of Keyless, a company specializing in zero-knowledge biometrics. Keyless has developed technology that enables biometric authentication without storing reconstructible biometric data. It is suitable for both customer and workforce identities.

The integration of this technology into existing identity security platforms underscores a clear market trend: companies are looking for authentication methods that are secure, privacy-friendly, and future-proof, especially as AI-based attacks and regulatory requirements increase in parallel.

A New Standard for Digital Identities

Zero-knowledge biometric authentication marks a paradigm shift in digital identity security. Instead of securing sensitive biometric data particularly heavily to protect it, this approach deliberately avoids making it accessible in the first place. The result is an authentication model that unites security, data privacy, and user-friendliness.

For IT leaders and security architects, zero-knowledge biometrics offers a solid foundation for future identity strategies, particularly where trust, scalability, and regulatory security are equally in demand. GIT

Ping Identity
www.pingidentity.com

Shared Services Take Shape as ENISA Guides EU Agencies Toward Greater Synergies

As Chair of the EU Agencies Network (EUAN) for 2025–2026, ENISA advanced the implementation of the Network's new governance framework, strengthened the role of EU Agencies as institutional partners, and boosted cybersecurity and efficiency through shared services. EUAN brings together 52 EU Agencies and Joint Undertakings, supporting over 14,000 staff across the EU. In early February 2026, Agency Directors and resource leaders met in Athens to address common challenges and deepen cooperation. During the meeting, ENISA, EFSA and EIT signed an MoU to expand their shared services pilot, covering HR, cybersecurity compliance and response, and legal services. ENISA also strengthened inter-institutional cooperation with the European Parliament, the Commission and the Council, contributing to discussions on the next Multiannual Financial Framework and key HR priorities. Cybersecurity remained central, with ENISA providing tools, guidance and awareness initiatives for Agencies. As its Chairmanship concludes, ENISA thanks stakeholders for their commitment and welcomes ELA as incoming EUAN Chair.

www.enisa.europa.eu

Advancis joins AI innovation platform IPAI

Advancis has joined the AI innovation platform IPAI, strengthening its commitment to responsible and applied AI. The company aims to optimize internal processes and advance its software solutions for highly critical environments using modern AI technologies. As part of IPAI's ecosystem in Heilbronn, one of Europe's leading hubs for trustworthy, application oriented AI; Advancis gains access to a wide network of technology partners, research institutions, and startups.

David Teppe, Head of Strategic Alliances at Advancis

This collaboration supports the development of scalable, AI driven solutions for integrated security and building management. According to David Teppe, Head of Strategic Alliances, the membership helps Advancis stay close to market innovation while expanding internal AI expertise and establishing safe, reliable AI standards. IPAI members include major organizations such as Audi, Deutsche Telekom, SAP, and Fraunhofer.

advancis.netww

Gunnebo Entrance Control Launches NexGate for Safer Self-Checkouts

Gunnebo Entrance Control has introduced NexGate, a compact entrance solution designed for high-traffic retail environments. Its sliding leaf barrier opens only when a valid receipt or barcode is scanned, supporting loss prevention without slowing customers. Flexible integrated or standalone scanning columns adapt to different store layouts and trolley use, improving manoeuvrability and reducing congestion. Dual safety photocells and obstacle-detection technology ensure safe operation, while LEDs guide customers intuitively. Anti-fraud photocells detect items passed beneath the barrier, and a timeout alarm alerts staff if the passage is blocked. With a small footprint, easy POS integration and low-maintenance design, NexGate offers retailers a secure, smooth and controlled exit process. Available in stainless steel or powder-coated finishes, it blends discreetly into modern store concepts.

www.gunneboentrancecontrol.com

EVENTS

50 Years of Wagner

Wagner demonstrates its “Passion for Fire Protection” at Logimat 2026

Under the motto “Passion for Details”, Logimat 2026 will open its doors in Stuttgart from March 24 to 26. As the leading international trade fair for intralogistics and process management, it focuses on efficient, compact, and highly automated warehouse solutions. Preventive fire protection is an often underestimated but crucial detail for their reliable operation. This is exactly where Wagner comes into play, presenting its solutions in Hall 7, Booth 7C13.

© conform GmbH

At the trade fair, Wagner Group GmbH will be presenting its fire protection solutions, which have made the company a leading provider in the field of fire detection and prevention for 50 years now.

For 50 years, the family-owned company has been passionately committed to holistic fire protection and has focused its innovative strength on developing practical solutions that meet the high safety requirements of today‘s logistics applications. With its concepts, Wagner helps to secure processes and minimize downtime. Modern high-bay warehouses and compact storage systems are characterized by high space efficiency, increasing digitalization, and maximum process density. This also increases the requirements for operational safety. Effective fire protection is therefore an integral part of holistic risk management and an essential factor for permanently high warehouse availability.

“Efficient intralogistics depends on many perfectly interlocking details,” explains Ralf Keck, Insurance Relations Manager at Wagner. “Preventive fire protection is one of these details that makes all the difference in an emergency. With our ‘Passion for Fire Protection’, we make a concrete contribution to sustainably strengthening operational resilience, securing processes, avoiding downtime, and protecting investments in the long term.”

Wagner focuses in particular on preventive fire protection concepts that prevent fires from occurring in the first place. The focus is on sustainable systems that combine safety and resource efficiency in a technologically intelligent way. The combination of early fire detection and active fire prevention in an oxygen-reduced protective atmosphere significantly minimizes risks. Especially in automated storage environments, where conventional extinguishing measures reach their limits, operators benefit from a continuously high level of protection and reliable operational readiness.

At Logimat 2026, Wagner will demonstrate how fire protection can be seamlessly integrated into modern intralogistics solutions, thereby becoming a key component for process reliability, system availability, and cost-effective operation. GIT

© Wagner Group GmbH

> Efficient intralogistics depends on many perfectly interlocking details
>
> **Ralf Keck, Insurance Relations Manager at Wagner**

Wagner Group GmbH
www.wagnergroup.com

FIRE ALARM EQUIPMENT

Fashion Fire Safe

Advanced Fire Protection for High Value Fashion Warehousing

Iris 2002 SRL, a specialist logistics provider serving the Italian luxury fashion industry, has enhanced fire safety across its warehousing operation using Hochiki's Latitude fire control panels networked with Hochiki ESP intelligent (addressable) fire detection and alarm devices, helping protect people, high value inventory and continuity in a demanding, high throughput environment.

The installation was delivered by Hochiki Italia's distributor DSA Technology SRL, working with authorised installation specialists EM Sistemi Di Sicurezza, to design a tailored solution for a complex site that includes a dedicated hanging garment section with an overhead trolley system and loading platform.

A Large, Open Plan Warehouse Challenge

With operations spanning a three floor, 6,600 sqm garment warehouse and a wider 9,000 sqm facility, Iris 2002 required a comprehensive system that could maintain protection without disrupting critical logistics activity.

The open plan design also created a practical signalling challenge, as the absence of structural columns made traditional Visual Alarm Device placement impractical in parts of the warehouse.

Flexible Detection and Clear Audio-Visual Signalling

To address the site's detection and evacuation needs, the team specified Hochiki YBO-BSB2 base sounder beacons, mounted beneath ESP intelligent sensors to provide combined audible and visual warnings. The base sounder beacons offer 51 EN54 approved audio tones and a high intensity flash, supporting compliant signalling in environments with high background noise. The ESP addressable sensor range was selected for its suitability across large, mixed warehouse zones and for features designed to reduce unwanted alarms, including automatic drift compensation and variable sensitivity.

At the heart of the solution, Hochiki Latitude fire control panels were installed across all three warehouses, with the entire system monitored from a single control station. With Latitude's remote monitoring option, facilities and health and safety teams can access the system 24/7 and gain real time visibility of panel status and site conditions, supporting a more proactive approach to compliance, oversight and operational continuity.

Simple Installation, Intuitive Operation

EM Sistemi Di Sicurezza highlighted the practical benefits of system flexibility during delivery: "The flexibility of Hochiki's system made the design and installation process easy." DSA Technology SRL also emphasised fast commissioning and end user usability: "Configuration and programming were extremely simple, reducing commissioning times. The user interface is clear and intuitive, ensuring immediate and safe management of the system for end operators."

A Strong Reference Point for Safer Logistics Facilities

This installation is a practical example of how logistics warehouse environments can be kept safer using a joined up, addressable fire detection and alarm system, one that combines scalable control, robust detection, clear audio-visual notification and simple ongoing operation. For facilities managers balancing compliance, uptime and the realities of busy sites, it shows the value of selecting life safety technology that is engineered for real buildings, real constraints and real working conditions. GIT

Hochiki Europe (UK) Ltd
hochikieurope.com

Hochiki ESP intelligent sensors paired with YBO-BSB2 base sounder beacons provide unified audio-visual signalling throughout the open warehouse, ensuring clear alerts even in high-noise operational areas

Addressable detection placed around the overhead trolley system uses automatic drift compensation to maintain reliable sensitivity despite constant air movement and fibre particles

Fire doors are integrated into the Latitude panel network, enabling real-time door status monitoring and ensuring rapid, panel-coordinated compartmentalisation during an alarm event

Gaelle Ramu, Senior Strategic Category und Business Development Manager EMEA bei Ansell

SAFETY GLOVES

Beyond the Acetone Barrier

The first acetone resistant disposable glove: TouchNTuff 93 800

Acetone is one of the most commonly used solvents in industrial cleaning and maintenance processes and is considered particularly critical due to its high diffusion capacity. Without adequate protection, it can pass unnoticed through glove materials and, over time, cause harmful effects to health, including potentially reproductive toxic impacts. Nevertheless, until now, workers had no disposable gloves available that offered reliable resistance to acetone. In this interview, Gaelle Ramu, Senior Strategic Category and Business Development Manager EMEA at Ansell, explains how the TouchNTuff 93 800 was developed to close this safety relevant gap for the first time.

GIT Security: Ms Ramu, you work in product development at Ansell. What was the specific reason for developing a disposable protective glove that effectively protects against acetone and other ketones?

Gaelle Ramu: I am the Ansell product manager for single-use gloves in the MEA region. Throughout my 13 years in this role, there have been growing numbers of inquiries for a single-use glove that protects against acetone. Currently, gloves that offer proper protection against acetone are chemical types. However, when our end users need to clean smaller components, these gloves are quite loose and don't offer the level of dexterity required for the task. Also, because of the wide cuff in the glove design, there's a risk of contamination. As a result, end users are using multiple layers of single-use gloves. Or mechanical gloves that don't offer chemical protection. Or, in the worst cases, they work completely unprotected. The risks involved in these practices made the development of a single-use glove that protects effectively against acetone a high priority.

As a company, we work closely with our customers, so we're acutely aware of their challenges and any unmet needs they may have. The development of the TouchNTuff 93-800 reflects our response to this issue. It's also indicative of our broad commitment to develop innovations to make workplaces safer, alongside the constant focus of our R&D team and the work they do in our global network of 18 strategic research facilities.

Acetone is extremely diffusive and can quickly penetrate the polymer structures of many gloves, especially the disposable nitrile ones that are often used by customers who require a high level of dexterity in their jobs. In addition, acetone rapidly degrades thin nitrile, causing the glove to lose its barrier function. What technology does Ansell use to address these challenges?

Gaelle Ramu: Thin nitrile gloves are not the answer. Due to their properties, they break up very quickly in contact with acetone and ketones, which are volatile and dangerous compounds. Without proper protection, exposure can cause a number of issues, including skin irritation, while permeation can create long-term problems such as issues with fertility.

The TouchNTuff 93-800 is the first disposable glove with enhanced chemical protection, compared to standard nitrile disposable gloves, which is designed to be resistant to acetone for at least 15 minutes. It's made of natural rubber latex (NRL), nitrile, and neoprene with Ansell's innovative three-layer Microchem technology, which provides Type A chemical resistance and eliminates the risks involved in using multiple gloves. This multi-layer technology is designed for superior protection and safety and is also used in our body protection solutions. Single-use gloves are not meant, or designed, for immersion, and we found from multiple testing that this existing combination of materials offers the best chemical splash protection.

The NRL is used on the outside and does not come in direct contact with the skin to address allergy concerns. Also, the latex grade we are using is low protein in order to further reduce the risk of latex allergies.

Which other chemicals does the TouchNTuff 93-800 protect its wearers from, and how was the protective function tested or verified?

Gaelle Ramu: The glove has had thorough testing for protection against more than 100 chemicals. In addition, our chemical engineers have also provided estimates for many other chemicals in our database. We have the industry's largest chemical permeation data of over 50,000 cases.

Using our Chemical Guardian service – a proprietary digital tool that provides access to Ansell's extensive database of chemical test results – simplifies the PPE selection process for a user's specific set

of chemicals. This data enables customers to choose the right glove for the right task based on criteria such as chemical hazard, application, permeation, and degradation.

Are there any additional properties and protective features that set the TouchNTuff 93-800 apart from the competition?

Gaelle Ramu: Its vivid orange colour enhances high visibility and foreign object detection (FOD). While the formulation and design enhance the fit, feel and flexibility compared to other reusable gloves on the market.

There is a big focus on acetone because that's the chemical protection that is most often requested. However, there are a lot of other ketones that the glove protects against. For example, it offers good chemical splash protection against Methyl Ethyl Ketone (MEK).

Acetone is flammable, so to avoid the risk of an ignition spark in the workplace, the glove is antistatic. It is also silicone-free. This is important, because silicone can prevent the correct application of paint or adhesives. Also, with the new EUDR regulation, which aims to ensure European products don't contribute to deforestation coming soon, the natural rubber latex we use is fully compliant.

Which standards does the glove comply with?

Gaelle Ramu: The TouchNTuff 93-800 is a unique combination of 15-minute acetone chemical splash protection, plus ISO cut A protection. Our end users highlighted their issue with the cleaning of sharp components, and although we cannot match the cut protection of a mechanical glove, the glove is certified EN388 2110A, which offers abrasion and cut protection suitable for disposable applications. The glove is quite thick and offers very good mechanical protection for a single-use glove with EN ISO 374-1 Type A - certified for high defence.

Sustainability has become indispensable in the field of occupational safety. However, there is often a conflict between the protective function of PPE and its sustainability. Are there actions taken towards sustainability in the production chain of the TouchNTuff 93-800 and the plant where the glove is produced?

Gaelle Ramu: The glove provides a more sustainable, eco-friendly choice in hand protection and is TÜV certified to contain over 60% bio-based formulation, and for the lower emissions involved. It's manufactured in Ansell's plant in Sri Lanka, which runs on 83% renewable energy from biomass, and is certified by Intertek for diverting >99% of waste from landfill. The plant is recognised with accredited environmental and energy management for sustainable production, including the use of solar panels, biomass boilers, and reuse of water. Sustainability is at Ansell's core. Everything we do begins and ends with safety, and with our commitment to better protect people, we must also protect the world we live in. We're working towards Net Zero emissions by 2040 and are dedicated to sustainable sourcing and manufacturing. It's not only about the material, but it's the whole production process. This includes the packaging, which is made of at least 70% recycled carton, certified plastic-free, and recyclable.

For which industries and applications was the TouchNTuff 93-800 primarily developed?

Gaelle Ramu: The TouchNTuff 93-800 targets a broad range of industries and applications, wherever acetone and other hazardous chemicals are used. This includes the aerospace industry, which, because of its FOD policy, was a key contributor to the orange colour choice. Although there were also other industries that wanted the colour differentiated from the standard TouchNTuff brand, to ensure the right choice of protection is made.

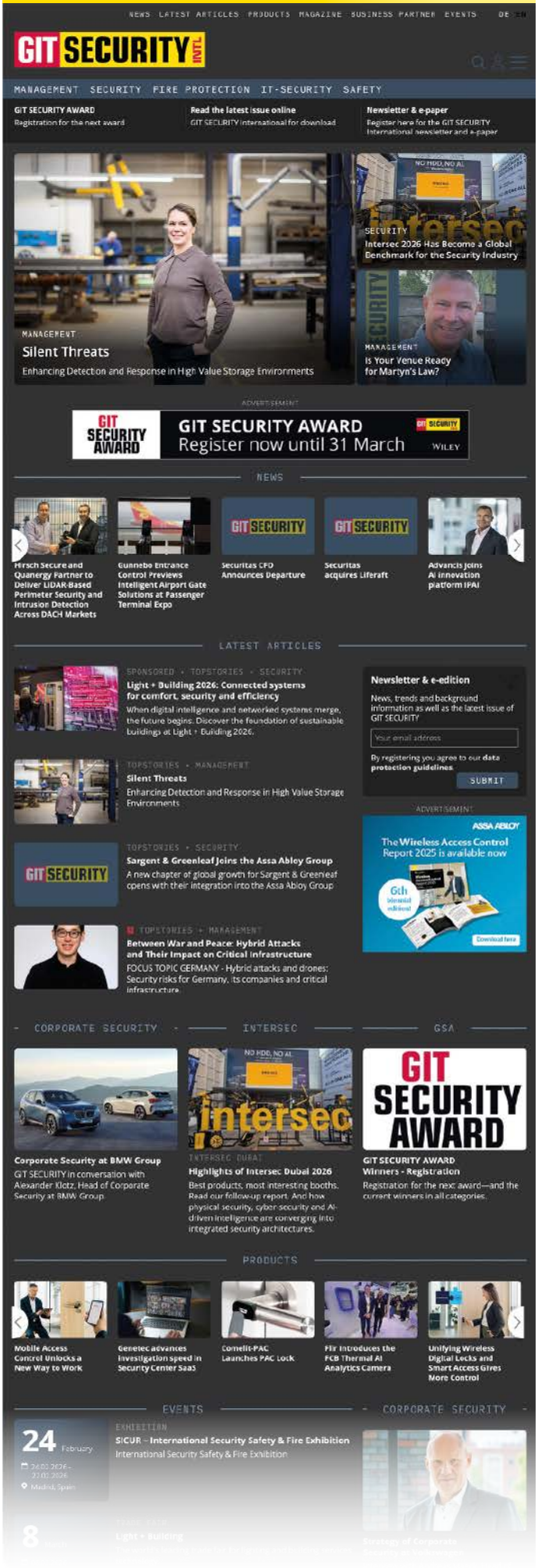
The glove is also suitable for automotive, chemicals, the manufacturing of paint and adhesives, the packaging industry, transportation, energy, printing, machinery and equipment, as well as manufacturing industries. TouchNTuff 93-800 can be used in applications such as cleaning (tools, components), degreasing, maintenance, blending, compounding materials, and chemical handling.

When will the TouchNTuff 93-800 be available on the market?

Gaelle Ramu: The TouchNTuff 93-800 will be officially launched on the market on March 1st 2026. Anyone who attended Ansell's stand at the recent A+A trade show could see the glove demoed and share in the excitement it created. GIT

Ansell LTD
www.ansell.com

This month at GIT-SECURITY.com



IMPRINT

Published by
Wiley-VCH GmbH
A Company of John Wiley & Sons, Inc
Boschstrasse 12 · 69469 Weinheim
GERMANY
www.GIT-SECURITY.com
GIT-GS@wiley.com

Editorial
- Cinzia Adorno
  +49 6201 606 114
  cinzia.adorno@wiley.com

- Matthias Erler
  +49 (0) 6129 5025300
  matthias.erler@wiley.com

Managing Director
- Dr. Guido F. Herrmann

Publishing Director
- Steffen Ebert
  Tel.: +49 (0) 6201/606-709
  steffen.ebert@wiley.com

Sales Managers
- Miryam Reubold
  Tel.: +49 (0) 6201/606-127
  miryam.reubold@wiley.com

- Dr. Michael Leising
  Tel.: +49 (0) 36 03/8942800
  michael.leising@wiley.com

Product Manager Safety & Security
- Dr. Timo Gimbel
  Tel.: +49 (0) 6201/606-049
  timo.gimbel@wiley.com

Wiley GIT Reader Service
65341 Eltville / Germany
Tel.: +49 6123 9238 246
Fax: +49 6123 9238 244
E-Mail: WileyGIT@vuservice.de
Our service is available for you from Monday to Friday 8 am – 5 pm CET

Production
- Jörg Stenger
- Andi Kettenbach (Layout)
- Elli Palzer (Lithography)
- Claudia Vogel (Sales Administrator)

WILEY

Bank Account
J.P. Morgan AG, Frankfurt
Account No.: 6161517443
Routing No.: 501 108 00
BIC: CHAS DE FX
IBAN: DE55501108006161517443

GIT SECURITY is published 4 times per year.

Subscription 2026
4 issues 60.60 €, single copy 17.00 € plus postage. Pupils and Students receive a discount of 50 % at sight of a valid certificate. Subscription orders valid until cancelled, notices 6 weeks before end of the year. Subscription orders can be revoked within 1 week in writing. Dispatch complaints are possible only within 4 weeks after publishing date.

PEFC-zertifiziert
Dieses Produkt stammt aus nachhaltig bewirtschafteten Wäldern und kontrollierten Quellen
PEFC/04-31-0714
www.pefc.de

Printed by
westermann DRUCK | pva
Printed in Germany | ISSN 2190-4367

Comfortably read your e-Issue of GIT SECURITY on your sofa:

Register here

SECURITY MANAGEMENT

Security Management

Ksenia Security S.p.A.
Strada Proviciale Valtesino, 49
63065 Ripatransone (AP), Italy
Tel. +39 0735 751646 · Fax +39 0735 652281
info@kseniasecurity.com · www.kseniasecurity.com
Security and Home & Building Automation

Security Management

NSC Sicherheitstechnik GmbH
Lange Wand 3 · D-33719 Bielefeld
Tel. +49(0)521/13629-0 · Fax +49(0)521/13629-29
info@nsc-sicherheit.de · www.nsc-sicherheit.de
Fire Alarms, CCTV, Voice Alarm Systems

FACILITY SECURITY

Facility Security

Dictator Technik GmbH
Gutenbergstr. 9 · D-86356 Neusäß
Tel. +49(0)821/24673-0 · Fax +49(0)821/24673-90
info@dictator.de · www.dictator.de
Drive units, hold open systems and smoke detectors, door control solutions

Facility Security

frogblue · Smart Building Technology
Luxemburger Straße 6 · 67657 Kaiserslautern
Tel: +49-631-520829-0
info@frogblue.com · www.frogblue.com/de
Frogblue is a leader in the development of wireless, Bluetooth®-based electrical installation solutions for professional use, which are produced entirely in Germany. (A ccess control, security, SmartHome, energy-efficient building technology)

VIDEO TECHNOLOGY

Video Technology

Dallmeier electronic GmbH & Co. KG
Bahnhofstrasse 16 · 93047 Regensburg
Tel. +49(0)941/8700-0 · Fax +49(0)941/8700-180
info@dallmeier.com · www.dallmeier.com
Video security technology made in Germany: multifocal sensor technology Panomera®, IP cameras, recording servers, intelligent video analysis, video management software

Video Technology

EIZO Europe GmbH
Belgrader Straße 2 · 41069 Mönchengladbach
Tel.: +49 2161 8210 0
info@eizo.de · www.eizo.eu/ip-decoding
Professional monitors and solutions for 24/7 use in video surveillance, IP decoding solutions with easy installation and computerless operation.

Video Technology

i-PRO EMEA B.V.
Laarderhoogtweg 25 · 1101 EB Amsterdam
Netherlands
https://i-pro.com/eu/en
High-quality CCTV solutions (IP & analogue), Video Automation and IA, Sophisticated technologies (FacePro, people masking), Cyber Security Protection for GDPR compliance, VMS: Video Insight

Video Technology

www.luna-hd.de
lunaHD
High Definition Video
Video surveillance • Video door intercom

TIME ACCESS

Time + Access

AceProx Identifikationssysteme GmbH
Bahnhofstr. 73 · 31691 Helpsen
Tel.: +49(0)5724-98360
info@aceprox.de · www.aceprox.de
RFID readers for access control, T&A and identification

Time + Access

ASSA ABLOY Opening Solutions EMEIA
Digital Access Solutions
Dukes Court, Dukes Street
Woking, GU21 5BH · Great Britain
www.assaabloy.com
Access control, Access management, Wireless locks, Electronic Access Control Systems

Time + Access

Bird Home Automation GmbH
Uhlandstr. 165 • 10719 Berlin
Tel. +49 30 12084824 • pr@doorbird.com
Access Control; Building Automation; Biometric Verification; IP Video Door Station; IP Intercom; RFID; Customized Intercom Systems; Made in Germany
www.doorbird.com

Time + Access

cryptin
CICHON STOLBERG

Cichon+Stolberg GmbH
Wankelstraße 47-49, 50996 Köln
Tel. +49(0)2236/397-200 · Fax +49(0)2236/61144
info@cryptin.de www.cryptin.de
Operational data collection, time recording, access control

Time + Access

FEIG ELECTRONIC GMBH
Industriestrasse 1a · 35781 Weilburg
Tel. +49(0)6471/3109-375 · Fax +49(0)6471/3109-99
sales@feig.de · www.feig.de
RFID Readers (LF, HF, UHF) for access control, vehicle identification, perimeter protection, payment systems and much more

Time + Access

phg
Peter Hengstler GmbH + Co. KG
D-78652 Deißlingen · Tel. +49(0)7420/89-0
datentechnik@phg.de · www.phg.de
RFID components for access control, timekeeping, factory data collection, canteen data, leisure applications, surface-mounted devices, flush-mounting components, biometrics, identification media and accessories

Time + Access

STid EMEA Headquarter
20, Parc d'activités des Pradeaux
13850 Greasque · France
Tel: +33 (0)4 42 12 60 60 · Fax: +33 (0)4 42 12 60 61
stid-security.com
access control, mobile access, electronic identification, mobile ID readers, vehicle access

PLANT SAFETY

Time + Access

primion Technology GmbH
Steinbeisstraße 2-4 · D-72510 Stetten a.K.M.
Tel. +49(0)7573/952-0 · Fax +49(0)7573/92034
info@primion.de · www.primion.de
Time management, access control and management, staff deployment planning , graphic alarm management, SAP communications solutions, pass and ID card production, Biometrics

Plant Safety

Pepperl+Fuchs SE
Lilienthalstraße 200 · 68307 Mannheim
Tel. 0621/776-1111 · Fax 0621/776-27-1111
fa-info@de.pepperl-fuchs.com
www.pepperl-fuchs.com
Security sensors, inductive, capacitive, opto-electronic and ultrasonic sensors, vision sensors, identification systems, interface modules

Now

Register for our free Newsletter

Your **Number 1** for over 20 years

e-Issue included!

News for Decision-makers and Managers in Safety & Security Matters

www.GIT-SICHERHEIT.de/de/newsletter/register

WILEY

Ksenia®
security innovation

conexa

The touchscreen IP keypad for controlling security and home automation systems.

Find out more!
www.kseniasecurity.com