VOLUME 22 I NOVEMBER 2025 I ISSUE 4 I 17 €

79 824

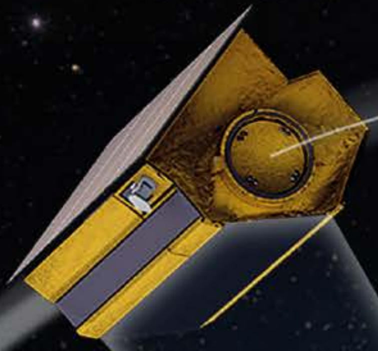
GIT SECURITY INTL

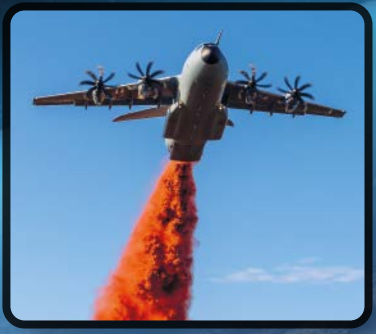
MAGAZINE FOR SAFETY AND SECURITY – WORLDWIDE

INTERVIEWS & PEOPLE
Frank Ewald (DHL), Michael Schreiber & Heiko Viehweger (Hirsch) & more p 14 / 24 / 39 / 46

VIDEO & ACCESS
NIS2 & Cybersecurity, Hanwha Vision & Morphean, Dallmeier for Snoqualmie Casino p 9 / 17 / 22

MUSEUMS
Hexagon's Lidar Vision, Guttuso Museum in Sicily p 27 / 28





© see page 6

Cover Story page 6:

From a Jet Fighter to Space Exploration

Security at Airbus Defence and Space

BEST-OF EXCERPT

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

WILEY

A Final Word Before We Close 2025

Cinzia Adorno

As we approach the end of the year, one question has defined nearly every conversation in the security industry: **How do we build resilience in a world that refuses to slow down?** Geopolitical instability, hybrid attacks, AI-driven threats, aging infrastructures — 2025 has shown us that security is no longer a technical discipline operating in the background. It has become a strategic, trust-driven mandate.

This theme runs through our final issue of the year. “What does it take to safeguard Europe's skies and space?” we asked Sven Dawson, Head of Corporate Security at Airbus Defence and Space. His answer is both sobering and galvanizing: **“There is no absolute security, but we must constantly improve our reaction time.”** In our cover story (p. 6), you will discover how Airbus defends sensitive programs, counters cyber-attacks, and cooperates with governments to protect Europe's strategic capabilities; from jet fighters to interplanetary missions.

But security doesn't end at the gates of a defense company. It extends to every critical sector in Europe, all of which must now adapt to the EU's strengthened NIS2 Directive. The regulation's “all-hazards” approach is reshaping the entire industry by finally merging the physical and digital realms. On p. 11, David Moser of Assa Abloy explains why outdated access systems are fast becoming a liability, and why cyber-physical convergence is no longer optional.

This convergence also appears in our conversation with Frank Ewald, DHL's Head of Corporate Security. **“Security is no longer a backstage function – it's a trust-driven business,”** he tells us. From predicting the invasion of Ukraine to practicing pandemic scenarios before COVID struck, DHL shows what modern resilience looks like: foresight, preparedness, and organizational agility. Read the full interview to understand why static protection simply no longer works (p. 14)

Meanwhile, billions of IoT devices continue to expand the attack surface, especially in video surveillance. Axis reminds us that “security isn't a product, it's a process,” a principle that becomes even more urgent in an age of deepfakes, firmware exploits, and five-figure bug bounties. Trust is now built on transparency and continuous innovation (p. 39)

And yet, digital threats are not the only ones evolving. **In Paris, it took seven minutes for thieves to smash display cases in the Louvre** and flee with Napoleonic jewels before anyone in the control room could react. On pp. 27, 28 we explore how Lidar and wireless intrusion systems are redefining museum protection.

To our readers, partners, and contributors: Thank you for following us throughout this challenging, innovative, and transformative year. Your insights, engagement, and expertise shape not only our pages but the future of our security.

Enjoy the read and recharge for 2026.

ISJ
ASSA ABLOY
Wireless Access Control Report 2025
Trends in Wireless Access Control

GIT SECURITY INTL.
MAGAZINE FOR SAFETY AND SECURITY – WORLDWIDE
From a Jet Fighter to Space Exploration
BEST-OF EXCERPT
WILEY

Cover Story

From a Jet Fighter to Space Exploration

Security at Airbus Defence and Space

page 6

Frank Ewald

Martin Jones

Abdul Mushin

Jolene Stewart

MANAGEMENT

SECURITY

Michael Schreiber und Heiko Viehweger

Andre Bastert

Holger Schmitz

CYBER-SECURITY

FIRE PROTECTION

BUILDING INTELLIGENCE

SAFETY

LITHIUM-ION BATTERIES

VIDEO SURVEILLANCE

INDEX

QUICK-FINDER

ORGANISATIONS, INSTITUTIONS AND COMPANIES IN THIS ISSUE

GIT SECURITY INTL.
MAGAZINE FOR SAFETY AND SECURITY – WORLDWIDE
Your Number 1 for over 20 years
WILEY

Beside Commercial Aircraft and Helicopters, Airbus Defence and Space is one of the three major business divisions of Airbus

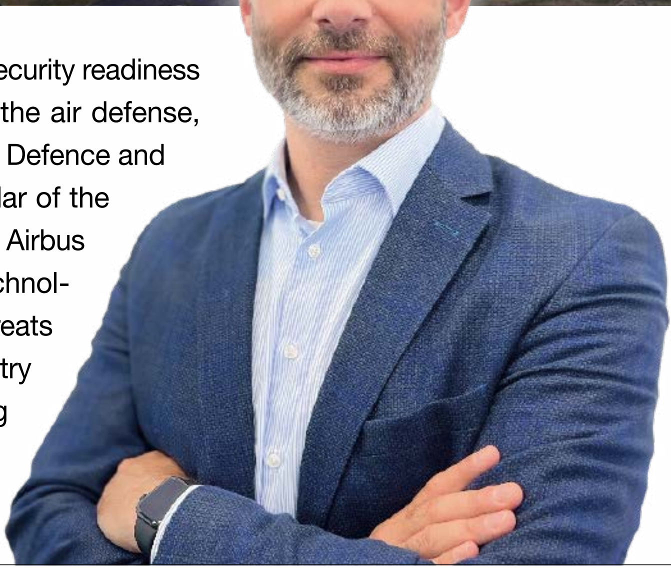
© Airbus Defence and Space SAS

COVER STORY

From a Jet Fighter to Space Exploration

Security at Airbus Defence and Space

The events of these times bring the question of the defense and security readiness of Europe sharply into focus. As one of the leading players in the air defense, satellite technology, cyber security, and space industries, Airbus Defence and Space is not only an industrial giant but also a fundamental pillar of the continent's security. How does a globally active company such as Airbus react to the current challenges? How does it protect its sites, technology and employees in an era in which the physical and digital threats are constantly increasing? And what responsibility does the industry carry with regard to politics and the state when strengthening Europa's resilience? GIT SECURITY International spoke with Sven Dawson, Head of Corporate Security Airbus Defence and Space.



GIT SECURITY International: Mr. Dawson, many thanks for finding the time in this busy period for this conversation with GIT SECURITY. Public awareness of the defense and space divisions of Airbus was probably never so high as in recent weeks and months …

Sven Dawson: That is true. The public awareness of Airbus Defence and Space has risen significantly over the past few months. This brings a great responsibility for us, but also a great opportunity. Our air defense, reconnaissance, satellite communication, cyber security, and space products and technology mean that we are a prime supplier when it comes to ensuring Europe's ability to react. At the same time, we have noticed that there is a new public understanding of how important resilience, defense readiness, and technological superiority are. The fact that Airbus Defence and Space is currently so prominent shows that we are not just an industrial company but also a strategic element of European security.

Before we look at the current situation more closely, let us first talk about Airbus Defence and Space itself, and in particular about the division of the company concerned with defense and space technology. The breadth of this is enormous – from jet fighters to space research ...

Sven Dawson: Airbus Defence and Space is one of the three main business sectors of Airbus – beside commercial aircraft and helicopters – and covers an unusually wide spectrum. Our job can range from classic defense programs such as the Eurofighter or the upcoming Eurodrone to satellite communication, reconnaissance systems and cyber security as well as space technology that stretches from earth observation to interplanetary exploration. We have a number of important locations in Germany that each have their own specialty. We combine aviation, defense and space competencies under one roof and can then develop integrated, future-oriented systems – such as the Future Combat Air System (FCAS), which incorporates the air, space, and cyber domains. Simply said: Airbus Defence and Space combines cutting-edge technology, highly capable locations in Germany and elsewhere, and security-related responsibility – and thereby contributes a decisive part of Europe's superiority.

Mr. Dawson, you are Head of Corporate Security and National Security Representative Germany. Could you give us an idea of the extent of your responsibility?

Sven Dawson: My position as Head of Corporate Security at Airbus Defence and Space brings the responsibility for the protection of our employees, our locations, information, technology and products. This involves a wide range of secure areas – from classic factory and staff security through information and cyber security up to the protection of critical technology and infrastructures.

As a National Security Representative Germany, I am also the point of contact with regard to the security-related interests of Airbus for government and authorities in Germany. Among other things, this includes close cooperation with ministries, intelligence services, and security agencies, in particular on matters of national secrecy requirements, approvals, and the meeting of legal requirements.

My team and I work daily on recognizing risks at an early stage, effectively managing threats, and increasing the resilience of the company. This involves not only their physical protection but also the protection of sensitive data, technology, and programs that are of strategic relevance for national and European security.

Our aim is to position Airbus Defence and Space as a reliable and secure partner for our customers, for the armed forces, NATO, and other institutions.

Could you give us some examples of what changes have been made at Airbus Defence and Space in the light of recent worldwide political events?

Sven Dawson: The situation has prompted us to significantly tighten up our security architecture. We have strengthened three central activities: first of all, physical site security: we have extended our protective measures for critical locations, development centers, and manufacturing sites. These include extended access control, increased video surveillance, and closer cooperation with the security authorities.

In addition, we have the Cyber Defense and IT Security: we have greatly increased our defensive structure, we are investing in the most modern threat detection technology, we are enlarging our Security Operations Centers, and working intensely with state authorities to defeat cyber attacks together.

The third central activity is the protection of critical technology and programs. We have introduced additional protective measures to protect sensitive information and development data exactly because we are involved in projects with national and European security relevance. Close coordination with the authorities such as the BMWE (Federal Ministry for Economic Affairs and Energy) and the BSI (Federal Office for Information Security) is essential.

We have also given our Awareness Program higher priority: our employees are a decisive element of our security. We therefore invest a great deal in training and awareness programs to further increase security consciousness in all areas.

The information exchange and cooperation between the authorities and industry runs differently in other countries, such as in France or Spain. You were working for twelve years yourself in a public office before you move to industry. Where d you see the differences?

Sven Dawson: The German authorities – unfortunately – are governed by legal restrictions that do not always consider or even promote cooperation and close communication with industry. Other countries, such as those you mentioned, are miles ahead in this respect. But we are seeing increasing interest on the part of the German authorities and a consequent improvement in communication.

What aspects could be improved in your opinion – also with regard to access to information, early warnings, espionage defense, drone flights, and other such things?

© Airbus Defence and Space SAU; P.PIGEYRE/MASTERFILMS

Aviation, defense, and space competencies are brought together under one roof at Airbus Defence and Space. In the picture: an aircraft of the German air force

Sven Dawson: There is a real need to improve the organization of this communication and cooperation. Currently, there is a lack of specific agreements or even coordination on the part of the authorities. Commerce has already organized itself and there is constant communication with our industry associations. Another big wish from commerce is the creation of a uniform national situational report that shows the various layers, such as the cyber threat level for example, for all those involved in commerce, public authorities and institutes.

Please turn page ▶

Airbus Defence and Space a core partner in air defense, reconnaissance, satellite communication, cyber security, and space when it comes to securing Europe's ability to react

© Airbus Defence and Space; PHOTO ESKENAZI DOMINIQUE_0608168617

Let us take a closer look at cyber attacks. Have they become more frequent? After all, you are dealing with highly sensitive technological and defense-relevant know-how – you only have to consider the jet fighters or helicopters ...?

Sven Dawson: Yes, we have been observing a big increase in the number of cyber attacks for some time – both in the quantity and in sophistication. This is not just traditional industrial espionage but increasingly also state-sponsored attacks that are designed to steal know-how or disrupt critical systems.

Our response to this is the consistent improvement of our cyber resilience. We have extended our Security Operations Centers, and are investing heavily in Threat Intelligence technology, and of course working closely with national and European authorities and partners. We take a holistic approach: we combine the most modern technology, continuous employee sensitizing, and close international networking to recognize and defend against threats at an early stage. At the same time: there is no absolute security. However, it is essential that we constantly improve our reaction time and our ability to limit the damage caused.

Cyber attacks are also a subject for smaller suppliers. How do you manage this matter along the supply chain at Airbus?

Sven Dawson: You are quite right: cyber attacks do no stop at the entrance gates of Airbus. Smaller suppliers are often the target of attackers because they frequently do not have the same IT security resources. We have elevated made the matter of supply chain (cyber)security to a prime strategic issue because our supply chain is an integral part of our security architecture.

What this means is that we have established clear security standards and requirements that are applicable to all partners and are regularly reviewed. We carry out audits and assessments to identify possible weaknesses at an early stage. Apart from this, we support our suppliers with training courses, Best Practice programs and advice so that even smaller companies can raise their security level. And we work closely with the national and European authorities as well as other companies to ensure unified standards along the entire supply chain.

Mr. Dawson, Europe wants to and must spend more on its defense. If this increases the demand, then a worsening of the already present general lack of trained staff can be seen on the horizon. How does Airbus manage this – with 'blue collar' and 'white collar' employees?

Sven Dawson: We have a multi-layered approach to this: we invest heavily in training young people, provide dual study courses and training programs and work closely together with universities and technical schools. We want to present the company as a modern, international employer – through flexible work patterns, development opportunities, and the unique added value of being involved in technologically advanced and security-related projects such as FCAS or space programs. We also support further qualification to prepare employees for the next challenges – in particular in the future branches of cyber security, AI and digital system integration. We consciously involve diversity and international talent to mitigate the shortage of qualified staff and simultaneously to strengthen our innovative power.

What is particularly unusual with regard to armaments, such as the necessary security checks for example?

Sven Dawson: Dealing with armaments has very specific requirements – and rightly so. In practice, this means that security checks according to legal regulations are compulsory for employees in sensitive areas of the company. These checks are carried out in close cooperation with the responsible state authorities and are a precondition of being able to work on classified projects. In addition, there are strict secrecy regulations, export control regulations, and approval procedures that we have built firmly into our processes. As Germany's largest player in this field, Airbus Defence and Space of course has the corresponding organization and compliance mechanisms to consistently meet these requirements. We do not view these regulations as a hurdle, but rather as a central element of the trust that customers such as the army, NATO, or European partners place in us. Those who are involved with armaments carry special responsibility – and we are acutely aware of this. GIT

Airbus Defence and Space GmbH
www.airbus.com

The area of responsibility of Sven Dawson stretches from classic factory and staff security through information and cyber security through to the protection of critical technology and infrastructure

© Airbus Defence and Space SAS

The Importance of the NIS2 Directive

© Ar_TH - stock.adobe.com

Physical Access and Security Management Strategies under NIS2

David Moser, SVP and Head of Digital and Access Solutions at Assa Abloy Opening Solutions EMEIA, addresses a major new feature on security management's compliance landscape: NIS2.

© Assa Abloy

In the ongoing implementation of the EU's NIS2 Directive, much attention has been paid to its implications for cyber security. Yet, arguably, the impact on organizations' physical security and access strategy is just as important. In fact, NIS2 ushers in a new degree of focus on cyber–physical resilience – with significant potential penalties for organizations that do not comply with the framework's demands.

NIS2 replaces 2016's original NIS Directive on Network and Information Security. It represents a major legislative tightening of the minimum requirements for IT security in critical infrastructure and expands them to include several new sectors. The European Commission estimates that around 160,000 organizations will be immediately impacted by NIS2.

The most important change for security and facilities managers to digest is the switch to an 'all-hazards approach' to regulation. In practice, this approach compels impacted organizations to reinforce their digital security measures with the additional processes and devices that physically protect the security of their digital infrastructure. Cyber–physical resilience – and increased convergence between the operations and goals of cyber and physical security teams – then becomes a key element in the response to an increase in both the volume and the sophistication of hybrid cyber–physical attacks.

NIS2 and Physical Security

The potential scope of NIS2 regulations encompasses a much-expanded range of organizations and sectors. Alongside the typical infrastructure sub-sectors such as energy and utilities, transport, telecoms, waste management, data centers and the like, comes a broader understanding of what constitutes 'critical' national infrastructure: healthcare (including research), digital services, and a range of manufacturing businesses including food, chemicals, automotive, and more. Organizations that operate in any of these sectors should consult the directive to ascertain whether they also face NIS2 obligations.

A significant element of the new obligations is the extended all-hazards approach, referenced above. According to Article 21 of the directive, entities must "take appropriate and proportionate technical, operational, and organizational measures to manage the risks to the security of network and information systems […] and to prevent or minimize the impact of security incidents on the recipients of their services and on other services." In other words, any areas of a site where malicious actors may gain physical access to digital infrastructure, whether IoT devices, access management terminals, servers or anything else, must now have appropriate protection against digital, physical, and hybrid attacks. Access control devices and protocols must be up to this task.

Potential punishments for non-compliance with NIS2 can be severe. According to the directive's text, organizations may face fines of up to €10 million, or 2% of their global annual turnover. Older locking systems therefore represent a major liability risk for many organizations.

NIS2 Impact on Access Control Workflows

NIS2's implications for security and facilities management – and potential financial penalties for organizations – are significant. The all-hazards approach is especially important here.

Measures to implement and monitor 'all-hazards' compliant processes include the fine-tuning of risk analysis for on-site digital devices; supply-chain security measures including safer procurement and data handling; physical access for personnel, including employees and visitors; cyber-hygiene training; planning for business continuity in the event of a breach, and more. Security teams should urgently evaluate their existing cyber–physical resilience to quickly identify areas where additional measures or upgrades are needed.

Access management is a key element of any impacted organization's NIS2 compliance efforts. Intelligent access solutions can contribute to improving cyber–physical resilience with, for example, enhanced identity management, auditability, and round-the-clock remote building control. Credentials that require regular revalidation and/or expire automatically can drastically reduce the risk of unauthorized keys in circulation – another potential vulnerability for digital infrastructure.

Digital access solutions from Assa Abloy empower you to secure every layer and can contribute significantly to achieving compliance with the NIS2 Directive. They help protect organizations and data by enabling control over who goes where and when for each user, with the ability to cancel lost credentials instantly. They support both online and offline access control, improving workflows through flexible management – whether remotely or on-site. The offering includes digital access systems or access hardware to upgrade existing setups, providing scalable control over access points that were previously unreachable, and securing protection classes one to four. Wireless solutions are simple to install and require no wiring or structural modifications.

Physical access is often considered one of the biggest back doors for cyber criminals in an era of growing hybrid attacks. Closing it with digital access enhancements will ensure NIS2 obligations are met – and free security decision-makers from compliance worries. Assa Abloy experts are available to guide you through the specific features and benefits that align with the directive's requirements and enhance your organization's cyber–physical security framework. GIT

Assa Abloy Opening Solutions EMEIA
www.assaabloy.com

Idis Europe Confirms Brian Lee as New Managing Director

© Idis Europe

Brian Lee

Idis Europe has confirmed the appointment of Brian Lee as its new Managing Director, as it drives the wider adoption of AI video surveillance technology with a focus on system performance and value. Brian Lee was most recently Senior VP of Marketing & Sales Development for Idis Americas, based in Dallas, and was instrumental in growing the North American and LATAM business. He previously held a headquarters position as Head of the Global Strategy Team for the company, South Korea's largest in-country video technology manufacturer. Now heading up the Idis Europe operation, he will continue to build on Idis's success in the region with an expanded sales team, a new focus on marketing and public relations strategy, and further development of Idis's network of integration partners in the UK and mainland Europe. Brian Lee also brings valuable experience to his new role from his background as a Director at LG Electronics and his master's degree in business administration from Korea University, Seoul. **www.idisglobal.com**

Paxton appoints Peter Koueik as Head of Technical Operations for MENA region

© Paxton

Peter Koueik

Paxton has announced that Peter Koueik is now Head of Technical Operations for the Middle East and North Africa. Based in Dubai, Peter will lead all technical support and training activities across the region, ensuring installers and system integrators have the practical knowledge and tools needed to install, configure, and maintain Paxton systems. This includes managing the Free System Integrator Training program, which provides hands-on sessions and online learning for both new and experienced installers. Peter said: "I'm delighted to step into this role as Head of Technical Operations for Paxton in the MENA. Our aim in the region is to be the system integrators' trusted partner, introduce them to our distributors, and provide them with the right skillset to be able to seamlessly commission and install Paxton products." **www.paxton-access.com**

Romanian Security Summit Marks Successful Debut in Bucharest

The inaugural Romanian Security Summit, held on November 5–6 at the Romexpo Exhibition Centre, brought together industry leaders, innovators, and security professionals for two days of networking and knowledge exchange. Organized by a&s Adria and the Romanian Association for Security Technology (ARTS), the event featured a dynamic exhibition and a conference program tackling strategic security challenges and emerging trends. With over 1,000 participants and strong representation from international and regional companies, the summit established itself as a key platform for advancing security solutions in Southeast Europe.
https://romaniansecuritysummit.com

© Romexpo

The opening ceremony was highlighted by the symbolic cutting of the red ribbon, attended by distinguished guests and partners, including Leo Levit, President of the ONVIF Steering Committee, Lidija Stolica, President of the Croatian Security Association, Aleksandar Nedić, Secretary of the Association for Private Security, Chamber of Commerce and Industry of Serbia, Et al..

Mahir Hodzic, President of the Adria Security Summit Organizing Committee, emphasized that shared vision, collaboration, and innovation are key to creating new value in the security industry.

111 Sparks of Innovation

Southeast Europe‘s Security Industry United in Skopje

The 10th anniversary edition of the Adria Security Summit, the largest event of the security industry in Southeast Europe, was successfully held on October 8 and 9 in Skopje.

Over two days, the Summit brought together more than 2,000 participants and 111 exhibitors from around the world, showcasing innovative solutions in video surveillance, access control, intrusion detection, fire protection, physical security, cybersecurity, IT, ICT, automation, and smart technologies. The event aimed to strengthen collaboration and knowledge exchange within the security and technology community of Southeast Europe. “We are proud that the tenth edition of the Summit reaffirmed our mission to connect the entire region through knowledge, innovation, and partnership. Skopje became the center of Europe’s security industry during these days, which gives us further motivation to expand this concept and continue improving a platform that contributes to the development of the sector,” said Mahir Hodžić, Chairman of the Organizing Committee of Adria Security Summit.

This year’s Summit featured a rich conference program with panels, lectures, and presentations by leading experts from the global security and technology sectors, as well as an extensive exhibition area where participants had the opportunity to showcase their solutions, establish new partnerships, and develop business opportunities. A special highlight was the introduction of the Adria Smart City platform, organized for the first time in parallel with the Summit,

The Winners by Category

- **Smart City Project:** Smart City – Belgrade, Hytera Communications
- **Most Innovative Product/ Solution:** HALO Smart Sensor – Multifunctional Detector for Health and Safety Protection, Alarm Automatika
- **Access Control:** BioStar Air, Suprema Europe
- **Video Surveillance:** Milestone XProtect, Milestone Systems
- **Intrusion Detection:** Connect FLX, M2M Services
- **Fire Alarm:** Ajax – EN54-line fire alarm solution, Alarm Automatika
- **PA/VA Systems:** Honeywell VARIODYN ONE – Next Generation Public Address and Voice Alarm System, Honeywell
- **Software:** AppVision, UltraVision Consult
- **Best Case Study:** Yard Logistics Digitalization at the OKTA Refinery with the AURA System, Sensor Skopje d.o.o.

dedicated to technologies for managing the urban environments of the future. During the closing ceremony, awards for outstanding achievements in the security industry were presented across nine categories, once again emphasizing the importance of innovation and the contribution of companies shaping the future of the sector in the region and beyond. The Adria Security Summit was organized by a&s Adria, a professional magazine for integrated security solutions, which is part of the world's largest a&s Group of security media owned by Messe Frankfurt, Europe's leading organizer of trade fairs and industrial events.

During the closing ceremony of the 10th anniversary edition of the Adria Security Summit, held in Skopje on October 8–9, the Adria Security Award prizes were presented in nine categories, recognizing outstanding achievements in the security industry. This year, for the second time since the awards were established, more than 50 qualified applications were submitted — a clear indicator of the growing importance of innovation and the contributions of companies shaping the future of the regional and global security sector. The awards honor companies that have demonstrated excellence, advanced technology application, and a strong commitment to industry development. The jury was composed of renowned international and regional experts: Dragan Petric (bug.hr), Bata Vulović (Lunatronik), Roberto Licari (RL Security Consultancy), Igor Milkovski, Laert Klemo (ATECH), Israel Gogol (asmag), and Matija Mandić (King ICT).“Adria Security Award is not only a recognition of innovation — it is a testament to the collective efforts of our community to position the regional security industry on the global stage. Through this program, we aim to highlight companies that set standards through their work and inspire others to strive for excellence,” said Mahir Hodžić, Chairman of the Adria Security Summit Organizing Committee.

The next edition of the Adria Security Summit will take place on October 7–8, 2026, in Zagreb, where Southeast Europe's security industry will once again gather to exchange ideas and shape the future of the sector. GIT

Adria Security Summit
www.adriasecuritysummit.com

© Images:

Partner A&E Program supports security planners with tools, expertise, and services

With the A&E Partner Program, planners and engineers have field-proven tools, resources, and expert know-how readily available to help them design resilient and future-ready video security solutions – backed by decades of experience. The program delivers maximum efficiency, transparency, and planning reliability throughout the specification, design, and implementation stages of security projects. Core components of the program include the PlanD professional 3D planning software, the PresentD mobile media platform, and CalcD for instant project cost visualization. The PlanD software combines intuitive usability with professional features for precise 3D camera planning and realistic visualizations. The PresentD web app provides on-the-go access to exclusive content ranging from white papers, battlecards, and presentations to project-specific installation cards. **www.dallmeier.com**

i-Pro to take over Japan Wholesale and Marketing functions for i-Pro Products from Panasonic Connect

i-Pro (formerly Panasonic Security), a global provider of professional security, public safety and medical applications, has signed an agreement with Panasonic Connect to take over the wholesale and marketing functions for i-Pro products in the Japanese market. The transition is scheduled to be completed by March 31, 2026, following the necessary regulatory approvals. As of April 1, 2026, approximately 500 dealers who currently procure i-Pro products via Panasonic Connect will begin conducting business directly with i-Pro. Contracts with end-users purchasing through Panasonic Connect or Electric Works Company (Panasonic Corporation) will remain unchanged. This approach aligns with the regionally integrated management model that i-Pro has been implementing globally since 2019. **www.i-pro.com**

Gunnebo Safe Storage Strengthens Its Net Zero Journey with SteelZero

© Gunnebo

Gunnebo Safe Storage has joined SteelZero, representing a strategic step in the company's sustainability roadmap and highlighting its determination to tackle the environmental footprint of its material supply chain. As a global corporate initiative of Climate Group uniting organisations committed to accelerating the transition to a net zero steel industry, SteelZero requires members to commit to using 50% low-emission steel by 2030 and achieving 100% net zero steel by 2050, while collaborating with partners and influencing sustainable industry practices. Steel is central to Gunnebo Safe Storage's products, including safes, vaults, strongrooms and secure storage solutions, driving on average 40% of Gunnebo's total carbon impact. For Gunnebo Safe Storage, reinforced steel is one of the most significant purchased materials and a key driver of its overall carbon footprint. Transitioning to certified low-emission and near-zero steel is therefore an essential part of its goal to become a net zero business by 2045. The company will now work alongside more than 40 other SteelZero members, together representing demand of over 10 million tonnes of steel each year. Collectively, this membership base is building the conditions needed for systemic change in the steel sector, encouraging innovation and scaling technologies that reduce carbon intensity. Sameen Khan, Senior Manager at SteelZero at Climate Group added: "Steel is one of the largest sources of industrial emissions, and Gunnebo Safe Storage is proving that leadership in steel decarbonisation can come from any sector. By working closely with their supply chain and prioritising low-emission steel, they're showing how collaboration and embedding best practices are essential in accelerating the industry's transition to net zero."

www.gunnebo.com

© DHL Group/Autorin: Sonja Beyland

Senior Vice President, Head of Corporate Security & Crisis Management, DHL Group

Prevent. Protect. Recover.

Corporate Security at DHL Group

In an interview with Frank Ewald, Senior Vice President, Head of Corporate Security & Crisis Management at the DHL Group, it becomes clear how the logistics industry acts as a magnifying glass for essential trends of our time. From global trade to climate change to digitalization – these factors drive the „Strategy 2030" of the DHL Group, which aims for sustainable growth. With 80 percent of revenue generated outside Germany, corporate security must keep an eye on security-relevant trends and events worldwide. In a conversation with GIT SICHERHEIT, Frank Ewald explains the challenges and strategies of corporate security.

GIT SECURITY: Mr. Ewald, before we talk about your own tasks and functions, let's first talk about the DHL Group itself. What once emerged from the former Deutsche Post is today a growing logistics company with soon 600,000 employees. How do your global and German activities compare in size?

Frank Ewald: It is true, over the decades, the old Deutsche Bundespost has become a globally active and very successful company: Various acquisitions like DHL, Exel, or Danzas have provided a broad portfolio of logistics services and a global footprint. And I mean that literally: Almost two-thirds of our colleagues now work outside Germany, in offices, at ports, hubs, terminals, or on the roads of their countries. We like to talk about „over 220 countries and territories" in which the DHL Group is active, because sometimes statehood is not entirely undisputed. But as a globally active logistics company, our routes and networks span the entire world. Regarding corporate revenue, it is somewhat unclear, but if we look at the Post & Parcel Germany sector – the direct heir of the Deutsche Bundespost – this sector accounted for about 20% of our annual revenue of approximately €80 billion in 2023. Conversely, this means that about 80% is generated outside Germany. This in turn means that all security-relevant trends, incidents, and tensions of this increasingly uncertain world affect us. And thus also the area of security functions of the DHL Group.

DHL HUB Leipzig

© DHL Group

The classic post offices have largely been replaced by external operators or belong to Postbank and thus Deutsche Bank...

Frank Ewald: Yes, that is correct, but we are still intertwined in various ways. This is especially true for the nationwide network of parcel shops in Germany, which ensure very local supply in some cases. But this is also the case with the many larger partner branches of Postbank, which offer our products and services. Even though the formerly prominent post offices no longer exist, our customers can always find a DHL Group contact point nearby.

Post and parcel services as well as express and courier shipments are the largest business areas? For the latter, the DHL Group is said to have more aircraft than Lufthansa...?

Frank Ewald: That is correct – combined, Post & Parcel Germany and DHL Express account for about 50% of the company‘s revenue. Additionally, DHL Express continues to be highly profitable with its Time Definite services and has expanded significantly in recent years. Most of our cargo aircraft are operated there. This statement that we own more aircraft than Lufthansa, I have also heard, and it depends a bit on how you count. But it is confirmed in the case of pure cargo aircraft and the comparison to Lufthansa Cargo: Here, the DHL Group clearly leads, which is in the nature of our respective tasks – cargo transport for us; primarily passenger transport for Lufthansa. Fairly, it must also be said that Lufthansa transports a lot of „belly freight“ in passenger aircraft (Editor‘s note: Belly freight refers to the spaces in the aircraft that are located below the passenger deck. Goods are also transported there). If you add up all subsidiaries, you can assume that Lufthansa owns and operates more aircraft.

You are the Head of Corporate Security & Crisis Management of this vast and complex company. How is security management structured at the DHL Group overall – and what are your own responsibilities?

Frank Ewald: Such a global organization requires flexibility to react quickly and effectively. A certain degree of decentralization in the division of labor is therefore absolutely essential. My department – Corporate Security & Crisis Management – represents the strategic control center at the level of the Group Functions. Here, competencies are bundled, whose specialist areas work across organizational boundaries, such as the governance of Business Continuity Management (BCM), travel security, or the global security situation center. Each of our divisions, such as the aforementioned DHL Express, has its own security area, which then handles operational security issues down to the local level. Globally, the security organizations coordinate in a steering committee and set guidelines. Holding these coordinating threads in hand, making strategic security decisions, and advising top management competently is my task.

Sustainability and green transport logistics form the foundation of the 2030 Strategy

Could you explain the self-conception and goals of corporate security and crisis management at the DHL Group in more detail?

Frank Ewald: We have recently redefined our self-conception concisely as „Prevent. Protect. Recover.“ We see ourselves as an essential protective function for our colleagues, our operating resources, and of course the goods entrusted to us by our customers. „Prevent“ refers to our aim to avoid incidents in advance through appropriate preventive thinking, actions, and the use of technology. „Protect“ then brings the first components of hardening into play: How do we minimize the impact of harmful incidents? And „Recover“ is our aspiration to restore our operational processes to normal as quickly as possible after an incident. Our employees are absolutely at the center of this: If they see themselves as an active part of security and are confident in their actions, this strengthens all three aspects of our self-conception. This is the essence of our security culture at the DHL Group: We are all responsible for security, no matter what our main task is.

How does this translate into the strategies of corporate security?

Frank Ewald: We have just completed the process of formulating our security strategy for 2030 and derived the four strategic guidelines („Bottom Lines“) of the company: What does it mean for security to be the employer, provider, and investment of choice? And how do we define security sustainably? We have developed cross-divisional initiatives for all these bottom lines, such as harmonized security training for our employees or cross-departmental crisis management exercises. Additionally, we will prioritize certain initiatives. For example, we have actively approached selected customers as a security function and initiated close exchanges to improve cooperation. Initial feedback has been very positive. Furthermore, we have significantly expanded our geopolitical analysis capabilities, which are now proving beneficial. We are also strengthening our advisory and implementation capacities regarding security technologies. In this way, we protect our colleagues, our business, and our customers.

The understanding of corporate security today increasingly involves taking on consulting and coordinating functions within the company. Could you elaborate on how this is structured in your organization?

Frank Ewald: This is a key aspect of our work: we provide our expertise and knowledge to colleagues from all areas. Take, for example, the topic of advising on and implementing security technologies. Our security technicians are increasingly requested by divisions to plan and implement modern and resilient security technologies tailored to their needs while meeting all certification requirements or legal regulations. Through this, we have already achieved significant cost savings while maintaining high technical performance standards. As you can imagine, our colleagues are very busy. Coordination is also a central task for us. With five divisions and business-related services bundled in Global Business Services, there are many synergies to be leveraged! For instance, almost all divisions worldwide use the same security training program. This harmonizes core messages and prevents uncoordinated investments of time and money.

Please turn page ▶

The term „Business Resilience“ captures a trend describing holistic strategies for security management, particularly in the USA. How do you understand this term?

Frank Ewald: We understand resilience as holistic preparation for adverse events in terms of „Prevent. Protect. Recover.“ We recognize that we are a company built on physical and digital connections: while we have localized hubs and critical processes, we primarily operate a network of routes, paths, and data links. This impacts our approach – static protection alone is insufficient. We aim to identify and immunize critical business processes, harden our assets, contain and limit negative effects, as well as establish contingency options and redundancies where necessary – and then practice recovery responses. This forms the core of our company-wide business continuity strategy. To this end, we conduct numerous simulations annually.

You deal with diverse global risks – from political upheavals to tsunamis and other natural disasters. Could you describe how you prepare for these scenarios, gather information about them, and implement measures?

Frank Ewald: Part of this was already described under „Resilience.“ However, when it comes to quickly available and validated information, we operate an internal global security situation center. This center consolidates various information sources and evaluates events regarding potential impacts on the DHL Group. This may lead to local or regional measures or even activate our global crisis management team. We have also developed a crisis indicator methodology to act proactively when necessary. Regarding global disruptions mentioned earlier, we have significantly enhanced our geopolitical analysis and advisory capabilities. We monitor potential global crisis hotspots and coordinate with other corporate functions to achieve a comprehensive and balanced analysis as a basis for decision-making guidance. It's no secret which regions of the world we focus on monitoring.

Could you provide one or two additional examples from recent history?

Frank Ewald: Take the war in Ukraine, for example: In the lead-up to the 2022 invasion, our analysts developed various scenarios of how an escalation might unfold. The eventual invasion matched one of these predicted scenarios. Another anecdote would be that our crisis response team practiced the impact of a pandemic on the company a year before COVID-19 emerged. This likely gave us a head start when the real crisis hit.

IT security operates separately from corporate security at your organization, correct?

Frank Ewald: Yes, that's correct, and it's rooted in historical organizational structures. However, we collaborate closely at both divisional and Group levels. I personally coordinate frequently with my IT security counterpart, and many campaigns and initiatives are executed jointly. After all, we share the same protective mission, and our messaging often aligns.

To what extent are developments driven by artificial intelligence (AI) relevant to your work in corporate security?

Frank Ewald: Undoubtedly, digitalization and AI will profoundly transform our work. We're actively leveraging the opportunities of this global megatrend, though it demands new ways of thinking from our teams. We view AI positively, using it as an efficiency driver for tasks like analyzing large datasets or conducting security audits. However, we also monitor AI's risks. My team's experts have scrutinized these challenges, such as the nuances of tools like DeepSeek. Balancing opportunities and risks encapsulates our approach.

What key initiatives will corporate security prioritize this year?

Frank Ewald: Given the unpredictable nature of our field, priorities can shift abruptly. Barring unforeseen events, I'll focus heavily on advancing customer engagement in corporate security. We aim to position security as a key differentiator for the DHL Group and have planned numerous measures for 2025 to better integrate security with customer interactions, fostering trust and loyalty. Ultimately, security remains a trust-driven business.

Germany recently held elections. What expectations do you have for the new federal government, and where do you see the greatest need for action?

Frank Ewald: Having attended this year's Munich Security Conference, I witnessed the complexities of current global challenges. While the full scope of societal pressures is still unfolding, it's clear we must discard outdated mindsets and rebuild resilience. For businesses, reliable frameworks are critical – both economically and in meeting societal security demands. The new government's primary task will be enabling growth while addressing these dual imperatives. It's a monumental challenge, but urgency leaves no alternative. GIT

Deutsche Post DHL Group
www.group.dhl.com

Leader's 2026 Predictions — Babak Behzad, Head of AI at Verkada

"Agentic AI tools will be able to power a security operator's entire workflow, enabling them to focus on their highest-value work: Artificial intelligence is already redefining what it means to secure the physical world. Tools to date have been focused primarily on speeding up investigations, and while that is incredibly valuable, it's really just the start of what AI can do. As AI models become more capable and intuitive, they'll transform physical security into a proactive, intelligent discipline that helps teams detect and deter incidents before they escalate, not just respond after the fact. In the year ahead, we'll see AI quickly become an active partner to security operators. Natural language interfaces will make complex searches and investigations conversational. Predictive analytics will surface anomalies and trigger deterrence measures automatically before they need human intervention. All of this will free security professionals to focus on their highest-value work and create safer buildings, campuses, and communities around the world." **www.verkada.com**

A Big Security Plus

Scalable Video Surveillance by Direct-to-Cloud and the Hanwha Vision Partner Morphean

Here is the latest in a continuing series in which we introduce some leading partners of Hanwha Vision, and that leads us to Martin Jones, Director of Global Accounts at Morphean. They provide a cloud-based video surveillance, access control and business intelligence platform that enables users to monitor, administer and protect their operations securely and remotely. It also delivers actionable knowledge to support more informed decisions.

Martin Jones, Director of Global Accounts bei Morphean

Hanwha Vision: Could you tell us about your role at Morphean and your responsibilities?

Martin Jones: My name is Martin Jones and as Director of Global Accounts at Morphean I bear the responsibility of supporting our network of agencies so that they can offer end users valuable service-oriented solutions. A key element of the job is the close cooperation with our technology partners and internal teams to communicate customer expectations and market trends in our rapidly developing industry.

What does Morphean offer its customers and what is their specialist aspect within the video surveillance industry?

Martin Jones: Our core specialty lies in the provisions of a real Software-as-a-Service (SaaS) solution that is tailored to the growing demand for more intelligent, agile and cost-effective security environments. What distinguishes Morphean is that we use advanced video analysis, real-time warnings, and seamless integration with third-party systems. This empowers companies not only to improve their security, but also to gain valuable operational intelligence from a single point of view. Our solutions are particularly attractive for companies with multiple sites and those that want to change from the traditional on-site systems to cloud-native technology.

Tell us about the partnership with Hanwha Vision – how did it start and why does Hanwha Vision fit so well with your platform?

Martin Jones: Morphean and Hanwha Vision share the engagement for innovation and excellence in video surveillance. Together, we provide an impressive solution for heads of security that are looking for power, scalability and simplicity in their video surveillance systems. Our solution, Connect for Hanwha Vision, brings a true cloud experience within the security product palette of our partners.

Right from the beginning, we recognized that the sophisticated and versatile range of cameras from Hanwha Vision, combined with their open platform approach, perfectly matched our own vision for a versatile, cloud-based solution. The concentration of their teams on cyber security, edge analytics, and future-proof camera technology extended the capabilities of our platform and made it possible for us to deliver an integrated, powerful and secure cloud solution to our customers.

What are the developing trends in the market with the progress being made in video technology and how are the needs and priorities of customers changing?

Martin Jones: Customers are increasingly coming to us for solutions that go beyond traditional security and that offer added value through business intelligence that supports strategy planning and the decision-making process. They are also interested in KI-supported analyses, real-time incident response, and the integration of data from third parties. In addition, we are also seeing a remarkable shift toward cloud adoption, driven be the need for more versatility, centralized management, lower operating costs, and a quicker ROI.

Sustainability, cyber security and compliance are increasingly important aspects for end users, whereby the stakeholder is ever more aware and strict when it comes to the protection of data during transmission and storage. The approach of Hanwha Vision to cyber security with its NDAA conformity and GDPR-conformant devices was a significant reason for the partnership and is in total harmony with the cyber security approach of Morphean.

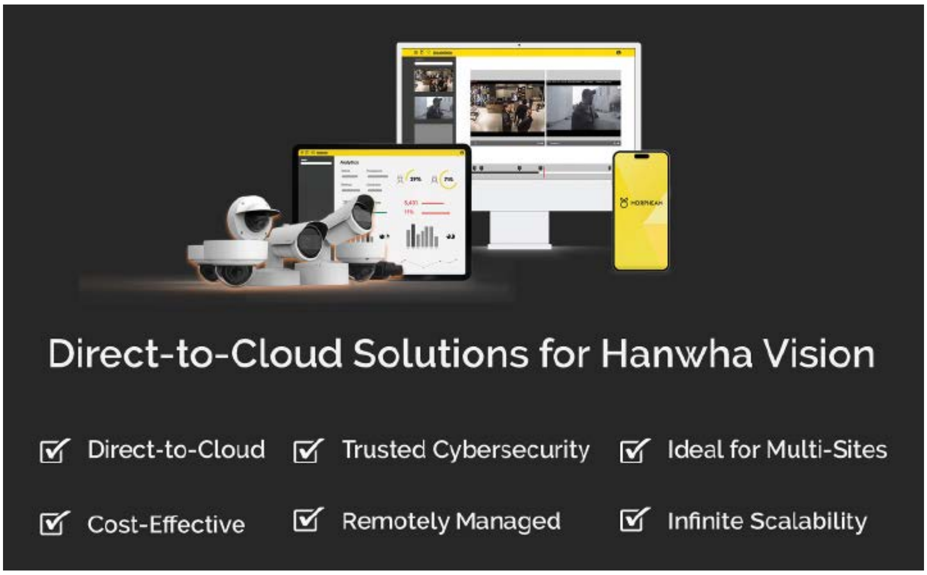
The modern security chief has a lot to be aware of. This is why they look for partners that not only deliver innovative solutions, but also have the expertise to advise on and apply them in a constantly changing environment and with a company's continually developing needs.

Please turn page ▶

How can organizations become future-proof through the introduction of a direct-to-cloud solution?

Martin Jones: Morphean's direct-to-cloud solution enables users to easily scale their solution, to remove hardware dependencies, and to benefit from ongoing software updates. This makes a generally more agile and versatile security solutions possible with the flexibility to add functionality when new technology comes onto the market. Maintaining conformity with the latest regulations and developing according to the newest requirements of an organization is also a notable advantage of introducing a direct-to-cloud solution. For example, when a facility expands to numerous sites that are geographically spread out, there are additional benefits that appear almost immediately, such as centralized operations, data resilience, and reduced maintenance costs.

The direct-to-cloud solution from Morphean delivers a range of benefits, from live surveillance and remote maintenance of Hanwha Vision devices, through to versatile cloud data retention and connection to alarm reception centers. The integration of Hanwha Vision and Morphean provides a powerful security and business intelligence solution in the cloud for organizations and installations of all sizes. GIT



Hanwha Vision
www.hanwhavision.eu

© Images: Morphean

TDSi's Gardis Pro v3.1

Integrated access control and security manufacturer TDSi has announced the release of Gardis Pro Version 3.1, the latest enhanced iteration of its Gardis Access Control Management Software. Gardis 3.1 introduces expanded biometric support and intelligent credential management, delivering improved hardware reporting capabilities and new third-party integration options to further enhance system performance and flexibility. The latest update to TDSi's Gardis Pro Software introduces a range of new features designed to enhance security, performance, and user experience. Version 3.1 adds support for the Digitouch Biometric Reader, enabling fast and cost-effective fingerprint authentication, and introduces automatic credential status updates to strengthen access control management. Administrators also benefit from customisable event log retention, improving compliance and system performance. New third-party integration with Nettla allows facility bookings to automatically trigger secure, time-limited access permissions, while updates such as accented character support, enhanced expander and door status reporting, and lift button press logging further improve system flexibility and monitoring precision. Additional refinements include a new Duress PIN alert function for discreet security responses and multiple backend performance enhancements that deliver greater stability and responsiveness across the platform. The latest version of TDSi's Gardis Pro Software builds upon the release of Version 3 earlier this year, which introduced a wide range of new features and enhancements including intuitive access control tools, advanced reporting, streamlined setup processes, a simplified licensing workflow, new multi-factor authentication options, and improved data import and user interface refinements. Gardis Pro Version 3.1 is available now and can be downloaded from the TDSi Product Registration site. TDSi installers and customers are encouraged to upgrade to Version 3.1 to take full advantage of the latest features and performance improvements. **www.tdsi.co.uk**

Europe's Triple Alliance

Airbus, Leonardo and Thales have signed a Memorandum of Understanding ("MoU") aimed at combining their respective space activities into a new company. ("MoU") aimed at combining their respective space activities into a new company.

By joining forces, Airbus, Leonardo and Thales aim to strengthen Europe's strategic autonomy in space, a major sector that underpins critical infrastructure and services related to telecommunications, global navigation, earth observation, science, exploration and national security. This new company also intends to serve as the trusted partner for developing and implementing national sovereign space programmes. This new company will pool, build and develop a comprehensive portfolio of complementary technologies and end-to-end solutions, from space infrastructure to services (excluding space launchers). It will accelerate innovation in this strategic market, in order to create a unified, integrated and resilient European space player, with the critical mass to compete globally and grow on the export markets. The project is expected to unlock incremental revenues, leveraging an expanded portfolio of end-to-end products and services leading to a more competitive offering, and greater global commercial reach. The combined capabilities also pave the way for even more innovative new programmes to enlarge the new company's market positioning. Further operational synergies in, among others, engineering, manufacturing and project management, are anticipated to drive long-term efficiency and value creation. **www.leonardo.com**

Bright Futures

Light + Intelligent Building Middle East Returns with Record Global Participation

Abdul Mushin,
Show Director
Light + Building ME

Now in its 19th edition, Light + Intelligent Building Middle East 2026 will take place from 12-14 January at the Dubai World Trade Centre MENA's leading event for lighting and building technology will host 450+ exhibitors from over 30 countries. Conferences Thinklight, InSpotLight and the Smart Building Summit headline the programme, while renowned international companies including Signify, Ledvance, KNX, Honeywell, Opple, Airzone, Theben, Illus and many more will be featured on the show floor.

Dubai, UAE: Light + Intelligent Building Middle East, the MENA region's leading event for lighting and building technology, returns to the Dubai World Trade Centre from 12-14 January 2026. With a growing global presence, Light + Intelligent Building Middle East will host more than 450 exhibitors from over 30 countries, with overseas companies accounting for over 90% of the international showcase. Co-located with Intersec Dubai, Light + Intelligent Building Middle East will bring together over 16,000 global industry leaders, innovators, and government bodies to explore cutting-edge products and solutions.

According to Grand View Research, the LED lighting market in the Middle East and Africa generated revenues of US$6.66 billion in 2024, accounting for 7.6% of the global market. The sector is expected to grow at a CAGR of 8.1% from 2025 to 2030, reaching an estimated US$10.34 billion by the end of the decade. With a strong market outlook, Light + Intelligent Building Middle East will feature leading international brands in the industry including Signify, Ledvance, Opple, Honeywell Lighting, Schréder and Illus. In addition, Light + Intelligent Building Middle East will highlight key players from the intelligent building sector such as KNX, Theben, Airzone, TE Connectivity and more.

"As Light + Intelligent Building Middle East marks its 19th edition, the event has become the region's premier meeting point for lighting and building technology. From pioneering products on the show floor, to forward-thinking discussions during our conferences and workshops, the event highlights how innovation is transforming the industry", said Abdul Muhsin, Show Director for Light + Intelligent Building Middle East.The conference element of the event, which includes Thinklight, the Smart Building Summit, and InSpotLight, provides an expanded programme this year, offering high-level insights from regional and international experts.

Now in its fourth edition, the Smart Building Summit will showcase how technologies such as artificial intelligence, smart sensors, and automated systems are transforming buildings to enhance sustainability and the user experience.

A truly global showcase: 442 exhibitors from 34 countries presented the latest lighting and intelligent building technologies at Light + Intelligent Building Middle East 2025, alongside the largest-ever Light Middle East Awards

The 18th edition in 2025 welcomed 15,948 visitors to Dubai World Trade Centre, marking a 10% increase in attendance and a 15% expansion in exhibition space, reflecting the region's growing demand for smart lighting and building solutions

The focus comes at a pivotal time as the intelligent building market is forecast by 6Wresearch to reach US$9.2 billion by 2030. Within the Middle East, revenues are forecasted to expand at a CAGR of 8% from 2024 to 2030 due to increased investment in smart infrastructure and sustainable technologies. Attended by architects, tech innovators, policymakers and sustainability experts, the Smart Building Summit will feature a new Tech Talks session, giving companies in the smart building sector the opportunity to present their products and technologies alongside expert-led discussions. For the first time, an advisory board has been established for the Smart Building Summit, comprising government representatives and industry leaders from across the region.

Commenting on the introduction of the board, Muhsin added: "In line with our commitment to delivering greater value and relevance, we are proud to announce the formation of a dedicated Advisory Board for the Smart Building Summit. By bringing together decision-makers in the industry, the board guides the strategic direction of the summit, ensuring discussions reflect the latest innovations, priorities and long-term opportunities for the market." A cornerstone of the event, Thinklight provides a platform for lighting professionals to exchange knowledge and network, collectively shaping the future of lighting, design, and technology in the region.

The 2026 Thinklight conference centres on the theme "Vision to Impact: From Inspiring Ideas to Lasting Legacies," and will deliver a comprehensive programme across three distinct formats. Highlights include a 45-minute Design Deep Dive keynote led by a renowned lighting designer; Project Perspectives, featuring focused 15-minute sessions on innovative projects; and Conversations in Light, 30-minute live interviews offering behind-the-scenes insights.

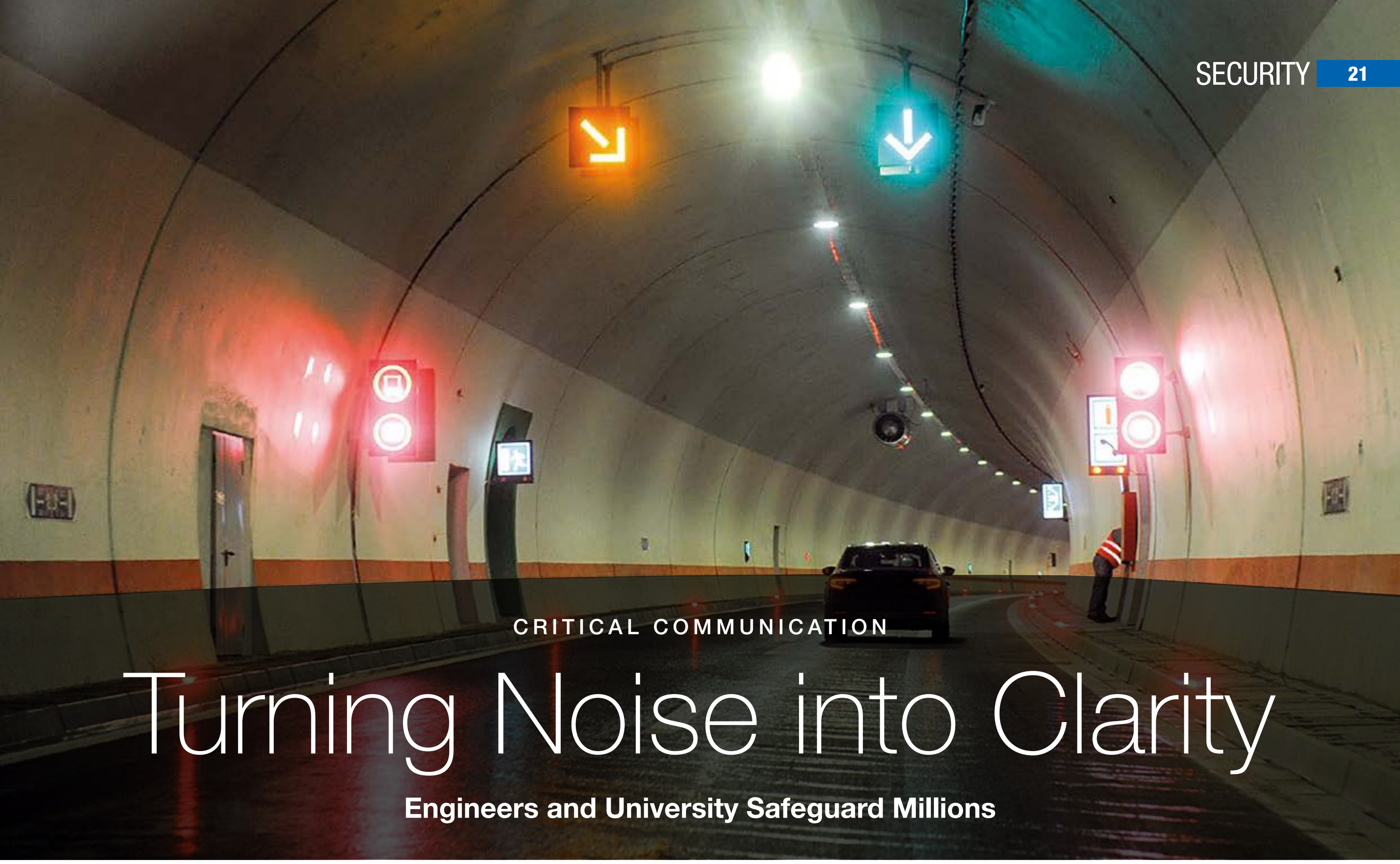
InSpotLight will once again highlight the innovations, designs and technology shaping the future of lighting. Over three days, InSpotLight will include a line-up of dynamic product presentations, thought-provoking sessions and hands-on learning experiences. A notable workshop at the InSpotLight stage for the 2026 edition focuses on "The AI Shift: Lighting Design Workflows in the Age of Intelligent Tools". The session offers a hands-on opportunity to learn how AI can supercharge creativity, streamline delivery, and reshape the future of lighting design highlighting the power of image and video generation platforms for creating lighting renders, visuals, and animations; alongside trained AI agents that automate lighting schedules, Leed and Dark-sky compliance, and technical documentation. A tribute to vision, excellence and innovation, the Light Middle East Awards will be held on 14 January at Conrad Dubai. Now in its 12th edition, the awards ceremony is recognised as the region's largest and most influential platform celebrating excellence in lighting, and honouring individuals, products, projects and partnerships that are shaping the industry worldwide.

Built around three overarching categories, which include 'Project of the Year', 'Product of the Year' and 'Partner of the Year' the Light Middle East Awards are judged through a meticulous evaluation process by an independent panel of over 30 distinguished local and international industry experts. Light + Intelligent Building Middle East comprises six product sections: Technical Lighting, Electric Lamps and Components, Decorative Lighting, Architectural Lighting, Electrical Engineering, and Smart Home and Building Automation. The event will be held in Za'abeel Halls 1-3 and Hall 1 at the Dubai World Trade Centre. GIT

Registration for
Light + Intelligent Building
Middle East is now open

Messe Frankfurt Middle East GmbH
www.ae.messefrankfurt.com

© Images: Messe Frankfurt Middle East GmbH



CRITICAL COMMUNICATION

Turning Noise into Clarity

Engineers and University Safeguard Millions

Railway stations, airports and stadiums are often noisy and reverberant. In emergencies – such as fires or terrorist attacks – this can make public announcements difficult to understand and put thousands of people at risk. Engineers from Ambient System in collaboration with researchers at Gdańsk University of Technology in Poland, have developed a system that automatically adjusts the tone, level and pace of public address messages. Powered by two proprietary algorithms, it is already deployed across railway, metro and airports networks in multiple countries.

This Polish innovation improves speech clarity in noisy, reverberant spaces, enhancing public safety by making announcements clearer and easier to hear. It is already deployed in demanding environments such as the Delhi Metro – one of the world's busiest and noisiest transport hubs, serving millions of passengers every day- as well as across railway and metro networks in Poland, Turkey, Sweden and Finland. It performs equally well in vast halls and narrow corridors – anywhere with difficult/challenging acoustic conditions. "Our aim was to create a system that not only meets rigorous international standards but, above all, improves comfort and the sense of safety for people in public, commercial and industrial facilities. The smartVES Public Address Voice Alarm system (PAVA) was developed through close collaboration between Ambient System engineers and the scientific team at Gdańsk University of Technology. It demonstrates how effectively commercial and academic expertise can be combined," said Marcin Starzyński, CEO of Ambient System. "We implemented two proprietary digital audio-processing algorithms. Adaptive filtering continuously adjusts announcements to surrounding acoustic environment, ensuring speech remains intelligible despite background noise. The speech time-transposition algorithm analyses the operator's voice and corrects speech tempo in real time—even during live announcements when a speaker may stumble or speak too quickly under stress. As a result, messages remain clear even in large spaces with significant reverberation," added Prof. Józef Kotus of Gdańsk University of Technology.

Intelligent Algorithms

Two algorithms, that are critical to ensuring announcements remain clear, underpin smartVES performance: the speech time-transposition algorithm and the adaptive filtering algorithm. The first dynamically adjusts playback speed to the acoustics of the space, including live operator messages so rushed or hesitant speech stays intelligible. The second assesses the environment's acoustic profile and existing background sounds, then reshapes the speech signal so announcements cut through background noise by emphasizing frequency ranges less affected by interference. The smartVES system is not the first breakthrough to emerge from Ambient System's partnership with Gdańsk University of Technology. Earlier joint projects produced proprietary AI- and machine-learning-based technology that can detect security threats in real time from audio signals and immediately alert safety systems.

Tackling Information Overload

Information overload—often called "infobesity"—is not limited to the online world, where people spend an average of nearly seven hours a day1 on the internet. In the real world we also face an excess of visual and acoustic signals. Overlapping sounds, conversations and automated messages can make speech unintelligible. This is precisely where new technologies help ensure that critical announcements stay clear when they matter most. GIT

Ambient System
www.ambientsystem.eu/en

© Images:

VIDEO

System Upgrade

Scalable video security technology for Snoqualmie Casino and Hotel

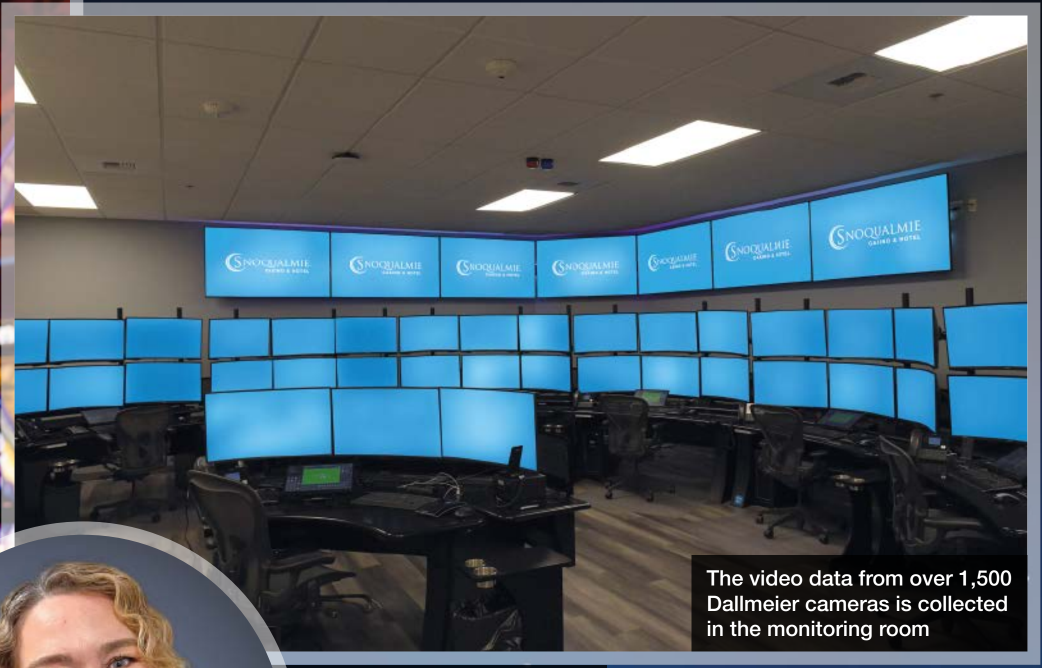
Snoqualmie Casino and Hotel is located about 30 minutes east of Seattle in the US state of Washington. It is named after the Native American tribe of the same name – the 'People of the Moon'. The casino offers nearly 1,800 slot machines and 58 Vegas-style table games. Snoqualmie Casino and Hotel has relied on Dallmeier's video surveillance solutions since 2015, and the proven technology is being used for the current system expansion.

Nearly 1,800 slot machines and 58 Vegas-style table games are secured by Dallmeier solutions

Video surveillance covers all relevant areas of the property, including the gaming floor, front-of-house and back-of-house areas, restaurants, and car parks. The Dallmeier system has proven itself reliable and scalable for over a decade, despite growing requirements and technical developments. However, renovations, expansion plans and new requirements for internal processes have made it necessary to expand the existing surveillance solution. Jolene Stewart, Snoqualmie Casino and Hotel's Executive Director of Security and Surveillance, reported on the requirements and advantages of a Dallmeier solution.

A System That Grows With You

The Washington State Gambling Commission requires casinos to be continuously monitored. The aim was therefore to adapt the existing system to the changed conditions, both functionally and technologically, without replacing the proven infrastructure. It was essential to meet the regulatory requirements while ensuring a safe and pleasant environment for guests and employees. The emphasis was on reliability, as well as process optimization, system availability, and the capacity for easy integration of new technology.



The video data from over 1,500 Dallmeier cameras is collected in the monitoring room

Jolene Stewart, Executive Director of Security and Surveillance at Snoqualmie Casino and Hotel

Customized Solution for a Comprehensive Overview

The existing surveillance system was upgraded to include specific features as part of the expansion. Only Dallmeier components were used, including the Hemisphere SeMSy (version 5) modular video management system and Domera cameras. The dome cameras have pre-installed neural networks and integrated edge analytics apps, offering a wide range of intelligent video analysis applications. Their motorized three-axis adjustment makes remote configuration easy. The whole system provides central control of the 1,500 cameras and efficient evaluation of the video data.

Planning and implementation were carried out in close cooperation with integrator North American Video (NAV), who adapted the system to the spatial conditions and operational processes as required. “The long-standing and solution-oriented cooperation with all parties involved was crucial in enabling us to jointly implement a solution that meets the specific requirements,” adds Joe McDevitt, President of Dallmeier USA.

A Sustainable Solution

“We have continuously expanded our video security technology over the past decade to meet our requirements,” says Jolene Stewart, Snoqualmie Casino and Hotel’s Executive Director of Security and Surveillance. The system’s high reliability, no downtime and easy maintenance are impressive, characteristics that are crucial for efficiency in daily casino operations.

It also pays off economically in the long term: “Reliability is a key cost factor in the surveillance industry. The fact that we have not had any expensive replacements or unexpected service calls over the years speaks for itself,” she adds. GIT

Video surveillance covers all relevant areas of the property: gaming floor, front and back-of-house areas, restaurants, and parking areas

Dallmeier electronic GmbH & Co.KG
www.dallmeier.com

© Images: Snoqualmie Casino & Hotel

PERIMETER

Guarding Every Edge

Hirsch Secure: Project-Proven Technology Under a New Name

Michael Schreiber, Vice President Sales EMEA and APAC at Hirsch Secure

Sorhea and TIL Technologies are known in the DACH region for perimeter protection and sophisticated access control. Could you give us a brief introduction to the new Hirsch Secure company?

Michael Schreiber: We continue to be a part of the Vitaprotech Group and have now combined our competencies in high security technology in the DACH region into Hirsch Secure GmbH. We provide comprehensive access control, video analysis, perimeter protection, and identity verification solutions for our target market of integrators and installers. The new structure is based on specialized brands that are clearly applied to sales channels. At the core, the company consists of the combination of the activities of Sorhea, TIL Technologies and Hirsch (formerly Identiv). We have been working under the new structure since June of this year. At Hirsch Secure, we concentrate on solutions for integrators and installers, and offer a modular portfolio in these sectors.

Heiko Viehweger: We have been something like the 'hidden champion' of the industry for some time. That is because some of our products are sold as OEM products under the brand name of well-known manufacturers. Seen internationally, we already have a good reputation in the USA, the UK, and France and, with Steven Humphreys as Deputy CEO at Vitaprotech, we have a very experienced man at the helm. In Germany, our customer base is growing primarily through project business in perimeter protection and in the security of critical infrastructure. To grow further, we are strengthening our technical service personnel. Heiko Baumgartner is now our external adviser who will assist us in matters of public relations and networking.

Where do you see the strengths of Hirsch Secure?

Michael Schreiber: In the DACH region we are concentrating on the core activities of intrusion and perimeter protection, and access control as well as video surveillance and analysis. We want to impress integrators and installers of these systems – and ultimately the end users – with our products and solutions. The basis for this are first-class products for high security areas, field-proven integrations and our long-term project experience. There are local experts and advisors available, and globally active teams are working on research and product development in the background. We can be even closer to our customers because of the new organization.

Heiko Viehweger: If you look at company security as a whole, our work starts at the perimeter of the compound. We provide all the modern methods of perimeter security, also for small companies or sensitive private properties, right up to the high security of companies with critical infrastructure and military areas. Within the perimeter, we secure access to buildings of all types, down to the office desk or the production line. If the customer requests, we can offer a central dashboard for the administration of the security from the perimeter to the core area, effectively a comprehensive and integrated security management system that makes the best use of existing investments. We make the whole system fit for the future, to meet the requirements of the KRITIS law for example, not least because we invest in both our own products and also in artificial intelligence, cloud technology, PSIM and VMS systems, and cyber security. We consider ourselves to be a 'one-stop-shop'. This means that the customer has just one point of contact, if they wish, who will put together a complete solution that includes the necessary competent planning. We then plan together with the integrator or installer exactly what the customer wants, deliver all the components, and integrate existing elements or those provided by third parties.

The Sorhea perimeter protection products are well-known in the market. What does the whole product range in this sector now include?

Heiko Viehweger: We really have everything to offer here that the market demands: perimeter sensors, fence-mounted cable, infra-red barriers, sensors with dual-technology, microwave barriers, detection fences, underground cable and, of course, also video analysis systems. You could say without exaggerating that we have the broadest product range of perimeter detection systems on the market. This alone is not a guarantee for successful project completion, but has a significant benefit: we distinguish ourselves from companies that can only provide one or two detection methods by being able to choose the ideal solution for every sensitive loca-

Heiko Viehweger, Head of Sales DACH at Hirsch Secure

Vitaprotech and Hirsch are well-known names in the USA and France for high-security technology and integrated access control, video analysis, perimeter protection, and identity verification solutions. The Vitaprotech group of companies has bundled all of the security activities of Sorhea, TIL Technologies and Hirsch (formerly Identiv) worldwide under the name Hirsch Secure since June of this year. The next step was taken in Germany, Austria, and Switzerland with the founding of Hirsch Secure GmbH. GIT SECURITY International spoke with Michael Schreiber, Vice President Sales EMEA and APAC, and Heiko Viehweger, Head of Sales DACH, about the new structure and the product palette of Hirsch Secure.

tion or particular area. We can also install a second layer of security for particularly endangered systems, thanks to our range of products, to compensate for any possible weakness of one type of technology, or to provide a redundant system. Using innovative software and reliable hardware, we are able to protect every category of endangered location – from a company site with gates, façades, roofs, and boundary walls to special situations such as railway infrastructure.

Having a broad product spectrum does not necessarily guarantee the best individual product. How do you manage in-depth quality control?

Heiko Viehweger: We do use a variety of technologies, but we do also have a reputation as the 'Best of Breed'. We take part in international comparisons and tests, and face the competition wherever possible. We took part very successfully in the independent GIT Perimeter Protection System Test, in which our light-beam technology achieved excellent results. The Maxiris 3100 infra-red beam was granted top marks and the system was recommended for providing first-class protection. In the same test, we submitted our Velocity Perimeter video analysis and were able to further optimize the system from the results of the test. The final result was that the solution was among the top performers this year during

Please turn page ▸

The Hirsch Secure Team at the foundation of the company in June 2025 the benchmark test of a large German integrator. We are not averse to comparisons at an international level, and have successfully completed long-term field trials in Scandinavia at various military locations. The same applies to Switzerland where we were successfully tested at high security locations.

Hirsch Secure does not manufacture and video surveillance hardware itself. Which cameras do you employ in your solutions?

Heiko Viehweger: That is right, we work together with selected hardware partners, such as Vivotek for example, when the end user does not want to use an existing system or prefer a particular supplier. The Vivotek devices excel in particular with their high level of cyber security and attractive price-performance ratio. We can supply complete video recording systems, and we have the Velocity Perimeter video management system with intelligent video analysis and AI software in our product range for those customers that do not want to the systems of well-known PSIM or VMS providers. We do however provide product SDKs and integration of all our products for their systems. Our Velocity Perimeter video analysis has been in use under the name Foxstream for more than 15 years in many hundreds of installations throughout Europe. Efficient and powerful algorithms recognize intruders in every scene and environment, and eliminate false alarms, which ensures accurate video verification. Our software products are enhanced by our own Velocity Central PSIM.

Which products and solutions do you use for access control?

Michael Schreiber: For access control we use products that are less well known in the DACH market but have already been successfully used throughout Europe. We offer centralized access control systems that cover a wide range of application scenarios. They include modern card and ID readers as well as intelligent access management solutions that enable access control to be efficiently organized. Products are used that are based on Hirsch, TDSi and TIL Technologies products, and that have proven themselves thousands of times over in the USA, the UK, and France not only in price-sensitive projects but also in high security areas where our BSI or ANSSI certified access control solutions meet the highest security requirements. In the UK, our products have been tested a number of times by the National Protective Security Authority for their suitability in highly secure infrastructure. We also utilize innovative identification methods such as the use of smart phones or biometric systems. The portfolio is enhanced by versatile solutions using radio and offline locks that enable secure and needs-based access governance. The powerful controllers ensure reliable control over all access events.

How do you work together with integrators and installers?

Heiko Viehweger: Our project work experience really comes to the fore when partnering with integrators. We rely on a real partnership with the security integrators, developers, and the end users. Both sides profit from the cooperation with nationally represented integrators and local installers, and we openly contribute all our experience to these projects because we know that only together can we deal with the growing commercial and technological requirements of our customers and legislators. GIT

Hirsch Secure GmbH
www.hirschsecure.de

© Images: Hirsch Secure GmbH

AI accelerated "Clean Voice from Noise" wins gold at 'Nuit de la Sécurité Globale 2025' in Paris

TKH subsidiary Commend International was awarded gold for its „Clean Voice from Noise" solution in emergency situations at the Nuit de la Sécurité Globale 2025 in Paris in the ‚QHSE & Personal Protection' category. This innovative technology uses deep neural networks to separate speech from background noise and make transmissions virtually echo- and interference-free.

The „Clean Voice from Noise" solution, developed in close cooperation with the Institute for Electronic Music and Acoustics (IEM) at the University of Music and Performing Arts Graz, results in extremely clear, intelligible emergency call communication that is equivalent to transmission in a noise-free environment. The neural networks behind the solution are trained using machine learning to reliably distinguish speech from noise in real-life situations. In awarding the gold medal, the jury praised the innovative combination of artificial intelligence, practical safety technology, and measurable improvement in speech intelligibility.

www.tkhsecurity.com

© TKH

SMART BUILDINGS

Lidar and the Louvre

Stopping the Heist before it happens with Lidar

Seven minutes. That's how long the recent Louvre heist took. In broad daylight, a group of thieves rode up on a construction platform, smashed display cases, stole several historical jewels tied to the Napoleonic dynasty and escaped on scooters before anyone in the control room even realised what was happening. It sounds like a scene straight out of "Mission: Impossible." Only this time, Tom Cruise wasn't there.

Author:
Martin Vojtek,
Business Director 3D Surveillance at Hexagon's Safety, Infrastructure & Geospatial division

In movies, we often see tight webs of red laser beams guarding treasures, with the hero gracefully sliding between them. Reality, however, is far less cinematic. Most museums still rely on mechanical sensors, simple infrared barriers, cameras and the most fallible component of all: the human eye. But the human eye doesn't measure space. A camera records an image, but it doesn't know that a display case has shifted by three centimeters, or that a visitor's hand just crossed an invisible boundary. That's where a new kind of perception comes in — Lidar.

From Hollywood Fantasy to Real-World Security

Forget the tangled maze of laser beams you've seen in films. A modern 128-channel rotating Lidar fires hundreds of thousands of laser pulses per rotation — and it does this up to 10 times per second. That's millions of spatial measurements every second, creating an invisible web of light that maps the scene in 3D, without anyone ever noticing. What Lidar builds is called a point cloud — a live three-dimensional model of the environment. The system constantly compares this "snapshot" with the current scene. If anything changes — a hand moves closer to an artifact, a case is displaced or an object disappears — Lidar detects it instantly.

When Technology Sees in 3D

Lidar technology (such as Lidarvision, developed by Hexagon), brings true 3D situational awareness into museums and galleries. It doesn't just see that someone is moving; it knows where, how fast and in what trajectory. Each detected object is tracked with its precise dimensions, velocity and spatial position. If a visitor steps too close to a protected exhibit, the system triggers an alarm. Pan-tilt-zoom (PTZ) cameras automatically turn to the exact spot and start recording. The operator no longer has to stare at dozens of screens, hoping to catch the right moment. Lidar data also serves as forensic evidence — allowing investigators to replay the incident as a full 3D reconstruction. They can see exactly how intruders moved, from entry to exit, with centimeter precision.

Beyond Thieves: Everyday Situational Awareness

Lidar isn't just a tool against master criminals. It helps with daily operations, too — recognizing when someone lingers suspiciously near a sensitive exhibit, when an unauthorised object enters the room or even when a visitor collapses. The system can trigger a silent alert, notify security staff or automatically redirect nearby cameras.

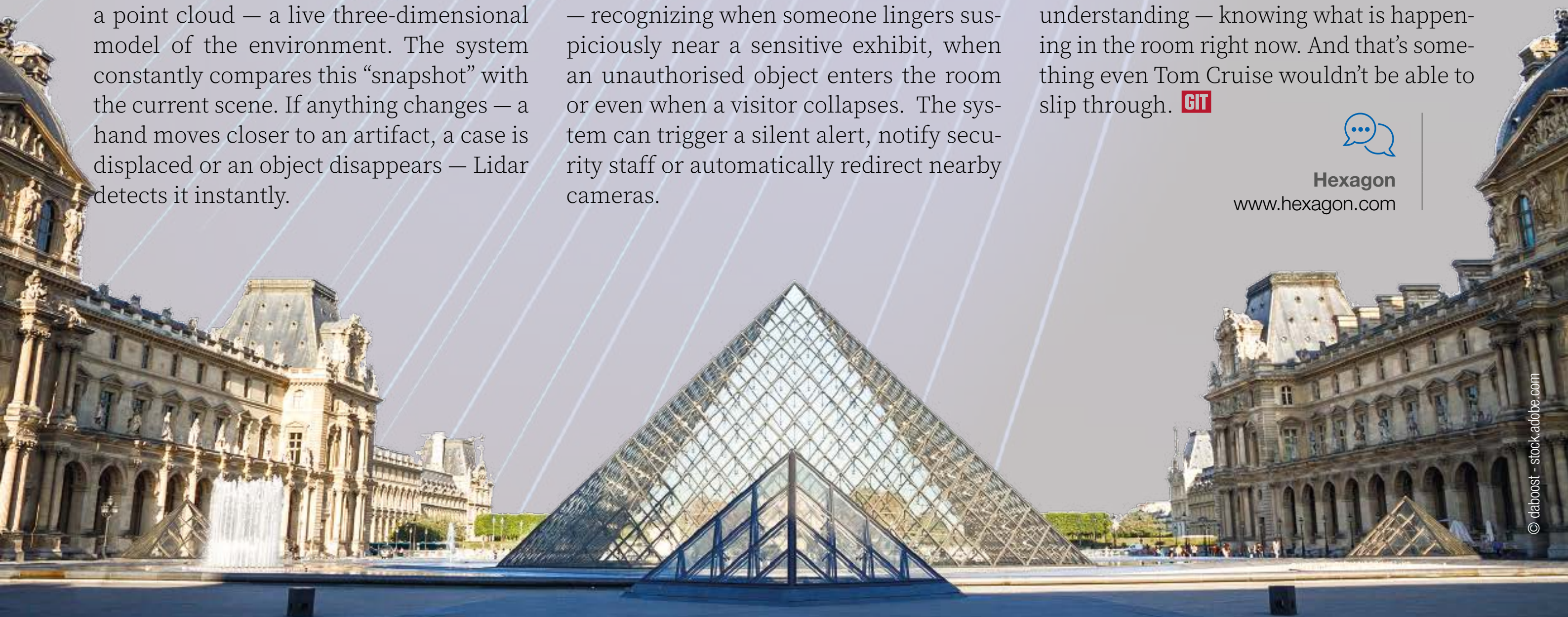
History that Never Comes Back

Art theft is not a cinematic rarity — it's a recurring tragedy. In 1990, 13 paintings worth more than half a billion dollars vanished from Boston's Isabella Stewart Gardner Museum. None have ever been recovered. Even Leonardo da Vinci's Mona Lisa was stolen from the Louvre in 1911 — though it was miraculously found two years later. That case, however, remains the exception. Thieves often fail to realise that cultural artifacts are not commodities. When they melt them down for gold or strip them for gems, they don't just destroy value — they erase history.

Spatial Understanding is the Future of Security

No security system is flawless. But while cameras merely watch, Lidar understands space. From a single compact device, it monitors the 3D environment in real time, detects anomalies and reacts immediately. Modern security is no longer about higher fences or better cameras. It's about spatial understanding — knowing what is happening in the room right now. And that's something even Tom Cruise wouldn't be able to slip through. GIT

Hexagon
www.hexagon.com



© gala - stock.adobe.com

© daboost - stock.adobe.com

Villa Cattolica, built in 1736 in the historic heart of Bagheria in Palermo, houses the Guttuso Museum

© Guido - stock.adobe.com

SMART BUILDING

Protect Museums

How Ajax Secures the Guttuso Museum in Sicily

In the historical heart of Bagheria, Palermo, Villa Cattolica houses the Guttuso Museum, which stores and exhibits works by one of Italy's famous modern painters, Renato Guttuso. Built in 1736, the villa faced a critical security challenge — to preserve its assets while embracing security measures that respect its historical significance. The security system installed at the villa was outdated, unreliable, and lacked informative capabilities, prompting the need for a modern alternative.

Designing security systems for historical facilities like Villa Cattolica presents unique challenges. Wired systems, which typically involve extensive drilling for installation, pose a significant threat to the architectural integrity of such structures. Historical buildings, with their thick walls, intricate designs, and delicate features, have strict prohibitions against drilling. In response to the challenge, Tecnotel Energy S.r.l. was tasked with delivering a reliable and efficient security solution to safeguard premises without compromising the site's architectural heritage. Installers designed the solution, taking into account the unique characteristics of the villa, and implemented 104 devices to cover all nuances. It was decided to equip the site with Hub 2 Plus Jeweller. Capable of managing up to 200 devices, it proved to be an optimal solution for extensive multi-floor facilities like Villa Cattolica. The hub features four communication channels, connecting to four different internet providers — two via Ethernet and Wi-Fi, and two via cellular networks. In the event of issues with one channel, the hub seamlessly switches to another, ensuring reliable communication with the Central Monitoring Station (CMS) and Ajax apps.

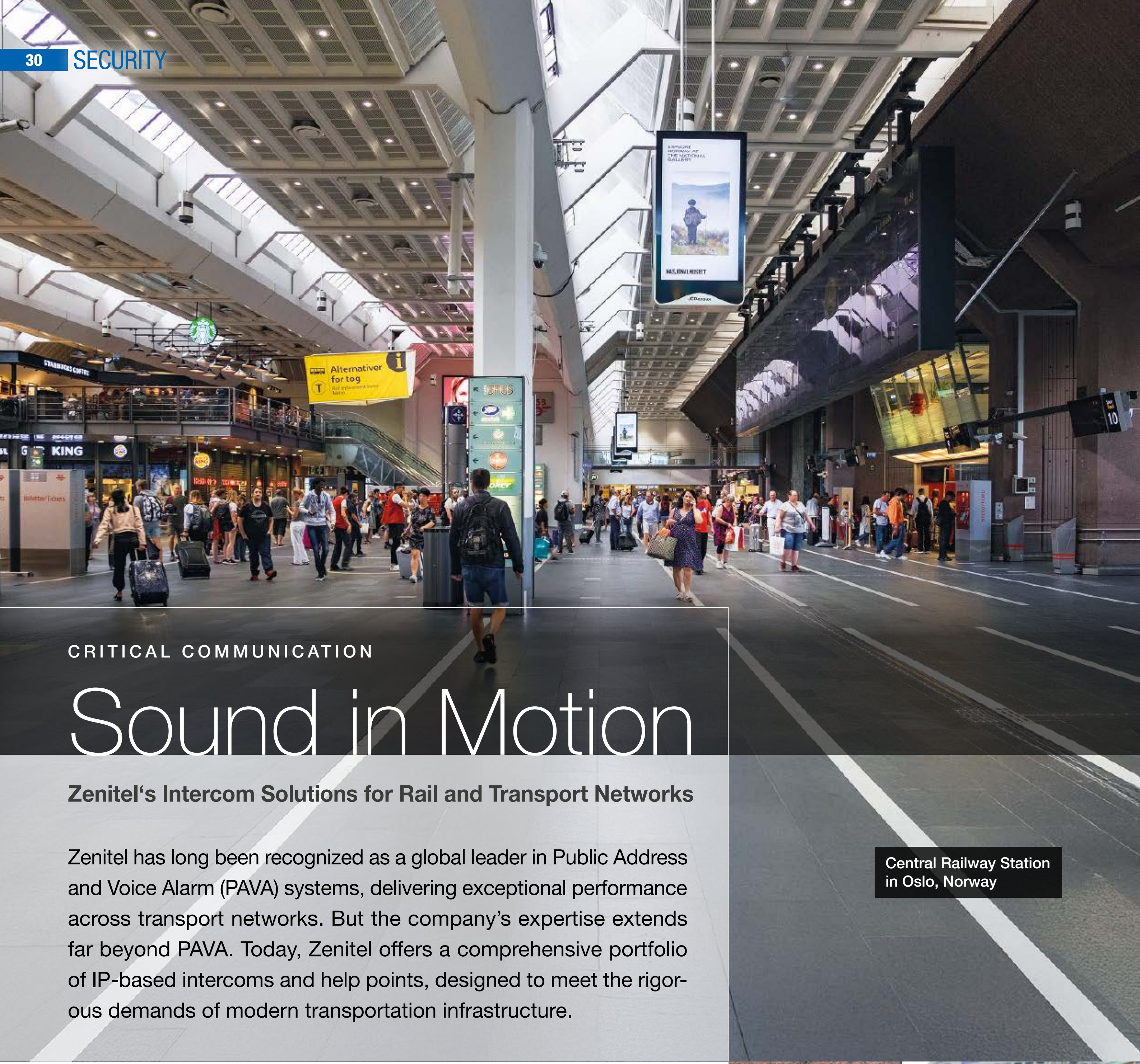
Fifteen DoorProtect Plus Jeweller detectors were chosen to protect entrances and balcony doors. Equipped with opening, shock, and tilt sensors, these devices can swiftly detect intrusions into the facility. MotionCam Jeweller was chosen for motion detection. The client requested a reliable mechanism that filters out false alarms caused by employees who sometimes forget to disarm the security system while entering the museum. In case of an alarm, MotionCam Jeweller sends an animated series of photos into Ajax apps. Using photo verification, the museum administration can quickly determine whether the threat is real and decide if the rapid response unit should be called. Given the complex radio signal conditions of the multi-floor structure and thick walls, range extenders were used to expand wireless coverage. Tecnotel Energy installed three range extenders, including ReX 2 Jeweller, which supports alarm photo verification from MotionCam Jeweller detectors. These range extenders boost the range of all Ajax devices, eliminating the need for an additional control panel. As a result, this leads to more efficient system management and reduced project costs. StreetSiren Jeweller sirens were placed on different sides of the building to ensure the alarm signal was audible from all directions, while the LED indication provided visibility. The sirens also serve as a deterrent to potential intruders.

Superior StreetSiren DoubleDeck Jeweller features a radio interference detection algorithm. It detects sudden noise level changes to differentiate temporary disruptions from deliberate jamming. If jamming is confirmed, it triggers an alarm.Surveillance cameras from a different manufacturer had already been installed at the facility. All Ajax systems offer an easy process for third-party CCTV integration via the SDK. As a result, the live view is now available in Ajax apps, streaming with efficiency and low latency. Automation scenarios were configured to arm/disarm the system according to the museum's working hours. The scenarios can be easily reconfigured on-site or remotely: changing settings in Ajax apps takes only a minute when working hours are updated. Wireless connectivity and range extenders eliminate the need for intrusive cabling and make Ajax the ideal solution for addressing the challenges posed by historical buildings. With Ajax photo verification, system users and monitoring company operators can promptly verify whether an alarm is real and save costs on rapid response unit calls. Additionally, integrating video surveillance cameras into the security system allows users to easily access images and videos from the cameras directly within Ajax apps. GIT

© Ajax Systems

Since drilling is strictly prohibited due to the historic building fabric, the installers had to find other solutions for installing the equipment

Ajax Systems
https://ajax.systems



CRITICAL COMMUNICATION

Sound in Motion

Zenitel‘s Intercom Solutions for Rail and Transport Networks

Zenitel has long been recognized as a global leader in Public Address and Voice Alarm (PAVA) systems, delivering exceptional performance across transport networks. But the company’s expertise extends far beyond PAVA. Today, Zenitel offers a comprehensive portfolio of IP-based intercoms and help points, designed to meet the rigorous demands of modern transportation infrastructure.

Central Railway Station in Oslo, Norway

Their solutions are engineered for demanding environments such as busy stations, trackside locations, or onboard trains, offering robust performance where reliability is critical. Built-in noise cancellation and automatic volume control durability ensure reliable and efficient communication at all times. The range includes models with IK ratings for impact resistance and IP66 ratings for protection against dust and water ingress. Their durable construction makes them ideal for outdoor and trackside installations.

For high-risk or exposed areas, Zenitel offers Vandal Resistant IP Intercom Stations such as the VR3G-1 and TCIS-2 designed with reinforced steel front plates. With IK10 ratings, these units provide maximum protection against vandalism and physical abuse.

The ECP-C1 Emergency Call Point intercom exemplifies both reliability and smart functionality, developed in close collaboration with a leading transport authority. Designed for critical communication, it features Zenitel’s advanced audio processing technology and enables direct calls to a designated Emergency Response Centre via a single red call button. To support accessibility, the unit includes a built-in Audio Frequency Induction Loop (AFIL) for users with hearing aids. It is fully compatible with the Zenitel Connect-Pro intercom management solution, and integration is straightforward requiring only one external connection thanks to its Power over Ethernet (PoE) capability.

Zenitel also offers a wide range of modular intercom kits, so integrators

TCIS-6 Audio Intercom

can find an option that works perfectly in any given space. IP kits such as the TKIS-2 IP Audio kit and TKIV+ IP Video kit utilise the latest technology to create unparalleled HD audio and video quality, along with Open Duplex, Active Noise Cancellation, Automatic Volume Adjustment, and a 10W Class D amplifier.

Many of Zenitel's intercoms and kits, comply with the EN 50121-4 standard for Railway Applications, specifically addressing EMC emissions and immunity of signalling and telecommunications equipment. This rigorous standard ensures that the devices neither cause electromagnetic interference with other critical systems nor suffer performance degradation due to the electromagnetic disturbances typical in rail environments. Compliance with EN 50121-4 is essential for maintaining safety and reliability across railway networks, where critical communication and system integrity are paramount. By meeting these stringent requirements, Zenitel's solutions provide operators with confidence that their communication infrastructure will perform consistently, even in the most challenging electromagnetic conditions.

All Zenitel intercom systems are IP-based and operate using secure SIP protocols, ensuring easy integration into existing transport networks while delivering superior audio quality. A wide range of customization options are also available. These include tailored finishes, localised text, and built-in induction loops to meet accessibility standards and adapt to specific regional requirements. For environments where aesthetics are a priority, certain intercom kits can even be installed discreetly behind custom, customer-facing panels, maintaining the visual integrity of station designs. The provider is committed to delivering exceptional reliability and lasting value to its customers. By integrating PAVA, intercom, help points, and access control into a single unified critical communication platform, Zenitel enables streamlined deployment, simplified maintenance, and improved system-wide situational awareness.

Single Button Emergency Call Point with Built in AFIL Hearing Loop

„At Zenitel, we understand that no two transport environments are the same. That's why we offer a highly customisable range of communication solutions - from station platforms and help points to trackside and rolling stock," explains Henry Rawlins, VP Product Management at Zenitel. "With our extensive product portfolio and ability to tailor everything from appearance to functionality, we provide the right fit for every application — without compromising on performance or reliability."

Zenitel's range of intercom and IP Speakers are now available on the Network Rail i-Store. The i-Store is Network Rail's centralised catalogue for approved and trusted equipment, used by contractors and project teams throughout the UK network. Every product listed has undergone checks to meet Network Rail's exacting standards. The latest inclusion ensures Zenitel's full range of solutions are pre-approved for procurement, streamlining specification and deployment across all Network Rail infrastructure projects. GIT

Zenitel
www.zenitel.com

© Images: Zenitel

Suprema to Showcase Cloud-Native Access Control Platform at GSX 2025

At GSX 2025, held from September 29 – October 1 in New Orleans, Louisiana, U.S. Suprema demonstrated how Biostar Air is transforming access control through three core capabilities: zero on-premises architecture, native biometric authentication, and seamless multi-site management. These features reduce IT complexity and enable rapid deployment. BioStar Air also supports a wide range of credentials, including facial authentication, RFID cards, mobile access, and QR codes. Through a single dashboard, accessible via mobile or web, administrators can manage access anytime, anywhere, for a single site or multiple international sites. Biostar Air is designed to address the rapidly growing demand for cloud-native, subscription-based access control in the U.S. market. Organizations such as coworking offices, residential complexes, franchise chains, and school campuses increasingly require solutions that support scalable deployment, remote management, and stronger compliance with data protection standards. With BioStar Air, enterprises can scale across multiple sites without the burden of infrastructure costs. The platform enables reliable, fast deployment and smooth integration with third-party systems allowing organizations to expand security operations quickly and efficiently.

© Suprema

"Biostar Air represents the future of access control, delivering cloud-driven security that is simple, scalable, and secure," said Bob McKee, President of Suprema America. "At GSX 2025, we are excited to show customers how Biostar Air can reduce complexity, streamline operations, and unlock new levels of agility in security management."

www.supremainc.com/en

Dare To Be First

Ajax Systems is set to host its 7th annual showcase, Ajax Special Event: Dare to be First, streaming live on November 21, 2025, via the company's official YouTube channels.

This flagship event will introduce next-generation solutions in fire and life safety, video surveillance, and intrusion protection — highlighting how these technologies seamlessly integrate into a single, unified system. The presentation will also spotlight Ajax Services and evolving software features designed to elevate user experience and empower security professionals.

Under the theme Dare to be First, Ajax invites the industry to embrace innovation, tackle long-standing challenges, and set new benchmarks in safety and smart security.

The event will be broadcast globally in over 20 languages, with voiceovers and subtitles available. **www.ajax.systems**

Join the Ajax Special Event – Register here

© Ajax Systems

Hikvision WonderHub Becomes the World‘s First Large-Format Display to Achieve TCO Certified Generation 10

Hikvision Digital Technology Co., Ltd. („Hikvision") announced that its WonderHub interactive display (models listed below) has achieved TCO Certified, generation 10. This makes WonderHub the first large-format product in the global display industry to receive this prestigious certification from TCO Development, the leading international sustainability certification organization. The TCO Certified certification represents one of the most rigorous sustainability assessments in the technology industry, requiring comprehensive evaluation of a product‘s complete lifecycle environmental impact.The certification process covers every stage from raw material sourcing and manufacturing to energy efficiency during operation and end-of-life recycling. Beyond environmental metrics, the assessment includes strict auditing of corporate social responsibility practices, ensuring companies demonstrate genuine commitment to sustainable business operations. Hikvision‘s WonderHub exceeds EU environmental standards throughout its development and production. The company has implemented stringent controls on hazardous substances including heavy metals, flame retardants, and plasticizers, ensuring the product meets the highest international safety and environmental requirements from materials sourcing through manufacturing processes. **www.hikvision.com/en**

Dacorum Borough Council Upgrades Communal Doors

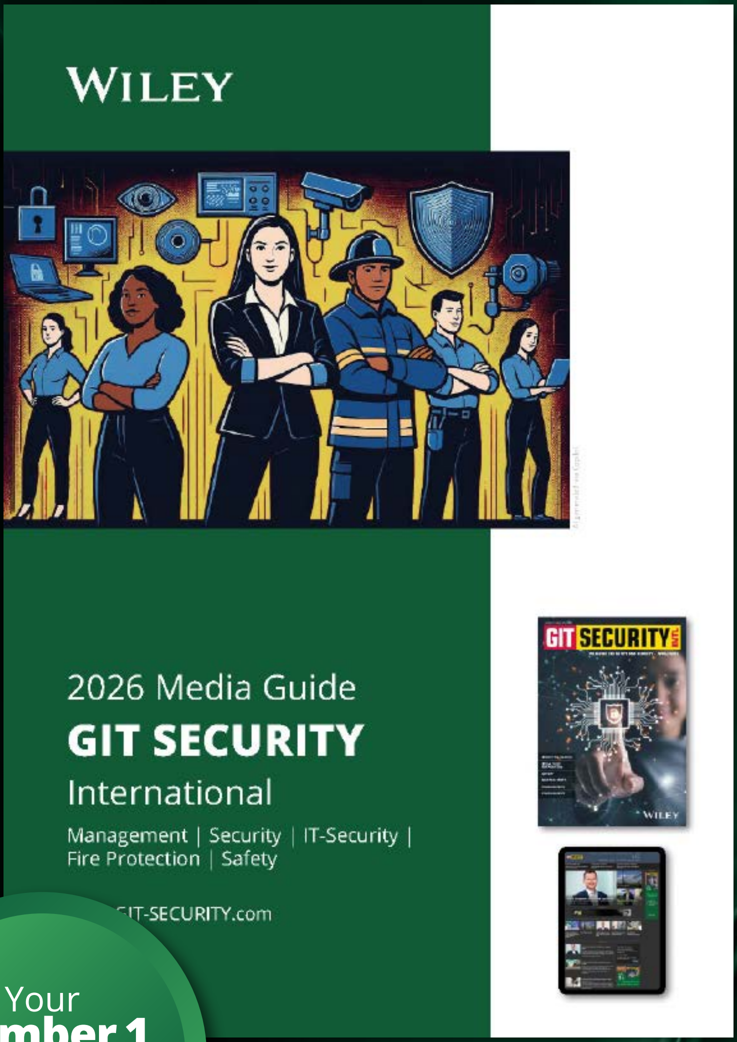
Amthal Group Companies has partnered with Dacorum Borough Council to upgrade doors across communal housing facilities, improving accessibility, security and everyday convenience for residents.

The project focused on replacing doors that had reached the end of their service life with latest solutions, designed to meet current standards and residents' needs. By installing secure doors to close effectively, Amthal enhanced safety whilst supporting ease of movement throughout communal spaces. As part of the upgrades, external doors were fitted with suited keys to ensure only authorised residents could access the blocks. Free swing door closers were installed on existing fire doors, maintaining fire integrity while making operation effortless for residents, particularly those in assisted living who may face mobility challenges. Throughout the project, Amthal coordinated closely with Dacorum Borough Council to minimise disruption to residents and ensure a smooth installation process. **www.amthalgroup.com**

© Amthal Group Companies

Intersec 2026: UAE's vision for a safer future

The 27th edition will run from 12–14 January 2026 at Dubai World Trade Centre, under the patronage of His Highness Sheikh Mansoor Bin Mohammed bin Rashid Al Maktoum, and backed by strategic support from The General Command of Dubai Civil Defense (DCD) and SIRA. The forthcoming edition is set to deliver an enriched programme and expanded features, with a remit to advance emergency response capabilities and secure digital and physical infrastructure. The event will welcome global leaders showcasing the latest innovative technologies and frontline solutions, aligned with the UAE's vision for a secure and sustainable future, which has seen the country ranked safest in the world in 2025 by global aggregator, Numbeo. **https://ae.messefrankfurt.com/dubai/en.html**



ACCESS CONTROL

Mobile Convenience

iLoq's new mobile-first smart access system extends its global reach

The iLoq 5 Series+ smart access system, designed specifically for residential buildings, launched in North America earlier this year, is now also available in Australia and New Zealand, with plans to expand the offering to Europe in 2026. The access system is a significant upgrade to the company's 5 Series system, ensuring that the lock cylinders and access management system meet both residents' and building managers' expectations for ease of use and security levels.

iLoq, a global provider of battery-free smart access systems, has just launched its new 5 Series+ locking system and access management platform. This is a mobile-first solution made for the residential market. The launch taps into a broader digitization trend that is moving away from mechanical locks and keys toward keyless access management. This means greater convenience for residents, such as being able to share digital keys with family members, delivery providers, or service staff remotely without the need to replace or duplicate physical keys. The roll out of the new systems started in the United States and has now expanded to Australia, New Zealand, and Canada, with launches in other global markets expected over the remainder of 2025 and 2026.

"Access management should be about giving residents peace of mind and giving property managers tools that save time and reduce costs. Everyday life is increasingly managed through mobile devices, yet access to homes and shared spaces has lagged behind. With the 5 Series+, we are aiming to bridge the convenience gap by providing digital access tools that are as flexible as the mobile apps we use to bank, shop, and communicate," explains Tomi Karjalainen, Chief Innovation Officer at iLoq.

Mobile Convenience

The launch comes at a time when property owners and facility managers are under increasing pressure to enhance building management and access systems, reduce operating costs, and meet residents' rising demand for the convenience of mobile-first access services. Unlike mechanical locks or competing smart locks that depend on batteries and wiring, 5 Series+ operates without electricity or batteries. Access rights are managed entirely in the cloud and activated through a resident's smart mobile phone.

In addition to new upgraded locks, 5 Series+ also comes with a significantly upgraded back-office access-management platform. The new platform is modular, meaning building managers can add the functionality they need, leaving out unnecessary features.

Fast ROI

A key advantage the 5 Series+ delivers for investors in residential buildings is the return on investment time frame. It is widely acknowledged that mechanical locks are less expensive to install than digital ones. Still, they often require additional long-term costs, including key replacements, lock changes, and delivery or maintenance work. By contrast, battery-free locking systems based on mobile access are virtually maintenance-free, ensuring fast investment returns. According to data from iLoq, most residential building owners see a return on investment within the first few years of the installation's lifetime.

The 5 Series+ locking system and access management platform addresses the trend toward keyless access control

"iLoq's battery-free and keyless smart locks have been a game-changer in the industry. They are integral components of modern access, and we are delighted to see our solutions being rolled out around the world," Karjalainen continues. Adoption of mobile-based access systems is expected to continue, with the global mobile access control system market projected to expand from approximately US$ 4.8 billion in 2024 to US$ 15.5 billion by 2032.

The iLoq 5 Series+ hardware requires no wires and no batteries

Iloq
www.iloq.com

© Images: iloq

ACCESS

Procuratie Vecchie Reborn

Heritage Meets Dom’s Advanced Fire and Access Systems

A symbol of power and grace, the Procuratie Vecchie once safeguarded Venice’s treasures and its vulnerable. Now restored, it reopens its doors with a new mission. Venice, a city enthroned upon water and stone, stands as a testament to human ingenuity and artistry. Its canals reflect a history of power and beauty, nowhere more evident than in Piazza San Marco, the heart of the Venetian Republic.

Here, the Procuratie Vecchie has stood for over 500 years as a symbol of resilience. Once home to the Procurators, guardians of St. Mark’s Basilica and its treasures, this sentinel has undergone a restoration that weaves together history, architecture, and contemporary purpose into a legacy for generations to come.

Reopened in 2022, this historic building now acts as a bridge from its illustrious past into a vibrant present, inviting the world to step inside.

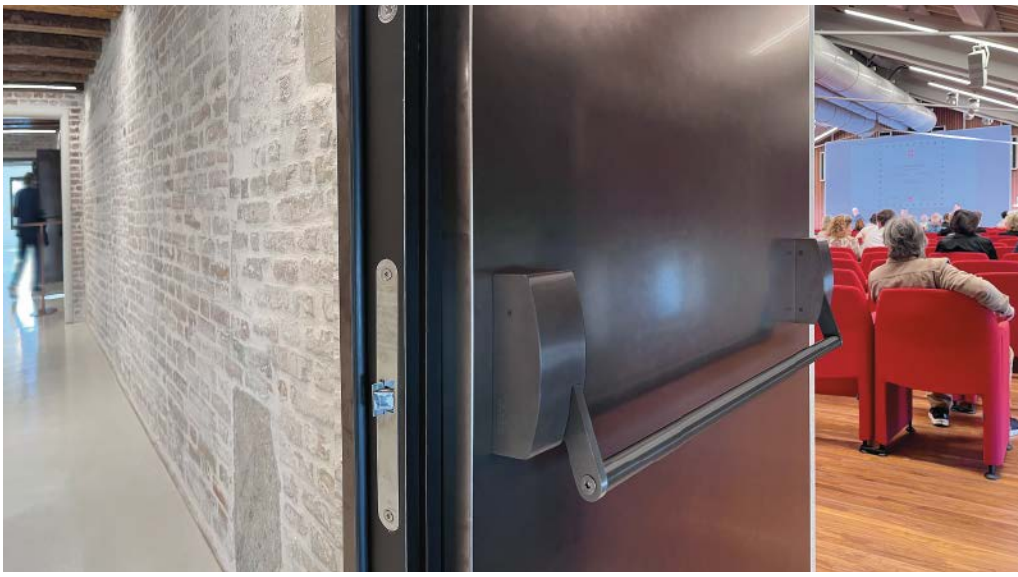
Watching over the City

To walk through Venice is to wander through time. The city’s palaces, churches, and bridges speak of a maritime empire that once dominated the Mediterranean. Completed in the early 16th century, under the vision of architects like Jacopo Sansovino, the Procuratie Vecchie graces Piazza San Marco with its elegant arches and classical facade. For centuries, it served as an administrative and residential space for the Procurators. Later it became the headquarters of the Assicurazioni Generali – now more commonly known as Generali Insurance – a testament to Venice’s enduring economic might. Through floods, wars, and time, the edifice has stood firm, its walls protecting stories of a golden age. Yet by the late 20th century, the Procuratie Vecchie had fallen into disuse, its grandeur muted but never lost.

Opening the Doors

In 2016, Generali Real Estate launched an ambitious restoration led by David Chipperfield Architects Milano. They were guided by three principles: conservation, revelation and innovation. Conservation efforts meticulously restored ornate rooms, preserving centuries-old wall and ceiling decorations. Revelation unveiled 16th-century attics and Venetian terrazzo floors; and Innovation brought modern enhancements, such as a new staircase to the third floor, now home to The Human Safety Net foundation. Here, the organisation runs public exhibitions, coworking spaces, an auditorium and a café in support of its work with vulnerable parents and refugees. Overseen by the Superintendency of Venice and the Ministry of Cultural Heritage, the goal was not just to repair a structure but also to mark a new milestone: the first time the Procuratie Vecchie opened its doors to the public. Restoring a building in Venice is no small feat. Car-free and criss-crossed by canals, the city’s environment is unique and prone to flooding. All these posed significant challenges. Materials arrived by hand, often at night, without modern machinery. The 2019 acqua alta – unusually high tides – tested the team’s resilience, yet they persevered. Local artisans and modern experts united, blending Venetian craftsmanship with contemporary solutions.

Historic interiors meet contemporary purpose: the renovated spaces of the Procuratie Vecchie reveal original Venetian terrazzo floors and restored attics, now hosting exhibitions and collaborative work areas for The Human Safety Net



Custom REI fire doors finished with marble powder and equipped with antipanic handles by Antipanic Spa ensure safety without compromising the historic character of the Procuratie Vecchie

Integrating Modern Functionality

A key aspect of the Procuratie Vecchie project was to adapt the historic building for modern use while preserving its timeless character. This required a thoughtful integration of safety and accessibility features without disrupting its historical essence.

Here, Antipanic Spa, a member of DOM Security, played a vital role. Their expertise came into focus particularly on the third floor, where a grand corridor lined with arches now features imposing REI fire doors finished with marble powder. Antipanic, in collaboration with Danish design brand, d line, crafted bespoke antipanic handles for these doors. Physical Vapor Deposition (PVD) technology was used to achieve both high durability and refined elegance. Approximately 30 of these handles were crafted to complement the building's fire-resistant doors, ensuring that safety measures enhanced rather than detracted from the structure's aesthetic integrity.

Antipanic's tailored solutions are a striking example of how modern technology can breathe new life into historic spaces, honouring their heritage while securing their future. As part of the restoration's grand design, their contribution successfully navigated Venice's logistical and environmental challenges, and struck a balance between preservation and progress. It was a significant contribution to ensuring the building continues as both a monument and a functional space.

A Legacy For Tomorrow

The Procuratie Vecchie reopened In April 2022, its grandeur restored and its purpose redefined. What was once a sanctuary for the Procurators, guardians of St. Mark's legacy, now welcomes all to explore its history and engage with its present. Antipanic's contribution, though introduced late in the process, was essential. Their expertise in crafting safety systems for historic buildings ensured that this 500-year-old treasure could meet modern demands.

Today, as visitors wander its halls, they experience a harmony of eras: the echoes of the Procurators' stewardship meld with the vitality of a modern cultural hub. The Procuratie Vecchie now stands as a guardian reborn, preserving Venice's unbreakable spirit not only in stone, but in the lives it touches. GIT

Dom Security
www.dom-security.com

© Images: Dom Security

Italy Triumphs at the 2025 European Cybersecurity Challenge

Warsaw hosts Europe's top young cyber talents in a thrilling competition of skill, strategy, and collaboration

© ENISA

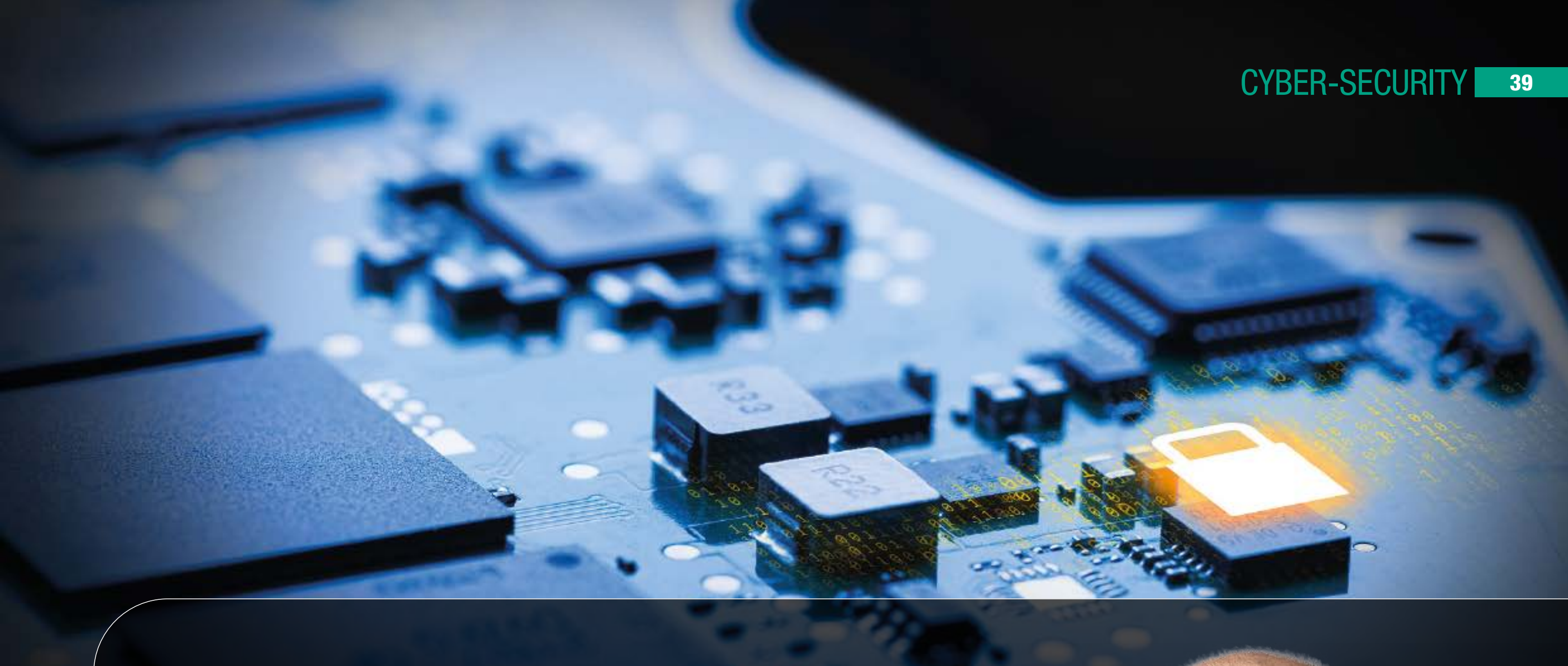
39 teams, 1 winner: Italy celebrates their victory at the 2025 European Cybersecurity Challenge in Warsaw

Italy has claimed victory at the 11th edition of the European Cybersecurity Challenge (ECSC), held from 6 to 9 October in Warsaw, Poland. The national team outperformed 38 others from across Europe and beyond, securing the top spot on the podium. Denmark followed in second place, with Germany taking third. Organised by Poland's National Research Institute NASK and supported by the EU Agency for Cybersecurity (ENISA), the ECSC brought together young cybersecurity talents from EU Member States, EFTA countries, EU candidate nations, and international guest teams. The event was inaugurated by Poland's Deputy Prime Minister and Minister of Digital Affairs, Krzysztof Gawkowski, who underscored the strategic importance of cybersecurity in today's hybrid threat landscape. Over two intense competition days, participants tackled a wide array of Capture the Flag (CTF) challenges. Day one featured a Jeopardy-style format, while day two shifted to an Attack/Defense scenario. The tasks spanned hardware and mobile security, cryptography, reverse engineering, binary exploitation, and digital forensics—demanding not only technical prowess but also rapid, collaborative decision-making under pressure. ENISA Executive Director Juhan Lepassaar praised the ECSC as a "unique opportunity for young European talents to test their digital skills, creativity, and teamwork in real-world conditions." Luca Tagliaretti, Executive Director of the European Cybersecurity Competence Centre, highlighted the event's role in fostering trust, cooperation, and a shared sense of purpose among Europe's future cybersecurity leaders. In a further push for diversity, a Female+ Bootcamp followed the main event, offering training and mentorship to female participants. This initiative will lead to the formation of a Female Team Europe, set to compete internationally in Dublin in 2026. The ECSC continues to serve as a vital platform for nurturing cybersecurity expertise, building networks, and inspiring the next generation of digital defenders. GIT

European Union Agency for Cybersecurity (ENISA)
www.enisa.europa.eu

Skills for Security welcomes Axis Communications as new Platinum Sponsor

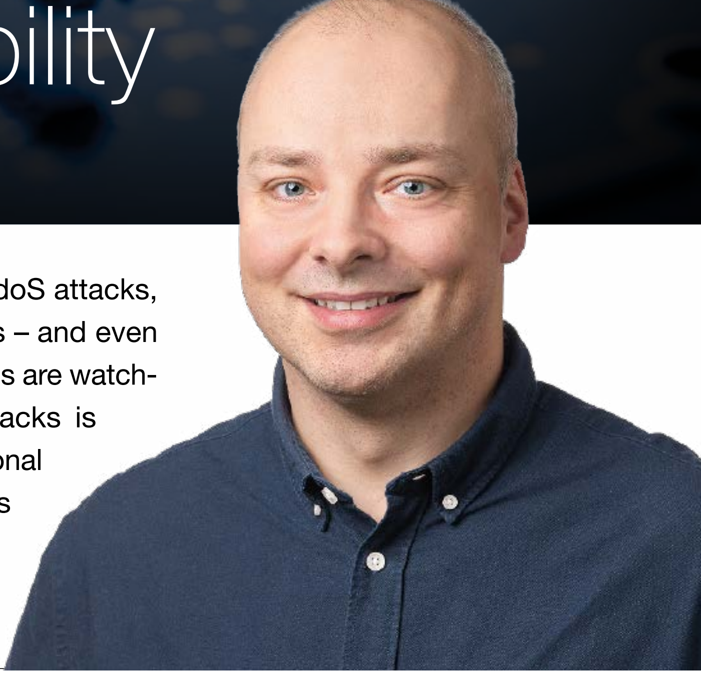
Skills for Security, the UK's leading fire and security apprenticeship training provider, is proud to welcome Axis Communications as its latest Platinum Sponsor, with an aim to focus on practical skills development and raising professional standards. This new partnership highlights Axis' commitment to raising the bar in training, skills development and career progression for security professionals across the UK. Working closely with Skills for Security, Axis will support high-quality apprenticeship programmes and initiatives designed to nurture new talent. The Platinum Sponsorship programme, developed by Skills for Security, offers leading brands a way to support and engage with the apprenticeship ecosystem. Through this partnership, sponsors gain visibility, access to networking opportunities, and direct opportunities to train the next generation of professionals As a Platinum Sponsor, Axis will champion high standards in fire and security training, supporting initiatives that bridge education and industry. Together, helping to raise awareness of the opportunities available to the next generation of security professionals. **www.axis.com**



The IoT Vulnerability

Cyber Security in Video Surveillance

Cyber attacks open the way to controlling devices, to DdoS attacks, attacks against public institutions, hospitals and schools – and even in the war against the Ukraine, Russian air defense systems are watching to plan their attacks. The number of reported attacks is increasing massively every year. GIT SECURITY International spoke with Andre Bastert, Global Product Manager Axis OS at Axis Communications, about his company's cyber security strategy.



Andre Bastert, Global Product Manager Axis OS

GIT SECURITY International: Mr. Bastert, as far as possible, cameras should not have any cyber security vulnerabilities. And in spite of this, IP cameras are the most frequently attacked of all devices. How do you see the situation?

Andre Bastert: The situation really is worrying. International reports on the vulnerability of IoT devices confirm it. The sheer number – we are talking about billions of networked IoT devices – and their often insufficient protection present an enormous problem for everyone concerned, and that includes manufacturers, operators, or regulation authorities. It is therefore not surprising that the IoT market has been increasingly flooded with new laws, regulations, and standards. Unfortunately, not all manufacturers have managed to incorporate cyber security into all of their products. The resultant 'IoT target' is a growing risk that has to be addressed.

So although a cyber security strategy is absolutely essential for a manufacturer such as Axis, it cannot achieve anything on its own without the user. Could you explain the development of your strategy since Axis first published a vulnerability report in 2016?

Andre Bastert: We have come a long way since 2016 and are proud of the progress that we have made in vulnerability management. We intensively studied the Best Practices from the IT industry back then, and learned from what the leading companies were doing. We developed our own 'Axis Vulnerability Management Policy' on that basis. This explains transparently how we deal with weaknesses – from identification, through patching and to the processes and the communication with our partners and customers as soon as a deficit is identified.

Could you tell us more about the cooperation with external researchers – penetration tests, for example – and also your joining the Common Vulnerabilities and Exposures (CVE) Program 2021?

Andre Bastert: In 2021, we joined the Mitre CVE Program as a CVE Numbering Authority (CNA). Every identified vulnerability receives a CVE-ID, a unique identification number, together with a comprehensive Security Advisory and additional information. The CVE Program immediately forwards these externally so that our customers are informed, can react quickly, and install patches. The distribution of information and the associated transparency and scope of this process are the big

Please turn page ▶

Cameras are the frequent subject of cyber attacks and must therefore be particularly well protected

advantages of this program and a major benefit for us and our customers. The 'Knowledge Transfer' that takes place has allowed us to develop our vulnerability management further and make it more professional by adapting our processes in a similar way to IT giants such as Google, Microsoft, or Cisco.

A further step forward was the start of our first Bug Bounty Program together with Bugcrowd. This is where we reward ethical hackers financially for their responsible reporting of weaknesses. This method alone has allowed us to rectify more than 30 weaknesses. Add to these the numerous penetration tests that Axis either orders yearly or are initiated by our customers. These have enabled us to identify and patch more than 50 vulnerabilities in the meantime.

A further milestone on the subject of vulnerability management is our cooperation with the Bundesamt für Security in der Informationstechnik (BSI). More than 220 network products from Axis now carry the IT security label of the BSI. A core commitment of this is to proactively inform the BSI market regulators about any weaknesses that have been discovered. Security-relevant information is then distributed rapidly – an important step towards implementation of the Cybersecurity Resilience Acts (CRA) of the European Union in Germany.

Our strategy adopts international cooperation and a multi-layer security concept with a range of measures that make our products step-for-step ever more robust – through penetration tests, the Bug Bounty Program, transparent communication and regulatory cooperation. Cyber security is however not a one-off project, but a continual process that requires engagement at all levels. Only a strategy that is based on mutual exchange and professional cooperation will strengthen our product security.

Let us take a closer look at your 'Axis Edge Vault' security platform ...

Andre Bastert: What we call the 'Axis Edge Vault' consists in principle of the entirety of all hardware-based, advanced security technology at Axis – and thereby forms the foundation of cyber security in our network products. For example, our customers expect that their Axis product starts exclusively with Axis-authorized software and not with just any code. Equally, they expect that the product was not manipulated during transport and that it can be verified as a real Axis device with total certainty. This is ensured by functionality such as Secure Boot, Signed OS, and the Axis Device ID.

In addition to this, highly sensitive data such as certificates, private keys for network communication, or access information for door control, is securely stored without the possibility of extraction. That is why we exclusively use TPM modules and Secure Elements in our devices that are certified to Common Criteria and FIPS 140. The internationally certified TPM modules and Secure Elements that we use in our products are also used, among other applications, in smart phones or for the creation of passports and therefore provide the same level of security.

In the light of the increasing threat from deep fakes and manipulated video files, our cameras also offer the ability to cryptographically sign video streams. This permits customers to be certain that the video stream is real. Since 2020/2021, we have committed not to deliver any Axis IoT device without this security function.

You issue corresponding updates when you recognize a critical software security problem. How do you discover the weaknesses?

Andre Bastert: We actively drive cooperation with independent security researchers, ethical hackers, as well as professional security companies, among them many of our own customers. The basis of our trust is mutual, and transparency and openness are key to successful protection. We therefore expressly welcome that many of our customers regularly call in professional security companies themselves to carry out penetration tests and check the security standard of Axis products.

Vulnerability reports reach us via various different channels: either directly via an online form in the context of penetration tests, or via our Bug Bounty program in conjunction with the team from Bugcrowd. We currently pay up to US$ 50k for reports on critical security vulnerabilities – a clear sign of our engagement and our appreciation of the community.

How long does it take on average between the first report and Patch Day?

Andre Bastert: In general we are able to make corresponding patches available within six to twelve weeks, depending on the complexity of the vulnerability and the number of affected products – always under the premise that we can closely coordinate the publication of the vulnerability with the reporter so that our customers have enough time to apply the patch. With regard to so-called 'Zero Day vulnerabilities', of which we have luckily had none so far, we obviously have to react more quickly because these are weaknesses that can be actively exploited. It is normal at Axis that a single patch is rolled out for between 200 and 300 network products and multiple software tracks. It requires precise coordination to ensure that this is rapidly possible.

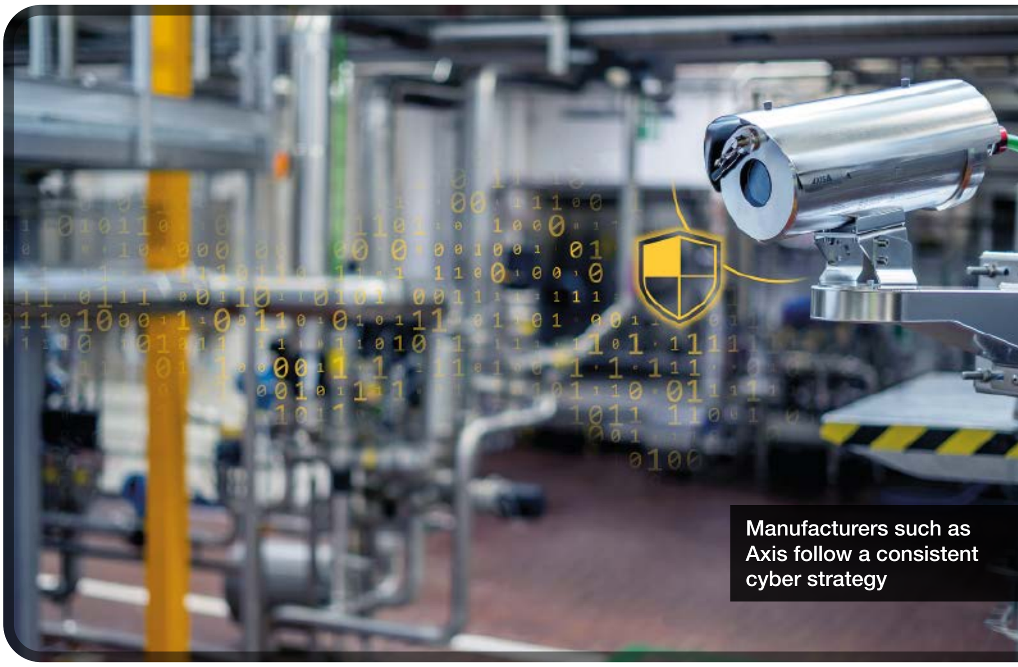
How do you communicate this to your customers?

Andre Bastert: We recommend that our customers regularly and proactively check their Axis network products to keep them up-to-date. That is the most effective protection against security vulnerabilities. We publish information promptly via our Release Schedule about the version in which a vulnerability has been removed. However, we never publish details that could threaten the 'Responsible Disclosure' process. We also offer a Security Notification Service. After registering, customers will automatically receive an email as soon as new vulnerability patches become available. This provides enough time to plan updates and minimize risks. If our customers or partners have any need for further information, our sales and technical support are available free of charge 24/7.

How do you advise and support end-users in general? Do you make a comprehensive resource pack available?

Andre Bastert: Our customers are able to find out about the cyber security of our products before purchasing them, whether via the Axis website, from our partners, or in direct dialog via email or by phone to our sales department. We make current information on international standards, certifications, and penetration tests available on our Axis Trust Center.

We provide a Hardening Guide with firm recommendations for the secure configuration and operation of our products. If a device has to be forensically investigated, for example after a cyber attack, the Forensic Guide will help. We also have integration instructions available, for example, for cooperation with well-known network suppliers such as HPE Aruba Networking. We always aim to help our customers proactively to integrate their Axis products securely and smoothly into existing IT environments.



Manufacturers such as Axis follow a consistent cyber strategy

This video shows how Axis operates its vulnerability management to protect its Axis OS firmware

Axis Communications
www.axis.com

© Images: Axis Communications

BUILDING INTELLIGENCE

Fire Tech Meets Architecture

Comelit-PAC Brings Smart Fire Protection to Liverpool Waters' Iconic Aquitania

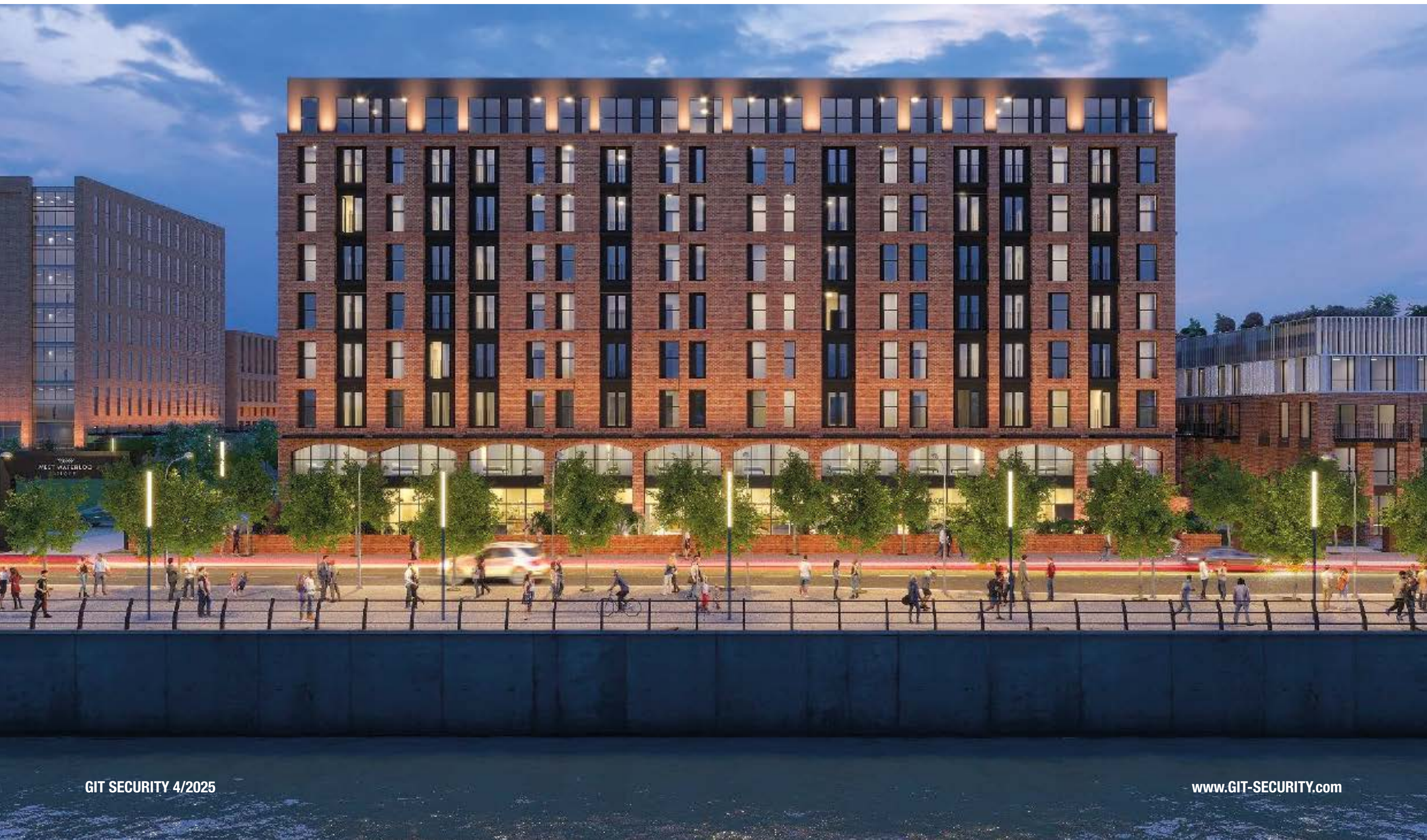
As part of the ambitious Liverpool Waters regeneration programme, Comelit-PAC in collaboration with Merselec Ltd and Romal Capital, has delivered an advanced, fully integrated fire safety solution for the Aquitania development at West Waterloo Place.

Liverpool Waters is one of Europe's largest regeneration projects, transforming the city's historic docks into a vibrant mixed-use waterfront. Romal's phase 4 Aquitania, marks a key phase in Liverpool Waters transformation, combining striking architecture with robust life safety systems for its 135 high-specification apartments and townhouses.

Says CEO of Romal Capital, Greg Malouf for Aquitania: "Resident safety was our highest priority. From the initial design stage, we worked with Comelit-PAC to ensure the fire system would meet legislation alongside the expectations of a smart, stylish development. The installed solution provides the protection we need and the flexibility to manage operations efficiently. We're already planning to extend the works into our phase four, Mauretania."Working in partnership with specialist contractor Merselec Ltd, the bespoke system spans all escape and circulation areas and uses programmed cause-and-effect logic to coordinate fire detection, smoke extraction, and lift management. This ensures the building responds as a single, intelligent network in the event of an emergency.

A standout feature is the integration with automatic opening vents (AOVs). These activate immediately during smoke control events, whilst maintaining a lockout feature for managing airflow and directing smoke away from escape routes to aid safe evacuation. The system also connects directly with lift controls to ensure safe operation and avoid use during an incident.

Jon Wilcock of Merselec Ltd added: "The integration requirements and performance standards made this a technically demanding project. Our close collaboration with Comelit-PAC allowed us to deliver a robust system that performs reliably in a live residential environment and could be installed to blend with its luxury surroundings."



To support day-to-day management, Comelit-PAC incorporated cloud-based remote monitoring. This gives building managers real-time status updates and instant alerts, enabling swift incident response and preventative maintenance.

Mandy Bowden, Fire Manager at Comelit-PAC, added: "Aquitania's complexity required a carefully coordinated approach that blended technical performance with the building and apartments aesthetic design principles. Our partnership with Merselec Ltd delivered a tailored solution with remote monitoring capabilities, ensuring both resident safety and ease of management. We look forward to continuing our work together on phase three."

Comelit-PAC is working with Merselec on the specification phase for Romal's next LW's waterfront development, the Mauretania. This will deliver 129 new-build apartments in Liverpool Waters' emerging Central Docks neighbourhood, as part of the city's West Waterloo Place development. GIT

To support day-to-day management, Comelit-PAC incorporated cloud-based remote monitoring. This gives building managers real-time status update

© Images: Comelit PAC

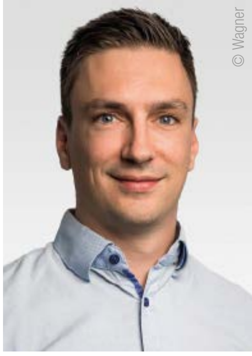
Comelit-PAC
www.comelit-pac.co.uk

Wagner at Buildinx 2025

Wagner Group GmbH will be presented new solutions for fire protection in modern logistics properties at Buildinx in Dortmund from November 18 to 20, 2025. The focus of the trade fair presentation at booth 5.B80 in hall 5 was on digitalization and carbon-neutral fire prevention – two key areas for more safety, efficiency, and sustainability in the real estate industry. In addition, Wagner demonstrated how risks in sensitive technical areas can be reduced effectively and how these areas can be protected against malfunctions with an aspirating smoke detection system that was specially developed for server and control cabinets. The Titanus Rack Sens aspirating smoke detector is ideal for use in the IT infrastructure of automated distribution centers. The compact system detects even the smallest smoke particles at an early stage and enables rapid intervention before business interruptions or property damage occur. In addition to early detection, the system can be combined with targeted extinguishing; the extinguishing agent can be placed directly in the cabinet or outside. This ensures maximum operational readiness and reliable protection for critical digital processes. With its Fire Protection 4.0 approach, Wagner uses AI-supported condition monitoring as an example to show how innovative digital technologies increase the safety of systems while reducing operating costs. Carbon-neutral fire prevention is made possible by innovative fuel cell technology, which operates emission-free and also meets the highest safety standards through oxygen reduction. This provides an innovative, economical, and sustainable fire protection solution with the added value of simultaneous emission-free and self-sufficient energy production. **www.wagnergroup.com**

© Wagner

Jens Büchler



© Wagner

Tobias Frank

The transport base enables rescue teams to bring the cabinet out into the open in the event of a fire

LITHIUM-ION BATTERIES

Limited Overheating

Secure Storage of Lithium-Ion Batteries in VDMA-Certified Safety Cabinets

How can lithium batteries be stored and charged safely? An answer to this question will be provided by Asecos at the A+A trade fair in Dusseldorf (4 – 7 November 2025). The dangerous substance storage and handling experts will also be bringing along their Ion Line safety cabinets, the Pro and Ultra models of which are now also VDMA certified. Here is an article by Dipl.-Ing. Sven Sievers, Head of Product Management and Development at Asecos.

Lithium-ion batteries are considered fundamentally safe, but they can represent a fire risk when they have a technical fault or are handled incorrectly. The continual increase in the use of this type of accumulator brings with it an increase in the safety requirements. To keep the potential risk as low as possible, these modern energy packs should be stored and charged in specially-developed safety cabinets, such as those of the Asecos Ion Line. But why can lithium batteries be dangerous? And how can we handle them more carefully?

Thermal Runaway – an Invisible Danger

A fault within a lithium cell – perhaps caused by being dropped – can often remain undiscovered, and the battery will continue to be used. Damaged cells can however become unstable and they start to give off their energy unchecked in the form of heat. It is particularly dangerous when charging if additional heat is generated. Once a certain temperature is reached, dependent upon the chemical constitution of the cell, a so-called 'thermal runaway' can take place: the cell overheats, the melting point of the lithium is exceeded, and there is an internal short-circuit with a resultant chain reaction that affects further cells – and a short but rapid development of the fire.

Type 90 safety cabinets are a good choice to store and charge lithium batteries because they are an equal alternative to fire-resistant separate areas (F90). As the danger is actually from the stored batteries, the cabinets must also offer fire protection from within as well as from outside. This double fire resistance ability for 90 minutes is considered the minimum standard that should be demonstrated by manufacturers. It is achieved by the Ion Line through two established fire resistance tests: one from outside to the inside according to DIN EN 14470-1, and one from inside to the outside, following DIN EN 1363-1. The Ion Line Pro and Ultra models are also VDMA certified.

VDMA 24994:2024-08 – a New Test Procedure

Only since August 2024 has the VDMA Recommendation 24994:2024-08 defined unified test requirements for fire-resistant safety cabinets for the storage and charging of lithium batteries. At the core is a so-called 'real fire test', during which conventional lithium-ion batteries are bound together and brought to a controlled ther-

Lithium batteries can be safely stored and charged in the Asecos Ion-Line safety cabinets

mal runaway inside the cabinet. This develops into a chain reaction where the cells release gas, ignite, and partially explode – at short-term temperatures of over 700 °C. The entire cabinet must completely withstand this worst-case-scenario – without flames or debris being emitted from the cabinet.

If this test is passed, there follows an audit of the manufacturing site. Only then will the cabinet be certified. This all ensures the conformity of the test and the product with VDMA 24994:2024-08. Certified battery cabinets then bear the certification label, just like the Asecos Ion Line Pro and Ultra models.

The Ultra, which is also GS certified, offers the highest level of safety within the Ion Line, and was the first safety cabinet of its type awarded by the independent ECB certification service with protection class I/O90 – the highest standard according to VDMA 24994:2024-08.

The Equipment Makes the Difference

To provide the necessary safety in practice, battery safety cabinets should be fitted with fire detectors and alarm forwarding. The Ion Line models also have a transport base and quick-release sockets for the event of a rapid evacuation. Rescue services can then decide for themselves whether to extinguish the cabinet where it stands, or to move it outside. The integrated charging equipment is switched off automatically in the event of a fire to prevent further heating. The Ion Line models are also equipped with isolated shelves; they prevent the fire from spreading between the storage levels, so-called 'propagation'. Efficient charging heat dispersal and rapid smoke detection are ensured.

The Pro and Ultra models also have a three-point door closing mechanism. This provides additional resistance during a fire and helps to prevent fumes from escaping.

Experience Them Live

Which solution will provide you with the best everyday safety can be discussed with the manufacturer at the A+A in Dusseldorf: the dangerous material storage and handling experts will not only exhibit their latest models at the event, but also spread their knowledge and experience. Their exhibition attendance will be accompanied by the 'Forum by asecos academy' – with short presentations and a lot of knowhow. Further information and a free ticket to the exhibition can be obtained on the company's website.

Asecos GmbH
www.asecos.com

© Images: Asecos

Holger Schmitz, Sales Manager Industry at Eizo

VIDEO SURVEILLANCE

In View

Monitors for Video Surveillance in Manufacturing Environments

Video surveillance in manufacturing areas is often very important because it ensures that areas that are otherwise difficult to see remain in view, but only if the image quality of the monitors is good enough. The monitor developer and manufacturer Eizo has gathered many years of experience, on the production lines and control areas of surface treatment and steel production plants. GIT SECURITY spoke about this with Holger Schmitz, Sales Manager Industry at Eizo.

GIT SECURITY International: Mr. Schmitz, the larger a manufacturing facility is, the harder it is to maintain an overview. You have accumulated experience in a lot of industries.

Holger Schmitz: Yes, that is right. Many well-known companies operate manufacturing plants that have very large production areas, for example in surface treatment, in type manufacture, in welding cabins, in steel production, the metal and plastic processing industries as well as in the chemicals industry.

Good monitors contribute greatly to safety. Could you tell us about this using some examples? Perhaps we should start with the control center?

Holger Schmitz: You can imagine it like this: the machine operators are given a lot of information by their production machines. This information is presented in the control room on monitors of various sizes. The aim here is to always have the most important data in view. Our new 43“ FlexScan EV4340X is an interesting size to replace multiple smaller monitors. It is very suitable for use in control rooms and can display four times as much information as a Full HD monitor (1920 x 1080 pixels) thanks to its 4K resolution (3840 x 2160 pixels).

… and on the factory floor itself …?

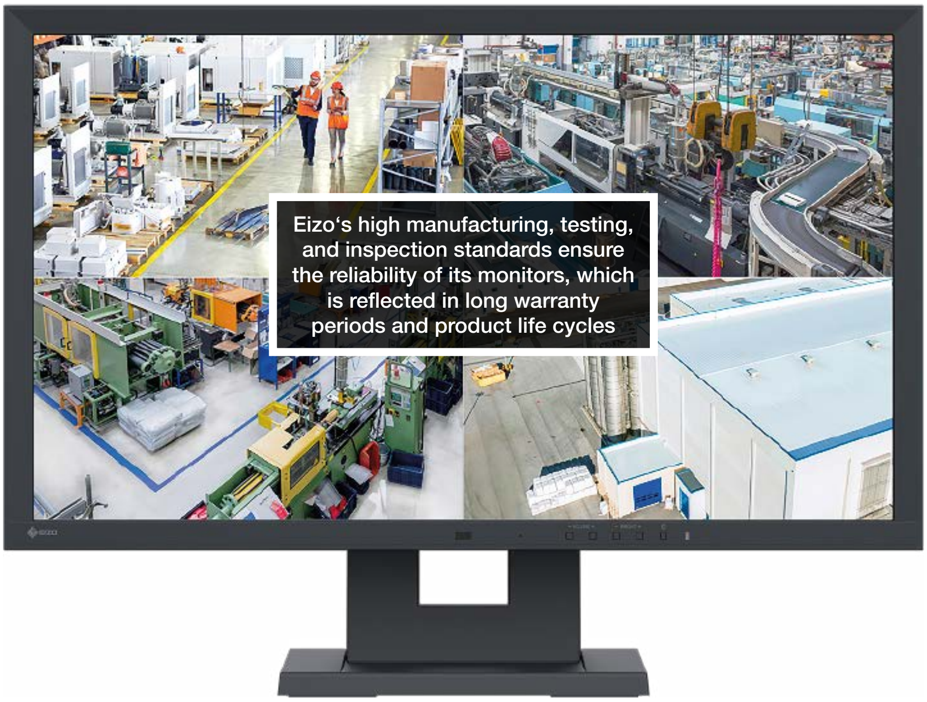
Holger Schmitz: Our IP decoder monitors, that are available in 23 and 27 inch models, are ideal for video surveillance on the production line itself. They enable direct connection to security and surveillance cameras without a computer. They can easily by integrated in an existing security system or a video management system (VMS).

What do monitors in general have to be able to do in a manufacturing environment?

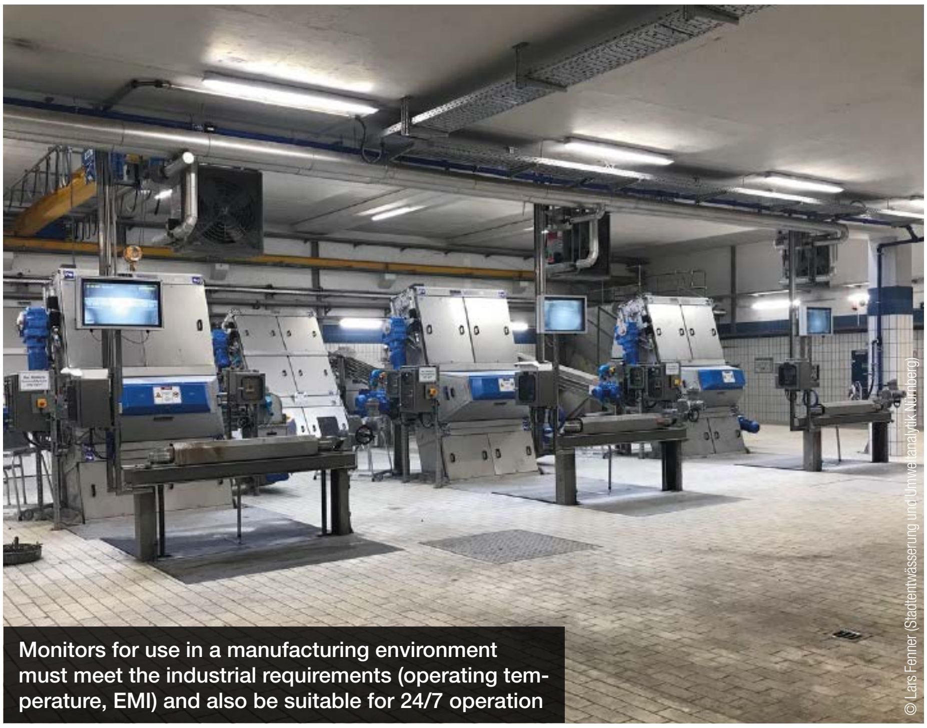
Holger Schmitz: Monitors that are used in production must meet the industrial requirements, such as the operating temperature and EMI standards, and also be built for 24/7 operation. They must also be reliable and have a long service life. High manufacturing, testing, and inspection standards at Eizo ensure the reliability of the monitors, reflected by the long guarantee period and useful life.

Which Eizo monitors are suitable here? And what are their particular features and benefits?

Holger Schmitz: Our FlexScan monitor series are available in a wide range of diagonal sizes from 21 to 43 inches, making them particularly suitable for control rooms. They are also equipped with all the com-



Eizo‘s high manufacturing, testing, and inspection standards ensure the reliability of its monitors, which is reflected in long warranty periods and product life cycles



Monitors for use in a manufacturing environment must meet the industrial requirements (operating temperature, EMI) and also be suitable for 24/7 operation

© Lars Fenner (Stadtentwässerung und Umweltanalytik Nürnberg)

mon interfaces, such as VGA, DVI, HDMI, or DP. The DuraVision series are a range of monitors that are designed for continuous operation and, depending on the model, come with or without touch operation.

What particular advantages are there when using the Eizo IP decoder monitors?

Holger Schmitz: Let us go back to the machine operator. There is often no direct eye contact to parts of the production system when there is a fault. With the help of a video surveillance system, these areas can be seen on our 23“ and 27“ IP decoder monitors so that an evaluation of the fault can be made and appropriate action taken. A commercial (or conventional) monitor that is connected to a PC is frequently not wanted for operational reasons. The IP decoder monitors from Eizo can be easily mounted on the wall or ceiling thanks to their VESA fitting. Only one supply cable is necessary for the built-in power supply. Neither a computer nor other hardware is necessary for operation, which simplifies installation and also saves time and effort.

Your monitors can also be integrated into most video management software – whereby this is not often found in manufacturing environments ...

Holger Schmitz: Eizo works together with leading providers of security and surveillance solutions to ensure technical compatibility and the best possible functionality with various video management systems (VMS). Our IP decoder solutions are already integrated, among others, with the VMS providers Accellence, Genetec, Milestone, and Hexagon (formerly Qognify). When used in production environments, the topology is usually a point-to-point connection between the camera and an IP decoder. And our IP decoder monitors and our versatile IP decoder box are ideally suited to this application because no recording is taking place in the background.

Every project is different – that also applies in particular to industrial production sites and similar situations. How do you work together with your customers from the initial planning through to commissioning?

Holger Schmitz: We support our partners right from the start of the project. Direct contact to the end user is very important here to ensure that the best possible solution is provided to meet their expectations. Apart from technical support, we also offer evaluation on site with suitable demonstration units. A further advantage is that the customer has one point of contact during the whole project that can also help with installation and operation when required. Our long-service employees and a low employee turnover ensure that this still applies for projects lasting many years. GIT

Eizo Europe GmbH
www.eizo.eu/industry

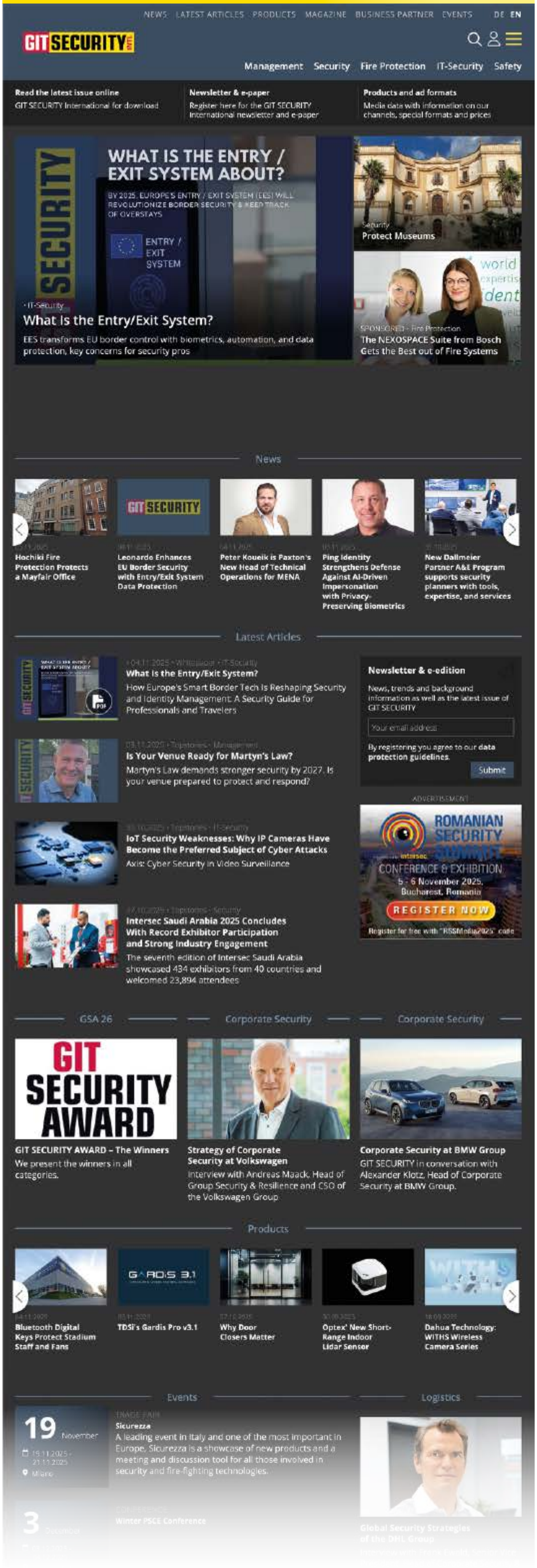
© Images: Eizo Europe

Gunnebo Entrance Control Enhances Passenger Experience at Queenstown Airport

Gunnebo Entrance Control has partnered with Queenstown Airport (ZQN) and Custom Technology Systems Ltd to elevate the domestic departure experience, providing greater convenience and security for passengers. Queenstown Airport, a key gateway to New Zealand's South Island and the country's fourth-busiest airport, has evolved continuously since opening in 1935. Now serving more than 2.6 million passengers each year, it connects major domestic destinations and east coast Australia, driving ongoing improvements to passenger facilities and operational efficiency. As part of a dedicated programme to enhance the domestic departures journey, ZQN reworked existing café space. A glass wall was installed to relocate the café airside, integrating it with the gate lounge. This provided direct food and beverage access for passengers and created additional seating, all within the same footprint. To support the new layout, Custom Technology Systems Ltd and Gunnebo Entrance Control worked closely with the on-site teams to deliver a tailored entrance control solution that balanced security and passenger flow whilst accommodating spatial limitations.

www.gunneboentrancecontrol.com

This month at GIT-SECURITY.com



NEWS LATEST ARTICLES PRODUCTS MAGAZINE BUSINESS PARTNER EVENTS DE EN

Management Security Fire Protection IT-Security Safety

Read the latest issue online
GIT SECURITY International for download

Newsletter & e-paper
Register here for the GIT SECURITY International newsletter and e-paper

Products and ad formats
Media data with information on our channels, special formats and prices

• IT-Security
What Is the Entry/Exit System?
EES transforms EU border control with biometrics, automation, and data protection, key concerns for security pros

Security
Protect Museums

SPONSORED • Fire Protection
The NEXOSPACE Suite from Bosch Gets the Best out of Fire Systems

News

Hochiki Fire Protection Protects a Mayfair Office

Leonardo Enhances EU Border Security with Entry/Exit System Data Protection

Peter Koueik is Paxton's New Head of Technical Operations for MENA

Ping Identity Strengthens Defense Against AI-Driven Impersonation with Privacy-Preserving Biometrics

New Dallmeier Partner A&E Program supports security planners with tools, expertise, and services

Latest Articles

• 04.11.2025 • Whitepaper • IT-Security
What Is the Entry/Exit System?
How Europe's Smart Border Tech Is Reshaping Security and Identity Management: A Security Guide for Professionals and Travelers

03.11.2025 • Topstories • Management
Is Your Venue Ready for Martyn's Law?
Martyn's Law demands stronger security by 2027. Is your venue prepared to protect and respond?

IoT Security Weaknesses: Why IP Cameras Have Become the Preferred Subject of Cyber Attacks
Axis: Cyber Security in Video Surveillance

Intersec Saudi Arabia 2025 Concludes With Record Exhibitor Participation and Strong Industry Engagement
The seventh edition of Intersec Saudi Arabia showcased 434 exhibitors from 40 countries and welcomed 23,894 attendees

Newsletter & e-edition
News, trends and background information as well as the latest issue of GIT SECURITY
Your email address
By registering you agree to our **data protection guidelines.**
Submit

ADVERTISEMENT
ROMANIAN SECURITY SUMMIT
CONFERENCE & EXHIBITION
5 - 6 November 2025, Bucharest, Romania
REGISTER NOW
Register for free with "RSSMedia2025" code

GSA 26 — Corporate Security — Corporate Security

GIT SECURITY AWARD – The Winners
We present the winners in all categories.

Strategy of Corporate Security at Volkswagen
Interview with Andreas Maack, Head of Group Security & Resilience and CSO of the Volkswagen Group

Corporate Security at BMW Group
GIT SECURITY in conversation with Alexander Klotz, Head of Corporate Security at BMW Group.

Products

Bluetooth Digital Keys Protect Stadium Staff and Fans

TDSi's Gardis Pro v3.1

Why Door Closers Matter

Optex' New Short-Range Indoor Lidar Sensor

Dahua Technology: WITHS Wireless Camera Series

Events — Logistics

19 November
19.11.2025 - 21.11.2025
Milano
TRADE FAIR
Sicurezza
A leading event in Italy and one of the most important in Europe. Sicurezza is a showcase of new products and a meeting and discussion tool for all those involved in security and fire-fighting technologies.

3 December
CONFERENCE
Winter PSCE Conference

Global Security Strategies of the DHL Group

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 2025
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.

The publishing house is granted the exclusive right, with regard to space, time and content to use the works/editorial contributions in unchanged or edited form for any and all purposes any number of times itself, or to transfer the rights for the use of other organizations in which it holds partnership interests, as well as to third parties. This right of use relates to print as well as electronic media, including the Internet, as well as databases/data carriers of any kind.

All names, symbols etc. mentioned and/or printed in this issue may be registered trademarks of their respective owners.

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

SECURITY MANAGEMENT

Facility Security

SimonsVoss technologies

SimonsVoss Technologies GmbH
Feringastr. 4 · D-85774 Unterföhring
Tel. +49(0)89/99228-180 · Fax +49(0)89/99228-222
marketing-simonsvoss@allegion.com
www.simons-voss.de

Digital locking and access control, intelligent locking components with the latest software. System 3060 plants fulfill highly complex requirements in large buildings. They are simply and quickly expandable and work consistently wireless.

TIME ACCESS

Security Management

Ksenia security innovation

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

VIDEO TECHNOLOGY

Time + Access

AceProx Identifikationssysteme GmbH

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

Security Management

NSC Sicherheitstechnik GmbH

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

Video Technology

Dallmeier

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

Time + Access

ASSA ABLOY Entrance Systems

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

FACILITY SECURITY

Video Technology

EIZO

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.

Time + Access

DoorBird Technology meets Design.

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

Facility Security

DICTATOR

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

Video Technology

i-PRO

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

Time + Access

cichon + stolberg cryptin

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

Facility Security

frogblue SMART BUILDING TECHNOLOGY GERMANY

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

www.luna-hd.de

lunaHD High Definition Video

Video surveillance • Video door intercom

Time + Access

DNAKE

DNAKE (Xiamen) Intelligent Technology Co., Ltd.
No.8, Haijing North 2nd Rd., Xiamen, Fujian, China
Tel.: +86 592-5705812
sales01@dnake.com · www.dnake-global.com
Intercom System, IP Video Intercom, 2-Wire IP Intercom, Cloud Intercom Service, Access Control

Time + Access

FEIG

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

primion
AZKOYEN Time & Security Division

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

FIRE PROTECTION

Time + Access

gantner
INSPIRED ACCESS

GANTNER Electronic GmbH
Bundesstraße 12 · 6714 Nüziders · Austria
Tel. +43 5552 33944
info@gantner.com · www.gantner.com
access control solutions/biometrics, time management, data capture, locking systems

Be Part of the Section

GIT BusinessPartner
The Purchasing Section for direct contact

Just send a mail to
miryam.reubold@wiley.com

We will be glad to advise you!

PLANT SAFETY

Time + Access

phg
Die richtige Verbindung

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

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

PEPPERL+FUCHS

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

THE NEXT GENERATION OF SMART BUILDING AUTOMATION

Future-proof. Innovative. Energy-efficient.

MADE IN GERMANY

WIRELESS.
LIMITLESS.
MAXIMUM SECURITY.

For projects of any size!

frogblue™
SMART BUILDING TECHNOLOGY GERMANY

Luxemburger Straße 6
D - 67657 Kaiserslautern
frogblue.de
info@frogblue.com
+49 631 520829-0