VOLUME 23 | SEPTEMBER 2026 | ISSUE 3 | 17 €

GIT SECURITY INTL

79 824

MAGAZINE FOR SAFETY AND SECURITY – WORLDWIDE

CSO INTERVIEW
Roche's Marco Skolik und Joerg Kastner: Well prepared for crises? p 8

FIRE PROTECTION
Aljona Ijoschina, Stephen Beadle, Oliver Doerle: Digital and Networked Test Procedures p 16

GIT PERIMETER TEST
We test Optex systems p 30



VIP:
Oliver Giesen p 58

Cover Story page 42

ASSA ABLOY:
Digital Access, Familiar Keys

A BEST-OF IN PRINT

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

WILEY



CLIQ®

The smart way to digitalize access

Take your access management into the digital era – smoothly, securely, and without overhauling existing infrastructure. With CLIQ, you upgrade from mechanical to digital access at your own pace to gain greater control today and adaptability for tomorrow.

Download our whitepaper to learn more about making the switch to digital access

ASSA ABLOY

Stronger Together, Safer Tomorrow



September brings a safety and security landscape that is becoming increasingly connected, intelligent, and, in many ways, more demanding. Across industries and borders, organizations are navigating a mix of technological innovation, regulatory pressures, geopolitical uncertainty, and rising expectations around resilience. In this issue of GIT SECURITY International, we take a closer look at how safety and security professionals are responding to these challenges with practical solutions, fresh ideas, and a clear focus on the future.

One of our highlights is the exclusive interview with Roche's crisis and emergency management leaders, who explain why preparation is not a one-off exercise but a continuous process of collaboration, training, and trust. Their message is refreshingly clear: resilience starts long before a crisis begins. We also preview Security Essen 2026, where the industry's key players will gather to discuss AI, critical infrastructure protection, and the growing convergence of physical and digital security.

In our Fire Protection section, we explore how digital and networked testing is transforming maintenance workflows, compliance, and transparency. From connected detector testing to cloud-based maintenance processes, fire safety is becoming smarter, faster, and with far less reliance on paperwork. And yes, finally, technology is doing some of the heavy lifting.

The Security section takes us from fiber-optic sensing for critical infrastructure protection to a hands-on perimeter test of cutting-edge Distributed Acoustic Sensing technology. We also speak with industry leaders from Advancis and Dallmeier about the future of integrated security management, AI, cloud platforms, and trusted European technology. Spoiler alert: the control room of tomorrow is already taking shape today.

In our Safety section, we meet the next generation of leadership at Elten, examine Adidas' entry into the industrial safety footwear market, and discover how disaster robotics are moving from research projects into real-world emergency response operations. It is a reminder that innovation is not just about protecting assets, but also about protecting people.

And our cover story with Assa Abloy looks at a topic many organizations are facing today: how to transition from mechanical to digital access management without losing simplicity, flexibility, or control. Sometimes the smartest solutions are those that combine the best of both worlds.

We hope you enjoy the issue, find plenty of inspiration, and perhaps discover a few ideas worth discussing with colleagues over coffee.

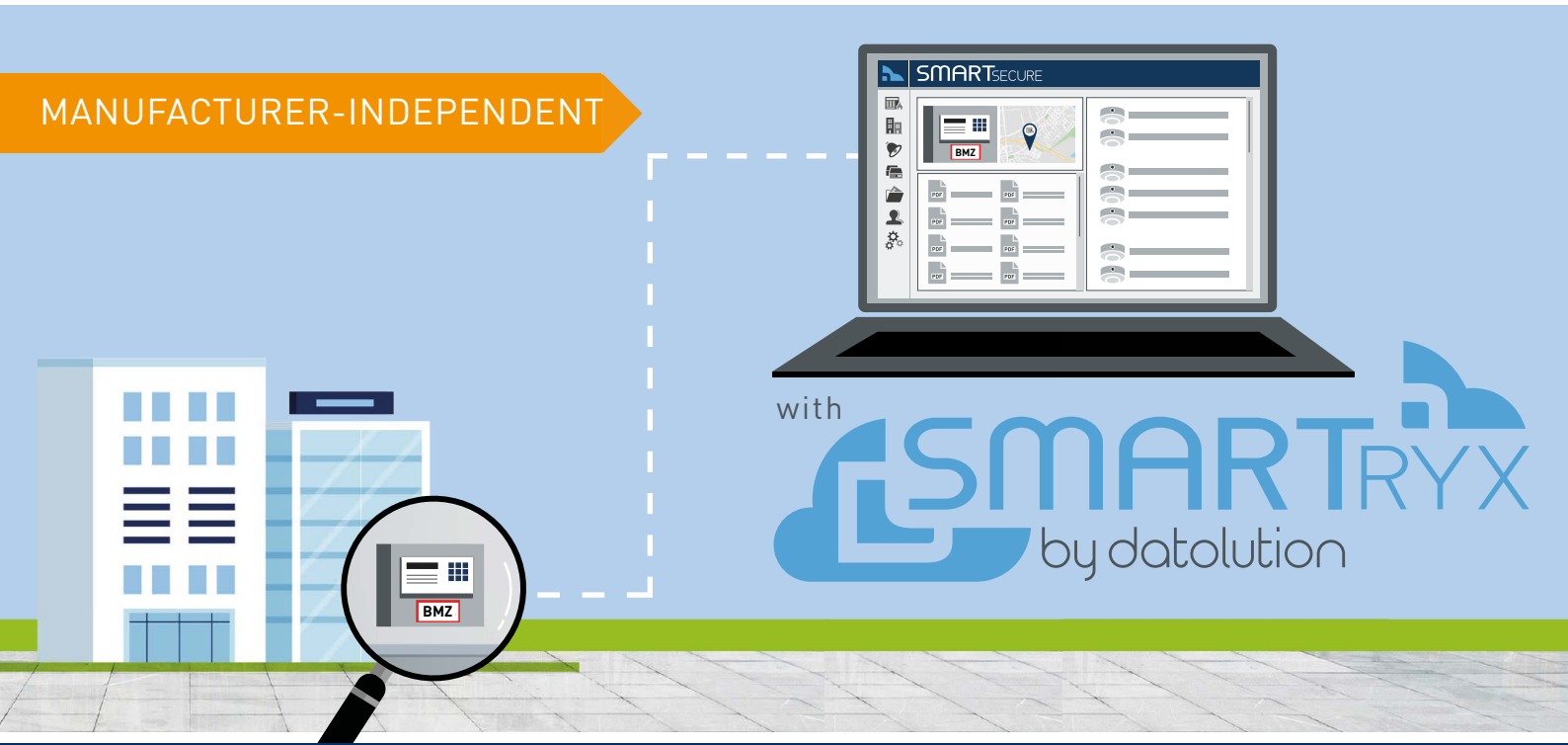


Best regards,
Your Steffen Ebert and the
GIT SECURITY International Team

WE DIGITISE
FIRE ALARM SYSTEMS

ISO 27001 CERTIFIED

MANUFACTURER-INDEPENDENT



with SMARTRYX by datolution

DATOLUTION GmbH | Weinstraße 45 | G - 91058 Erlangen | +49 9131 811730 | info@datolution.de | www.datolution.de



COVER STORY

ASSA ABLOY:

Digital Access, Familiar Keys

page 42



GIT-SICHERHEIT.DE/EN/PRODUCTS
PRODUCTS FOR PROFESSIONALS
Product and Lead Platform for Safety and Security



Marco Skolik



Riham Sedik



Aljona Ijoschina, Stephen Beadle, Oliver Doerle

3 Editorial
Steffen Ebert

MANAGEMENT

FOCUS GERMANY | CSO INTERVIEW
8 Bridging the Preparation Gap
The Pharmaceuticals and Diagnostics Company Roche is Well Prepared for Crises

FOCUS EUROPE | EVENT
12 Connected Security
The Security Industry Will Meet in Late September in Essen, Germany

FOCUS SAUDI-ARABIA | EVENT
14 Shaping Tomorrow's Environment
Intersec Saudi Arabia

FIRE PROTECTION

DIGITAL TESTING
16 More Intelligent, More Transparent, Faster
Digital and Networked Test Procedures in Fire Protection

WILD FIRES
20 Fire Information Consolidation
Modernizing the Emergency Response to Wildfires

SOLUTIONS
21 A Cool Compliance Companion
An Interview with Tobias Väthjunker, CEO of Kirotec, a Top Player in Fire Protection Solutions

23 When the Cost Exceeds the Fire
Correct specification is a question of business continuity

SECURITY

INNER COVER
25 Monitoring the Vastness
Distributed Fiber Optic Sensing to Protect Critical Infrastructure and Large Sites

FOCUS FRANCE | TEST SITES UNDER TEST
30 A Change of Perspective at the Perimeter
New Capabilities Put to the Test at Optex: Distributed Acoustic Sensing (DAS)

DISPLAYS
34 On Screen Partners
24/7 Secure Control Centers: Eizo Monitors in Continuous Use at Stadler Systec

PHYSICAL SECURITY MANAGEMENT
36 The Way of Integration
Software Solutions for Physical Security: An Interview with Dr. Jens Hartmann, VP Sales, Advancis

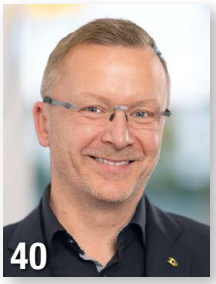
PHYSICAL SECURITY MANAGEMENT
38 From Video Data to Actionable Evidence
How Octave Coda Video 9.2 Streamlines Investigations and Security Workflows



Klaus Friebe



Clemens Pohl



Christian Linthaler



Hendrik van Elten

VIDEO SECURITY

40 Looking Ahead At Video Surveillance
An Interview with Top Player Video Security: Christian Linthaler, Dallmeier CSO

COVER STORY

42 A Versatile Combination
Digital Access with the Familiarity of a Key

FOCUS NETHERLANDS | ACCESS CONTROL

46 Solving a Puzzle at Muziekgebouw
How an Electronic Locking System Now Provides Security at a Concert Venue



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

SAFETY

SAFETY SHOES

48 "Stay Courageous Without Becoming Reckless"
Generation change at Elten: Hendrik van Elten on growth, the brand and new requirements for safety shoes

SAFETY SHOES

51 Sports DNA Meets Workplace Safety
Adidas enters the industrial safety footwear market with a new range designed for logistics, manufacturing and transportation professionals

HSE MANAGEMENT

52 From Transportation to Recycling
5 Ways HSE Managers Can Make More Sustainable PPE Decisions

ROBOTICS

54 European Disaster Robotics
DRZ Takes Products from Research to Real-World Deployment

56 BusinessPartner

58 VIP
Oliver Giesen, Head of the Bayer AG Plant Fire Department, Berlin location

INDEX

QUICK-FINDER

ORGANISATIONS, INSTITUTIONS AND COMPANIES IN THIS ISSUE

AceProx 57
Adidas 51
Advancis Software & Services 11, 12, 36
AP Sensing 25
Assa Abloy Front/Inside Front Cover, 12, 22, 33, 42, 57
Axis Communications 12, 14
Barox Kommunikation 24
BASF 50
Bayer 58
Bird Home Automation 57
BolognaFiere 13
Boon Edam 6
Cichon+Stolberg 57
Dallmeier electronic 12, 39, 40, 45, 56
Datolution 3, 16, 17, 18, 19
Deep Robotics 55
Detectortesters/No Climb 16, 33
Deutsches Rettungsrobotik-Zentrum 54
Dictator 56
Dom UK 46
Dormakaba 12
Dupont de Nemours 52
EcoVadis 53
Eizo Europe 34, 37, 56
Elten 48
Erfolgslabor 3
Ethos Media Group 13
European Union (EU) 8, 20, 27, 37, 42
Feig Electronic 57
Fiera Milano 13, Back Cover
Genetec 14, 39, 45
HB Protective Wear 53
Hexagon 38
HID Global 33, 39
Hirsch UK 39
Hochiki Europe 19, 23
International Security Ligue 7
Intersec Saudi Arabia 14
i-Pro Emea 24, 56
Kentix 22
Kirotec 21, 22
Ksenia Security 56
London Ambulance NHS Trust 42, 44
Luna HD 56
Madrid Police Department 54
March Networks 41
Messe Essen 12, 15
Messe Frankfurt Middle East 14
Milestone Systems 12, 31, 32
Mobotix 6, 22
Motorola Solutions 6
NASA 20
No Climb/Detectortesters 16, 33
NSC 56
Octave 20, 24, 38
Onvif 45
Optex Security 7, 24, 30
Pepperl+Fuchs SE 57
PHG Peter Hengstler 57
Primion Technology 45, 57
Priorit 21
Roche Diagnostics 8
Sachverständigenbüro Markus Piendl 30
Salto Systems 12
Schraner Group 18
Secardeo 24
Secsolutionforum 13
Securitas 7
St. Louis Lambert Intl. Airport (STL) 45
STid 57
TDSi by Hirsch 45
Vivotek Inc. 41
VuWall Technology Inc. 35
WatchGuard Technologies GmbH 6

NEWS

Denmark Extends and Upgrades Public Safety Communications with Motorola Solutions



Motorola Solutions is currently extending Denmark's national TETRA communications network, Sikkerhedsnettet (SINE), through 2034 with the latest Dimetra X Core software and includes Dimetra Connect. This extends the network reach with seamless roaming to the mobile phone network while maintaining secure radio features and encryption. While land mobile radio (LMR) networks, such as SINE, continue to be the gold-standard for mission-critical voice communications, if a user moves beyond SINE's LMR coverage, the system automatically switches to send and receive the radio's voice and data via the mobile phone network. As the first nation to deploy Dimetra Connect, Denmark is setting a new benchmark for public safety communications across Europe. This modernization provides 45,000 first responders with a seamless connection they can trust wherever the mission takes them, combining trusted radio reliability with broadband versatility.

www.motorola.com

WatchGuard Appoints MEA Regional Director



Rabih Itani

WatchGuard Technologies has appointed Rabih Itani as Regional Director for the Middle East and Africa (MEA). This comes at a time of significant growth across the region, with the Middle East cybersecurity market projected to more than double. Rabih will report to Frederic Saint-Joigny, Vice President EMEA, and will lead WatchGuard's go-to-market strategy across MEA, focusing on driving revenue growth, expanding the company's direct presence, and strengthening its channel ecosystem of distributors, MSPs, and resellers. He will also accelerate adoption of WatchGuard's Unified Security Platform across the region. Rabih is a veteran of the ICT and cybersecurity industry with a pioneering role in helping the MEA region embrace disruptive technologies. Having worked across the full ecosystem — as a customer, integrator, and technology provider — he brings a uniquely well-rounded perspective on the region's digital transformation and cyber resilience journeys.

www.watchguard.com

Mobotix Appoints New Chief Sales and Marketing Officer



Aleksandar Smiljanic

The Supervisory Board of Mobotix AG has appointed Aleksandar Smiljanic as the company's new Chief Sales and Marketing Officer (CSMO). Effective October 1, 2026, he will join the Executive Management Board alongside Giovanni Santamaria (CRO), Dr. Christian Cabirol (CTO) and Klaus Kiener (COO). His focus will be on further expanding the company's global core business in AI-powered video security while strategically entering new, high-margin growth markets. Aleksandar brings many years of international leadership experience in technically demanding B2B markets. He is already familiar with the company through previous joint projects involving security-critical applications, and has built a strong international network, particularly within the defense sector, military medicine and high-growth international markets.

www.mobotix.com

Boon Edam Joins Convergint's Global Elite Partner Program

Boon Edam, a global provider of physical security entrance products, has joined Convergint's Global Elite Partner Program, providing an opportunity for improved market penetration and new business development. "This partnership builds on nearly two decades of collaboration", said Frank Mackenzie, CCO at Boon Edam. "It reinforces our commitment to strategic relationships with organizations that share our values and dedication to delivering innovative solutions that protect people, property, and assets." This shared business philosophy is supported by Boon Edam's comprehensive portfolio of security entrances, including optical turnstiles, full-height mechanical turnstiles, security revolving doors, and security mantrap portals integrated with leading biometric and sensor technology.

www.boonedam.com



F-L: Greg Schreiber and Frank Mackenzie (Boon Edam), Chris McCurdy and Grace Li (Convergint) and Kurt Measom (Boon Edam)

SERVICE

Procurement Statistics Unveiled

An Independent Look at Procurement Practices and Their Effects

The International Security Ligue has released a major new edition of its GSB Pulse, presenting what is likely the largest sector-specific examination of public procurement ever conducted. Built on nearly 40,000 tender records, the report sheds unprecedented light on how public authorities purchase security services — and what that means for taxpayers, frontline security professionals, and public safety.

For years, stakeholders have speculated about the drivers of contract awards in the security sector. The Ligue's global data project aims to replace assumptions with facts, answering a simple but consequential question: if we looked deeply at tens of thousands of tenders, what story would the data tell?

The findings are clear. Across Europe, price remains overwhelmingly dominant in procurement decisions for guarding services, with an average weighting of 85 % since 2018. This places security procurement closer to refuse collection and cleaning services than to other professionalized service categories.

Deciding Criteria

"The results confirm something that many practitioners had long suspected: price remains structurally dominant in guarding contracts, even in procurement systems that formally encourage quality-based awards," said Stefan Huber, Executive Director of the International Security Ligue. "The reality on the ground is that price still hijacks the process."

The report pulls back the curtains on multiple aspects of public procurement for security services.

- Market data includes the frequency of framework agreements, tender-to-award time frames, supplier profiles, procedure type, contract value, and competition level.
- Data correlation analysis includes conditions that support a multi-criteria approach to contract awards.

> The reality on the ground is that price still hijacks the process.

- Price weighting analysis provides insight into the influence of price in award decisions, including historical trends and cross-sector comparisons.

Worrying Results

The consequences are far reaching: when public authorities rely primarily on lowest bids, they often receive inferior service, undermine transparency, and unintentionally incentivize a race to the bottom in wages, training, and working conditions. Procurement practices directly shape the lives of frontline security professionals.

This latest issue of GSB Pulse shares initial results from the International Security Ligue's global, long term research initiative to illuminate structural patterns in security procurement. It is available now, and readers are encouraged to share it widely to help advance a factual understanding of forces driving public procurement of security services. GIT

The report is free to download at

International Security Ligue
www.international-security-ligue.org

Leaders in sensing. # Trusted worldwide.



optex-europe.com
OPTEX Sensing Innovation



The emergency services successfully tackled several deliberately set fires and carried out rescues in order to coordinate procedures and points of contact in the event of an emergency

CSO INTERVIEW

Bridging the Preparation Gap

The Pharmaceuticals and Diagnostics Company Roche is Well Prepared for Crises

Roche Penzberg is a biotechnology site that coordinates closely with emergency services, holds regular drills, and has defined points of contact with external responders. GIT SECURITY International spoke with Marco Skolik, Corporate Security Head, and Jörg Kastner, Head of Crisis and Emergency Management.

GIT SECURITY: Mr. Skolik, Mr. Kastner, the German Bundestag recently passed the Kritis umbrella law. It has long been clear that it would be enacted because it involves the implementation of an EU directive. Does Roche already comply with all the requirements of the law?

Marco Skolik: Of course, Roche has been working intensively on implementing the underlying EU directive for quite some time, but the subject matter is very complex overall. On the one hand, it involves requirements for critical infrastructure; on the other hand, as a facility, we are also classified as a 'major accident facility'.

Jörg Kastner: At this point, it has not yet been definitively determined whether the Penzberg site actually falls under the new provisions of the Critical Infrastructure Framework Act. The relevant thresholds will be established at a later date via a statutory order. Should the law apply to us, we will of course comply with the relevant requirements. However, we expect that the main implications for us will primarily involve additional documentation and reporting requirements. We are already very well positioned in all other aspects. Crisis and emergency management are not just on paper at our company – they are actively put into practice. As a biotechnology company, it is in our very best interests to make our processes as resilient as possible so that we can reliably care for patients worldwide at all times – in keeping with our corporate purpose: "Doing now what patients need next."

The law is primarily aimed at operators of critical infrastructure as part of a reorganization of Germany's security architecture – but it also places greater responsibility on authorities and organizations with security tasks (BOS). In your view, what is the current state of collaboration between BOS and companies?

Marco Skolik: In my view, there is already good contact at many levels. At the same time, there is still potential to further strengthen the cooperation and improve processes. While there are many facilities that have built very close and trusting relationships with the relevant authorities and organizations over the years – including our site in Penzberg – this collaboration is by no means universal, even though it is absolutely critical for effective hazard prevention and crisis management.

I therefore hope very much that the authorities themselves will also shift their mindset and proactively reach out to critical infrastructure companies as well as facilities at risk of major incidents. In my view, a significantly greater focus on public-private partnerships would be beneficial here. After all, an effective emergency response is not only demonstrated during an actual emergency but also during the preparation for it. Even major crises can be better managed when authorities and companies work hand in hand. Existing resources must be used effectively. This also applies to our population when it comes to self-reliance.

Jörg Kastner: In my view, it is also important that critical infrastructure facilities be taken into account when preparing for incidents,

even if these do not fit a typical operational scenario. Companies bring their own potential, specific hazard situations, and unique conditions to the table, all of which must be incorporated into planning.

This applies in particular to overarching response plans for emergency scenarios, such as the response plan for life-threatening situations in Bavaria. While this plan outlines measures for all public emergency response units, it has so far failed to take into account – or only inadequately – the internal corporate structures such as company fire departments, rescue services, or company security facilities, as well as the specific conditions within the industrial sector. In our view, there is still work to be done here.



Jörg Kastner, Head of Crisis and Emergency Management



Marco Skolik, Head of Corporate Security at Roche

Let us break this down a bit using the Roche sites for which you are responsible. Firstly, to put things into context: Roche in Penzberg is practically a city in its own right – and at the same time a significant part of Penzberg?

Marco Skolik: Roche in Penzberg is one of the largest biotechnology centers in Europe and an innovative center of excellence for life sciences in the greater Munich area. With 7,900 employees, the site is the largest employer in the Bavarian Oberland and one of the region's most important economic drivers. The facility, which spans 590,000 square meters, is a globally significant hub for the research, development, and production of bio-pharmaceutical active ingredients, diagnostic tests and reagents, analytical systems, as well as molecular tumor profiling and gene therapy. From Penzberg, we are thus contributing to better healthcare for patients worldwide.

You're probably quite familiar with the police, fire department, emergency medical services there, both personally and in terms of their organizational structure, aren't you?

Marco Skolik: Yes, that is certainly true. We have a particularly good and regular exchange with the police, the surrounding fire departments, and the emergency medical services. Response scenarios are planned jointly in advance and also tested in practice. There are also processes in place for certain aspects of day-to-day operations that have already been coordinated. For example, these include close cooperation between our plant security and the police – such as when filing a police report, which in many cases can be done directly with plant security without having to visit the relevant police station in person. Cooperation between our plant fire department and the Penzberg Volunteer Fire Department during operations in and around the plant is also firmly established. Particularly noteworthy is the effective and trusting cooperation with the Penzberg Police Station and the Upper Bavaria South Police Headquarters. A partnership has developed here over the years that is by no means a given in this form.

Jörg Kastner: We also maintain a very good and regular exchange with the lower-level civil protection authority at the Weilheim-Schongau District Office. All issues that concern Roche are discussed here openly, constructively, and in a spirit of partnership.

You organize joint drills now, as is often done in large companies. Who actually takes the initiative in this?

Jörg Kastner: Fundamentally we see it as our responsibility to proactively coordinate the scenarios relevant to our site with the external emergency responders and to conduct regular drills. Our operations classify our company as a so-called 'major-accident facility'. This imposes a clear obligation on us to comply with the requirements of the Major Accidents Ordinance and to protect both the public and the environment from harm to the best of our ability at all times.

Marco Skolik: This applies equally to our employees and to our physical assets. We have a strong duty of care and set high standards for the safety of our colleagues. We are also required by the government of Upper Bavaria to conduct regular drills in collaboration with external emergency response teams. Against this backdrop, we made a conscious decision last year to hold a large-scale drill annually at our Penzberg



The interaction between in-house and external emergency services was practiced using patients played by actors

site. These drills are conducted alternately with internal personnel and in collaboration with external units. We see ourselves not only as participants in these drills but also as active partners in emergency response. Whether through our on-site fire department, the plant rescue service, or with support from company security – for example, using drone technology – we are always available to assist with public or external emergency operations. Accordingly, we are also open to requests from external organizations to conduct exercises on our plant premises.

What exactly do you define as the objective here?

Marco Skolik: The central objective is for the participating parties to get to know each other better and to seamlessly coordinate internal and external response procedures. The interfaces with the various authorities and organizations are highly complex in and of themselves. In the event of an emergency, however, these processes must mesh seamlessly – like a precisely calibrated clockwork mechanism. This is exactly where the joint exercises lay the necessary groundwork: they ensure clarity in roles, reliability in procedures, and trust in collaboration – even before things get serious.

Jörg Kastner: The objective goes well beyond the actual day of the exercise. Even the preparation for such a large-scale exercise provides significant added value for everyone involved. Within this framework, the various stakeholders engage in dialogue with one another at an early stage; existing emergency and response plans are reviewed together and assessed to ensure they are appropriately coordinated.

In the run-up to our last exercise, for example, we provided specific training for our internal teams – namely the plant fire department, plant emergency medical services, and the emergency and crisis management team – in collaboration with external partners to simulate police response scenarios. We deliberately opened these training sessions to public emergency response personnel as well. This significantly strengthened mutual understanding of each other's roles, procedures, and decision-making processes. The actual exercise then serves as a kind of 'reality check' for the jointly developed concepts. It clearly reveals where further coordination is needed and what is already working well. The insights gained are subsequently evaluated systematically and consistently incorporated into the further development of our plans. The goal is to continuously improve cooperation in the event of an emergency and to be even more resilient overall.



Roche's plant security team took on key coordination tasks as part of a large-scale exercise held in Penzberg in Fall 2025

Who are the participants, and what is the general flow of the exercise?

Marco Skolik: As a general rule, we always involve the surrounding fire departments, emergency medical services, and the police in all our large-scale exercises with external forces. Depending on the specific scenario, however, we set different priorities, which are accordingly reflected in the deployment of resources. In the last large-scale exercise, we concentrated on plant security and the police for the first time. The scenario was a police emergency situation – in a sense, the ultimate test among hazardous scenarios. It is exactly here that coordination between all the participating units is particularly complex. Non-police emergency responders may only begin operations after receiving authorization from the police and are subject to the command of a local incident command team from the lower-level civil protection authority. This particular organizational structure (BAO) presents numerous pitfalls, which is why realistic exercises in this context are absolutely critical to success.

This is another reason why we involved external institutions such as the Bavarian Center for Special Emergency Situations, InPASS (Institute for Patient Safety), and the Bavarian Association for Safety in Business, as well as external staff consultants in the preparation, observation, and debriefing afterwards.

The exercise scenario covered the entire chain of response: from the initial emergency call through police response with support from plant security – particularly through local knowledge, drone technology, and the guidance of those affected – all the way to the triage and care of 'injured' individuals by emergency medical services, as well as the suppression of several artificially created fires by the company's fire department. The exercise was designed to be correspondingly challenging and comprehensive.

Jörg Kastner: The foundation of a successful operation is often laid in the very first phase. That is why we tried to make the scenario as realistic as possible. It began with what was initially a more or less routine site security operation, although the very first situation report was already a critical point. The security operations center then informed internal personnel of the threat situation and simultaneously relayed the report to the police operations center and the integrated control center. After the police had resolved the situation, internal and external emergency responders worked together to treat and transport the simulated patients and extinguish the artificially created fires. An important aspect that we practiced in this format for the first time was the care of uninjured individuals by the support service and crisis intervention team. At the command level, it was not only important to coordinate the operational response teams but also to ensure cooperation between the command structure and our internal emergency and crisis management team.

Did drones play a role?

Marco Skolik: Yes, the use of a drone was absolutely critical to success in this scenario. It was already in the air and providing a live overview of the entire situation just six minutes after the operation began. This real-time information enabled the rapid containment of the danger zone and the targeted deployment of police forces. We were able to take decisions much more quickly and with greater confidence, which contributed significantly to the swift and successful resolution of the incident.

What did both sides take away from this exercise, and what conclusions do you draw for your own security strategy?

Marco Skolik: Above all, both sides took away one key lesson: safety comes from practice, trust, and clear points of coordination. The exercise showed where procedures are already working very well and where we still need to fine-tune them together. For our security strategy, this means that we will consistently continue on the path we have chosen. with regular exercises, close coordination, and a clear focus on practical preparation rather than purely formal concepts.

Jörg Kastner: In addition to some important insights into specific details, the topic of psychosocial emergency care was a key finding of the exercise. Several thousand people are on our company premises every day,

and they could be affected in various ways in the event of a major incident. Against this backdrop, we subsequently re-planned and further developed this aspect in collaboration with our internal resources and the district's Psychosocial Emergency Care Working Group.

The situation posed a challenge not only for the operational response teams but also for our emergency and crisis management team. Many colleagues were confronted with such a scenario for the first time. Due to the initially unclear situation, it was not possible for the team to convene immediately on-site. During this phase, however, we were able to rely on the existing structures and tools for virtual collaboration within the crisis management team. Specific questions also came to light during the process, such as how an open team workspace can be organizationally isolated in a sensible way in such a situation. These insights are now being directly incorporated into the further development of our security and crisis response plans.

But do you also have ideas about the requirements for collaboration with government agencies in special operational situations? In particular, do you emphasize not only the connection between security and safety, but also the interaction between internal and external forces as an integral part of defining the all-hazards plan?

Marco Skolik: Yes, those are our expectations. From our perspective, authorities must consistently consider security and safety aspects together and view internal corporate structures as an integral part of the all-hazards approach. In the event of an incident, companies fire departments, security, and emergency response teams are not peripheral players but an integral part of hazard mitigation. Early involvement, clear responsibilities, and active cooperation on an equal footing are crucial for this.

Jörg Kastner: From our perspective, it is important that corporate hazard prevention be recognized as an equal partner at all levels. Effective crisis and emergency management can only function if internal and external stakeholders collaborate early on and in a structured manner, especially in special operational situations.

A common understanding is necessary considering the challenges ahead: emergency and crisis management is not a 'job on the side, but must be conducted professionally, continuously, and with clear responsibilities. The all-hazards approach thrives precisely on this interplay between security and safety, as well as on the close integration of corporate structures with government response and command organizations.

Mr. Skolik, Mr. Kastner, we touched on this at the outset: these normative realignments are not taking place in a vacuum, but against the backdrop of geopolitical changes. Just geographically alone, Germany in particular is a logistical hub for military movements, maybe for refugees as well. The 'Operations Plan Germany' is viewed not only as a military and governmental task but also as a responsibility for society as a whole. Could you outline how your company is involved in this?

Marco Skolik: We are not yet actively involved. At the same time, as a company, we have a strong vested interest in being prepared for every conceivable scenario – especially in the light of current geopolitical developments. So we are continuously analyzing the situation and reviewing and refining our internal processes. We are currently developing our overarching strategy to actively engage with stakeholders such as the Bundeswehr in the future. The goal is to systematically advance integration with the 'Operations Plan Germany' and to create a functional, resilient interface between corporate preparedness and societal resilience.

Jörg Kastner: As Marco already mentioned, the information available to us on this matter is still rather limited at this point. Nevertheless, our core mission as a healthcare company is clearly defined: we supply patients worldwide with life-saving medication and diagnostics equipment. It is in our best interests to be able to fulfill this mission even under difficult conditions. As a company, we are already making a significant contribution to the resilience of our society in this way. Our system of emergency, crisis, and business continuity management is specifically designed to ensure that we remain capable of operating even in such scenarios, and able to restore stable operations as quickly as possible should disruptions occur. GIT

Roche Diagnostics GmbH
www.roche.de

© Images: Roche

Organize your Security.

With our Software Solutions **WinGuard** and **AIM**.

Get more info about our Solutions.

advancis.net

advancis



Training, banks, drones, and critical infrastructure are just some of the topics of numerous conferences, congresses, and forums at Security Essen 2026

EVENT

Connected Security

The Security Industry Will Meet in Late September in Essen, Germany

Artificial intelligence is driving rapid innovation, and the protection of critical infrastructure is becoming increasingly important in the face of growing cyber threats and geopolitical developments. At the same time, there is a growing need for companies, public authorities and operators to adopt a holistic approach to physical and digital security. Security Essen, taking place from 22 to 25 September 2026 at Messe Essen, will demonstrate how this development is reshaping the sector and which solutions will shape the market in the future.

The event will bring together around 500 exhibitors from 40 countries and offers trade visitors a comprehensive overview of the latest technology, innovations and trends, and the full spectrum of modern security solutions. The range on offer extends from access control, mechatronics and mechanical security systems, through fire and burglary protection, perimeter security and video surveillance, to services, special protection vehicles and solutions for civil protection and civil defense.

One trend is particularly evident: the boundaries between the individual areas are becoming increasingly blurred. Modern risk management systems integrate video technology, access control and intruder detection technology on a single platform. Artificial intelligence helps security managers to identify risks more quickly and assess incidents more efficiently. Cloud-based applications enable the cross-site management of complex security infrastructures, whilst intelligent sensor technology and automation are setting new standards in prevention and response times.

Major Market Players

Companies such as Advancis and Milestone are showcasing solutions for modern security and risk management. Assa Abloy, dormakaba, Salto and Telenot are presenting innovations in access control and building security. In the field of intelligent video and perimeter security, exhibitors include Axis Communications, Dallmeier and Strops, among others. The line-up is complemented by numerous other market leaders, specialists, innovative companies and start-ups from all sectors of the security industry. Trade visitors will be able to take a close look at the technologies and solutions that will shape the security industry in the coming years.

Julia Jacob, Project Manager for Security Essen: "The security industry is becoming more closely integrated today than ever before. At Security Essen, we will demonstrate how artificial intelligence, digital connectivity and innovative technologies are coming together to form comprehensive security solutions – and we will bring together precisely those manufacturers, users, planners, and decision-makers who are actively shaping this development."



Some 500 exhibitors from around the globe will present their inventions, solutions, and concepts to an inquisitive public

Knowledge Transfer Included

The exchange of information between the various stakeholders in the security industry does not take place solely at the exhibition stands: with its extensive supporting program, Security Essen creates additional platforms for knowledge transfer, discussions, and networking opportunities between manufacturers, end-users, academia, associations, and public authorities.

The program kicks off on 22 September with the Training and Further Education Day, organized by the BDSW (Federal Association of the Security Industry) in collaboration with Messe Essen, and the Emergency Services Day, organized by Ebner Verlag. The DNS Digital Networking Security Conference will also begin on the first day of the trade fair, organized in partnership with Datakontext; on 22 and 23 September, it will address the latest developments in cybersecurity, digital resilience and networked security solutions.

The European Drone Congress, taking place on 23 and 24 September and organized by the BDSW, will shine a spotlight on technology that is becoming increasingly important both for civil security applications and for public authorities and organizations with security responsibilities. Another highlight of the program is Banks and Savings Banks Day on 24 September, which will examine current challenges and solutions for the protection of financial institutions. This event is being organized by the European Security Systems Association (ESSA) e.V.



A significant exchange of information and many answered questions are assured during Security Essen 2026

Critical Discussions

On 25 September, the KRITIS Spotlight event at the Forum in Hall 7 will focus on the protection of critical infrastructure. The event will center on the implications of the KRITIS framework law and the requirements that KRITIS operators face now and in the future. Specialist presentations and discussions will provide practical insights and highlight potential solutions to implement the new requirements. The Security Experts Forum will also be hosting practical presentations and discussions throughout the exhibition, where exhibitors will present their innovations and provide insights into the latest developments, best practices, and new technology.

For the first time, Security Essen is taking place alongside EUDEX – the Euro Defence Expo. This new trade fair for the defense industry complements Security Essen with topics that are gaining in importance in the light of current developments in security policy. The protection of critical infrastructure, civil protection, crisis preparedness, and resilient security concepts can now only be envisaged through collaboration between the private sector, public authorities, and the armed forces. Holding both events in parallel creates new opportunities for professional exchange and cooperation between the civilian security sector and the defense industry.

This will particularly benefit trade visitors who are engaged in holistic security strategies and wish to focus on the interfaces between physical security, cyber security, civil protection, and defense. The combination of both trade fairs creates a unique platform for innovation, knowledge transfer, and networking. GIT

Security Essen takes place from 22 to 25 September 2026 at Messe Essen, Germany

Messe Essen
www.security-essen.de

© Images: Messe Essen

secsolutionforum 2026



The new secsolutionforum will debut on October 7–8 at BolognaFiere as part of Urban Tech 2026, the Urban Technology Show. The event will span 4,000 m² of exhibition space across nine simultaneously active conference rooms, including the Plenary Hall. The stage will feature over 100 top-tier speakers, guided by six expert moderators. The agenda covers over 100 events, from keynote speeches and talk shows to workshops, round tables, and training sessions, across 25+ themes that span the entire security universe: video surveillance, cybersecurity, access control, regulatory frameworks, and technologically complex topics such as artificial intelligence applied to the protection of people, infrastructure and data. Two prestigious awards will also be presented: the secsolutionforum Urban Security Award, recognizing the most virtuous public administrations for their work on integrated urban security, and a second award dedicated to outstanding corporate best practices. **www.secsolutionforum.it**

Sicurezza – This Year And Next

'MIBA Levante' is the MIBA spin-off, organized by Fiera Milano in collaboration with Pentastudio, scheduled to take place at Fiera del Levante in Bari on November 18–19, 2026. MIBA is the combination of four related exhibitions that address all aspects of smart buildings, including of course Sicurezza. It will provide a comprehensive and cross-sector representation of all the tools available to companies, designers, and technicians to carry out the energy and digital transition of the building heritage, with a constant focus on the specific needs of the Mediterranean regions. The choice of Apulia reflects the dynamics of the region: the construction sector in Southern Italy exceeds €90 billion. There are currently 150 exhibitors scheduled to take part, and some 40 workshops and conferences taking place over the two days.

www.smartbuildinglevante.it

EVENT

Shaping Tomorrow's Environment

Intersec Saudi Arabia



GIT SECURITY recently had the opportunity to interview Riham Sedik, the Exhibition Director for Intersec Saudi Arabia. She provides many interesting insights into the event here, at a time of political tension and shifting security priorities.

GIT SECURITY: Intersec Saudi Arabia is considered the leading platform for security, safety and fire protection in the Kingdom. What strategic objectives is this year's edition in November pursuing?

Riham Sedik: Our objective this year is to ensure that Intersec Saudi Arabia continues to serve as the Kingdom's leading platform for bringing together the people, technologies and ideas shaping the future of security, safety and fire protection. The exhibition is designed to bring together government authorities, project owners, developers, consultants, and global solution providers, thereby creating opportunities for collaboration, knowledge exchange, and business development across the sector.

This year's edition will also place a strong emphasis on connected approaches to security, cybersecurity, fire protection, and emergency response. Organizations are increasingly looking for solutions that improve operational resilience and business continuity rather than treating these disciplines independently.

Could you name a few of the highlights or curated thematic areas that visitors can look forward to this year?

Riham Sedik: Visitors can expect one of our largest editions to date, with more than 500 exhibitors from over 40 countries showcasing the latest solutions across security, safety and fire protection. Among the confirmed exhibitors are Bristol, NAFFCO, Axis Communications, Genetec, and Saudi Sicli, demonstrating the breadth of innovation being introduced to the Saudi market.

There will be two CPD-certified conferences; the Future Security Summit and the Fire Protection & Technology Summit, that will bring together more than 110 international experts, policymakers and industry leaders. Discussions will include topics ranging from AI-enabled security and cyber-physical convergence to crisis management, infrastructure resilience and next-generation fire protection. As part of the Fire Protection & Technology Summit, the National Fire Protection Association will lead a dedicated second day, titled Innovating Fire & Life Safety: Bridging Global Standards with Local Vision.

The exhibition itself will welcome more than 500 exhibitors from over 40 countries, showcasing solutions across commercial security, homeland security, cybersecurity, fire and rescue, and safety and health. Visitors will also benefit from curated networking opportunities, including the Premium Club, which connects international suppliers with pre-qualified buyers, project stakeholders, and senior decision-makers.

Which products and technologies will be particularly important this year? AI is likely to be among the most prominent topics? What else would you highlight from your perspective?

Riham Sedik: Artificial intelligence will certainly be one of the defining themes at this year's exhibition, particularly in areas such as intelligent surveillance, predictive threat detection, AI-enabled monitoring and command-and-control systems. However, it forms part of a much broader shift towards more integrated and connected security ecosystems.

We are also seeing growing interest in cyber-physical security convergence, advanced access control, perimeter protection, operational resilience and next-generation fire detection and suppression technologies. Increasingly, organizations are looking for solutions that can work seamlessly across physical security, cybersecurity and life safety to improve situational awareness and support faster decision-making.

The exhibition's conference program will explore how these technologies are moving from concept to practical implementation, while also examining the governance, skills and operational frameworks needed to support their long-term adoption.

Let's take a closer look at the Kingdom. A significant transformation is underway – the keyword being Vision 2030. How will this be reflected at Intersec, for example in terms of new security, safety and resilience requirements?

Riham Sedik: Vision 2030 is driving a new generation of infrastructure across Saudi Arabia, from giga-projects and smart cities to transport networks, logistics hubs, and major public destinations. These develop-

ments need to be safe, secure, resilient, and designed for the future.

Held under the patronage of His Royal Highness Prince Abdulaziz bin Saud bin Naif bin Abdulaziz Al Saud, Minister of Interior, and in association with the Ministry of Interior and Saudi Civil Defense, the exhibition serves as a trusted forum for collaboration, knowledge exchange and sourcing.

During this year's edition, we expect the strongest conversations to focus on integration, intelligence and resilience, with growing demand for AI-enabled surveillance, intelligent monitoring, access control, unified command-and-control platforms, and cyber-physical security strategies. Crisis preparedness and public safety are also becoming increasingly important as the Kingdom continues to expand its urban, transport and entertainment infrastructure.

From a fire protection perspective, there will be a strong emphasis on digital life safety systems, AI-enhanced early-warning technology, the protection of critical infrastructure, and emerging areas such as battery and electric-vehicle fire safety.

The Iran war has partly destabilized the region – and Saudi Arabia is geographically close to several conflict zones. The blockade of the Strait of Hormuz also affects the country in a particular way. What does this mean for you as the organizer of an important security trade fair?

Riham Sedik: The current regional environment reinforces the importance of resilience, preparedness and effective collaboration across the security ecosystem. Organizations responsible for protecting critical infrastructure, supply chains, and essential services are increasingly focused on strengthening their ability to anticipate, respond to, and recover from a wide range of risks. This does not change the exhibition's purpose but does reinforce its relevance. Ultimately, the exhibition provides a platform for constructive dialogue to prepare for an increasingly complex security landscape.

Finally: how is the security and fire protection industry in the region evolving in general? What would you especially like to draw visitors' attention to at Intersec Saudi Arabia 2026?

Riham Sedik: The security, safety, and fire protection sectors across the region are evolving rapidly as organizations adopt more integrated and technology-driven approaches to protecting people, infrastructure, and operations. Visitors will have the opportunity to explore practical solutions spanning AI-enabled security, integrated life safety systems, cybersecurity, fire protection and critical infrastructure resilience, while learning from industry leaders through the exhibition's conference program.

Ultimately, Intersec Saudi Arabia is where the conversations shaping tomorrow's safer, smarter, and more resilient environments begin. As Saudi Arabia continues to invest in giga-projects, smart cities, and critical infrastructure, the ability to integrate security, safety, and fire protection will become increasingly important, and these are the conversations we look forward to facilitating at Intersec Saudi Arabia 2026. GIT

Intersec Saudi Arabia will open its doors from 16 – 18 November 2026 at Riyadh Front Exhibition & Conference Center. The event is for trade professionals, 18+ only.

Messe Frankfurt Middle East
info@uae.messefrankfurt.com
https://intersec-saudiarabia.ksa.messefrankfurt.com



DIGITAL TESTING

More Intelligent, More Transparent, Faster

Digital and Networked Test Procedures in Fire Protection

DT Connect from Detectortesters and the Smartryx solution from Datolution demonstrate how digital testing of fire protection has changed. Stephen Beadle (Global Marcomms Manager at Detectortesters), Oliver Doerle (Head of Customer Experience) and Aljona Ijoschina (Co-Managing Director at Datolution) explain in a conversation with GIT SECURITY how networked test equipment, cloud platforms, and intelligent data integration can accelerate procedures, provide transparency, and deliver legally valid evidence.



XTR2 tests both smoke and heat detectors, capturing the result of each test and transferring it to the DT Connect app

© Detectortesters

GIT SECURITY: Mr. Beadle, when we last spoke, Detectortesters had just launched its first digital solution, DT Connect. How has that developed since then?

Stephen Beadle: DT Connect marked the start of our portfolio of connected products and enabled fire safety technicians to benefit from a solution that combined functional smoke and heat testing with automatic digital test certification.

Since its launch, the solution has proven its value to the global fire safety market: to date, users have tested more than 500,000 detectors, generating test reports for over 15,000 sites across 50 countries.

It is worth recalling exactly what DT Connect offers. Could you briefly explain the purpose of the solution and how it fits in with the traditional test equipment for which you are known?

Stephen Beadle: We introduced DT Connect to cover the growing need for documented proof of testing. The key technical challenge was to develop a reliable method for independently verifying that the detector had been triggered at the test site – in other words, to confirm live and on-site that the detector was functioning correctly and had triggered in response to smoke or heat.



Stephen Beadle,
Global Marcomms Manager,
Detectortesters



Oliver Doerle,
Head of Customer Experience &
Industry Affairs, Detectortesters



Aljona Ijoschina,
Co-Managing Director,
Datolution

To achieve this, DT Connect was combined with the XTR2. The XTR2 is our most advanced functional test device, enabling rapid testing for smoke and heat using a single unit. The test cup contains 21 optical sensors which detect the optical alarm indicators generated by the detector as soon as it enters the alarm state, and transmit the result via Bluetooth to the DT Connect app. The software automatically records this test result along with the date, time and location to provide definitive test verification for each detector on site.

In response to demand from users of our conventional testers, we have now also introduced DT Connect for users of products from our Solo range.



The Smartryx app helps engineers manage site visits and enables genuine one-person maintenance

Mr. Doerle, data and compliance are major issues in the industry. How do you help fire safety professionals overcome challenges in these areas?

Oliver Doerle: The challenge is that compliance often involves more paperwork. Technicians would rather spend their time ensuring that fire safety systems are functioning properly than filling in reports. With XTR2 and DT Connect, we have combined testing and reporting into a single workflow. The inspection data collected is used to generate professional compliance reports that maintenance companies can pass on to their clients, providing immediate proof of the work carried out – without any manual data entry.

The result is simple: fire safety professionals spend less time on administrative tasks and more time on fire safety, whilst building owners receive clear, verifiable evidence that the inspections have taken place. The technician carries out the inspection as usual; the report is generated automatically in the background.

Why do you think these issues have become so important? What is driving the focus on regulatory compliance?

Oliver Doerle: One driver is increased public scrutiny following high-profile incidents, including the Grenfell Tower disaster in the UK. When such events occur, attention turns to whether fire safety systems have been properly maintained and whether there is evidence to prove it. At the same time, building owners and those responsible have become increasingly aware of their obligations. Even though inspections and maintenance work are often delegated to specialist contractors, the responsibility ultimately lies with the building owner.

Technology has also shaped the debate. Advances in cloud platforms, connected devices and digital reporting mean that it is now far easier to collect and manage compliance data. Taking all these factors together, it quickly becomes clear why compliance has become such a key industry issue.

You mention that there are many companies offering tools to support compliance. What led to the collaboration with Datolution?

Stephen Beadle: Many larger maintenance companies already use their own or third-party compliance platforms. This means that whilst many users work directly with DT Connect, others require the inspection data to be integrated into more comprehensive compliance and asset management systems.

We have addressed this need by developing a Software Development Kit (SDK) that enables other software solution providers to connect to the XTR2 test data and subsequently utilise the recorded data within their own platforms. This allows the detector test reports generated during the inspection to be combined with other data collected during the on-site visit. This helps maintenance companies to create more comprehensive records that can be accessed from a single

Please turn page



The partnership between Detectortesters (DT) and Datolution was announced at Feuer-Trutz in Nuremberg. F. l.t.r.: Gareth Dibden, Senior Customer Success Manager (DT), Markus Koschade, Business Development Manager (DT), Aljona Ljoschina, Co-Managing Director (Datolution), Stephen Beadle, Global Marcomms Manager (DT)

platform. Datolution is one of the companies we are collaborating with in this area, alongside other partners in the UK.

'Datolution' appears to be a combination of the terms 'data' and 'revolution'. Could you please begin by explaining the concept behind it, Ms. Ljoschina?

Aljona Ljoschina: Datolution is indeed a deliberate fusion of the terms 'data', 'revolution' and 'solution'. As part of the Schraner Group, we are at home in the fire alarm industry. Important system data is generated here on a daily basis. Surprisingly, to this day only a fraction of this data is analysed and utilised.

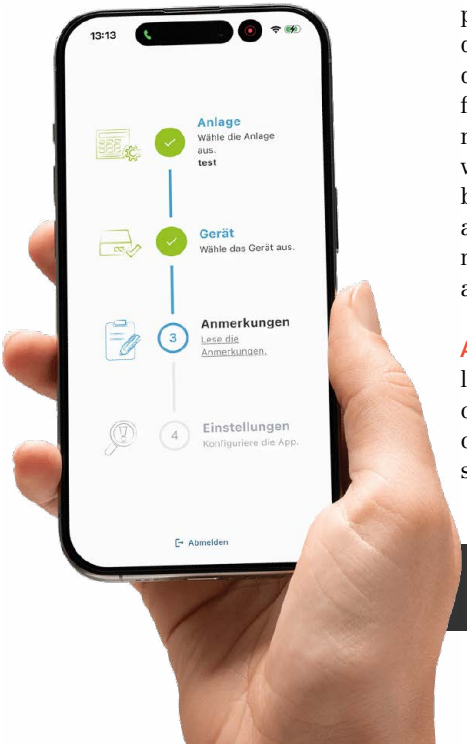
Our 'revolution' therefore consists of making complex safety system data usable and actionable. In short, we turn raw system data into real solutions, thereby saving our customers time, stress and effort. As the protection of this sensitive data is our top priority, we have been operating an Information Security Management System (ISMS) since April 2022, which was first certified to ISO/IEC 27001 in early 2023 and recertified in early 2026.

The core tool is your Smartryx app, which is available both to Fire & Rescue Services and, in the context we are discussing today, as a maintenance app. Could you briefly explain how it works and the functionality it provides?

Aljona Ljoschina: Exactly, with our Smartryx system we digitise fire alarm systems – and do so consistently in a manufacturer-neutral way. The way it works is quickly explained: first, the system configuration is uploaded to our SmartSecure cloud, creating a virtual, static replica of the system. A gateway is connected to enable communication. Anyone wishing to monitor the system 24/7 installs a fixed gateway. For maintenance purposes alone, a mobile device is usually sufficient. The gateway then securely transmits all live notifications, such as alarms or faults, to our server. Via application-specific apps, this information can then be used for notification, fault or maintenance management, regardless of location.

The system really comes into its own when it comes to maintenance: before the technician heads out to the customer's site, a code-compliant test plan is generated in the cloud with just a few clicks. The technician opens this in their Smartryx Maintenance app and can see at a glance what needs to be done. As the app is connected to the system in real time via the mobile gateway, we enable genuine one-person maintenance. The technician can see immediately whether they have triggered a detector using test gas. There is no need for the tedious process of checking via radio with a colleague at the fire panel, as Smartryx automatically marks the detector as successfully tested. Once the job is complete, a single click on 'Complete' is all that is required. At that very moment, the system generates a comprehensive, code-compliant PDF report – including all comments, photos and digital signatures. The technician can email this report to the operator straight away.

In short: we reduce staffing requirements, put an end to error-prone paperwork and make the entire process fast, transparent and, above all, legally compliant.



Smartryx Maintenance app: see at a glance what needs to be done

Today's fire alarms and fire alarm control panels are data-driven, networked and can be maintained remotely. What specific features and new possibilities do your solution and your collaboration offer?

Oliver Doerle: When we launched the product, our aim was to digitise the inspection of fire alarms and to create reliable inspection reports. Our collaboration with Datolution represents the next step on this journey by linking the test data from the fire detectors with information from other areas of the fire protection system.

A good example is when a technician tests a detector. If the detector responds correctly, this event is visible on the fire alarm control panel. However, if a detector is tested and fails to activate due to a fault, the control panel does not necessarily indicate that the detector was tested and failed. By combining data from XTR2 with information from the fire alarm control panel, technicians gain a much clearer picture. They can not only see which detectors have triggered successfully, but also which detectors have been tested and require further inspection. This provides more robust evidence of system performance and the maintenance measures carried out.

Aljona Ljoschina: The major added value lies in the seamless integration of both companies' technologies into a single application. This means that confirmation of a successful detector test is now intelligently synchronised. The Smartryx Maintenance

App processes both the signal from the fire alarm system and the confirmation from the XTR2 tester. By combining these two previously separate processes into a single smart step, we achieve enormous time savings for the technician.

Another key advantage is the direct control of the XTR2. This means that, via our app, you not only have an overview of the operating statuses, but can also intuitively switch the operating mode during maintenance.

Let's take a closer look at this: what does the integration of Detectortesters into Datolution's solutions look like in practice, and what key benefits does this bring for technicians and building owners?

Aljona Ijoschina: Essentially, the digitalisation of the entire maintenance process ensures maximum transparency and a faster flow of information between all parties involved. This results in significant added value. For the building owner, this primarily means full transparency, as the maintenance results are immediately traceable, which greatly strengthens confidence in the installer's work. For the technician, this provides a high degree of process reliability, because when the notifications from the XTR2 aligns seamlessly with the Smartryx notifications, they have immediate assurance about their work right there on site. And ultimately, everyone benefits from legally compliant evidence, as the entire maintenance history can be fully documented through digital records – whether for auditors or experts.

Fire safety is increasingly becoming part of integrated building concepts where the focus is not exclusively on safety functions. How do you view this development?

Oliver Doerle: I consider this to be one of the most important developments shaping our industry. Buildings are becoming increasingly interconnected environments, and customers expect different technologies and systems to work together seamlessly.

No single company can be an expert in every aspect of building management. At Detectortesters, our expertise lies in testing fire alarms, but that is only one part of a much broader ecosystem.

Aljona Ijoschina: We regard this development as absolutely essential. Fire alarm systems were long self-contained systems whose valuable data remained hidden within the building. Integration into holistic building platforms is fundamentally changing that.

For us, this trend confirms our own approach: we must free fire alarm data from its isolation. A modern fire alarm system is essentially a highly available, standardised sensor network that permeates the entire building. When we integrate this data into higher-level platforms via cloud technologies and open interfaces, it creates enormous added value – far beyond mere hazard detection. The core function of saving lives remains unaffected, but the system data suddenly helps to optimise facility management or enable predictive maintenance.

Within this ecosystem, we see ourselves as the spider at the centre of the web, bridging the gap between strictly standardised safety technology and modern platforms. To this end, we focus specifically on intelligent cloud-to-cloud connections and strong partnerships, such as our collaboration with Detectortesters. GIT

Datolution
www.datolution.de

Detectortesters
www.Detectortesters.com

Trusted European fire detection expertise for over 100 years

False alarms stop work, waste time and damage confidence in the systems protecting your building, the answer starts with specifying the right system.

Fire detection specialists since 1918

Local territory support from local experts

EN 54 product range and BOSEC certified systems

ISO 9001 quality management

Proven track record across Europe, scan the QR code to learn more.

HOCHIKI





"We would highly recommend Hochiki for any life safety system requirements"
— EL.CO. Srl

BOSEC Certified

EN54 certified



© fifthplanet - stock.adobe.com

WILD FIRES

Fire Information Consolidation

Modernizing the Emergency Response to Wildfires

When it comes to managing wildfires, the faster they can be detected, the quicker and safer they are to contain. Mapping and sensing technology has significantly improved the ability to identify high-risk areas and support preventative measures. However, wildfires are likely to become increasingly common as hotter, drier conditions become more widespread.

© Octave

Sam Sheppard is a public safety industry specialist for Octave

Wildfires present a raft of significant challenges in planning and managing the response. They can ignite and spread quickly with an abundance of combustible material to feed them. Add in wind, and the situation can become extremely dangerous very quickly. The 2023 Alexandroupoli wildfire in north-eastern Greece, for example, burned more than 900 square kilometers, becoming the largest wildfire ever recorded in the European Union.

The speed of fire detection has improved significantly in recent years, from hours to minutes, but getting them under control is a far greater challenge. Public safety agencies and organizations around the world are learning lessons from the handling of each wildfire, implementing new processes and preventative measures to try and prevent fires and mitigate their impact.

Proactive Prevention

There are simple but effective steps such as prohibiting the use of BBQs or fire pits during prolonged dry spells, along with smoking bans in designated areas. But as temperatures continue to rise and lightning storms increase, wildfires will continue to occur naturally. Other preparation and pre-staging initiatives include creating evacuation zones and running public campaigns to ensure that communities know which zone they are in. Evacuation routes can be preplanned and stress-tested using predictive modeling to determine the volume of traffic with which they can cope. For example, how long would it take 10,000 vehicles to move at the same time along a two-lane road? Having this information helps to determine the amount of warning that will be needed to evacuate areas safely and control congestion.

Response Logistics

Right now, emergency services and other key stakeholders in parts of France and Spain are coordinating their efforts and working around the clock to prevent fires from spreading, including the evacuation of more than a quarter of a million people from areas that are swelled with tourists and holidaymakers. At a national level, emergency alerts systems such as France's FR-Alert and the Spanish ES-Alert have been introduced in recent years and used to send messages en masse to citizens in danger from wildfires.

Real-Time Intelligence and Collaboration

Plans and predetermined workflows that command and control centers trigger in an emergency work best when integrated within a centralized and secure communication and collaboration platform. Such a system ingests information from multiple sources to provide the situational awareness needed to coordinate a single or multi-agency response.

The situation can change quickly during a wildfire. For example, falling trees and overhead power lines, along with heavy smoke, can make pre-planned evacuation and emergency vehicle routes impassable. Access to real-time geospatial data, fixed cameras, drone and aerial footage, weather and air-quality sensors, alongside updates from evacuees and first responders are all essential to be able to dispatch traffic teams to redirect vehicles, or to change messages on digital road signs, send fire and rescue crews to the right places and manage ambulance crews to help control capacity at hospitals.

In the case of large-scale wildfires, such a platform can also help when working with international aid. France has been assisted by Croatia, Portugal, the Czech Republic and Slovakia, with resources such as water bombing carriers, water tractors, and helicopters.

AI Innovation

Fires in France and Spain have affected parts of the country densely populated by tourists of many different nationalities at this time of year, and language barriers can delay clear communication. It is here that AI is helping to break down these barriers, with innovations such as real-time translation and call summaries beginning to be introduced into command and control rooms.

According to NASA, extreme wildfire activity has more than doubled worldwide over the last two decades, including parts of the world that until recently had not experienced such extreme events. However, unified communication and collaboration platforms are not only valuable during major incidents; they also help to improve the management of daily operations. GIT

Octave Intelligence
www.octavepublicsafety.com



Tobias Väthjunker, CEO of Kirotec (until recently Chairman of the Board of Priorit, a subsidiary of Kirotec) (right side), Dr. Timo Gimbel, Team GIT SECURITY International (left side)

SOLUTIONS

A Cool Compliance Companion

An Interview with Tobias Väthjunker, CEO of Kirotec, a Top Player in Fire Protection Solutions

GIT SECURITY meets with leading companies and thought leaders in the safety and security industry. In this interview, we speak with Tobias Väthjunker, CEO of Kirotec (until recently CEO of Priorit, a subsidiary of Kirotec), about current challenges and future developments.

GIT SECURITY: Mr. Väthjunker, how do you assess the current economic situation, and what strategic conclusions do you draw from it?

Tobias Väthjunker: The overall economic trend is characterized by both high dynamism and high uncertainty. Ultimately, this affects all companies. We are active in preventive fire protection and are therefore closely tied to the construction industry. There, we see reluctance to invest, high financing costs, constant cost increases, and long, sluggish planning and approval processes.

Fire protection is heavily driven by regulations, and these regulations are constantly increasing. This is precisely what serves as a stable driver of demand for us. Operators of real estate portfolios, as well as production and industrial properties, must continuously upgrade their systems. Fire safety cannot be postponed; it is an ongoing priority, and compliance is mandatory.

For us, this means we must strike a balance between sales and procurement markets. We respond to fluctuations in demand with flexible value-creation structures. We do not make decisions based on supposed certainties or old routines, but rather on numbers, data, and facts. We do not want to miss out on developments or make the wrong decisions. Strategically, this means an even stronger customer focus, expanding our renovation business, and investing in new products and niche markets that are emerging as a result of current market dynamics.

What challenges do you see among your customers, partners, and suppliers – and how are you responding to them?

Tobias Väthjunker: Our customers face the constant challenge of complying with fire safety regulations. Regulatory pressure is steadily increasing. Added to this are ongoing cost increases, which are particularly critical for projects with long durations. If the information available at the outset is poor, if fire protection solutions are unreliable, if products have defects, or if service delivery is weak, then projects become more expensive and the effort required increases. This is a reality we see frequently.

We must therefore support our clients even earlier in the process. We contribute our expertise, provide technical support, and ensure planning certainty. Our commitment to quality – both in terms of technical standards and timelines – is crucial for enabling stable project implementation and reducing uncertainties regarding costs and compliance.

At the same time, we are experiencing structural change. Going it alone is becoming more difficult. Especially in small and medium-sized businesses with 50 to 250 employees, the question of the future is coming up more and more frequently. For many, partnerships or joining a group are very sensible solutions.

Where do you see growth potential – domestically, in exports, and within your product portfolio?

Tobias Väthjunker: We see opportunities in several areas: providing more support for our customers, expanding our renovation business, and broadening our product portfolio. We have particularly strong potential in exports. There are countries with higher

Please turn page

growth momentum than Germany, and we want to increase our market share there. To enable this growth, we invest a seven-figure sum annually in the development of new products. In addition, over the past fifteen months, we have established four partnerships with companies that have a complementary business model – both in development and in sales. We have high expectations for these partnerships.

Another key component is our acquisition strategy. Together with Priorit and our partner, Aurelius Wachstumskapital, we are building a group that pools resources, leverages synergies, and is more resilient to fluctuations in demand. Digitization, investments, efficiency – all of these can be better managed within a group. Priorit's product portfolio has grown over more than 25 years, but there is always room for improvement. User-friendliness and assembly processes are key priorities for us in addressing rising cost pressures. In addition, we are introducing EPDs for all our products to send a clear signal regarding sustainability. A concrete example is our new lithium-ion cabinet. We have tested it according to VDMA testing principles; it is currently undergoing the certification process and will be a very interesting solution for industrial and public-sector customers. And yes – we played a key role in defining, in the first place, what such a cabinet must be capable of. That did not exist before. We have a great team from R&D, regulatory affairs, sales, and export that is driving these initiatives forward together.

Especially in international business, we benefit from meeting the high German and European standards. At the same time, regulatory agencies in other countries operate differently, and you need to be in it for the long haul. That is why we are expanding our training programs for international markets – and our experience with them has been very positive.

How do you see the industry developing over the next five years?

Tobias Väthjunker: When I talk to people in the market, many expect a moderate recovery. Some sectors will see disproportionately strong growth: infrastructure, renovation, commercial construction – and data centers in particular. In Frankfurt alone, several new facilities are being built. The investment amounts are extremely high, and fire protection plays a massive role. The risk of fire spread must be minimized to safeguard these investments. We have some very interesting solutions for this, such as access panel locks and systems for partitioning rooms. We are currently engaged in very exciting discussions and see great potential.

Regardless of the economic climate, there are megatrends that offer enormous opportunities: digitization through AI, automation, demographic change, and the ecological transformation of the economy. These developments will shape the industry. And structural change will continue. Collaborations, partnerships, and group models – this will be the path for many companies to successfully navigate the next five years and beyond. GIT



SafeLeader
The GIT Talk with the Market Leaders



Watch now:
the full interview in
our video podcast



Kirotech
www.kirotec.de



Sharpened Portfolio Strategy

Mobotix AG is sharpening its product strategy with a clear focus on high-performance, modular platforms and expanding the capabilities of its flagship ONE Series while simplifying its overall portfolio. Selected product lines will be transitioned out on a planned schedule, which will put focus on platforms that deliver the highest performance and longest-term value for partners and customers. "We are consciously focusing on fewer, but significantly more powerful platforms," explains Dr. Christian Cabirol, CTO of Mobotix AG. "Our goal is to offer our partners and customers a clear, future-proof system landscape without compromising on functionality or quality." At the heart of this realignment is the new generation of modular Mobotix platforms with integrated AI functionality, centered on the Mobotix ONE series. **www.mobotix.com**

Integrated Data Center Security and Monitoring



To prepare their infrastructure for the challenges of the future, Heidelberg iT Management have implemented KentixONE, an integrated platform that unifies security, environmental monitoring, and energy management within a single system. This consolidates eight critical functions that had previously been monitored holistically via a connected network of multi-sensors. KentixONE's integrated protections include access control with IP wall readers and multi-level authentication, environmental monitoring tracking temperature, humidity, and air quality, and energy monitoring via smart power distribution units and calibrated electricity meters. Leakage sensors in raised floors and critical areas detect potential water damage and trigger an alarm on detection. Network video cameras document any security incidents, and the platform's intuitive web interface and mobile app give Heidelberg iT's operations team 24/7 access to critical data, whether they are on-site or off. Sensitive operational data remains under local control, while granular access management, full audit trails, and real-time alerts ensure only authorized site-users gain access. By controlling and monitoring all devices within KentixONE, Heidelberg iT achieved full visibility of security and environmental systems. Automated energy billing and load monitoring, with customizable reports to track consumption, further streamline their operations. The system's scalability ensures that Heidelberg iT can quickly adapt to evolving requirements: its REST API enables seamless integration with existing or new systems. Heidelberg iT's implementation of KentixONE demonstrates how unified physical security and monitoring can drive efficiency, compliance, and scalability. **www.assaabloy.com**



Morello cherries: Kervo is a specialist fruit processing business in Neer, Netherlands

© Natalia - stock.adobe.com

FALSE ALARMS

When the Cost Exceeds the Fire

Correct specification is a question of business continuity

False alarms are not an abstract inconvenience for facilities managers and system integrators across Europe. They carry a direct cost: halted production lines, evacuated staff, emergency service callouts and the potential loss of in-process product. The financial impact registers every time a facility stops for a false alarm, and long before anyone has reached the fire exit.

"This is a conversation I have regularly with customers," says Klaus Friebe, Regional Sales Manager for Northern Europe at Hochiki Europe. "The technical challenge of protecting demanding industrial environments is well understood. What receives less attention is the operational cost when the wrong product is specified. Correct specification is not just a compliance question – it is a business continuity question."

Too Hot To Handle

That distinction was central to a recent installation at Kervo, a specialist fruit processing business in Neer, Netherlands, which has cultivated and processed Morello cherries since 1980 and now supplies bakeries and fresh food retailers across Europe and the UK. When Kervo moved into a new manufacturing facility, installer JTI Brandbeveiliging faced an immediate challenge: the steam generated during food production and cleaning created conditions that standard detection devices handle poorly.

"We needed devices that could manage the false alarm risk without compromising detection performance," says Luciën van Eldijk, lead engineer at JTI Brandbeveiliging. "Hochiki's weatherproof call points, sounders and sensors provided exactly that. Combined with the Latitude fire control panel, they gave the customer a system that works reliably in a genuinely demanding environment."



Klaus Friebe, Regional Sales Manager, Northern Europe, Hochiki Europe

Standards Compliant

The Kervo facility reaches over 40 meters in height and required more than 2.5 km of cabling. Hochiki's weatherproof ESP addressable devices were deployed throughout, supported by the Latitude panel, which carries EN 54 certification: the applicable compliance standard for fire detection systems in the Netherlands. The Latitude panel also holds BOSEC certification, a mandatory requirement for fire detection systems in Belgium. The system supports up to 5,000 event log entries with 20,000 inputs and outputs across the network, providing both the scale Kervo required and capacity for future expansion as the business grows.

For industrial and food processing operators across Northern Europe, the Kervo project demonstrates that false alarm management is a specification decision, not an operational inevitability. Hochiki's ESP range and Latitude platform are EN 54 certified, meeting the compliance requirements applicable in the Netherlands and across the wider European market. For specifiers and installers working in Belgium, the Latitude panel's BOSEC certification provides the additional assurance that the Belgian market demands. GIT

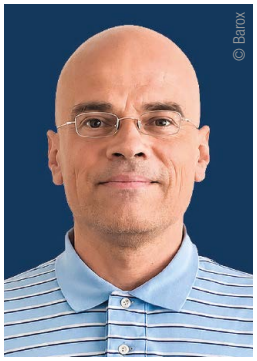


Hochiki's analogue addressable range (ESP intelligent) together with the Latitude system are EN54 Part 13 certified and with the BOSEC certification also in place, they provide the best complete and compliant fire detection system for businesses across the Belgium region as well as bordering countries such as Luxemburg, the Netherlands and Germany.

Hochiki Europe
www.hochikieurope.com

© Images: Hochiki Europe

barox Strengthens Eastern European Growth Strategy



Nikolay Mitev

barox Kommunikation AG has appointed Nikolay Mitev as Regional Sales Manager for Eastern Europe, reinforcing the company's commitment to expanding its presence across the region. Based in Sofia, Bulgaria, Nikolay will be responsible for driving business growth across Eastern Europe and the CIS. His role will be to develop new market opportunities and promote barox's full portfolio of managed Ethernet switches and media converters. He will also work to raise awareness of barox's extensive range of Video Management System (VMS) and Physical Security Information Management (PSIM) integrations, collaborating closely with end users, systems integrators, distributors, and technology partners. **www.barox.ch**

i-PRO Names Steve Riley as New President of EMEA

i-Pro, a global provider of professional security and public safety solutions, has appointed Steve Riley as President, EMEA. As i-Pro's EMEA business continues to expand, the company is adapting its regional leadership structure to support ongoing growth, navigate increasing business complexity, and ensure the organization continues to scale effectively across the region. Steve Riley will lead the overall EMEA organization, focusing on regional strategy, organizational development, governance, and business leadership. Jose Riolobos will continue to lead the commercial expansion as Vice President of Sales, EMEA, focusing on customer and partner engagement, and accelerating sales growth across the region. **www.i-pro.com**

CertEntra v2 for Certificate Automation Released

Secardeo certEntra v2 is now available as an Azure Web App, enabling centralized, automated registration of digital user certificates for Entra ID users. This allows S/MIME certificates to be obtained from a public certificate authority and deployed to all of the user's Intune-managed devices for end-to-end encryption and digital signing. It also allows the registration and distribution of user authentication certificates (CBA) from a private CA. Centralized key archiving ensures that private keys can be distributed and later restored. certEntra v2 is the first solution on the market to use post-quantum cryptography (PQC) in a hybrid method with ML-KEM/RSA for the long-term protection of archived keys. It allows easy deployment as an Azure Web App or on an on-premises VM, and full integration with Entra ID, Intune, Azure Key Vault, Azure SQL, Exchange Online, and Microsoft 365. **www.secardeo.com**

Octave Celebrates Inaugural Ovations Awards

Octave Intelligence has announced the recipients of the Octave Ovations. The 2026 awards were presented during a ceremony at the Octave Live OnTour event in Austin, Texas, USA. The inaugural Octave Ovations recognize customers who turn data and intelligence into decisive action. The awards celebrate work that sharpens performance, amplifies efficiency and delivers measurable outcomes. These customers have partnered with Octave to simplify complexity across design, build, operations and protection – at any scope and at scale. Their submissions detailed the key market forces shaping their industries, the challenges they faced, the benefits achieved through Octave solutions and their outlook for the future. Other regional Innovator Award winners will be presented at upcoming Octave Live OnTour series events in Rio de Janeiro, Brazil (Aug. 19–20), Singapore (Sept. 17–18), Shanghai, China (Sept. 22–23) and Munich, Germany (Oct. 13–14). **www.octave.com**

Outdoor Curtain Detectors for Residential and Commercial Perimeter Protection



Optex has launched the TXI Series, a range of high-mount outdoor curtain detectors. Built to create an invisible curtain barrier along a building façade, the products address the external security challenge of balancing reliable human detection with minimizing nuisance alarms. By creating a controlled detection curtain at the perimeter, the TXI Series is specifically designed to provide earlier detection before an intruder reaches the building itself. Common applications include ground-floor perimeter protection, balconies, warehouses, office buildings and retail sites whereAt the heart of the TXI is Optex's patent-pending Triple AND Logic that uses three independent sensing areas to create three detection zones, with an alarm only triggered when all three zones detect simultaneously. a narrow detection field can help to define and secure the boundary of a property. **www.optex-europe.com**

Octave named Global Command and Control Company of 2026

Octave Intelligence has been named Frost & Sullivan's 2026 Global Command and Control Company of the Year, the technology analysis and research firm's highest honor, as the market participant that exemplifies visionary innovation, market-leading performance and unmatched customer care. The award recognizes Octave's leadership in advancing command and control capabilities for organizations operating complex, high-consequence environments. Central to this is the Octave Coda portfolio, which combines video management, sensor data, incident management, analytics and operational workflows in a single software environment. Frost & Sullivan evaluates companies through a rigorous benchmarking process for strategy effectiveness and strategy execution. Octave excelled in both, Frost & Sullivan stated. **www.octave.com**

GIT SECURITY INTL

INNER COVER – SECURITY



Monitoring the Vastness

Distributed Fiber Optic Sensing to Protect Critical Infrastructure and Large Sites

APSENSING.

INNER COVER

Monitoring the Vastness

Distributed Fiber Optic Sensing to Protect Critical Infrastructure and Large Sites



In this interview with GIT SECURITY, Clemens Pohl, CEO of AP Sensing, explains how fiber optic cables act as continuous sensors to detect third-party intrusion at an early stage, safeguarding critical assets and the uninterrupted operation of essential infrastructure.

GIT SECURITY International: Mr. Pohl, AP Sensing develops fiber optic sensing systems. Before we dive into how they work and the applications they support, could you briefly introduce the company?

Clemens Pohl: AP Sensing develops Distributed Fiber Optic Sensing (DFOS) solutions that help monitor critical infrastructure, making it safer and more efficient. Our sensing technology enables operators to detect risks, third-party intrusion (TPI), and emerging system failures at an early stage, allowing them to respond quickly. This helps maximize the availability of critical assets. Our roots trace back to Hewlett-Packard. AP Sensing was founded in 2007 as a spin-off from HP's test and measurement business, where research and development in fiber optic measurement technology had been underway since the 1980s.

Today, we employ more than 180 people across five continents. Our solutions are deployed by more than 1000 customers in over 70 countries. These customers operate in power utilities, fire detection, pipeline monitoring, railway and transportation infrastructure, perimeter security, and defense.

Many of these are critical infrastructure assets, which have received much greater attention in recent years.

Clemens Pohl: Over the past few years we have seen just how dependent our society is on critical infrastructure. Power grids, pipelines, telecommunications networks, railways, and submarine cables form the backbone of our daily lives. When one of these systems fails, the consequences are often felt far beyond the immediate location.

At the same time, a series of high-profile incidents has highlighted just how vulnerable these assets can be. The sabotage of the Nord Stream pipelines, damage to submarine cables in the North Sea and Baltic Sea as well as attacks on railway infrastructure have brought the issue into the public spotlight.

Another challenge is that our infrastructure is becoming increasingly extensive and complex. As the energy transition accelerates, new offshore wind farms, transmission lines, battery storage facilities, and cross-border energy interconnections are being built. Many of these assets span hundreds of kilometers, often crossing remote or difficult-to-access areas. Protecting infrastructure on this scale presents a unique challenge. It is simply not feasible to station personnel every few kilometers or continuously monitor every asset on site.

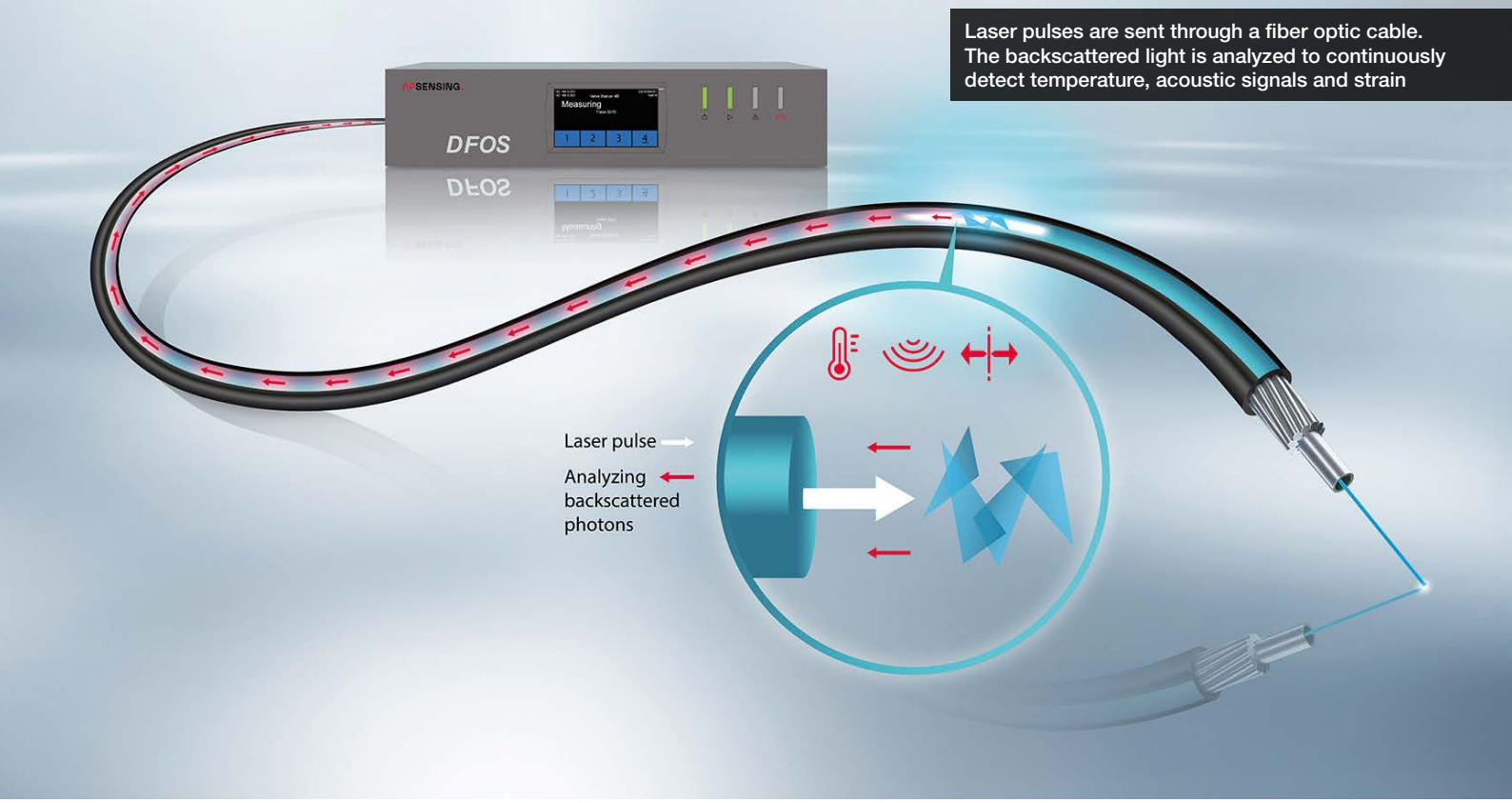
That is why operators need new ways to maintain continuous visibility of the condition of their infrastructure and to detect unusual activity as soon as it occurs. Ultimately, it is about ensuring the security and reliability of the systems that our societies depend on every day.

Your portfolio includes Linear Heat Detection (LHD), Distributed Temperature Sensing (DTS), Distributed Acoustic Sensing (DAS), and Distributed Temperature & Strain Sensing (DTSS). Could you walk us through the differences and explain where each technology is typically used?

Clemens Pohl: All of these solutions are based on the same fundamental principle: we use fiber optic cables as sensors. This allows us to gather information continuously along the entire length of the cable, over distances of many kilometers, rather than at individual measurement points. The difference between these technologies lies in the type of information we extract from the fiber.

With Linear Heat Detection and Distributed Temperature Sensing, we measure the exact temperature at every meter along the cable, even over long distances. These technologies are widely used for fire detection as well as to monitor power cables and pipelines.

Distributed Acoustic Sensing, on the other hand, detects vibrations and acoustic signals along the fiber, effectively turning it into thousands of virtual microphones. This makes it possible to detect excavation work



Laser pulses are sent through a fiber optic cable. The backscattered light is analyzed to continuously detect temperature, acoustic signals and strain

near power cables and pipelines, third-party intrusion, or activity along fences and other critical infrastructure. Beyond infrastructure protection, DAS is also used for earthquake research and tsunami warning systems.

Distributed Temperature & Strain Sensing adds another layer of information by measuring mechanical strain in addition to temperature. This makes it particularly well suited for structural health monitoring of bridges, tunnels, pipelines, and other critical assets. The technology is also used to monitor dams and levees, as well as in geoscience applications such as landslide detection.

Ultimately, all of these technologies share the same objective: they provide continuous visibility across time and distance, enabling operators to detect threats early and operate their assets safely and efficiently.

Could you explain in a little more detail how Distributed Fiber Optic Sensing (DFOS) works?

Clemens Pohl: Put simply, we use a fiber optic cable as a continuous sensor. A measurement unit sends pulses of light through the fiber. A very small portion of that light is naturally scattered back along the fiber and returned to the instrument. When the environment surrounding the fiber changes, for example, due to heat, vibrations, or mechanical strain, the characteristics of the backscattered light change as well. By analyzing these changes in real time, we can determine exactly where an event occurs along the fiber and identify the type of event.

There is often a trade-off between high detection sensitivity and false alarms. How does your technology address that challenge?

Clemens Pohl: That trade-off certainly exists, and high sensitivity is essential for the detection of critical events at an early stage. At the same time, operators need to be able to trust that every alarm is meaningful. Warnings can quickly lose their credibility if a system generates too many false alarms. That is why it is no longer just about the performance of the sensing technology itself, but equally about intelligent analysis of the data.

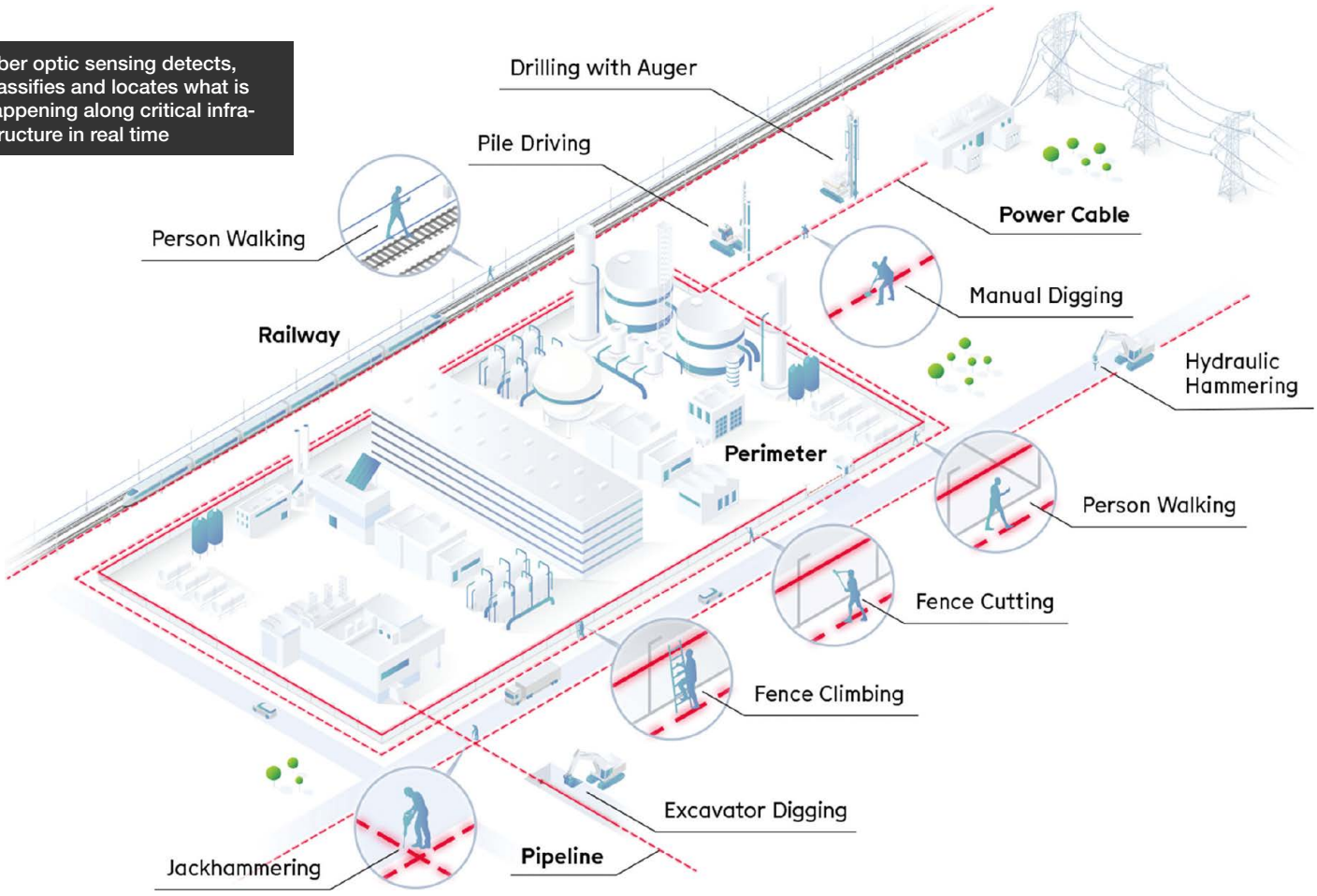
Today's systems are far better at distinguishing between critical events and normal environmental influences than they were just a few years ago. This is made possible by the extensive data we have collected from thousands of installations worldwide, combined with advanced analytics and machine learning. As a result, we achieve reliable detection performance while maintaining a high-quality alarm system. Our goal is not only to detect events reliably, but also to classify and locate them accurately. Only by combining these capabilities can operators receive the right information at the right time.

The market for fiber optic sensing systems is growing rapidly, driven in large part by the expansion of renewable energy and evolving regulations for critical infrastructure. As a result, these technologies have become well established across a wide range of industries. Is AP Sensing active in all of these markets?

Clemens Pohl: Absolutely. We are seeing growing demand for reliable monitoring solutions across all of these markets. The energy transition is creating new challenges, whether it's the expansion of power grids, the development of new energy infrastructure, or the protection of pipelines and railway networks.

Alongside these technological developments, regulatory requirements are also becoming an important driver. Regulations such as the EU's NIS2 and Germany's Critical Infrastructure Resilience legislation place even greater emphasis on resilience, transparency, and the early detection of potential risks. Operators need continuous visibility into what's happening along their critical infrastructure these days so they can respond quickly when incidents occur.

Please turn page



Fiber optic sensing detects, classifies and locates what is happening along critical infrastructure in real time

These developments are nothing new for us. For many years, we have helped customers to identify potential threats at an early stage and make informed decisions based on real-time data. We see this as a long-term transformation: the way critical infrastructure is monitored, managed, and protected is fundamentally changing.

Could you give us a concrete example of how your systems are used to protect critical infrastructure?

Clemens Pohl: Certainly. A good example is pipeline monitoring. Even routine construction work near a pipeline can pose a significant risk. Our Distributed Acoustic Sensing solution monitors nearly 500 kilometers of pipeline on a major pipeline project in Eastern Europe. If an excavator is operating near the pipeline, for example, the system detects the resulting vibrations and acoustic signals, pinpoints the location, and alerts the operator in real time. This enables potential threats to be assessed before any damage occurs.

Another example is high-voltage interconnectors linking European countries. We monitor submarine power cables spanning more than 300 kilometers that play a vital role in Europe's energy supply and the integration of renewable energy. These interconnectors are critical infrastructure in the truest sense. Our systems detect activity near the cable route, including events such as ships' anchors being dragged across the seabed or fishing gear coming into contact with the cable corridor. Operators can identify these risks at an early stage and respond quickly.

While these applications are very different, the underlying principle is always the same. We transform a fiber optic cable into a continuous sensor, providing continuous visibility and a real-time operational picture, which enables operators to make informed decisions based on real-time data.

Could you give us another example from a different application area where AP Sensing has extensive experience?

Clemens Pohl: Another good example would be the monitoring of export cables for offshore wind farms that are essential to connect offshore wind farms to the power grid. Repairs are often complex and costly if these are damaged, require specialized vessels and depend on favorable weather conditions. That is why it is so important to identify potential issues as early as possible.

In France, we have equipped several offshore wind projects with fiber optic sensing technology. Underground and submarine export cables are continuously monitored using Distributed Temperature Sensing and Distributed Acoustic Sensing.

Distributed Temperature Sensing helps to identify hotspots at an early stage. This is important because thermal anomalies often develop gradually. In one case, the system detected a localized temperature increase over several weeks. The cause turned out to be agricultural activity above the cable route. The operator was able to investigate the issue and take action before it developed into a more serious problem.

Distributed Acoustic Sensing complements this monitoring by detecting construction work and other activity near the cable route. This gives operators better situational awareness and helps them to assess whether an event requires immediate attention.

Offshore wind is a great example of what we are trying to achieve. It is no longer enough to react only after a fault has occurred. Operators need continuous, real-time insight into the condition of their

infrastructure. Only then can they identify critical situations early, plan maintenance more effectively, and ensure the long-term availability of the grid connection.

AP Sensing is also active in the defense sector. How do the requirements for military applications differ from those of civilian infrastructure?

Clemens Pohl: We do not comment on specific defense projects or customers as a matter of principle. More broadly, however, we are seeing growing interest in DFOS for security-critical applications. The technology offers several advantages in these environments. Fiber optic cables are completely passive, making them immune to jamming, spoofing, and electromagnetic interference. The cables themselves are also highly robust. They continue to operate reliably in harsh environments, including extreme temperatures, dusty conditions, and even areas with elevated radiation levels. Fiber optic cables can also be deployed quickly, whether mounted on fences or installed underground.

In the defense sector, as in civilian applications, the focus is on monitoring critical infrastructure and detecting activity near sensitive areas at an early stage. Distributed Fiber Optic Sensing is particularly well suited for this because a single fiber optic cable can continuously monitor long distances. The technology can detect movement, vehicles, or other activity along borders, military facilities, or military communications infrastructure, providing operators with a continuous, real-time operational picture.

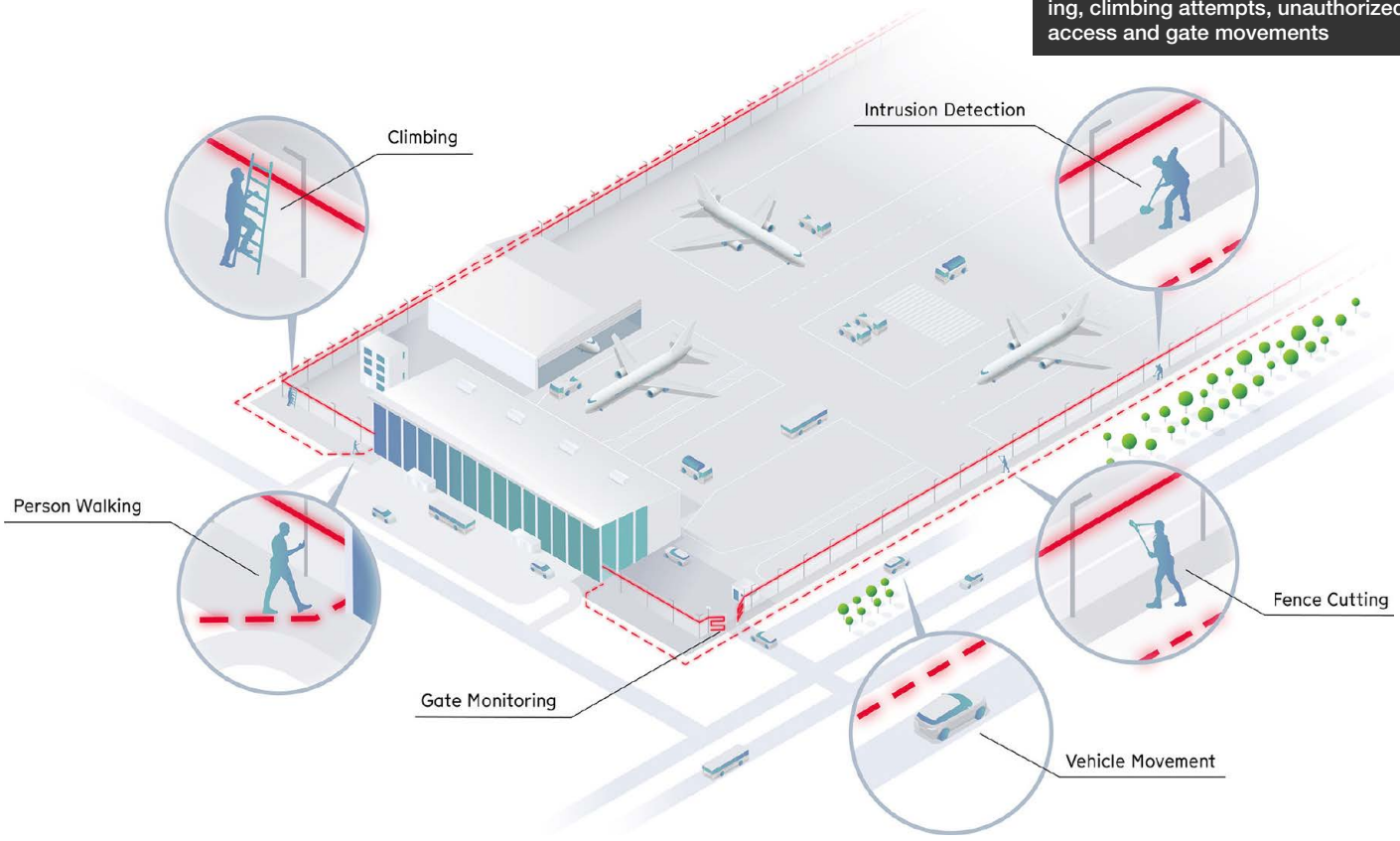
The underlying technology is the same as in civilian applications and the physical principles do not change. We measure changes in temperature, vibrations, and acoustic signals along a fiber optic cable and analyze the resulting data. The main difference lies in the operational requirements. In civilian applications, the objective is often to reliably detect larger events, such as construction work, dragging anchors, or other potential threats near critical infrastructure. In defense applications, the focus is often on much more subtle activity such as very small movements or signs of intrusion near sensitive assets at the earliest possible stage.

Interoperability is another key requirement in defense environments. Our systems typically operate as part of a broader security architecture rather than as standalone solutions. The ability to exchange data with other sensors and platforms, and to integrate seamlessly into existing command, control, and surveillance systems, is often just as important as the sensing technology itself.

Ultimately, civilian and defense applications share the same objective. Operators and security personnel need reliable information about what is happening along their infrastructure. The main differences lie in the threat scenarios and the resulting requirements for detection performance and system integration. GIT

AP Sensing GmbH
www.apsensing.com

© Images: AP Sensing



For perimeter monitoring, fiber optic sensing reliably detects fence tampering, climbing attempts, unauthorized access and gate movements

GIT TEST SERIES

Reliable Protection Across Long Perimeters

Optex EchoPoint excels in field testing with precise fibre-optic detection and intelligent event classification

Perimeters extending over many kilometres are among the most demanding challenges in modern security technology. At an Optex test site, GIT SECURITY International joined independent security technology expert Markus Piendl to examine how Distributed Acoustic Sensing (DAS) and the EchoPoint fibre-optic detection system can use optical fibre to detect, locate and classify events across vast distances.

The Japanese Optex Group has been developing intelligent sensing technologies for a wide range of applications for many decades. Its portfolio includes passive infrared detectors, active infrared beams, REDSCAN LiDAR systems and fibre-optic solutions from its subsidiary Fiber SenSys. These different sensing technologies can be combined to create multi-layered security concepts.

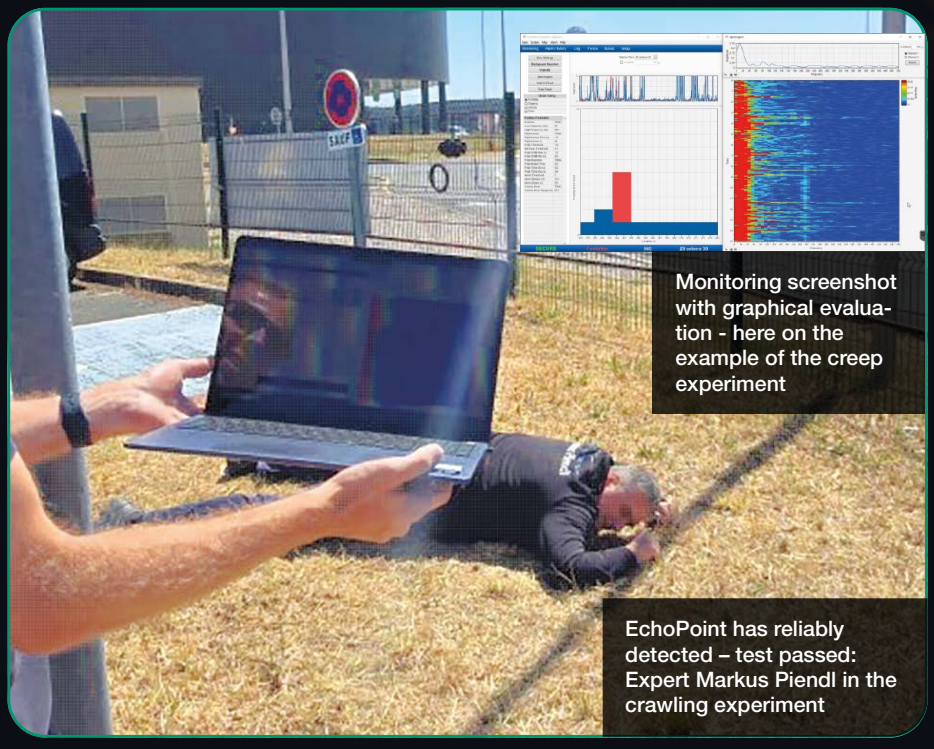
EchoPoint is the focus of this GIT field test. Within the portfolio, its role is to provide continuous monitoring of extensive infrastructure over distances of many kilometres.

Practice, not promises

The setting was one of Optex's professionally equipped test sites in Europe. From the moment of arrival, one thing was clear: this was a stress test, not a showroom presentation. Amid fence lines, buried optical fibre and a variety of test areas, DAS was put through its paces under realistic conditions.

Rather than being given a conventional product presentation, expert Markus Piendl was offered a detailed view of EchoPoint's planning, installation and commissioning. Following a technical briefing on the system architecture, detection zones and alarm management, he was able to investigate his own questions directly on the test site. Both fence-mounted sensing and buried detection were assessed under realistic conditions.

Aurélien Martin, Technical Pre-Sales Engineer at Optex, began by explaining the underlying principle. In Distributed Acoustic Sensing, an optical fibre cable serves as a continuous sensing element. Mechanical and acoustic impacts along the monitored route alter the light backscattered within the fibre. The EchoPoint perimeter protection system analyses these changes, assigns them to an event location and supports the classification of different types of events.



Monitoring screenshot with graphical evaluation - here on the example of the creep experiment

EchoPoint has reliably detected – test passed: Expert Markus Piendl in the crawling experiment

One key advantage: fence-mounted, buried or hybrid installation

EchoPoint impressed Markus Piendl from the very first test scenarios. One of its particular strengths, he noted, is the flexibility of its installation. Depending on local conditions, the EchoPoint sensing cable can be attached to a fence, buried in the ground or deployed as a hybrid combination of both methods within a single project. "A major advantage in real-world projects," the expert concluded. The first clear mark in EchoPoint's favour.

There is another compelling feature: optical fibre is entirely passive. There are no active electronic components along the monitored route. As Piendl observed, this makes the technology particularly suitable for applications with stringent requirements for reliability, electromagnetic compatibility and lightning resistance. Another positive entry in the test record.

As testing progressed, Markus Piendl highlighted another benefit in his discus-

sion with Optex Technical Director Geoffrey Michaud: continuous surveillance over long distances. EchoPoint supports the creation of virtual detection zones and, according to the manufacturer, locates events along the sensing fibre to within plus or minus six metres. By mapping the fibre route to geospatial position data, alarms can be linked to GPS coordinates and displayed on a site map.

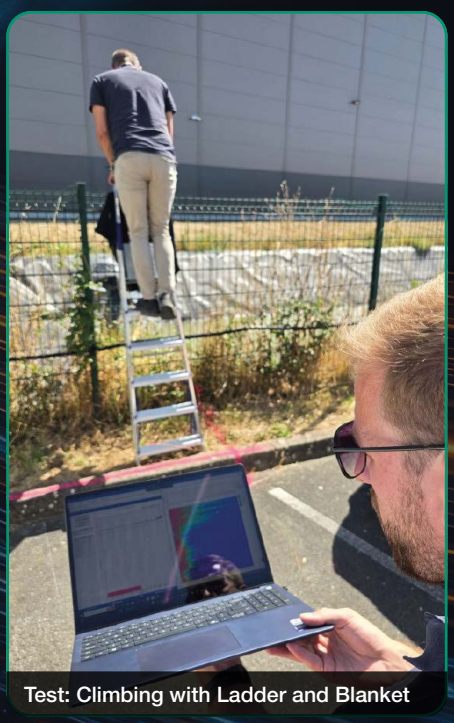
Integration with video management, PSIM and control-room systems then supports targeted verification and incident handling. Depending on the system configuration, monitoring can also be designed with fault tolerance or redundancy. Another tick on tester Piendl's checklist.

Intelligent event classification

According to Markus Piendl, a key difference from conventional perimeter systems is that Distributed Acoustic Sensing does more than establish that an event is taking place. It also analyses the characteristic vibration patterns travelling along the optical fibre. Different impacts, such as footsteps, vehicle movements, excavation work or interference with a fence, produce distinct acoustic signatures. This gives the detection data significantly greater meaning.



Test: Sensitivity Settings



Test: Climbing with Ladder and Blanket

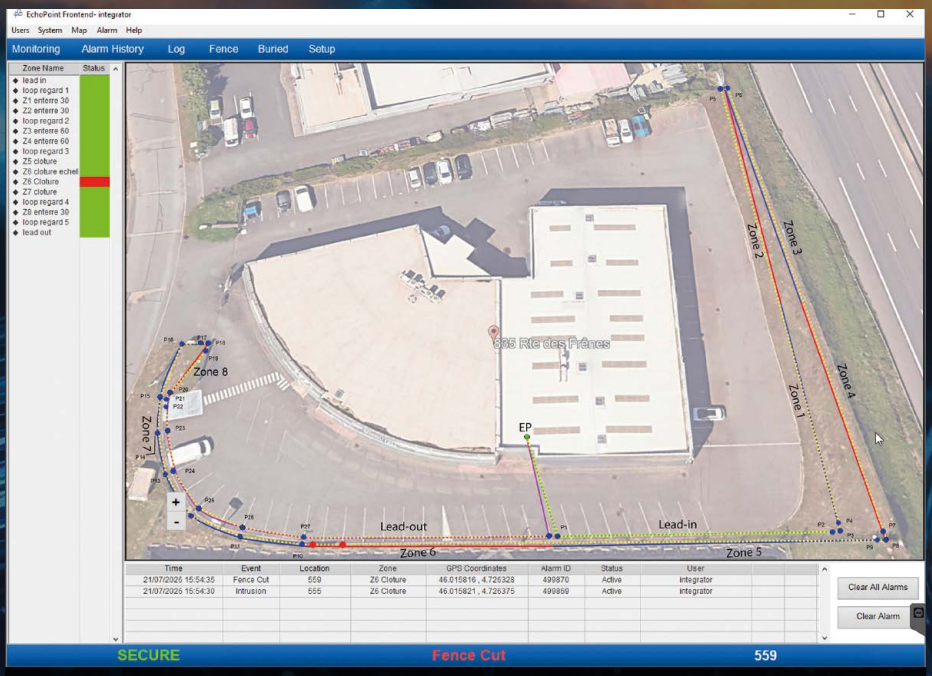
A decisive strength in the test was EchoPoint's continuous analysis of these signatures. The system assigns them to an event location and classifies them according to their characteristics. Alongside the position alert, security teams therefore receive an initial indication of the type of event that is likely to have occurred.

This makes the situation easier to assess and enables a faster response. Combined with

Please turn page



Mit EchoPoint überwacht Optex große Perimeter wie Flughäfen oder Industrieanlagen und lokalisiert Eindringversuche präzise entlang der gesamten Zaunlinie



EchoPoint Frontend: Blick auf das Test-Areal

video verification, it creates a multi-stage security concept: the optical fibre provides detection, while cameras or additional sensors confirm the event. The result is a lower nuisance alarm rate (NAR), allowing response teams to be deployed more precisely.

Results and findings

The outcome of the test programme was clear: expert Markus Piendl was thoroughly satisfied.

- EchoPoint reliably detected every prepared attack scenario on both the fence-mounted and buried sensing routes.
- Pre-alarms, main alarms and tamper alarms could be monitored in real time and assigned to the corresponding events.
- The effects of configuration changes were immediately visible.

The event positions reported by EchoPoint were compared with the GPS coordinates of the test points. At the same time, video verification provided visual confirmation of each event. The conclusion was once again unequivocal: passed in full.

The connection to Milestone XProtect management software provided a clear demonstration of how detection, verification and alarm handling can be intelligently combined, with EchoPoint as the central component.


Test: Glass fiber optic splicing splice on the fence


Test: Recessed floor sensors



Independent Expert Assessment

Recommendation for EchoPoint

According to Markus Piendl, Optex EchoPoint passed every test scenario with distinction. The test site itself also made a strong impression, as did the practical installation of the EchoPoint technology and the opportunity to conduct bespoke attack scenarios under realistic conditions. His full verdict:

"EchoPoint responded to every attack scenario tested in a consistent and reliable manner. It was particularly helpful to be able to track pre-alarms, main alarms and tamper alarms in real time, and to compare the reported event positions with the GPS coordinates of the test points. Flexible installation on a fence, underground or as a hybrid solution opens up a wide range of applications across extensive perimeters and offers clear infrastructure benefits. Combined with video verification and video management, the result was a complete and practical alarm-handling process. My final conclusion is clear: I can recommend EchoPoint without reservation for perimeter protection projects."

Value beyond the test

Rick Wakeham, Senior Technology Manager EMEA at Optex and also a witness to the independent test, endorsed Piendl's assessment of the robustness of fibre-optic detection for extensive perimeters and the continuous monitoring of large protection zones.

"At a time when extreme weather events are becoming more frequent, issues such as lightning and surge protection are gaining in importance. Owing to their physical construction, fibre-optic systems offer decisive advantages here over conventional sensor solutions."

The testing also produced a useful potential benefit for Optex customers. Wakeham was particularly interested in Piendl's proposal that artificial intelligence could in future be used to analyse log files automatically. The aim could be to help installers optimise system configuration and troubleshoot faults as early as the commissioning stage.

Piendl's suggestion that architects and specialist planners should be made aware of the possibilities of fibre-optic buried detection at an early stage was also met with interest and approval.

Piendl commented: "For sites and areas requiring protection, it is important for this technology to be considered during the planning phase, so that it can deliver an additional security benefit." GIT

The Test Programme for EchoPoint

Both the fence-mounted and buried configurations were tested in practice. The trials were repeated in dry, cloudless weather at 28 °C and in moderate wind. The programme covered the following points:

Fence detection

- Sensor installation and project design
- Configuration of detection zones
- Climbing over the fence
- Positioning a ladder against the fence, including the use of a blanket as a damping layer
- Forcing open and cutting through the fence mesh
- Assessment of alarm performance

PASSED IN FULL

Buried detection

- Walking along the monitored route
- Running within the detection area
- Crawling within the detection area
- Rolling through the detection area
- Adjusting sensitivity
- Analysis of pre-alarms and main alarms
- Assessment of location accuracy

PASSED IN FULL

System integration

- Live display of sensor data
- Video verification
- Alarm handling
- Integration with Milestone XProtect
- Comparison of reported event positions with the GPS coordinates of the test points

PASSED IN FULL

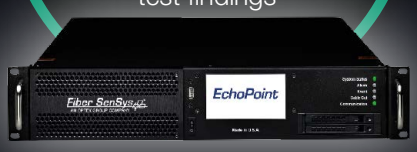
Optex
www.optex-europe.com

Sachverständigenbüro Markus Piendl
www.markuspiendl.com

Coming soon in GIT SECURITY

EchoPoint
The Proven Performer

Features, benefits and test findings





Stadler Systec, an integrator, is a long-standing partner of Eizo

© Stadler

DISPLAYS

On Screen Partners

24/7 Secure Control Centers: Eizo Monitors in Continuous Use at Stadler Systec

Stadler Systec specializes in turnkey technology integration for high-availability control rooms, providing a one-stop solution. The company has found a long-term partner in Eizo.

Monitors are an essential part of daily operations in control centers for critical infrastructure. They must not only deliver outstanding image quality but also function reliably for many years – and usually around the clock. For the owner-managed company Stadler Systec, which specializes in turnkey technology integration for control centers, control rooms, and monitoring stations, choosing the right monitor manufacturer is therefore a strategic decision. Key factors in this decision include both the technical performance of the products and a reliable, long-term partnership.

Technology, Quality, and Reliability

"In the project business, what matters most to us is quick availability, reliability, support, and product quality. Eizo delivers on all these points. You can tell that the products are designed for demanding environments. The long warranties on many models are a clear sign that the manufacturer is confident in its quality," says Markus Stadler, CEO of Stadler Systec. "Reliable support and on-time delivery are extremely important to us in the project business. With Eizo, we experience support that is reliable and where you can actually reach someone. This direct, friendly, and committed collaboration is a real plus, especially when you need a quick, clean solution in the middle of an ongoing project," Stadler continued.

Stadler Systec has previously completed major office projects, also in the banking sector where Eizo was already a well-established name. With a stronger focus on control centers and control rooms – environments where technology must function continuously and downtime is not an option – it made sense to rely on a brand that has already proven itself time and again in practice. The partnership has now been in place for over ten years.



© Eizo

Systec usually mounts the monitors on its proprietary monitor mounting arm system

Added Value in Project Business

From a sales perspective, the added value of the partnership is particularly evident in specific project work: "We have already used Eizo monitors in numerous projects across a wide range of industries – such as the chemical industry, grid control centers, traffic control centers, and amusement parks," reports David Mrnak, sales manager at Stadler Systec.

"We primarily use 24-inch models such as the EV2400R, EV2456, and EV2460, but also larger displays like the EV2760 (27 inches)

EV3895 38“ Ultrawide Monitor

The curved ultrawide monitor with 3840 x 1600 pixels gives almost three times the resolution of a Full HD monitor:

- 24:10 format
- 3840x1600 pixels (111 ppi)
- USB-C with display port signal channel, LAN
- KVM switch and picture-by-picture
- 5 year guarantee incl. on-site exchange service



or EV3895 (37.5 inches, ultrawide). It is crucial for us as a systems integrator that we can rely on long-term product availability, replacement parts, and consistently excellent support – from quick quote generation and expert technical advice to reliable after-sales service. That is exactly what makes Eizo so valuable to us and our customers.”

Bulk Packaging

“We mount the monitors on our proprietary monitor mounting arm system in nearly all of our projects. This allows us to create customized desk and monitor configurations,” explains David Mrnak. “We do not need traditional stands for this. Bulk packaging without stands is therefore ideal for us, especially since the requirements in an office environment differ significantly from those in a mission-critical control room.”

A Look into the Future

“Ergonomics and image quality remain key factors, as do long-term availability and spare parts support. Standard monitors are still a very good choice for many applications,” explains David Mrnak. “Depending on the use case, however, curved models may also be worth considering, provided that the format is suitable for both the application and the technical components used for signal transmission.

Which monitor solutions will be preferred in the future depends heavily on the industry and the customer’s requirements. It is also conceivable that larger display sizes will see increasing use, provided the technology operates reliably and the customer is willing to cover the associated additional costs. Although 24-inch models continue to dominate the market at present, there is a growing willingness to invest in larger sizes, such as 27 or 32 inches, for greater comfort and a better overview. Ultrawide monitors are also becoming attractive in scenarios where versatile applications have many uses.” GIT

Eizo Europe
www.eizoglobal.com

XTR2

STILL CARRYING TWO TESTERS?

There is a simpler way. Smoke and heat testing in one tool.

Watch how XTR2 works

detectortesters

security essen 26 Stand No. 7:F17





Dr. Jens Hartmann of Advancis (right) during the talk on the podcast "SecureLeader" with Dr. Timo Gimbel and Steffen Ebert from the GIT SECURITY team (left).

PHYSICAL SECURITY MANAGEMENT

The Way of Integration

Software Solutions for Physical Security: SecureLeader Talk with Dr. Jens Hartmann, VP Sales, Advancis

GIT SECURITY: Mr. Hartmann, how do you assess current market trends – and how is Advancis positioning itself strategically?

Jens Hartmann: If we look at the macroeconomic situation, the German economy is not exactly running smoothly right now. But things look different in the security industry. We are getting a boost from regulations like KRITIS and NIS2. Today, investments are no longer justified solely on technical grounds, but rather based on risk, availability, operability, and cost-effectiveness. And in our niche – risk management, integration, and process mapping – we are seeing sustainable global growth of around fifteen percent per year. This reinforces our commitment to continue investing.

Two years ago, we brought a minority investor on board to accelerate our international growth. At the same time, our global presence provides us with many insights from other markets. In the U.S. and Asia, for example, we are seeing much faster adoption of cloud technology and AI. The German market is more conservative – often for good reason – but we are incorporating these trends into our product development in a controlled manner. This ensures that we remain competitive internationally while also meeting the requirements of the German market. Our experience from over 2,800 control center systems implemented worldwide helps us to address these requirements in a very practical way – across industries, regions, and project sizes.

Many operators are struggling with heterogeneous legacy systems and increasing regulatory requirements. Where do you see the biggest challenges – and how does Advancis help?

Jens Hartmann: The core technologies – fire, intrusion, video, and access – are widely available and of a high standard. But uncontrolled growth and complexity have set in over the years: multiple fire alarm systems, multiple intrusion systems, different manufacturers, and various operator stations. At some point, the question arises: is this still manageable? Simultaneously, regulatory requirements are bringing security much more into the spotlight for some companies. It is no longer about a single location, but about clusters – entire corporate landscapes. The number of systems I have to manage in the event of an incident is increasing dramatically.

The first step toward solving this challenge is integration: I need to make everything visible centrally. This is exactly where our software solutions, WinGuard and AIM, come in. But integration alone is not enough; companies need a map of their security processes. What happens in the event of an incident? Who makes the decisions? Who takes action? Who documents it? This is physical security governance – and this is precisely where our guided workflows deliver added value that goes beyond mere technical integration.

When integration and process mapping come together, they create transparency, quality, and speed. Workflows, decisions, and actions are documented in a traceable manner. This simultaneously establishes a robust foundation for regulatory compliance.

Internationally, we see similar challenges, just framed differently. In Southeast Asia, they talk about 'Smart Cities'; in the Middle East, 'Safe Cities'. But ultimately, it always comes down to high security requirements and high integration complexity. Our products work globally – we address the 'last mile' – that is, engagement, local specifics, and project implementation – through our own staff in the regions, in collaboration with our global partner network.

Which technological developments are you currently driving forward in particular – and what role do API architectures, AI, and cybersecurity play?

Jens Hartmann: WinGuard is our strong, standard product, but we wanted more flexibility, more speed, and the opportunity to explore new business models for ourselves and our partners. That is why we have opened up our core software and created

a standardized API – the Advancis Open Platform, or AOP for short. This allows development partners, system integrators, and even end customers to extend WinGuard: build their own interfaces, develop their own applications, and implement custom integrations. We currently have 550 interfaces and develop 20 to 30 new ones ourselves every year – but with AOP, we can multiply the size of the ecosystem.

Of course, the question of security arises. An API creates opportunities, but also risks. That is why it is technically managed, monitored, and embedded in our 'security-by-design' and 'security-by-default' approach. We have been conducting external penetration tests for years and have aligned our development processes accordingly. The EU Cyber Resilience Act confirms that this is exactly the right approach.

We are also advancing AI initiatives, and we want to support installers in project configuration – faster and with higher quality. We also want to reduce the workload for operators in control centers, especially during periods of high incident volume. But AI must not be a black box; it must remain traceable and auditable. We must be able to explain why an AI-driven recommendation is generated.

Another major topic is cloud-native technology. We are transforming our portfolio so that we can enable platform operations for many customers simultaneously. This creates speed, transparency, and new business models such as Security-as-a-Service. Our partners can focus on configuration, processes, and integration, while platform operations and security are provided by us.

Looking five years ahead – how will the market evolve, and what role will Advancis play?

Jens Hartmann: AI will be standard in control centers in five years. Processes will be AI-supported but will remain traceable and auditable. The complexity of the systems will continue to increase, and that is precisely why integration combined with process control will become even more important. Cloud-based platforms will become the norm. We will operate centrally, roll out faster, optimize more quickly, and make new features available immediately. Partners will use hybrid models – local servers for interfaces, a central platform for processes and operations.

Business models will change; usage-based models, Security-as-a-Service, flexible platforms – all of this will become a reality. Closed system ecosystems will come under increasing pressure; open, secure, and scalable platforms will become the standard. And we will position ourselves as a provider that brings together technology, processes, security, and scalability. I see an industry that is evolving rapidly, but also one that is driving positive change. AI, the cloud, automation – these are not threats, but opportunities, and we want to actively shape them. GIT

SecureLeader
The GIT Talk with the Market Leaders

Watch now:
the full interview in
our video podcast

Advancis
https://advancis.net

Engineered to Endure, Designed to Reassure

EIZO's professional solutions for video surveillance

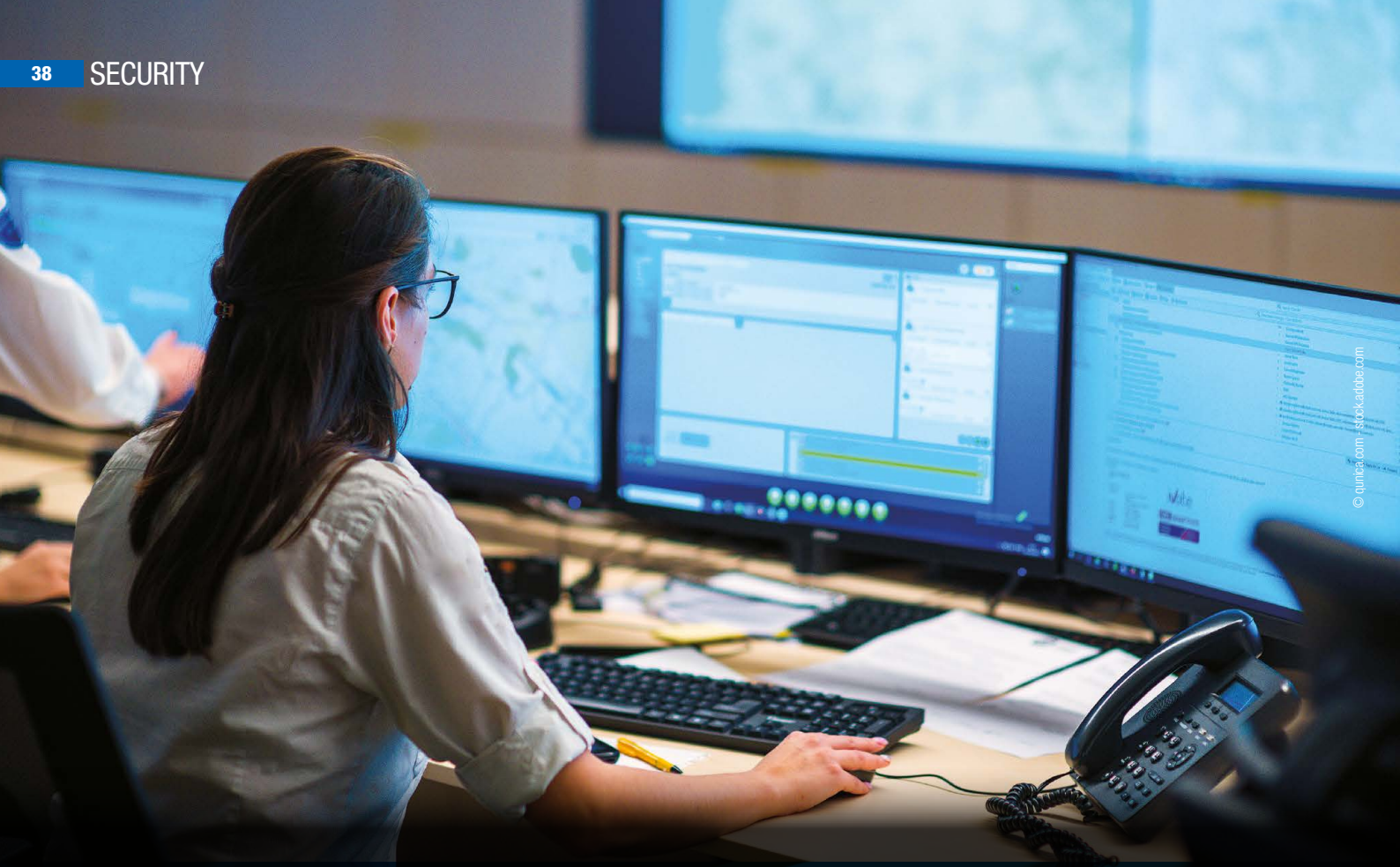
DuraVision® | VisionCore™

The right equipment for every application: Including IP decoding monitors with integrated hardware decoding, flexible installations with IP decoding or streaming gateway boxes, and image optimization systems with hardware and software solutions.



More information at
www.eizo.eu/video-surveillance

EIZO®



© qunica.com - stock.adobe.com

PHYSICAL SECURITY MANAGEMENT

From Video Data to Actionable Evidence

How Octave Coda Video 9.2 Streamlines Investigations and Security Workflows

According to research conducted by our magazine GIT SECURITY International, with version 9.2 of its Coda Video platform, Octave introduces a set of functional enhancements designed to reduce friction in daily security workflows and support more consistent investigative outcomes.

Modern security operations face growing pressure to process increasing volumes of video data while delivering fast, reliable investigative results. Video management systems therefore play a critical role not only in recording incidents but also in transforming visual information into usable evidence.

A process-oriented approach to video investigations

According to our research, Coda Video 9.2 marks an important step in the further development of the enterprise-class video management software of the Hexagon spin-off company Octave. Rather than focusing solely on individual features, the update introduces a more process-oriented perspective on investigations. At the centre of this approach is Smart Evidence Management (SEM), a concept aimed at improving how digital evidence is collected, compiled and shared across security teams.

In many security environments, small inefficiencies accumulate over time. Investigators often spend significant effort navigating video material, exporting clips and preparing evidence for internal or external stakeholders. SEM addresses these challenges by reducing unnecessary manual steps and creating a more consistent workflow, particularly for organisations handling high case volumes.

Improved evidence handling and investigative clarity

One of the core enhancements in Coda Video 9.2, as GIT SECURITY International's research shows, lies in its expanded video export and inview navigation capabilities. These functions allow operators to assemble relevant video sequences more quickly and present them in a clear, structured manner. As a result, evidence packages become easier to understand and more defensible, supporting both internal decision-making and formal investigations.

By shortening the time required to move from raw footage to usable evidence, security teams can accelerate case resolution while

maintaining consistency and traceability. This is particularly relevant in regulated environments where documentation quality and auditability are essential.

Higher display performance for demanding environments

Operational efficiency also depends heavily on system responsiveness. With version 9.2, Octave has significantly enhanced display performance in the native client. Operators can now view a greater number of video streams simultaneously and at higher resolutions without compromising stability or responsiveness.

This improvement reduces cognitive and operational strain in control rooms, where delayed or fragmented video playback can hinder situational awareness. A smoother visual experience supports quicker interpretation of events and enables more confident operational decisions in time-critical situations.

Seamless integration of multisensory camera systems

The growing use of multisensor cameras presents both opportunities and challenges for video management platforms. Coda Video 9.2 addresses this by enabling seamless integration of multisensor systems that cover large areas while preserving a high level of detail.

Such capabilities are particularly relevant for complex infrastructures such as airports, rail networks and mass transit systems. In these environments, operators require both wide-area overviews and the ability to analyse specific incidents in detail without switching between disconnected views or systems.

Advanced support for panoramic surveillance

Installations using Dallmeier Panomera cameras benefit from an expanded feature set in Coda Video 9.2. Automated stitching and lossless zoom functions allow operators to move seamlessly between overview and detail views within the same visual context.

This capability enhances situational awareness and reduces the need for manual camera switching. As a result, operators can maintain a continuous understanding of complex scenes, which is essential in environments with high pedestrian density or dynamic movement patterns.

Simplified deployment and web-based access

Beyond investigative functions, Coda Video 9.2 also introduces practical improvements for system deployment and administration. A new unified module installer simplifies installation and updates, reducing operational effort for IT and security teams. In parallel, enhancements to the Octave Coda Web Client improve accessibility and usability for browser-based access.

Together, these updates support more efficient system roll-outs and day-to-day management, particularly in distributed or multi-site security architectures.

Supporting data-driven security decisions

Taken as a whole, the enhancements in Coda Video 9.2 reflect a broader shift in physical security towards data-driven decision-making. By reducing workflow friction, improving visual performance and integrating advanced camera technologies, the platform supports a more structured and reliable investigative process.

For organisations facing increasing security complexity and accountability requirements, such capabilities help translate video data into actionable insights without adding operational burden. GIT

Octave Intelligence plc
www.octave.com

Transparent Gateway Solves Europe's High-Security Compliance Challenge



© HID Global

HID has launched the HID M1 Transparent Gateway, a security module that sits between existing Open Supervised Device Protocol (OSDP) controllers and readers to perform all cryptographic operations in a secured location. The gateway enables organizations to achieve transparent architecture compliance without the need to replace their existing physical access control infrastructure. High-security facilities across Europe increasingly face regulatory mandates requiring transparent architecture — a framework where cryptographic operations occur in physically secured locations rather than at vulnerable perimeter readers. The HID M1 sits between existing OSDP controllers and readers, handling all transparent architecture cryptographic operations independently. From the PACS software's perspective, the controller continues communicating exactly as before.

www.hidglobal.com

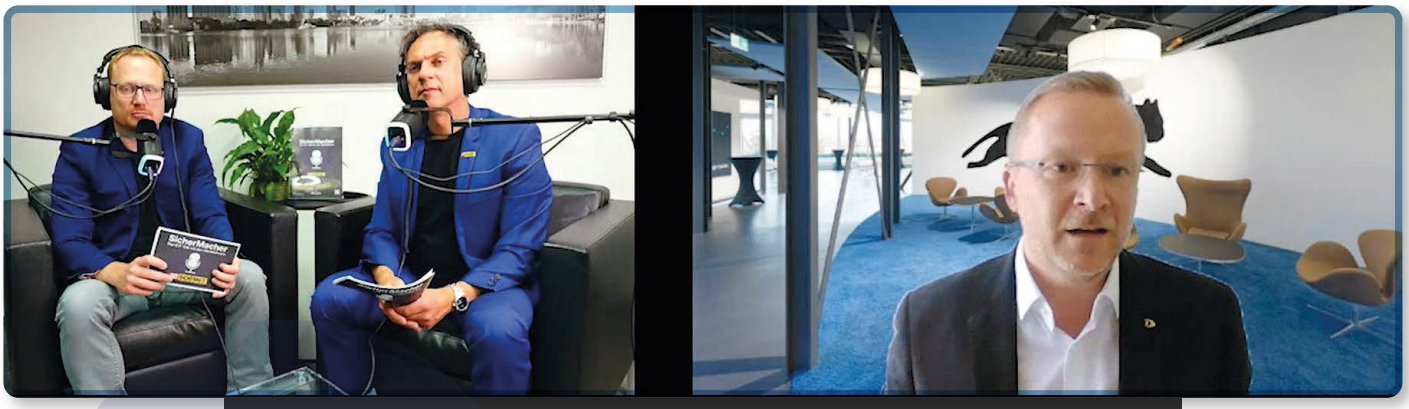
Perimeter Security Technology Integrates With Security Center

Hirsch UK has successfully integrated its advanced perimeter security technology with Genetec Security Center, giving Genetec customers a powerful new way to address complex perimeter protection challenges through a unified security platform. The integration is enabled through SecureBus integration technology, and includes support for Hirsch UK's flagship perimeter technologies, including FenceSecure PIDS, PulseSecure electric fencing, and HatchSecure hatch detection systems. The platform also supports infrared beams, fiber optic perimeter intrusion detection systems, and dual detection technology, creating a scalable and adaptable perimeter security solution for critical infrastructure, commercial estates, and high-security environments.



© Genetec

www.genetec.com



© Wiley/GIT SICHERHEIT

Christian Linthaler, CSO of Dallmeier (right), during an interview on the video podcast „SecureLeader“ with Dr. Timo Gimbel and Steffen Ebert from the GIT SECURITY (left).

VIDEO SECURITY

Looking Ahead At Video Surveillance

SecureLeader GIT Talk with Top Player Video Security: Christian Linthaler, Dallmeier CSO

GIT SECURITY meets with leading companies and thought leaders in the security industry. In this SecureLeader Talk, we speak with Christian Linthaler, CSO at Dallmeier, about current challenges and future developments.

GIT SECURITY: Mr. Linthaler, how do you assess the current market situation, and what role does security play today?

Christian Linthaler: The economic situation can currently be best described with one word: “uncertain”. Geopolitical tensions, rising costs, and significant price fluctuations for components such as server technology and hard drives make long-term calculations considerably more difficult. Planning becomes particularly challenging for projects with long lead times. At the same time, many companies are showing a certain reluctance to invest.

But in many industries, security is not the kind of expense that can be postponed at will. Demand is still high, especially where security is a prerequisite for day-to-day operations. Companies are increasingly focusing on the total lifecycle costs of a solution.

Issues such as cybersecurity, trustworthy supply chains, and European development are becoming increasingly important. ‘Made in Germany’ means not only durable hardware but also transparent development processes and consistent protection against potential security risks.

What challenges are customers most concerned with today?

Christian Linthaler: The requirements for modern video security systems have fundamentally changed: customers no longer expect just traditional video surveillance for documenting events; modern systems are expected to analyze, trigger automated alerts, and simultaneously help to optimize operational processes.

Video technology is increasingly evolving into an optical sensor that delivers valuable data for a wide variety of business areas. In logistics or industry, for example, motion and process data can be analyzed without the need to constantly view live footage. Information about customer flows, capacity utilization, or process workflows can be fed directly into analytics and business intelligence systems.

The requirements for data protection and cybersecurity are also increasing. Companies are therefore increasingly scrutinizing where products are developed, who has access to systems, and how security standards are implemented. Another challenge is the shortage of skilled workers, so security solutions must therefore not create an additional burden but must actively reduce the workload on employees.

What arises from the introduction of new regulations and legal requirements?

Christian Linthaler: We view them primarily as an opportunity. In particular, the NIS 2 Directive, the Cyber Resilience Act, the AI Act, and the KRITIS Framework Act reflect requirements that have been an integral part of product development at Dallmeier for many years. Data protection, cybersecurity, transparency, and trustworthy technology are among our core strategic principles. European manufacturers in particular can benefit from this development.

Particularly attractive growth markets include all sectors where security is directly essential to operations: airports, energy sup-

ply, transportation infrastructure, stadiums, and large-scale industrial facilities. Another growth driver is the digitization of security processes. Video is increasingly providing not just retrospective documentation, but is also becoming part of operational decisions and automated processes. The demand for trustworthy technology is growing too. Customers these days are interested not only in where a product is manufactured, but also in where research and development take place.

What technological developments will shape the coming years?

Christian Linthaler: A current trend is shifting more and more intelligence directly to the camera: instead of merely recording images, cameras are designed to analyze them independently and provide relevant information. Our Panomera V8, for example, can capture areas of up to 10,000 square meters without blind spot, thanks to its 180-degree field of view. AI-powered search functions are gaining in importance: with the so-called 'Attribute Finder', individuals can be identified based on characteristics such as the color of their outerwear, or bags.

Artificial intelligence is also becoming increasingly powerful in perimeter security: modern systems analyze not only objects but also behavioral patterns. Potential intruders often do not move openly across a site but instead crawl, roll, or camouflage themselves. Such behavior is specifically trained into the systems so that they can also detect unusual intrusion attempts. An important point here is that on-site, self-learning AI systems are not very practical. What is crucial though is high-quality training data and continuous improvements to the neural networks, which are then incorporated into the products via software updates.

Cloud solutions are playing an increasingly important role: the video data itself should continue to be stored locally, while administration, license management, and certain services are provided via secure cloud infrastructures.

What will video security look like in five years?

Christian Linthaler: The future will be shaped less by individual products and more by integrated end-to-end solutions. Cameras, recording systems, management platforms, and AI applications will work together more closely. Trust will become a decisive competitive factor too. Artificial intelligence will become ever more important – not as a replacement for humans, but as an assistance system.

Hardware performance will continue to increase, with higher resolutions, more powerful processors, and more complex analyses performed directly on the camera becoming the norm. But the challenge remains to utilize these technical capabilities in a way that is both economically viable and user-friendly. The companies that will succeed are those that can combine technological innovation with trust, quality, and long-term cost-effectiveness. GIT



SecureLeader
The GIT Talk with the Market Leaders



Watch now:
the full interview in our video podcast



Dallmeier electronic GmbH & Co KG
www.dallmeier.com

Connecting Video, Data and AI

The growing convergence of video surveillance, operational data and artificial intelligence is accelerating the transformation of physical security platforms. Against this backdrop, March Networks has introduced its 2026 Mid-Year Release, expanding AI capabilities, cloud functionality and system interoperability across its security ecosystem. The release is particularly significant as it represents the company's first major product update following the integration of Vivotek's branded business earlier this year.

The update introduces enhanced AI-powered search capabilities designed to help operators locate relevant incidents more quickly within large volumes of recorded video. New cloud video intelligence functions further extend visibility across distributed sites, while additional support for Vivotek camera technologies broadens deployment flexibility for both existing and future installations. Compatibility with C•CURE access control systems strengthens the integration between video surveillance and physical access management, supporting a more unified operational environment.

March Networks positions the release as part of its broader "Connected Intelligence for Modern Security" strategy. The concept is intended to connect video, operational data and AI-driven analytics through a common intelligence layer capable of supporting investigations, incident response and operational decision-making. Rather than simply collecting more data, the approach focuses on identifying meaningful relationships between information sources and making them accessible through integrated workflows.

According to the company, organizations increasingly face the challenge of managing fragmented security, business and operational systems. The latest release therefore emphasizes ecosystem integration, enabling cameras, access control systems, business data and third-party technologies to work together more efficiently. By combining these data streams, security teams can investigate events faster, uncover patterns that might otherwise remain hidden and improve situational awareness across multiple facilities.

Headquartered in Ottawa, Canada, March Networks specializes in intelligent video surveillance and business intelligence solutions serving sectors including banking, retail, transportation and critical infrastructure. With the additional capabilities gained through the Vivotek integration, the company aims to further expand its position in the growing market for AI-enabled, connected security platforms.

marchnetworks.com



Improved medicine management with individual access rights at the London Ambulance Service

Cover Story

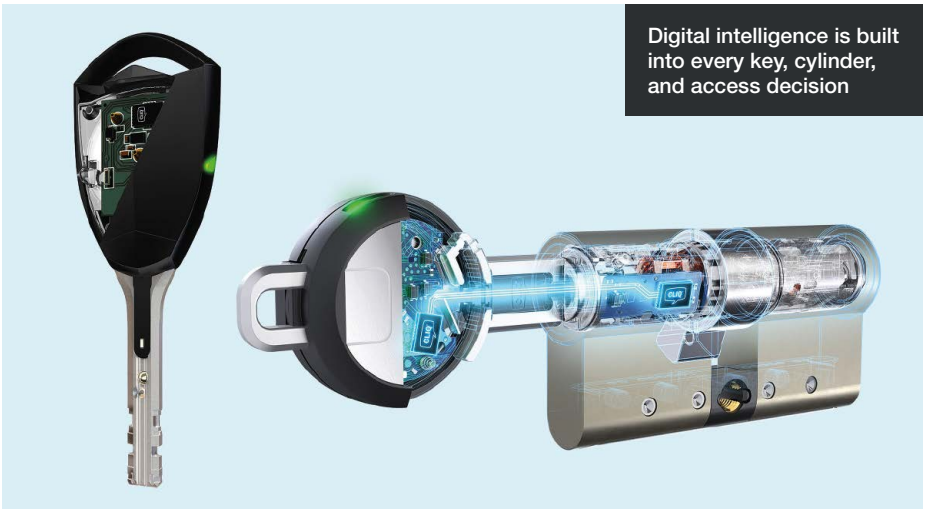
A Versatile Combination

Digital Access with the Familiarity of a Key

As organizations upscale, downsize, or onboard new locations, facility managers must more flexibly manage access control ever and frequently adapt to new situations. Increased service contracting has also handed many essential building functions over to third-party providers, rather than employees. They also need efficient building access that does not compromise security.

In addition, physical, cyber and 'hybrid' physical-cyber threats loom large, as do the regulations designed to protect critical sectors against them., They now include the EU's NIS2 guidance and Cyber Resilience Act (CRA). Compliance and the implementation of joined-up security and access management are ongoing challenges, particularly in the sectors on which NIS2 obligations fall most heavily: infrastructure, finance/banking, healthcare, energy, transport, and data centers.

Mechanical locking was not designed for such a complex, dynamic environment, yet this demanding landscape is becoming the 'new normal'. Despite these challenges, any new access or security solution must now



Digital intelligence is built into every key, cylinder, and access decision

battle for budget and justify its total cost of ownership (TCO), producing a definable return on investment (ROI) in the process.

Combining the Advantages of Keys and Digital Access

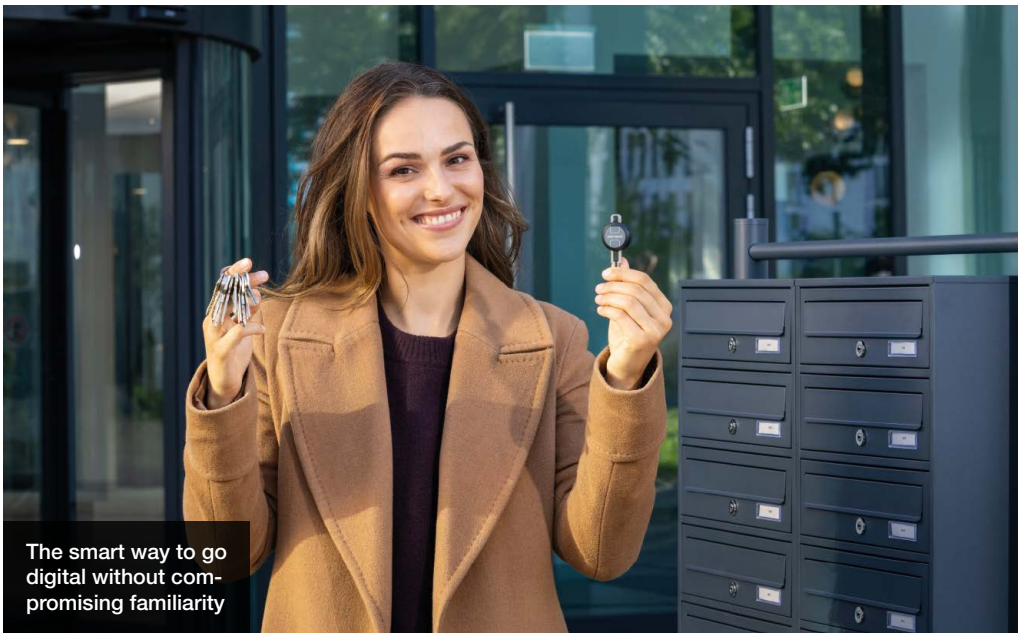
One major benefit of the mechanical key is its familiarity. A mechanical locking system with patent protection may still be an appropriate solution, but digitization offers many opportunities for business efficiency and compliance. Unlike mechanical security, a digital solution offers the ability to allocate time-based rather than blanket access authorization, and to amend it quickly and flexibly. A digital credential, such as a smart key, can be programmed or de-authorized in seconds, negating the threat posed by lost keys and the significant costs of changing cylinders and re-keying. When building technology can connect solutions for access, fire protection, and escape routes, for example, both user safety and facilities management benefit.

With a digital solution, audit capability is automated for every lock and user, benefiting compliance efforts; manual access tracking with mechanical keys is either time-consuming or, in many cases, impossible. Tracking and tracing access is one requirement of NIS2.

"Of course, moving from mechanical to digital access management is not like flicking a switch," says Frank Stier, VP & Head of PU Key-based Digital Cylinders at Assa Abloy Opening Solutions EMEIA. "Many organizations have large systems. They cannot change all at once, so digital systems must be able to scale gradually over time as budgets allow. The right programmable smart key system offers precisely this."

Choosing the Right Key-Based Digital Solution

Smart key systems are the fastest, least disruptive way to switch mechanical security for intelligent digital access. They immediately upgrade the flexibility of access management in organizations of any size or type. Electronic or electromechanical locking cylinders simply slot in place of the legacy mechanical devices, without door damage or wiring. Intuitive software and programmable digital keys give facility management teams granular control over the movements of staff and contractors. Some solutions allow security managers to administer mechanical and digital access within the same system.



The smart way to go digital without compromising familiarity

One smart key option is Assa Abloy's Cliq, which simplifies the granting, personalization, and management of access rights. Because this system logs every access event, audit trails are generated with a few clicks in the software control panel – streamlining compliance obligations with the latest generation of regulations. The product ecosystem includes more than sixty different cylinder and padlock types, ensuring almost any need can be met.

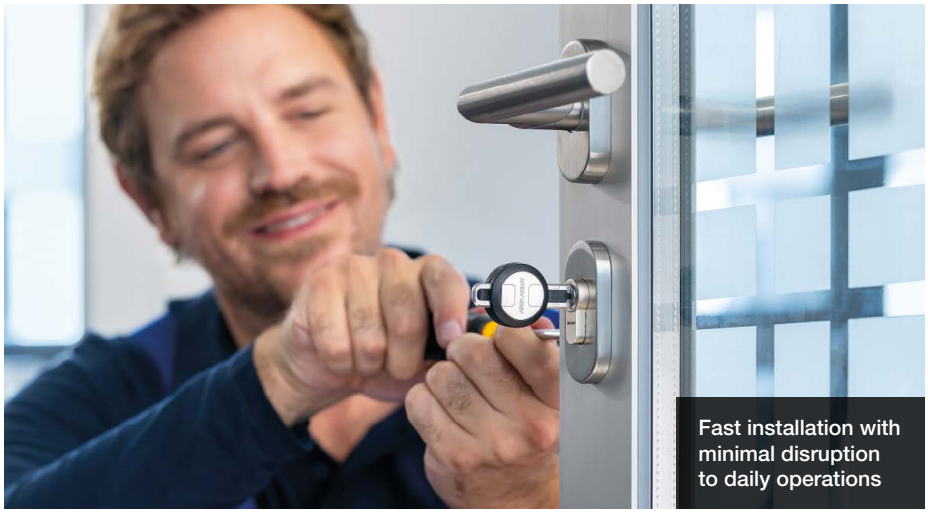
"We offer two versions within the Cliq family to meet varying individual situations," explains Stier. "Fully electronic eCliq offers maximum digital flexibility with a single mechanical profile and electronic coding. Cylinders meet the highest VdS requirement and operate maintenance-free. Electromechanical Protec^2 Cliq adds multiple mechanical profiles on top of the electronic coding, with the option to manage mechanical cylinders in the same unified system and/or develop custom-made locks for specific applications. These two versions are also interoperable with the same software."

Adaptability, scalability, security, convenience, and trust are just some of the reasons Cliq is already adopted in many of the most demanding access management environments for access management.

Remote Digital Management Anywhere in the World

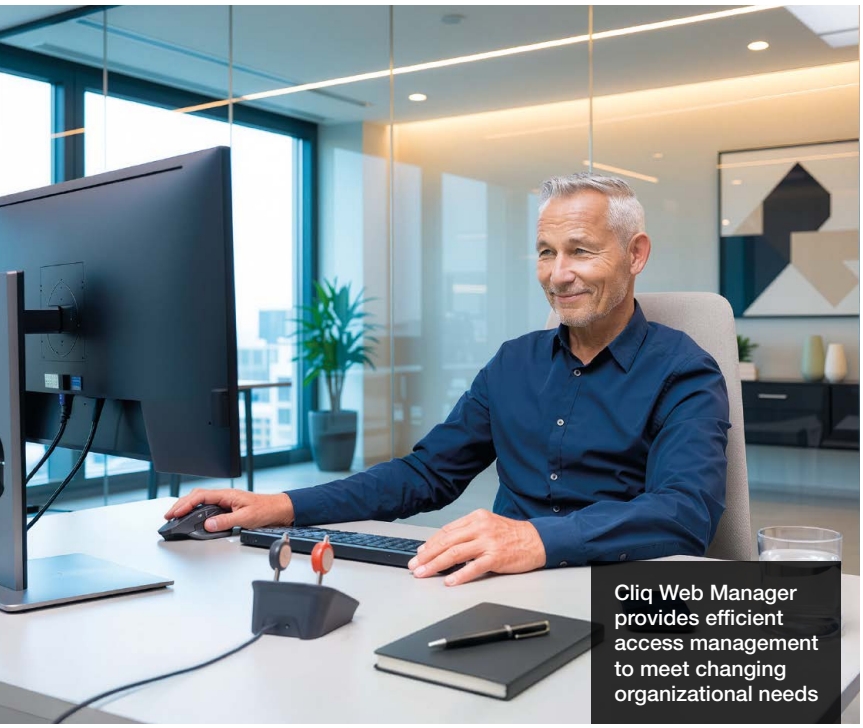
Founded in 2016, Orca Industriemontagen is a global industrial assembly and relocation services business with a high level of technical expertise. From planning to transport and final installation, Orca supports machine system assembly across industrial sectors, with a focus on food and pharmaceuticals. In addition to new installations, they offer secure relocation for used systems. Orca's experts and equipment are always on the move,. So they sought an access solution to ensure the security of multiple opening types of doorway across internationally distributed sites, as well as transport to/from and containers at these locations*.

Orca chose eCliq for intelligent digital key access with cloud-based management. Their needs were met by a combination of robust, reliable, wireless cylinders for almost any application,; a battery-powered digital key;, intuitive, cloud-based management;, and the convenient option to update users' access permissions remotely using the Cliq Connect smartphone app.



Fast installation with minimal disruption to daily operations

Please turn page



Cliq Web Manager provides efficient access management to meet changing organizational needs



eCliq and Protec² Cliq deliver the right level of security for every application

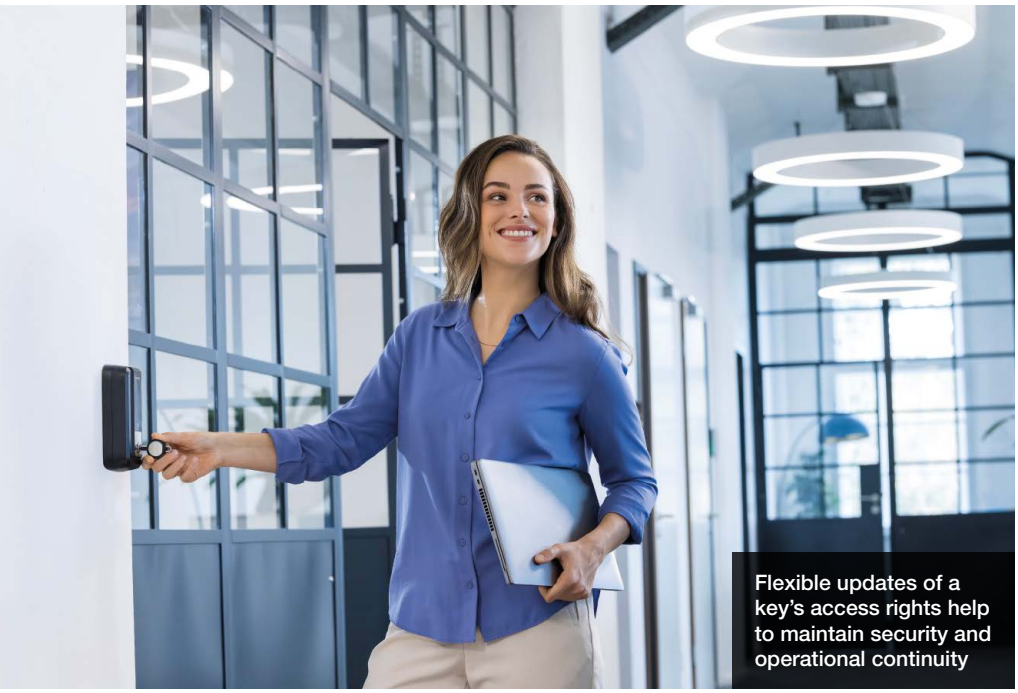
Employees now carry a single, digital eCliq key that is individually programmed only with just their relevant, time-limited access authorizations. When the management team in Germany approves access to a cylinder via the software, this authorization can be transmitted to the user's key in the app via Bluetooth – wherever s/he is in the world. System installation was equally simple: only a screwdriver was required to mount wireless cylinders at new or existing entrances and exits.

"The key advantage for us is the worldwide functionality and the ease of use. This is an enormous benefit in terms of security and convenience for people and materials," says Jochen Busch, Orca Industriemontagen's owner.

Protecting Medicines on the Move

Well -governed management of access to controlled drugs is always essential, especially with the urgent nature of care provided by the London Ambulance Service. The trust required a versatile and easy-to-use access control system, with multiple permission and skill levels across multiple locations**. As Gavin Mooney, Advanced Paramedic Practitioner and Trust Medication Safety Officer, explains: "Our previous access control system was not meeting our needs, as we had insufficient oversight of who had access to particular lockers or codes for the keys. We had to find a way in which paramedics could get access to drugs over a large geographical area, but we also needed to ensure the system was compliant, with auditability for security purposes."

With Protec² Cliq, each member of staff now carries an individual key, that can be activated via a wall panel or computer programming device at the start of a shift, giving access to areas and assets in accordance with their clearance. Over 4,000 keys were issued to London Ambulance Service paramedics, giving traceable access to drug cabinets at multiple stations across the whole estate. Cliq devices fit alongside and help to evolve their existing solution, giving the capability to manage a large estate by enabling new permissions or decommissioning a key instantaneously to ensure that keys cannot be used inappropriately.



Flexible updates of a key's access rights help to maintain security and operational continuity

* www.assaabloy.com/group/emeia/stories/customer-cases/orca
** www.abloy.com/global/en/securing-greatness/london-ambulance-service

To learn more about the costs and benefits of upgrading to smart key access, download a free Assa Abloy white paper ▶

Assa Abloy Opening Solutions
www.assaabloy.com

© Images: Assa Abloy Opening Solutions



SoFi Stadium Unifies Security Across 300-Acre Campus

Over time, the existing, siloed security systems at SoFi Stadium and Hollywood Park became harder to manage and couldn't scale easily. Managing digital evidence also involved slow, manual processes with limited accountability and cybersecurity safeguards. So IT and security agreed it was time for a physical security upgrade. Genetec Security Center now provides an easy-to-use platform to manage video, access control, and all other systems, with built-in tools that help speed up investigations and incident response. Every user interaction is automatically logged in the system with audit trails, and hundreds of full-time and thousands of part-time event staff automatically receive cardholder permissions based on their roles. **www.genetec.com**

TDSi by Hirsch Releases GARDiS Version 3.3

Integrated access control and security manufacturer TDSi by Hirsch has released GARDiS version 3.3, a major update for its access control software. Key additions include Ajax Cloud intruder integration, basic intruder panel connection on the GARDiS controller, simplified credential types, and enhancements to security controls and data governance. The integration allows hubs, devices and groups to be discovered and viewed within GARDiS, allowing authorized users to see status changes as they happen and to arm, disarm or manage bypass settings without moving between separate systems. Intruder panels, zones and groups can also be used within cause and effect rules, helping routine responses happen consistently and reducing the need for manual intervention. **www.tdsi.co.uk**

AI-Powered Video Intelligence for Converged Security

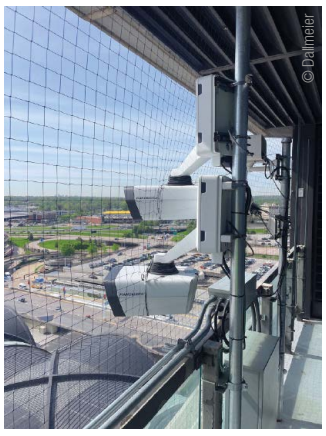
Primion and Iveda have entered into a new partnership and are making the Prime Video Intelligence solution available worldwide as a standalone application. In the long term, the companies plan to integrate the technology natively into Primion's converged security ecosystem. The solution enables companies to integrate additional layers of intelligence without having to replace existing systems. It takes data protection and compliance requirements into account and supports customers in critical environments as they continue to expand their security infrastructure. Prime Video Intelligence adds a new layer that makes security more adaptive, responsive and contextual. Operators can create custom detections using natural language, without model training or deployment delays. **www.primion.eu**

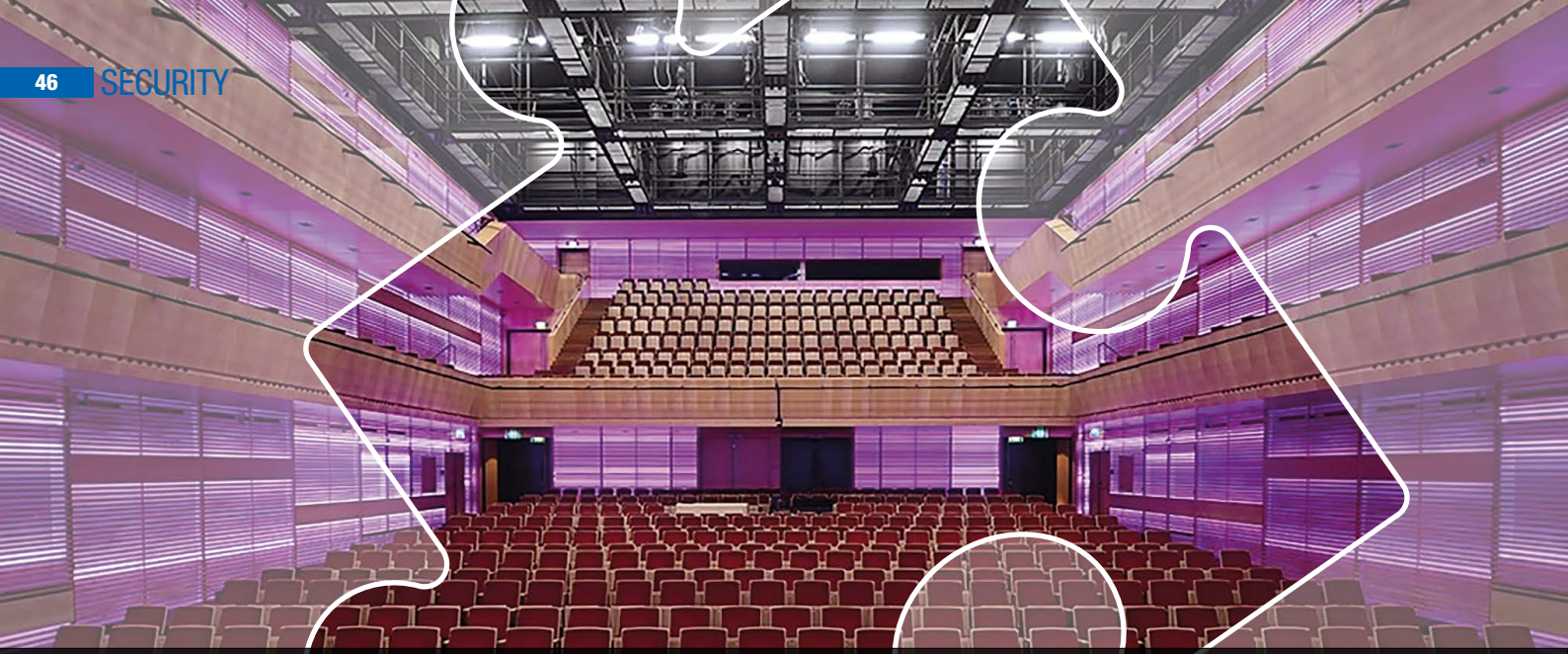
Important Draft Standard for Cloud-Based Video Surveillance

ONVIF, whose open standards make IP-based physical security products interoperable worldwide, has introduced the Release Candidate for ONVIF Profile V, a draft standard for cloud-based video surveillance. Profile V extends the ONVIF brand-independent approach to the cloud, giving system integrators, consultants and end users a way to build cloud video systems that are not tied to a single vendor. Profile V enables a conformant cloud-based video management system (VMS) to reach cameras behind a local firewall, typically without port forwarding or VPN configuration. The conformant device makes a secure outbound connection to the cloud VMS, then streams live video and, if applicable, audio over WebRTC to an ONVIF client or an authorized standard web client. The device can also send event notifications to the cloud VMS to take action. Video and audio are encrypted before they are pushed to cloud storage, such as Amazon S3 or Microsoft Azure Blob Storage. Profile V can be combined with other ONVIF video and access control profiles for integrated or hybrid systems. Profile V conformant products must implement the ONVIF Profile V Security Add-on, which covers two areas: it uses the OAuth 2.0 framework so that only authorized devices, clients and cloud services can connect and exchange data, and it encrypts recordings on their way to storage. ONVIF placed these requirements in an add-on instead of the profile itself because an add-on can be updated to keep pace with evolving security requirements without rewriting the full Profile V specification. The draft Profile V specification is available now for review by ONVIF members, and ONVIF expects to finalize it by the end of the year. **www.onvif.org**

STL Airport Deploys 360 ° Surveillance Using Panomera

Using Dallmeier's Panomera multifocal sensor technology, St. Louis Lambert International Airport (STL) has achieved comprehensive high-resolution coverage with approximately 90 % fewer cameras and 75 % less infrastructure compared to the original surveillance design. To date, STL has installed more than 27 Panomera cameras, multiple IPS 10000 recording appliances and five user workstations with the client software to complete the video system. Using only ten cameras, the airport achieves comprehensive situational awareness across the large airside areas including runways, taxiways and apron operations. As part of a planned deployment in the ticketing area, a Panomera V8 system will support AI-based video analysis functions such as passenger flow and waiting time analysis. **www.dallmeier.com**





ACCESS CONTROL

Solving a Puzzle at Muziekgebouw

How an Electronic Locking System Now Provides Security at a Concert Venue

Behind the scenes at Amsterdam's famed concert hall, a synchronized change was underway. Managing access had become increasingly complicated, but a smarter, more flexible approach was ready to take the stage.

For many years, the Muziekgebouw and Bimhuis have been the cultural and musical heart of the IJ waterfront in Amsterdam. With multiple tenants and many changing users – all with individual access rights – implementing a safe and user-friendly access control plan for the complex is a challenging task. Working in partnership with Dom Netherlands, the Foundation for the Management of the Muziekgebouw/Bimhuis Facilities found a secure, flexible, and user-friendly solution.



(l to r) Melvin de Wever and Leo Kruse

The landmark venue had been using an electronic access control system for quite some time. "Two years ago, the supplier announced that the system would soon no longer be supported or sold. That prompted us to look for an alternative solution," says Leo Kruse, Technical Manager from the Foundation for the Management of the Muziekgebouw/Bimhuis (BAMB).

An Access Control Wish List

Before exploring the market, Leo and his colleagues first created a wish list. "For that, we mainly looked at the system we were using and thought about what could be improved or simplified. We wanted more flexibility in assigning access rights. Under the old system, the supplier managed all access rights and could see who had what access. We barely had an overview, which made access management chaotic. We wanted to handle everything ourselves to be more flexible and have optimal control."

Programming changes was also challenging with the old system, Leo explains. "After a change, we had to manually visit all doors to update the locks with new access rights. That took a lot of time."

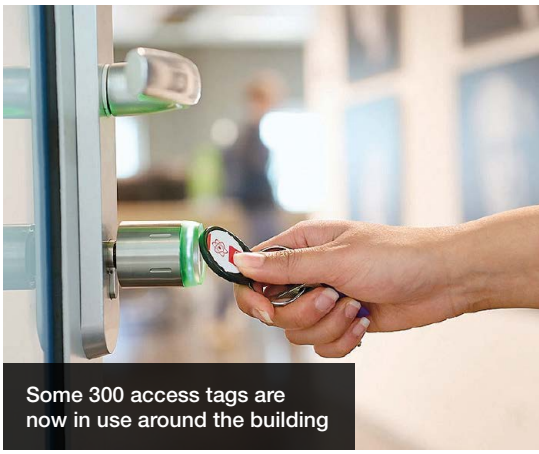
The Tech Rehearsal

After determining their requirements, and the conditions for the new access control system, Leo contacted Melvin de Wever, Account Manager at Dom Netherlands. "For such a complex and multifunctional building, our digital Dom Eniq system offers a safe and flexible solution. We could meet all the requirements with Dom Eniq," says Melvin.

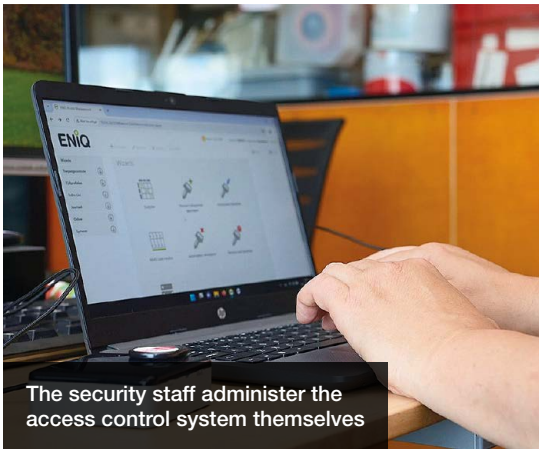
It was decided to test the system with demonstration units for two months, which were placed in the workspace used by Leo and his maintenance team. "Thanks to these demo units, we could experience how electronic locking works using the electronic



The Dom Eniq range



Some 300 access tags are now in use around the building



The security staff administer the access control system themselves

door fittings. We also gained hands-on experience assigning access rights to tags for staff and users during this period," says Leo.

A Seamless Second Act

The test period led to ongoing collaboration; the interior doors of the Muziekgebouw are now equipped with the digital Dom Eniq Guard door fittings. Installation was made easier by choosing the Wideline variant with a wide front plate. As Leo explains, "Many doors used fittings with rosettes, but the wide front plate of the Dom Eniq Guard door fittings allowed us to cover those holes easily. Additionally, the sleek design of the fittings provides an aesthetic finish, enhancing the appearance of the doors."

With an outer shell of the building open for most of the day, security and access control remain essential. Only at night are the two revolving doors of the main entrance locked. To prevent unauthorized access to spaces or offices during the day or evening, the management foundation has installed electronic Dom Eniq Guard or Eniq cylinder locks on all doors.

Self-Managed Access Control

Assigning and managing access rights is now handled directly by Muziekgebouw staff. "This allows us to respond quickly when necessary. That's important for a multifunctional building like ours," says Leo as he considers the challenges. "The building has elevators shared by various users, each only allowed access to their designated areas. The offices, occupied by different tenants across three floors, are in a separate wing. Employees using one area don't have rights to other floors. If they occasionally need access elsewhere, it can be adjusted quickly and easily."

Melvin adds, "With this data-on-card setup, access rights are stored on the tag. By placing the tag near an update point, any newly assigned rights are automatically updated on the tag." This flexibility is also essential for granting temporary access, such as allowing an artist's technician limited access to a control room.

Data Stored Locally

After a brief adjustment period, Leo and his team now experience only advantages with the switch. "The software we use to manage access rights is very user-friendly. Compared to the previous system, this is a huge improvement for us. We now have over 300 tags in circulation across different user groups, but it remains easy to manage. Additionally, we find the price-quality ratio very favorable."

The software data and tag access rights are stored locally on a server. As Melvin explains, "This is a stand-alone solution, where all data is stored on a local server. Backups are also stored locally. This ensures that, in this case, BAMB always owns and controls its data. None of this data is shared with us." GIT

Dom Security
www.dom-security.com

© Images: Dom Security

QR Codes Replace Traditional Intercoms

Visitor management continues to evolve as organizations look for more flexible and cloud-based access solutions. ProdataKey (PDK) has expanded its platform through a new integration with Entrio, a cloud-based intercom solution.

Instead of relying on traditional intercom hardware, visitors scan a QR code with their smartphone to initiate communication with a resident, employee or security operator. Once identity verification is completed, authorized users can remotely grant access to PDK-controlled doors.

The integrated solution is designed for commercial buildings, residential properties and distributed facilities seeking a modern, software-driven approach to managing visitor access. According to the companies, the platform can be deployed without additional intercom hardware while maintaining encrypted cloud-to-cloud communication. **www.prodatakey.com · www.entrioai.com**



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



From safety footwear to lifestyle products—Elten's new retro models are indistinguishable from classic sneakers, yet offer safety in protection classes S1 and S1PS

Hendrik van Elten belongs to the fifth generation of the van Elten family. Since January 2025, he has been actively involved in the further development of the company, working closely with his father Heiner van Elten. He is expected to follow in his footsteps and take over the management of the company in mid-2027

SAFETY SHOES

"Stay Courageous Without Becoming Reckless"

Generation change at Elten: Hendrik van Elten on growth, the brand and new requirements for safety shoes

Elten is about to enter a new chapter with the arrival of the fifth generation. In this interview, Hendrik van Elten talks about the generational change in the family business, international growth strategies and the need to preserve tradition, corporate culture and courage. The focus is also on changing requirements for safety shoes, stronger brand positioning and the role of digitalization and AI in the further development of processes and products.

Hendrik van Elten belongs to the fifth generation of the van Elten family. Since January 2025, he has been actively involved in the further development of the company, working closely with his father Heiner van Elten. He is expected to follow in his footsteps and take over the management of the company in mid-2027.

GIT SICHERHEIT: Mr. van Elten, you are joining your economically very successful family business. Do you see this as a tailwind or as a pressure of expectation to further expand?

Hendrik van Elten: A strong economic basis creates expectations, but also opportunities to try things out. I see it more as an incentive and a great opportunity. It gives us the opportunity to develop Elten from a national to a European market leader. My grandfather sold the majority of our products to the coal and steel industry in NRW. My father sold to various industries such as automotive and logistics in Germany. Now we want to

diversify even further, even beyond Europe. With a stable foundation behind us, I see this as more of a tailwind than pressure. I want to remain courageous in this process without becoming reckless.

How have you experienced the generational change so far – and what has been the biggest challenge for you personally in this process?

Hendrik van Elten: The collaboration works very well and harmoniously. We learn from each other, give each other new ideas and have positive discussions about changes. My father and I work very well together. After all, I see it as the task of a family business to build on the success of previous generations. If my father can still see himself in the company's direction in a few years' time, then I consider the generational change to be a success. I see the biggest challenge as gaining the trust of the employees. But I think I'm on the right track. If the team that has been responsible for the development of our company to date continues to follow the path in the future and sees itself reflected in it, I see that as a great endorsement.



From Uedem in the Lower Rhine region into the world – Hendrik van Elten wants to expand the family business from German to European market leader and even grow beyond European borders

Before joining Elten, you worked for four years at the start-up Flink, among others. What impulses from this time are you now bringing to a company steeped in tradition?

Hendrik van Elten: I learned how important it is to regularly question and optimize company processes in order to react to market changes. But I also saw in the start-up what I don't want here: high staff turnover. After four years at Flink, I was one of the employees who had been with the company the longest. At Elten, on the other hand, many employees stay with us for their entire working lives and beyond. In some cases, they bring the next generation into the company. I definitely want to maintain this culture.

Where do you see the greatest growth potential for safety shoes "Made by Elten"?

Hendrik van Elten: The Scandinavian market is particularly interesting for us, and we are expanding our sales team there. We are also more active in the UK than we were a few years ago. I also see potential for further growth beyond European borders. We have been working exclusively with a trading partner in Australia for several years now. I also find the Asia-Pacific region exciting. There are markets there that have growth potential and now also a price level that fits. And who knows, maybe even the US market will become interesting again in four years' time.

We must always keep an eye on industry trends and adapt our portfolio accordingly. Internationalization alone presents us with new challenges. Even in the UK, the customer imagines a different safety shoe than in Germany.

Who are the main customers for your products today – and how have their requirements evolved?

Hendrik van Elten: One of the most important sectors is the logistics and service industry. But we also want to focus more on areas such as the defense industry and technical services. The technical trade remains our main customer. It is the touchpoint and interface for the end customer. The product



The lightweight Tavixx XXFE lime-blue Low ESD S1 model weighs less than 400 grams

please turn page ▶



With its foot protection solutions and technological innovations, Elten aims to expand its international presence even further in the future. The Renzo Biomex GTX Boa blue Mid ESD S3 model shown here helps prevent ankle sprains.

portfolio combined with the expertise of the trade is crucial for us and our customers. At the same time, large companies often need complete supply concepts, which is why the exchange in the key account has become more important. Selling directly to end customers via our online store is also a sales channel that must be used nowadays.

I see three major trends in terms of requirements. Firstly: more individuality, for example through orthopaedic insole systems or multiple widths. For some years now, we have been offering 3D foot measurement, including orthopaedic advice, in order to be able to react to foot misalignments. This counteracts the wearer‘s problems, but also reduces absenteeism.

The second trend is the blending of leisure and work shoes. Many of our customers walk several kilometers a day. Lightness and comfort are the most important factors here. And design, because safety footwear is increasingly becoming a lifestyle product. That‘s why we use materials that are also used in running shoes, such as the cushioning materials Super Critical Foaming or Infinergy from BASF.

Finally, we are also focusing on cost reduction for our customers. It is our job to respond to the customer in the best possible way. I am sure that the longevity of the shoes and low employee downtime ultimately make the biggest contribution to sustainable cost reduction.

What added value do you expect from the use of AI in process optimization?

Hendrik van Elten : AI plays a role above all in areas where we can automate repetitive tasks – less in production and more in administration and sales. It helps to identify needs earlier, personalize consultations and simplify data analyses. We can then use the time saved for valuable interactions with our business partners. In addition, existing staff can specialize more and thus create additional added value for customers. In this way, we can also give employees the opportunity to develop further and play an active role in shaping the path to internationalization

One of their central concerns is to establish Elten more strongly as a brand. The aim is also to make the products more recognizable. What does that mean in concrete terms?

Hendrik van Elten: For me, this primarily means that Elten will become more clearly recognizable as a brand – both internally and externally. We want to establish a design language that makes our quality, technology and reliability visible. Our products should show at first glance what we stand for: modern safety shoes that are functional, comfortable and of high quality. To achieve this, we are sharpening our lines, working on a consistent product identity and investing in a brand world that meets the demands of modern users. Customers should choose our shoes not just because of the protection class, but because they recognize the brand and consciously choose it.

Elten can look back on over 115 years of company history. What were the company‘s most important milestones and do you think we are currently at a new turning point in its development?

Hendrik van Elten: If you look back over 115 years of company history, the most important milestones have always been the moments when we realigned ourselves. Our first leather work shoes were right at the beginning. Later, we also manufactured men‘s, women‘s and children‘s shoes for a long time before we consciously specialized in safety shoes at the end of the 1970 s.

Another moment in 2011 was the launch of the L 10 series, our first sneaker-style safety shoes. They looked like Chucks – we dared to do something that didn‘t exist on the market. We showed many people that safety shoes can not only protect, but also look good.

My grandfather supplied the majority of our shoes to the mining industry, my father later supplied them to the automotive and logistics sectors. And now we are once again at a turning point: internationalization, digitalization and demographic change are transforming our industry. We are sticking to our values of quality and reliability and our location in Uedem – but we remain flexible and courageous. If we can manage this balancing act – combining the speed of today‘s world with the diligence of a family business – then we have great opportunities. I would now like to shape this. GIT

Elten GmbH
Elten.com

© Images: Elten GmbH



SAFETY SHOES

Sports DNA Meets Workplace Safety

Adidas enters the industrial safety footwear market with a new range designed for logistics, manufacturing and transportation professionals

The boundaries between sports performance and occupational safety footwear continue to blur. With the launch of Adidas Pro Work, adidas and licensing partner GLO Brands are introducing a new safety footwear range that brings the design language, comfort philosophy and brand recognition of one of the world's best-known sports companies into industrial working environments. The collection has been developed specifically for sectors such as logistics, manufacturing, warehousing and transportation, where employees often spend long hours on their feet and increasingly expect more from their protective footwear than compliance alone.

A New Generation of Safety Footwear

According to the companies, the new range combines certified workplace protection with ergonomic performance and modern styling. The launch reflects a broader industry trend: today's workforce demands footwear that delivers comfort, cushioning and flexibility while still meeting the protection requirements of industrial environments. As a result, safety shoes are increasingly inspired by athletic footwear technologies and contemporary design principles.

For employers, the focus extends beyond compliance. Comfortable footwear can contribute to wearer acceptance, helping ensure that employees consistently use the protective equipment provided. Lightweight construction, improved fit and modern aesthetics have therefore become important purchasing criteria alongside traditional features such as toe protection, durability and slip resistance.

Performance and Protection

The new Adidas Pro Work line has been engineered to meet the evolving needs of industrial workers while maintaining the unmistakable look and feel associated with the adidas brand. By combining certified protection with a sports-inspired approach to comfort and design, the collection aims to support workers throughout long shifts in demanding environments.

The launch also highlights how significantly the industrial PPE market is changing. Once viewed purely as functional equipment, safety footwear is increasingly becoming part of a broader strategy focused on employee wellbeing, productivity and user acceptance. The arrival of a global sports brand in this segment underlines the growing importance of comfort, ergonomics and modern design in workplace safety.

Founded in Germany in 1949, adidas is one of the world's leading sportswear companies. Through Adidas Pro Work, the company is extending its expertise in athletic footwear into a professional safety category that continues to evolve beyond traditional concepts of protection. GIT

adidasprowork.com
glolicensing.com



DuPont Tyvek: extremely tear-resistant, lightweight and breathable non-woven fabric that is resistant to water, bacteria and chemicals. Particularly suitable for protective clothing in industrial environments

HSE MANAGEMENT

From Transportation to Recycling

5 Ways HSE Managers Can Make More Sustainable PPE Decisions

Health, safety and environment (HSE) managers play a crucial role in ensuring the safety of employees while also considering the environmental impact of their activities. One area where they can make a big difference is by applying circular economy principles to the selection of personal protective equipment (PPE). Below are five ways in which HSE managers can opt for a more sustainable choice of PPE.

1. Consider transportation routes

The transportation of PPE across various stations contributes to the generation of greenhouse gas emissions. Assessing the carbon footprint therefore involves considering the entire transport chain – from the manufacturer to the central warehouse, on to individual locations and finally to recycling or disposal. Shorter transportation routes and more efficient logistics concepts can reduce the environmental impact. Accordingly, it can make sense to give preference to suppliers who organize their supply chains regionally or bundle transports.

2. Reduce packaging and reuse where possible

Packaging materials cause resource consumption and waste. In many cases, individual packaging of protective clothing is not absolutely necessary. Bulk packaging or multiple packaging can be a viable alternative and reduce the amount of waste. The Tyvek 500 Xpert Eco Pack introduced by DuPont in 2015, for example, has already avoided 820 kg of waste per 35,000 garments, reduced the consumption of water and primary energy and lowered CO_2 emissions.

The circular economy requires that the necessary packaging is recyclable. Look for PPE suppliers that actively minimize the use of virgin materials by incorporating recycled materials into their PPE packaging.

3. Check the recyclability of the materials

Whether and how PPE can be recycled depends largely on the materials used. For example, most disposable garments are made from plastic mixtures, making it difficult to separate the different materials for reuse. And even if it is possible to extract the individual plastics, the material is often of poor quality and can only be used to a limited extent. This makes high-quality recycling difficult.



Tyvek is a single-material product made from high-density polyethylene (HDPE), which is easy to separate and therefore highly recyclable

Monomaterials, on the other hand, can be recycled more easily under suitable conditions, provided the products are not contaminated. For example, Tyvek from DuPont is a mono-material made of high-density polyethylene (HDPE) that can be easily extracted and results in a high-quality material that can be reused in several applications. When selecting PPE, it therefore makes sense to check to what extent the materials used are generally suitable for recycling processes and what take-back or recycling concepts exist.

4 Consider longevity and material use

Another approach to supporting the circular economy is to extend the useful life of PPE without compromising its protective function. Robust materials can reduce the risk of damage and reduce the number of garments disposed of prematurely. At the same time, the weight of the material influences the environmental balance: PPE made from lighter materials also reduces the environmental impact. The heavier the material, the more waste is produced at the end of the item's life.

Contaminated PPE usually has to be disposed of thermally. The choice of material also plays a role here, as materials differ in terms of their energy content and their behavior when incinerated. DuPont Tyvek, for example, can be incinerated safely. As a fuel, it delivers more than twice the energy value of coal and as much energy as oil, measured in BTU, which means it has good energy-from-waste potential.

5. Evaluate manufacturers' approach to sustainability

In cases where the chemical protective clothing becomes contaminated and cannot be recycled, there are other ways to improve sustainability. For example, DuPont recently launched the Tyvek 500 Xpert BioCircle, a coverall made from 100 % bio-cyclable HDPE and manufactured using an ISCC-certified mass balance approach, reducing its impact on the environment by 58 %.

The circular economy encompasses the entire life cycle of a product. Accordingly, it makes sense to select suppliers who consider sustainability not only in the product but also in their operational processes. This includes the use of renewable energy in production, transparent sustainability targets and transparent reporting. Information from independent assessment or reporting platforms such as EcoVadis can help with the classification. Equally relevant is whether and how companies define their long-term environmental goals and document their implementation. For example, the DuPont sites were already able to reduce greenhouse gas emissions in two areas by 58 % in 2023 compared to 2019, thus exceeding their 2030 target ahead of schedule.

By consciously choosing PPE, HSE managers can help reduce environmental impacts – for example through shorter transportation distances, less packaging, recyclable materials and more durable products. Cooperation with manufacturers who understand sustainability as an overarching principle of action can support this approach. In this way, occupational health and safety requirements can be better reconciled with ecological goals. GIT

You can find more detailed advice in DuPont's e-guide, 'Guide for HSE Managers on PPE with a Lower Environmental Impact'

DuPont Personal Protection
www.dupont.de

© Pictures: DuPont

Protective Wear Manufacturer Earns EcoVadis Silver

Sustainability continues to gain importance throughout the personal protective equipment industry. German manufacturer HB Protective Wear has announced that it achieved EcoVadis Silver status following its latest sustainability assessment. The company received 74 out of 100 points, placing it in the 86th percentile and among the top 15% of all companies evaluated worldwide.

EcoVadis assessments examine a broad range of criteria, including environmental performance, labor and human rights, ethics and sustainable procurement practices. For PPE manufacturers, such ratings are becoming increasingly important as industrial customers seek greater transparency throughout the supply chain and place growing emphasis on environmental and social responsibility alongside product performance.

Founded in Germany, HB Protective Wear specializes in protective clothing for demanding industrial environments, including arc-flash protection, heat and flame-resistant garments, ESD protection and multi-risk workwear. The company has increasingly focused on sustainability initiatives in recent years, including environmental reporting and transparency programs. Earlier this year, HB also highlighted top ratings for environmental transparency through the Carbon Disclosure Project (CDP).

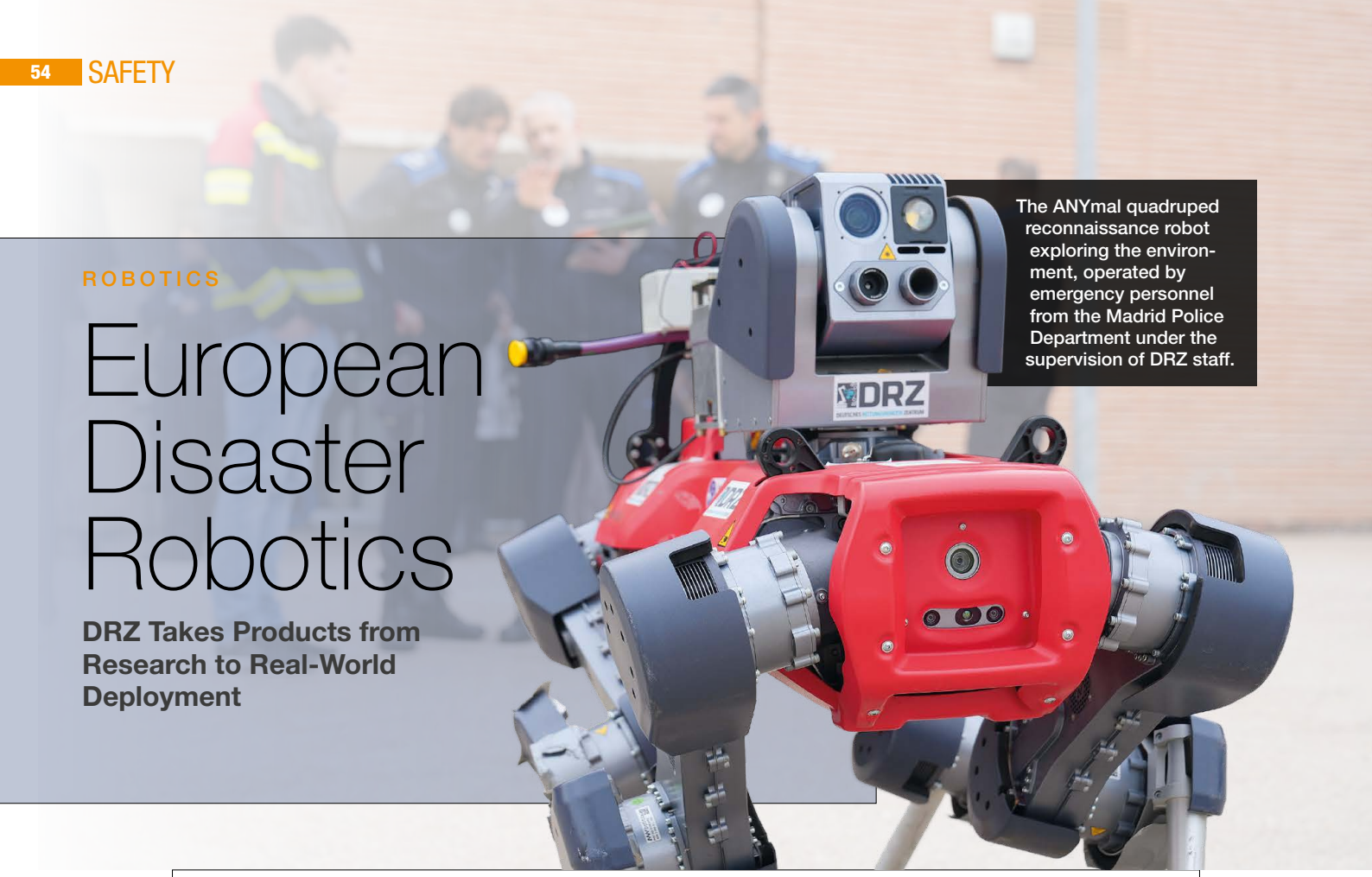
The latest EcoVadis recognition reflects a broader trend across the PPE sector. End users in industries such as utilities, manufacturing, energy and infrastructure are paying closer attention not only to product durability and protective performance but also to the environmental impact of manufacturing processes, material sourcing and corporate sustainability strategies. As procurement requirements continue to evolve, independently verified sustainability ratings are becoming an increasingly relevant factor in supplier selection and long-term purchasing decisions.

www.hb-online.com

ROBOTICS

European Disaster Robotics

DRZ Takes Products from Research to Real-World Deployment



The ANYmal quadruped reconnaissance robot exploring the environment, operated by emergency personnel from the Madrid Police Department under the supervision of DRZ staff.

Robotic systems can help to protect emergency responders in disaster situations where conditions are too dangerous for human intervention. The German Rescue Robotics Center (DRZ) actively shapes the development of such systems. As a full partner in the European Carma research project, the DRZ contributes its expertise directly to the development and testing of innovative robotics solutions for real-world operations.

The goal of the Carma project is to advance state-of-the-art disaster robotics technology for practical emergency response applications. Their focus is on autonomous systems that use advanced environmental mapping methods and artificial intelligence to assess complex operational environments, detect hazards, and support emergency personnel in decision-making processes – even in zero-visibility conditions through 2D radar mapping. In addition, collaboration between humans and machines should be significantly improved through speech processing and extended reality technology.



As part of the Carma pilot project, an injured person was rescued from a vehicle involved in a simulated CBRN incident and safely transported to a medical treatment station.

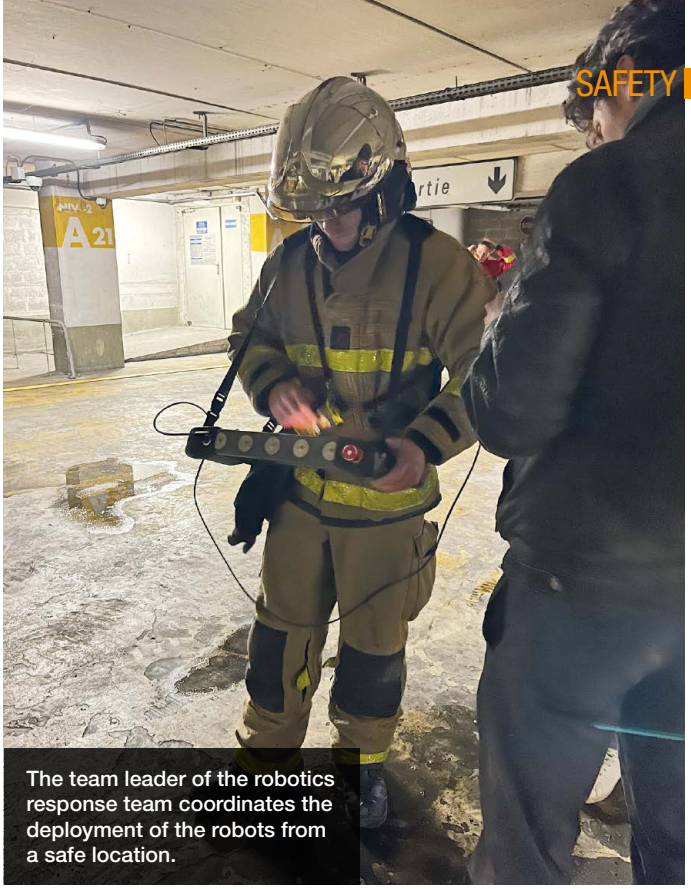
Safeguard Emergency Responders

The DRZ carries out the practical validation of these technologies. Developed systems were successfully tested under realistic conditions during two large-scale pilot trials in Madrid and Paris in March 2026 with the involvement of emergency responders. In Madrid, a complex traffic accident was simulated that involved the release of hazardous materials. Robotic systems – including the ANYmal quadruped robot deployed by the DRZ – took on key reconnaissance tasks and supported the detection of injured persons, enabling emergency teams to minimize entry into hazardous areas.

During the second pilot trial in Paris, the technology faced an especially challenging environment: a smoke-filled underground parking garage with a simulated fire. Despite limited visibility, the systems navigated reliably and provided relevant situational information. The combination of radar, thermal, and optical data, together with autonomous decision-making processes, proved critical to the success of the operation.



The TEC800 UGV from Angatec evacuates an injured person from an underground parking garage.



The team leader of the robotics response team coordinates the deployment of the robots from a safe location.

From Prototype To Product

With its experience in testing and integrating robotic systems into real operational procedures, the DRZ is making a significant contribution to ensuring that innovative technology is not only developed, but also validated and refined under real-life conditions. The objective is to seamlessly integrate rescue robotics into the daily operations of emergency services and civil protection organizations while sustainably reducing the burden on responders.

The insights gained during the pilot trials are now being incorporated into refined operational requirements that will guide further development of the systems. Final trials in Marseille, France and Attica, Greece in spring 2026 will demonstrate how the technology can be even more precisely adapted to the practical needs of emergency response operations. GIT

Deutsches Rettungsrobotik-Zentrum e. V.
www.rettungsrobotik.de

© Images: Deutsches Rettungsrobotik-Zentrum e. V.

Emergency Response – Robots Support Hazardous Rescue Missions

Robotic technologies are becoming an increasingly valuable resource for emergency responders operating in hazardous environments. Deep Robotics, a robotics company headquartered in Hangzhou, China, has expanded the deployment of its quadruped and wheeled-legged robotic platforms for firefighting, disaster response and industrial rescue applications. The initiative reflects a broader trend within emergency services: using robotic systems to gather critical information before personnel are exposed to potentially life-threatening conditions.

The company's X30 robot is equipped with 3D LiDAR, dual-spectrum imaging technology and gas detection sensors, enabling responders to assess dangerous environments remotely. The robot can generate real-time maps, identify potential hazards and detect toxic gases before teams enter affected areas. This capability is particularly relevant in incidents involving industrial fires, chemical leaks, collapsed structures or underground facilities where visibility and environmental conditions may change rapidly.

Complementing the X30 is the Lynx M20 wheeled-legged platform, which supports communications and logistics during complex deployments. According to Deep Robotics, the systems can establish communications links in areas where conventional networks are unavailable while also transporting equipment such as hoses, breathing apparatus and rescue tools. This allows emergency personnel to focus on operational tasks while reducing physical strain under demanding conditions.

The concept follows a “reconnaissance-first” approach increasingly adopted by emergency response organizations worldwide. Instead of sending personnel directly into uncertain environments, robotic platforms enter first to collect environmental and situational data. The resulting information can improve decision-making, accelerate incident assessment and reduce operational risks for firefighters and rescue teams.

Founded in 2017 by researchers from Zhejiang University, Deep Robotics specializes in quadruped, wheel-legged and humanoid robots for industrial inspection, critical infrastructure and public-safety applications. The company's systems are already deployed in sectors such as energy, transportation and emergency response, reflecting the growing transition of advanced robotics from research laboratories into operational field use.

www.deeprobotics.cn



VIDEO TECHNOLOGY

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

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.

Video Technology

i-PRO

i-PRO EMEA B.V.
Herikerbergweg 292, 1101CT 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

SECURITY MANAGEMENT

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

Security Management

NSC Sicherheitstechnik GmbH

NSC Sicherheitstechnik GmbH
Grete-Hermann-Str. 6
D - 33758 Schloß Holte-Stukenbrock
Tel. +49 (0) 5257 97799-0
Fax +49 (0) 5257 97799-29
info@nsc-sicherheit.de · www.nsc-sicherheit.de
CCTV, Fire Alarms, Voice alarm systems

FACILITY SECURITY

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

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!

Video Technology

www.luna-hd.de

lunaHD High Definition Video

Video surveillance • Video door intercom

TIME ACCESS

Time + Access

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

Time + Access

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

PLANT SAFETY

Time + Access

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

Time + Access

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

Plant Safety

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

Time + Access

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

Time + Access

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

Time + Access

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

Time + Access

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

© Olena - stock.adobe.com



Your **Number 1** for over 20 years

Register for our free Newsletter

NOW

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

e-Issue included!

WILEY

www.GIT-SECURITY.com

THE VIP LOUNGE



© Daniel Koke / Bayer

Oliver Giesen

Head of the Bayer AG Plant Fire Department, Berlin location

- 1994–1998: Bachelor's degree in Chemical Engineering (University of Applied Sciences)
- 2008–2010 Firefighter training (senior officer level)
- 2013–2015: Certified expert in preventive and building-related fire protection (EIPOS)
- Since 2010: Head of the Bayer AG plant fire department at the Berlin site
- Since 2016, Chairman of the Board of the Working Group for Industrial Fire Protection (AGBB Berlin e.V.); www.agbb.berlin
- Head of the Preventive Fire Protection Division of the German Plant Fire Department Association (WFVD e.V.)

Your career goal at age 20 was: At 20, I was in the middle of my training as a chemical laboratory technician, and it was clear to me at that point that I wanted to pursue a degree in the natural sciences. I decided to study chemical engineering – which has been excellent preparation for my current responsibilities.

What led you to take on a role in safety? I have to admit that I didn't dream of a career as a "Grisu" (Editor's Note: Known throughout Europe, Grisu the Dragon is the iconic cartoon dragon whose lifelong ambition is not to set fires, but to fight them) when I was a kid. When I was offered the position of head of the plant fire department, I was working as a project engineer at Bayer and was a member of the part-time plant fire department. At first, I was skeptical about whether this career path made sense for me, but I decided to go for it anyway. I quickly realized that working in the interdisciplinary emergency response teams and tackling the challenges of preventive fire safety were close to my heart. Today, I'm glad I chose this path.

In your opinion, what safety or security policy decision or project should have been implemented long ago? I'm a strong advocate of the idea that fire safety can and must be both efficient and economically sound. To achieve this, measures such as simplifying building codes, consistently minimizing the overabundance of regulations, and improving the technical training of those involved in fire safety must be implemented.

What do you consider to be the best invention in the field of safety or security? As an advocate of the "in-house fire department" model, it is, of course, the introduction of in-house emergency response organizations in Germany, which were established as part of industrialization. For companies, these offer significant added value and protect employees, jobs, and the company's assets. When properly organized, an in-house fire department can not only ensure hazard prevention but also generate economic value for the company.

Who do you think deserves an award? My family! Because they've always supported me over the years, and I could only achieve so much success with their help.

How do you relax? My personal "mindfulness" moment is every Wednesday from 7 to 9 p.m. That's when my choir rehearses. I've been singing with them for three years. The moment when the five vocal sections come together to create harmonies is pure relaxation for me.

What vacation spot would you recommend? I'm not sure if I want to share that – otherwise, it'll get even more crowded there. My absolute favorite place is in Andalusia, where I vacation with my family at least once a year.

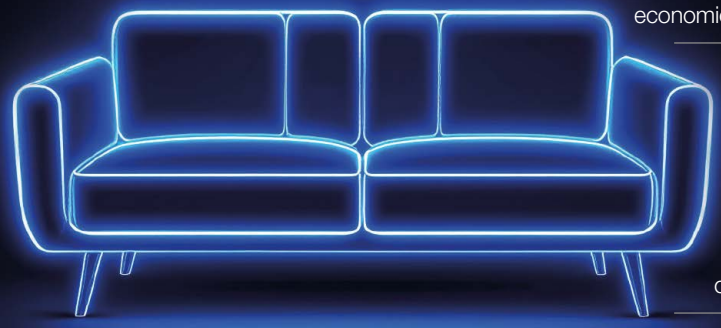
GIT SICHERHEIT is important to me because… the magazine helps build networks, and I'm a big fan of the 3K principle (Albrecht Broemme, former president ot the German THW): Know the right people in a crisis!

What was the last book you read? I actually read books mainly on vacation, and I like to read crime novels. On my last vacation, however, I made an exception and decided to read Albrecht Broemme's book "Deutschland in der Krise" (Germany in crisis).

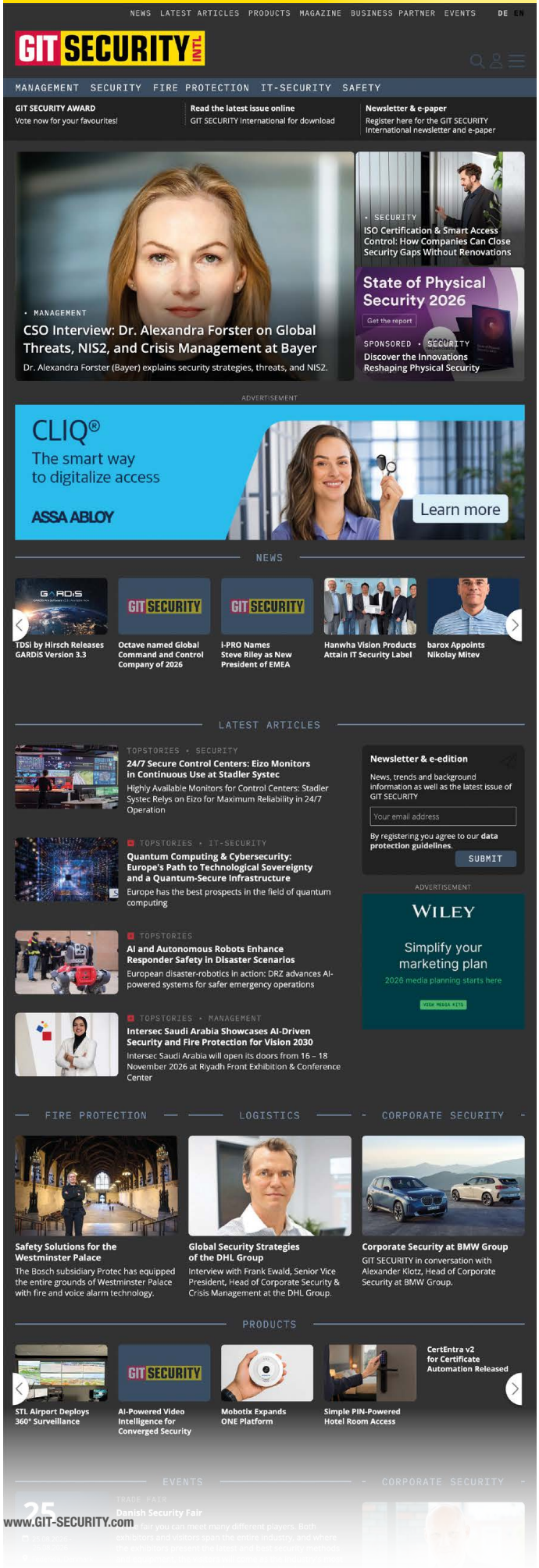
What kind of music do you like to listen to? My musical tastes were shaped in the early '90s, so I'm still a huge fan of grunge music and everything that followed that genre. Pearl Jam, Alice in Chains, and Stone Temple Pilots are the idols of my youth – they're the ones who inspired me to start playing guitar back then. Unlike back then, though, I'm much more open-minded musically these days and also listen to a lot of modern music – as long as it features guitars.

What motivates you? To generate positive value for our employer alongside my team, to help colleagues through hazard mitigation efforts, to protect assets, and to minimize business disruptions.

What concerns you – and what gives you confidence? The current political situation in the world and in Germany is a major concern for me as a family man and someone responsible for hazard prevention. What keeps me thinking positively as a firefighter, though, is that in both corporate emergency response teams and public fire departments, there are many people who – whether professionally or as volunteers – are intrinsically motivated to help and will be there to ensure our safety in an emergency.



This month at GIT-SECURITY.com



IMPRINT

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

Editorial
- Steffen Ebert
  +49 6201 606 709
  steffen.ebert@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

- Patricia Reinhard
  Tel.: +49 6201 606 027
  preinhard@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 International is published 4 times per year.

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

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.

Note on the use of artificial intelligence
When creating editorial content, we may use artificial intelligence tools to support activities such as research, drafting texts, or translations. All content is reviewed, edited, and approved by a human editor prior to publication.

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

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



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

Register here

SiCUREZZA

INTERNATIONAL SECURITY & FIRE EXHIBITION

17 – 19 NOVEMBER 2027 | Fiera Milano



MIBA

MILAN INTERNATIONAL BUILDING ALLIANCE

GEE GLOBAL ELEVATOR EXHIBITION | MADE EXPO | SMART BUILDING EXPO | SiCUREZZA

www.sicurezza.it/en/

FIERA MILANO