

# GIT

# SECURITY<sup>INTL</sup>

MAGAZINE FOR SAFETY AND SECURITY – WORLDWIDE

## CRITICAL INFRASTRUCTURE

CSO Patrick Hennies about Rail Security and Resilience

p 6

## RISK MANAGEMENT

Global Security for Boehringer Ingelheim

p 16

## PERIMETER PROTECTION

Netherlands Case: Securing Solar Farms

p 36



VIP:

Sven Dawson

p 50



CEO & AI Mastermind Pierre Racz:

## Genetec's AI Reality Check

Cover Story  
page 34

**VOTE NOW** FOR THE  
**NEXT WINNERS**

[WWW.SECURITY-AWARD.COM](http://WWW.SECURITY-AWARD.COM)

**GIT**  
**SECURITY**  
**AWARD**  
FINALISTS

WILEY

**A BEST-OF  
IN PRINT**



More news, full case studies & tech reports on  
[www.GIT-SECURITY.com](http://www.GIT-SECURITY.com)

# WILEY

WILEY

**VOTE  
NOW**

CLOSING DATE  
**SEPTEMBER 1<sup>st</sup>**

Information on the finalists,  
voting and readers' prize:

[www.security-award.com](http://www.security-award.com)



**GIT**  
**SECURITY  
AWARD**

**FINALISTS**

WILEY



WILEY



L-R: Patricia Reinhard, Dr Timo Gimbel, Sylvia Heider, Miryam Reubold, Matthias Erler, Stefan Ebert, Claudia Vogel, and on the far right, diving deep into the fine print: our layout detail expert Andi Kettenbach

# From Insight to Impact

Artificial intelligence, resilience, and the growing complexity of global threats – rarely has the safety and security industry been evolving at such pace. And rarely has it been so important to take a step back and ask: what truly works in practice?

With this issue of GIT SECURITY International, we explore precisely that question – from strategy to technology, from critical infrastructure to real-world applications. Or, to put it a bit more bluntly: less buzzwords, more substance.

Our cover story dives straight into one of the most debated topics of our time: the role of AI in physical security. In an exclusive conversation with mastermind Pierre Racz from Genetec, we gain insights into how artificial intelligence is actually used – not as a magic solution, but as a tool that must be applied with clarity and responsibility (page 34).

Resilience, meanwhile, remains a central theme across the issue. In our interview with Deutsche Bahn's CSO, we look at the security transformation of one of Europe's largest critical infrastructures – from drones and AI-supported video analysis to the broader challenge of safeguarding complex, highly visible transport systems (p 6).

Equally, the question of integration takes center stage. Whether in global risk management at Boehringer Ingelheim, where security expert Advancis consolidate diverse security systems into a unified control environment, or in modern access control architectures that increasingly rely on connectivity, power, and system integration – the message is clear: isolated solutions are a thing of the past (p 16).

At the same time, innovation continues to be driven by standardization and collaboration. Our feature on ONVIF's perspective on cloud architectures highlights how open approaches can unlock flexibility and avoid vendor lock-in – a lesson the industry has learned before and now needs to apply again (p 14).

And then there are the real-world cases: from securing solar farms in the Netherlands against organized theft to advancing fire safety in Bulgaria (p17) or modernizing fire protection systems in the UK (25). Different geographies, different challenges – but one common denominator: safety and security must deliver under real conditions, not just in theory.

We hope this issue offers both insight and inspiration. And perhaps even one or two moments where you pause, reflect – and think: this actually makes sense.

Enjoy an informative – and occasionally entertaining – read. Looking ahead, we are excited to continue this journey together with you. **GIT**

Best regards,  
Your GIT SECURITY International Team

New in town: SecureLeader / SafeLeader – The GIT Talk with the Market Leaders. Our new GIT SECURITY International format. Less PR. More real talk – from the people shaping safety and security.

More information:



## Make your access ready for what's ahead

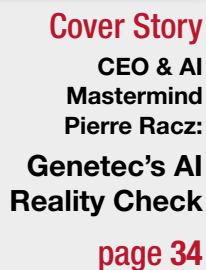
We help you digitalize and future-proof your buildings with a wide range of access solutions meeting your individual needs, supporting your move from the mechanical to the digital world. We are experts in access.

**With us, you digitalize with confidence.**



Learn more

**ASSA ABLOY**



## Product and Lead Platform for Safety and Security



Team GIT SECURITY International

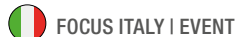
## CRITICAL INFRASTRUCTURE

## Drones Instead of Trackside Routes: DB Plans Automated Monitoring to Prevent Tampering and Disruptions

## STANDARDIZATION

## 14 A Cloudy Issue

## How Standards Can Drive Innovation in Physical Security



## 15 Mediterranean Building in Transition

## MIBA Levante: Security and Integration Take Centre Stage in Bari

## WORLDWIDE SOLUTION

## 16 Integrated Risk Management

Winguard from Advancis:  
How Boehringer Ingelheim is Modernizing  
its Global Risk Management



## 17 Fire Safety at Scale

## Hochiki Europe Strengthens Fire Safety Across Bulgaria

## ACCESS CONTROL

## 18 Navigating The New Landscape

From Perimeter to Core:  
Why Power, Connectivity and Integration  
are Becoming the True Drivers of  
Next-Generation Access Control

## BIOMETRICS

## 19 Facial Recognition, Responsibly

### Balancing Security, Privacy, and Trust

## TRENDS

## 20 No Security Without Secure Communication

Bernhard Klinger (PMeV/Germany):  
Why Secure Communication is Becoming  
a Key Resource for Resilience and the  
State's Ability to Act

## 23 GIT SECURITY AWARD

## Your Vote, Please

## FIRE PROTECTION

## DATA CENTERS

## 24 Compliant Duct Access

## The Benefits and Applications of Inspection Catches to Service Ducts in Data Centers



## 25 A Good Turn

## Comelit-PAC Supports the Samaritans with Fire Safety System Upgrade

34  
Pierre Racz38  
Gerhard Harand42  
Thomas Tschersich46  
Connor Doherty

## SECURITY

FOCUS FRANCE | ACCESS CONTROL

### 26 Yesterday's Craft – Today's Talent

A Monumental Task to the Last Detail

FOCUS USA | ACCESS CONTROL

### 28 The Biometric Edge

A High-Security Data Center Standardizes on Biometrics for Touchless Access Control

FOCUS SPAIN | ACCESS CONTROL

### 30 On The Ball

Hybrid Smart Key and Mobile Solution Digitizes Access at a Spanish Soccer Stadium

FOCUS SWEDEN | VIDEO

### 32 All In One

Smart Video Surveillance Provides Seamless Security for a Large Vehicle Fleet

## COVER STORY

### 34 To AI or not to AI

... that is the question. An Impression of Genetec's Application of AI right from the source

FOCUS NETHERLANDS | PERIMETER PROTECTION

### 36 Lightfingers In The Dark

How a Major Solar Farm in the Netherlands Was Made Secure

## SERIES: TESTING GROUNDS

### 38 Targeting Drones

Perimeter Security in a Practical Test: How the Wehrhan-TPS Urban Test Site Makes Real Attack Scenarios Visible

## CYBER-SECURITY

## CSO TALK

### 42 Guidelines

#### Do Not Deter Attackers

Deutsche Telekom CSO Warns of Ai-Accelerated Cyberattacks

## SAFETY

## DISTRIBUTION

### 46 First Call Partner for Engineers and Integrators

In Conversation with Connor Doherty: Fast Parts, Clear Data, Powerful Systems – How Digikey Designs Automation Holistically and With a Focus on Safety

# INDEX

## QUICK-FINDER

ORGANISATIONS, INSTITUTIONS  
AND COMPANIES IN THIS ISSUE

|                              |                       |
|------------------------------|-----------------------|
| <b>A</b> dvancis             | 16                    |
| Altronix                     | 9, 11, 18             |
| Assa Abloy                   | 3, 27, 29, 30, 31, 44 |
| <b>B</b> arox                | 31                    |
| <b>C</b> omelit-PAC          | 25                    |
| <b>D</b> allmeier            | 32, 37                |
| Deutsche Bahn                | 6                     |
| Deutsche Telekom             | 42                    |
| DigiKey                      | 46                    |
| Dom-UK                       | 26                    |
| <b>F</b> iera Milano         | 15                    |
| <b>G</b> enetec              | Front Cover, 34       |
| <b>H</b> ochiki Europe       | 17                    |
| HxGN Safety & Infrastructure | 31                    |
| <b>I</b> nvixium Group Inc   | 28                    |
| i-Pro                        | 31                    |
| <b>K</b> senia Security      | Outside Back Cover    |
| <b>M</b> ilestone Systems    | 19                    |
| Motorola                     | 21                    |
| <b>O</b> ctave               | 31                    |
| Onvif                        | 14                    |
| Optex                        | 36                    |
| <b>P</b> MeV                 | 20                    |
| Priorit                      | 24, 29                |
| <b>S</b> ynology             | 44                    |
| <b>V</b> ivotek              | 37                    |
| <b>W</b> ehrhan TPS          | 38                    |



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



## SecureLeader

The GIT Talk with the Market Leaders



**GIT SECURITY** LIVE



© Deutsche Bahn AG, Dominic Dupont

## CRITICAL INFRASTRUCTURE

# How to Put Safety on Track

## Drones Instead of Trackside Routes: DB Plans Automated Monitoring to Prevent Tampering and Disruptions

The Deutsche Bahn Group (DB), Germany's national railway company and one of Europe's largest transport and logistics providers, is facing a comprehensive security transformation. In our exclusive interview, DB CSO Dr. Patrick Hennies describes how DB is strengthening itself against threats – from long-term drone deployments and AI-supported video analysis to body cams for train staff. In the context of the new German Kritis Umbrella Act, implementing the EU CER Directive, Hennies emphasizes the close partnership with federal and security authorities and the need for uniform safety standards on the European rail network. Increased communication with local authorities, the expansion of cameras at busy stations and the use of modern sensor technology are intended to sustainably improve safety for customers, employees and society.

**GIT SICHERHEIT:** Dr. Hennies, a lot is changing at Deutsche Bahn – we'll talk about that in a moment. Could you start by outlining yourself, your professional background and your own vision for corporate security?

**Patrick Hennies:** I can now look back on almost two years at Deutsche Bahn. A time in which I was able to get to know a new world. In my professional life so far, I have gained a wide range of experience – in Europe, in Asia, worldwide and in very

different cultures. Every day it becomes clearer to me why so many people talk about Deutsche Bahn as a world of its own. In the security sector, we work with state-of-the-art technology and AI, and yet much remains analog. One example of this is the gigan-

tic infrastructure, access to which cannot be locked like a factory site. We produce 365 days a year, 24/7 under the constant supervision of politicians and our owner and always live in front of an audience of millions.

**...in principle an almost unmanageable task?**

**Patrick Hennies:** Where social and personal conflicts clash, we as a company can only counteract them to a limited extent. Technology and AI can only ever be part of a larger solution. Even if many people see us as a huge public sector company, we are a public limited company, not a public authority. Together with our municipal partners, we as a company have a very local and analogous role to play. This is why we often reach the limits of our possibilities, especially in the social sector, and need the support of local authorities. Without cooperation and networks, we will not be able to get to grips with the social problem in Germany and the effects in and around our 5,700 stations.

**Are you also involved in international exchanges with colleagues who are facing similar challenges?**

**Patrick Hennies:** A well-functioning national and international network means a lot to me. That's why I was happy to accept the election as Vice President of the international rail safety association COLPOFER. With 28 members from 22 countries, the association unites the safety organizations of important European railroad companies. The dialog with the other European railroads complements the national dialog with our partners and is crucial for the success of international high-speed and freight connections. It makes me proud to be able to play an active role in shaping this association.

”

Technology and AI can only ever be parts of a larger solution.

Dr. Patrick Hennies, Head of Group Security and Chief Security Officer (CSO) of the DB Group

I am convinced that we as DB contribute a great deal to advancing safety. I would also like us to look ahead much more consistently within the association. Resilience is foresight – in other words, being „ahead of the curve“, as we always say. This is the only way to act instead of reacting.

**Let's get an overview of the most important topics that you are currently dealing with in Group Security...**

**Patrick Hennies:** The safety of the railroad, its customers and employees always comes first. An inseparable part of this is the security partnership with the Federal Ministry of the Interior and the Federal Police, which

has been in place for over 25 years and whose 6,000 officers are responsible for emergency response and law enforcement in trains and stations around the clock. This partnership includes joint situation monitoring and operational concepts for major events such as public festivals or sporting events, prevention concepts, training of emergency services and the expansion of joint networks at home and abroad. I was impressed from the outset by how closely and trustingly DB and the Federal Police have been working together on many levels for years. Such cooperation between authorities and companies is by no means a matter of course. It requires a basis of trust, which we cultivate on a daily basis.

Deutsche Bahn is probably one of Europe's largest critical infrastructures in the field of transport and logistics. It is undergoing a huge reorganization and restructuring program – and of course in the midst of global political events. Let's start with the security situation and how it affects Deutsche Bahn. What has changed compared to the situation five or even ten years ago?

**Patrick Hennies:** The focus today is on resilience – and that is a huge feat. The focus is on strengthening our processes and infrastructure against external influences: virtual or physical attacks, the effects of large-scale storms, energy supply failures or pandemics. What we are building up in this area merges seamlessly into what military experts describe as defense capability. The

*please turn page ▶*



Federal Police and DB Security at Berlin's Ostbahnhof



Such multicopters have been in successful use at DB Security for several years

railroads play a key role in the civil and military defense of our country and Europe. This ranges from military transports to ensuring transportation and transport services under extreme conditions to projects in which we work together with the Bundeswehr to plan comprehensive concepts to protect the population or sensitive transport in the event of a crisis.

**At the same time, there is the German Kritis Umbrella Act that has just been passed?**

**Patrick Hennies:** Many of our activities are already in line with the future requirements of the Kritis Umbrella Act, which places high demands on operators of critical infrastructures. These range from the technical and personnel protection of railroad infrastructure to the constant further development of IT networks and their security, through to the comprehensive and consistent use of modern security technologies in property security. Strictly speaking, the Kritis Umbrella Act defines something that is close to the optimum of corporate security provision. It is therefore clear that we are also pursuing the objectives of the legislator in our own interests. However, this is a pioneering achievement: no one has ever implemented such a concept for a comprehensive infrastructure like the German railroad network.

Irrespective of this, DB, and in particular Group Security, has been working with the infrastructure divisions for some time to make systems and processes more resistant to interference and other influencing factors. We are talking about redundancies and business continuity. We are also questioning and rethinking processes from the perspective of current security scenarios. The focus is on the functioning of the railroads in Germany.

We are aware of the changing security situation every day. All conflicts in Europe

and the world influence our actions and strategies. In 2026, manipulation of systems or attacks on networks will not only come from activists who disrupt the economic and legal order. We have clear indications that state actors are also increasingly trying to influence technical processes and shake up our economy and society. Ultimately, it often remains unclear who really did it. However, one of the aims is certainly to disrupt our systems and our basic democratic order. However, these threats are not limited to the digital space. The effects of geopolitical tensions are also becoming increasingly apparent in the physical environment.

**What consequences and measures does this have for corporate security in particular? Can you give us a few examples?**

**Patrick Hennies:** We are looking at more than just our activities in Germany. Our purchasers, most of whom are active throughout Europe, or our experts who support our projects in other countries, are constantly on the move. The focus is always on ensuring travel safety and protecting supply chains. We remain in constant contact with the security authorities, first and foremost the Federal Police. But the Federal Ministry of the Interior, the Office for the Protection of the Constitution and the Federal Intelligence Service are also important partners in our dialog. This is crucial for our activities at home and abroad; conversely, we can bring back information from our global network.

Another example: we want to make greater use of long-range drones to monitor the 34,000 kilometers of track. They have to be secure from flight to data storage and transmission. So the use of products or components from certain regions of the world is out of the question. This is a cost factor and delays the use of new technologies.

**Speaking of costs. What does the economic pressure that Deutsche Bahn is under mean for the security architecture?**

**Patrick Hennies:** Increasing demands on the DB Group's security organization and the rapidly growing complexity of security tasks are being met with increasing economic pressure throughout the industry. Personnel and energy costs are rising. In addition, we are in competition with other means of transport and other railroad companies – for whom we also protect the railroad infrastructure in Germany. Safety is added value and a fundamental basic need, not an optional extra to improve quality. It is our task to guarantee this to the Group Executive Board, the workforce and the public, especially our customers. But only those who are sustainably profitable can be secure in the long term. Following the change in the Board of Management in October, we are now in the middle of one of the biggest change processes in the history of Deutsche Bahn. The Group is becoming leaner, management levels are being reduced and decisions are to be made where they have a direct impact. This will strengthen our operating business. This also applies to security.

Together with the security authorities and the owner, we are creating the framework conditions to make security visible and tangible for our customers throughout the entire rail system. Our work gives infrastructure and train operators – both within and outside DB – access to a reliable basis for specific security concepts. In short, we enable efficient security throughout the entire railroad system.

**But the corporate structure of Deutsche Bahn remains quite complex?**

**Patrick Hennies:** Within DB alone, many services are only possible thanks to the cooperation of numerous subsidiaries. One example: DB Regio runs local trains on DB InfraGO Fahrweg tracks, stops at DB InfraGO Personenbahnhöfe stations and orders its security staff from the internal service provider DB Sicherheit, whose employees provide security not only on trains but also at stations. This is the right thing to do for competitive and financial reasons. From our customers' point of view, however, it makes no difference at all who commissions or finances which security service. Our customers and employees need security that goes hand in hand.

Ideally, we will succeed in developing standardized approaches with railroad companies outside the DB Group as well. After all, there are now more than 480 companies in Germany that operate railroad infrastruc-

*please turn page ▶*



RACK MOUNT



HARDENED OUTDOOR



WALL MOUNT

## ACCESS & POWER INTEGRATION... ...ENDLESS POSSIBILITIES

**TROVE™** lets you design and deploy your preferred brand of access control with Altronix power solutions in virtually any environment.

- Simplifies board layout & wire management
- Reduces installation and labor cost
- Scalable for any size system
- Available as pre-configured and pre-wired kits

Streamline your access control deployments with **TROVE™**. Only from Altronix.

*Run With It™*

ture or are involved in train operations. Basic processes such as the introduction of technologies or the implementation of standards need to be managed at least for the entire DB Group. We have already established this structure for business continuity management and it is working extremely well. Of course, we take into account the competitive conditions and the fact that a Management Board of an AG has a statutory responsibility for results. However, we consistently bring together what belongs together. This results in savings and greater effectiveness at the same time. This means more security for the railroad, its customers and employees.

**How are the roles distributed within this structure – for example, strategic and operational tasks?**

**Patrick Hennies:** You are referring to the mapping of governance and operations. We bring together strategic roles in Governance. This is where contacts with politicians and authorities come together – uniformly for the entire Group. This is where the security strategy, the framework and the regulations for all business areas are created. The activities and regulations of individual divisions – for example DB Regio or DB Fernverkehr – are carried out on this basis. Consequently, uniform frameworks for security concepts or the commissioning of security services apply in operational implementation, but are adapted to the specific requirements

of the respective business units, as this is where operational responsibility lies. The third level is DB Security, which, as a service provider, carries out high-quality security assignments with its own staff. At the beginning of the year, we merged Group Security and DB Security, which has further strengthened the integration. This gives the service provider a framework for action to fulfill the contract in an optimal and transparent manner.

As a transport and logistics infrastructure, Deutsche Bahn is naturally integrated into the international transport networks, which requires international exchange – we have already touched on this briefly. Let's take a closer look at this.

Patrick Hennies: International exchange is more important than ever these days. DB is a key driver of cooperation in the heart of Europe. Both in terms of rail technology and safety for customers and employees. We are systematically expanding our contacts with the European railroads – the aim is to create a European rail network that is as standardized and customer-friendly as possible. We are finding that many issues and challenges in the different countries are quite comparable. Together we can find better solutions. Faster connections bring countries and railroads closer together.

**Can you give us a few examples?**

**Patrick Hennies:** We are talking to the British about trains from Germany to London and to the Italians about trains from Berlin to Naples through the Brenner Base Tunnel. In a few years' time, we will be operating the Fehmarnsund Tunnel under the Baltic Sea with the Danes – this also involves security issues that go beyond infrastructure protection and rail operations. For rail security, there are issues such as the cross-border deployment of security personnel or, in the case of trains to London, the necessary access controls to the train. I am clearly a European and will make my contribution to growing together and finding common solutions. Security does not end at the border.

Dr. Hennies, we have now talked about the DB Group itself, the global situation and the KRITIS umbrella law. Let's take a closer look at the changes brought about by new technologies, such as video technology and AI, sensor technology and drones. Perhaps we can pick out one or two things that are changing rail safety in particular?

**Patrick Hennies:** One of our top topics is the future use of long-haul drones. We have been successfully using multicopters at DB

Sicherheit, among others, for several years, but the technological leaps in recent years have opened up completely new possibilities for using drones. Until now, every drone has needed a drone pilot to control the device directly and on sight. Future drones will be able to automatically fly along railroad lines and be monitored from an operations center. They will be able to detect and clarify situations on site long before the emergency services arrive. This will make it possible to decide much more quickly whether and what measures are required. Depending on whether there are metal thieves on the move, trees blocking a track or people in the track area, for example, we can trigger the „right“ intervention from the outset or resume rail operations more quickly. However, we can also use drones to inspect cable ducts, for example, and detect tampering with the help of AI.

However, experience also shows that not everything that is technically possible can be used directly. That is why we are working together with industry and science to make technologies ready for practical use. The requirements of rail operations and data protection must also be taken into account. Only when the industry offers a solution that is ready for series production and all the necessary approvals have been obtained can it be used by us. So quite clearly: it's better to be a little later, but safe.

**Are you investing heavily in camera technology for railroad stations, track monitoring and other areas?**

**Patrick Hennies:** Together with the federal government, we have just completed a comprehensive expansion program for video technology. 11,000 cameras at the 1,000 busiest railroad stations now provide high-resolution images throughout. The Federal Police in particular benefit from the recordings when investigating crimes, only some of which, incidentally, have anything to do with the railroad or its customers and employees. We are often asked why not all stations have video cameras. The answer is quite simple: the legal framework does not allow it. The station is only equipped with video technology if the Federal Police make a corresponding risk assessment. This is based on factors such as visitor numbers or criminal offenses.

**What is the situation with video technology at other facilities, apart from train stations?**

**Patrick Hennies:** Protection against unauthorized access to facilities is another application for video technology. As a security organization, we want to use AI to auto-



Body cameras in use by DB Security – shown here on a team at Berlin Central Station

matically detect when people enter railroad facilities from the public area – be it a tunnel or a marshalling yard. In railroad stations, we want to be reliably informed with AI if people fall or settle in unsuitable places. Whether it's a medical emergency, a fight or a nap. We are keeping an eye on all of this with scientific support at the Berlin Südkreuz security station – our security lab – and will use it as soon as it works reliably and the necessary approvals have been obtained. To clarify: DB will not be working with facial recognition. The aim is to recognize dangerous situations, not to identify people.

One problem that is increasingly being reported is violence against rail staff. What exactly is the situation?

**Patrick Hennies:** Every attack on a colleague is one too many. There is no justification for assaults of any kind; violence has no place on trains, buses or in stations. The safety of our employees in all business areas has always been a top issue: it is omnipresent, constantly changing and needs to be rethought every day. We are continuously adapting our security concepts in close cooperation with

the security management teams in the business divisions, have introduced call for help apps, expanded video technology and consistently invested in de-escalation and behavioral training for employees. Unfortunately, however, we have to realize that we cannot stop the social trend of increasing disrespect, brutalization and violence.

The vast majority of situations that lead to violence arise from previous misconduct on the part of the aggressor. This ranges from traveling without a ticket to a passenger who is angry because the train is late or he realizes too late that he has boarded the wrong train. In many situations, a professional demeanor and a trained de-escalation strategy are not enough.

The death of one of our train attendants is sad proof that, despite all our efforts, there can be no absolute safety. All the more reason why it is our duty as an employer to always ensure the safety of our employees to the best of our ability. As Head of Security at DB, I take this very seriously.



DB Security: On-board Inspection Service

You organized a security summit after this fatal attack. What topics have you set there and what can DB employees expect?

**Patrick Hennies:** The security summit on February 13 was personally convened by our CEO Evelyn Palla and builds on our previous activities. What is new is that we have developed an action plan with federal and state politicians, associations, trade unions and

*please turn page ►*

### NETWAY SPECTRUM

**Hardened PoE Switches & Fiber Media Converters**

- Deploy IP devices at remote locations with or without local power
- Supports up to 90W per port
- Rapid battery charging provides extended power backup
- 115/230VAC or 277VAC input
- Manage and reset devices remotely with LINQ™ Network Power Management
- Lifetime warranty

*Run With It™*

© 2026 Altronix Corporation.

altronix.com



The security summit in Berlin on February 13, 2026, was convened following the fatal attack on a train attendant. From left to right: DB Security employee wearing a body camera, Evelyn Palla, Deutsche Bahn AG CEO, Patrick Schnieder, Federal Minister of Transport, and Christian Bernreiter, Chair of the Conference of Transport Ministers

interest groups on the basis of a common understanding. The topic was not new to anyone. We now have a broad consensus that will enable us to implement measures for DB colleagues and all other employees in the industry more quickly.

Together with the Federal Police and the DB business units as well as other stakeholders, we have been able to identify a range of measures that can be implemented effectively and quickly. We need speed in equipping our employees and must tackle the causes of increasing violence. It was important not to write long-term master plans, but rather to focus on issues that we can implement this year. The ongoing cooperation with the Federal Police has helped us to quickly establish a framework for a joint approach.

**What protective measures – bodycams, video technology, etc. – have you had good experiences with?**

**Patrick Hennies:** We have had very good success with bodycams. Our security staff have been wearing the devices since 2016, and since 2024, DB Regio's train crews and others have gradually been equipped. The train attendants have the same experience as the security staff: Anyone wearing a bodycam is virtually not attacked, as potential perpetrators can expect consequences. In addition to the conclusive documentation of an escalated situation, users of the bodycams therefore particularly appreciate the preventative deterrent effect before violence even occurs. It is therefore a pity that the legal requirements are very high – nevertheless, we will equip all employees in contact with customers with the devices

by the end of the year. This is one result of the security summit.

The involvement of the Conference of Transport Ministers is also crucial in order to give even greater consideration to the issue of safety in future tenders for local transport services and to supplement current transport contracts. Safety is not a negotiable additional service, but a basic requirement. Security must not be a question of money – nevertheless, the money for more staff or video technology must come from somewhere.

**Security-related incidents are often reported on social networks by private individuals and the media – this often happens faster than you as Deutsche Bahn can get clarity about the incident and its assessment...?**

**Patrick Hennies:** We have massively accelerated our reporting channels. Almost all employees with customer contact (and many others) can now enter security incidents from their smartphone into a central system in real time. We have made up a lot of ground with this. Our aim is to use AI in future to predict critical situations depending on the event or at least to recognize them in real time so that we can initiate countermeasures more quickly than before. This could be the additional stop of a train to enable a police operation or the timely gathering of security forces at a train station if, for example, rival soccer fans are deviating from known routes.

Unfortunately, we often see biased reporting in the media on security issues in trains and stations. This is often the result of activities on social networks. If you take a closer

look, the most aggressive TikTok stories and Instagram posts very often result from previous misconduct on the part of the sender. Inspectors are filmed and treated with contempt because the person concerned did not have a ticket. Train staff are threatened and insulted – usually for things that are not the employee's fault, such as missing carriages or delayed trains. Before we even know what has happened, a clip has thousands of clicks and finds its way into the daily media and online portals. Often to the detriment of individual employees, always to the detriment of Deutsche Bahn. We do our part to protect our employees and to be able to intervene more quickly. Above all, however, we would like to see more respect for our employees. Regardless of which professional group they belong to, they are all people who do a responsible job with great commitment and deserve our respect.

**Dr. Hennies, thank you very much for this in-depth interview. Finally, could you give us a brief personal outlook on the next projects and the near future of safety at Deutsche Bahn?**

**Patrick Hennies:** The security landscape has not been in such a state of flux for a long time. More and more risks and increasingly complex threats have to be managed on a daily basis. Whether it's securing critical infrastructure or convincing security concepts for local rail customers, the security factor is playing an increasingly important role in the everyday lives of people in Germany.

Transport companies cannot tackle social challenges in isolation if they shift from the streets to stations and trains. We are therefore increasingly approaching local authorities and their regulatory bodies in order to view stations and their surroundings as a unit and develop solutions together. Although we are not yet meeting with openness for successful cooperation everywhere, we are increasingly entering into a constructive dialog.

We would like to see uniform rules for the training and deployment of security personnel throughout Germany for local rail passenger transport services that are awarded on a competitive basis. At present, security is too often a question of budget in public procurement. Together with the other railroad companies, we are therefore committed to uniform minimum safety standards throughout Germany, which will benefit the millions of people who use our trains every day. **GIT**



Deutsche Bahn  
www.deutschebahn.com

# SecureLeader

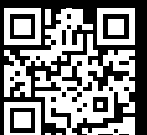
The GIT Talk with the Market Leaders



**GIT** **SECURITY** INTL

**Contact:**  
Miryam.Reubold@Wiley.com

**WILEY**





Leo Levit, Chair,  
ONVIF Board of  
Directors

## STANDARDIZATION

# A Cloudy Issue

## How Standards Can Drive Innovation in Physical Security

The promise of cloud technology is compelling: scalability, remote accessibility, advanced analytics, and reduced infrastructure costs. Yet many organizations hesitate to embrace cloud migration due to concerns about vendor lock-in, integration complexity, and a loss of competitive flexibility.

■ This hesitation is familiar. Two decades ago, proprietary protocols dominated the surveillance landscape. Organizations faced limited vendor choices, costly system upgrades, and an inability to mix best-of-breed components. The solution was standardization through ONVIF, which created an ecosystem of more than 30,000 compatible products and offered organizations the freedom of choice. As cloud adoption accelerates, we have an opportunity to apply these same standardization principles to unlock the cloud's full potential while preserving vendor flexibility.

### The Parallel Between Past and Present

Before ONVIF transformed our security ecosystem, organizations were locked into single-vendor environments. Adding a camera from a different manufacturer meant replacing infrastructure or facing expensive integration costs. Innovation was constrained by proprietary barriers, and organizations paid premium prices for limited choice.

By establishing common protocols, ONVIF enabled organizations to select cameras, recording systems, and management platforms based on quality and needs rather than compatibility constraints. Integrators gained flexibility to design tailored solutions. Manufacturers competed on features and value rather than proprietary lock-in. The result was accelerated innovation, reduced costs, and expanded options. As the industry now migrates to cloud architectures, proprietary platforms, closed APIs, and vendor-specific integration requirements threaten to build similar barriers. Without standardized camera-to-

cloud protocols, organizations face limited vendor choices, complex migrations, and reduced negotiating power.

The stakes are higher in the cloud era: unlike on-premises systems where vendor switching is difficult but possible, cloud dependencies create deeper operational entanglements. Data storage, analytics engines, interfaces, and management functions become tightly coupled to specific platforms, escalating exit costs and making organizational knowledge platform-specific.

### The Economics of Open Architecture

The economic advantages of standardized protocols extend beyond initial procurement costs. Organizations locked into sin-

gle-vendor cloud platforms face limited negotiating leverage during renewals, constrained expansion options, and significant switching costs if business needs change.

Consider a mid-sized organization deploying 200 cameras across multiple facilities. In a proprietary cloud environment, camera selection is limited to models compatible with the chosen platform. If a camera excels at license plate recognition but is not supported, the organization must compromise on performance or undertake costly workarounds.

With a standardized approach, the organization can select cameras based on specific requirements: thermal imaging for perimeter detection, high-resolution models for facial recognition, and cost-effective options for general surveillance. Cloud platforms compete on analytics capabilities and user experience rather than device compatibility. When new AI capabilities emerge, organizations can integrate them without replacing their infrastructure.

The competitive dynamics matter equally for manufacturers and integrators. Standardized protocols lower barriers to entry, enabling innovative companies to compete with established players. Providers can focus on differentiation through better analytics and intuitive interfaces rather than building proprietary ecosystems. Integrators gain flexibility to design optimal solutions rather than navigating compatibility matrices.

### Implementation Strategies

Standardization does not mandate a single deployment approach: organizations can choose strategies that align with their operational requirements while main-



taining flexibility. Pure cloud architectures centralize video management, storage, and analytics entirely in the cloud, maximizing scalability. Hybrid edge-cloud models distribute processing between cameras, local servers and cloud platforms, thereby balancing performance and cost. Multi-site deployments need consistent management while accommodating varying network conditions. Standardized protocols enable centralized cloud management of geographically dispersed systems without forcing hardware standardization across every location.

### Standards and Industry Readiness

The physical security industry's readiness for standardized cloud protocols is evident: cameras support sophisticated edge processing, network infrastructure can handle cloud traffic, and cloud platforms demon-

strate enterprise-grade reliability. The work to facilitate this transition is underway, and industry organizations such as ONVIF are developing camera-to-cloud standards that define how devices authenticate, stream video, share metadata, and enable remote configuration. However, these efforts require coordinated action across the ecosystem.

End users should prioritize standardization in procurement decisions, emphasizing that vendor flexibility and open protocols are non-negotiable. Integrators should advocate for standardized approaches, educating clients about long-term benefits. Manufacturers and cloud platform providers should commit to developing and supporting open protocols rather than pursuing proprietary advantages. We transformed the physical security industry once through standardization. To ensure the cloud era delivers on

its promise while preserving vendor flexibility and competitive dynamics, we have the opportunity to do so again – before proprietary approaches become entrenched.

The message is clear for organizations evaluating cloud strategies, for integrators designing systems, and for vendors developing products: standardization is not an obstacle to cloud adoption, but rather the foundation that makes successful cloud migration possible. **GIT**

**Author:**  
Leo Levit, ONVIF



**Onvif**  
[www.onvif.org](http://www.onvif.org)



FOCUS ITALY | EVENT

# Mediterranean Building in Transition

**MIBA Levante: Security and Integration Take Centre Stage in Bari**

■ With its debut in Bari on November 18–19, 2026, MIBA Levante brings the transformation of the Mediterranean building sector into focus – where sustainability, digitalisation and, increasingly, security converge.

The new event, a spin-off of the Milan International Building Alliance (MIBA), arrives at a pivotal moment. Southern Italy's construction market exceeds €90 billion, yet faces a shift as public funding programmes phase out and regulatory demands rise. In this environment, the resilience of buildings – not only in energy terms, but also in safety and protection – is becoming a key factor.

This is where SICUREZZA, the security and fire exhibition within MIBA Levante, gains strategic relevance. As buildings become more connected and complex, integrated security systems – from access

control and video surveillance to fire protection – are evolving into essential infrastructure. The Italian market reflects this trend: security and building automation have seen sustained growth, driven by digitalisation, compliance requirements and the convergence of physical and cyber security.

MIBA Levante brings together four interconnected exhibition formats – MADE Expo, SICUREZZA, SMART BUILDING Levante and the Global Elevator Exhibition – creating a cross-disciplinary platform. Among them, SICUREZZA stands out as a driver of innovation in intelligent, networked safety solutions. The focus is on systems that not only protect assets and people, but also integrate seamlessly into smart building environments.

Accompanying the exhibition is a high-level conference programme, developed

with universities, professional bodies and international associations. Topics such as decarbonisation, resilience and smart infrastructure are complemented by discussions on safety, regulatory frameworks and system integration – areas where the role of security technologies is rapidly expanding.

By addressing both technological progress and structural market change, MIBA Levante positions itself as a meeting point for the Mediterranean's building sector. In Bari, the dialogue will increasingly revolve around one central question: how to create buildings that are not only efficient and sustainable, but also secure by design. **GIT**



**Fiera Milano**  
[www.fieramilano.it](http://www.fieramilano.it)

Headquarters of  
Boehringer Ingelheim

## WORLDWIDE SOLUTION

# Integrated Risk Management

Winguard From Advancis: How Boehringer Ingelheim is Modernizing its Global Risk Management

Boehringer Ingelheim is one of the world's leading research-based pharmaceutical companies. Around 55,000 employees work internationally on the development of innovative therapies for humans and animals. The globally distributed research, production and administrative sites place high demands on security organization, alarm management and control center operation. The company relies on the open hazard management platform Winguard from Advancis.

In the industrial environment of pharmaceutical research, security systems must be monitored reliably and across all locations. In particular, this includes fire alarm, intrusion detection, access control and video systems as well as other technical systems. The aim is to achieve a consistent overview of the situation in the control center as well as fast and structured processing of events.

### Initial situation: Heterogeneous system landscape

Before the introduction of a central platform, many security systems at the German sites in Ingelheim am Rhein and Biberach an der Riß worked largely separately from one another. Different manufacturer solutions, proprietary interfaces and separate user interfaces made it difficult to achieve a uniform situation assessment in the control center.

As part of the „Control Center Germany“ project, a higher-level integration platform was therefore sought that could bring together different systems in a common system environment. As Michael Klier from IT O&L Security Operations explains, it was

particularly important for the company to bring together all security-related systems in one system. At the same time, the risk management system needed to be flexible enough to be used internationally and to support different operating models.

### Integration platform

The choice fell on Winguard, an open hazard management platform from Advancis Software & Services. The software serves as an integration and control centre platform via which various security subsystems can be connected and visualized centrally. Events from fire alarm, burglar alarm or other technical systems are consolidated in the system and displayed in graphical site plans. At the same time, alarm messages can be automatically forwarded to connected operations control systems. This gives control center staff a consolidated view of security-relevant events and enables them to initiate measures in a structured manner. In addition to the functional requirements, cooperation with the manufacturer also played a role. According to Klier, Advancis was particularly

convincing due to its short response times and competent support, which has proven its worth especially in critical incidents.

For the control centers, the integrated hazard management system is a central component in daily operations. By combining all safety-relevant information in one platform, incidents can be assessed more quickly and appropriate measures can be initiated without delay. This not only improves operational quality, but also ensures a high level of security for the sites, explains Jonas Michel, Head of Operations Center Germany.

### Digital support for operating processes

In addition to event processing, the system also supports organizational processes in safety operations. At Boehringer Ingelheim, for example, Winguard is used to manage so-called switching orders. These are used when detector zones have to be temporarily deactivated in the course of maintenance or construction work.

The corresponding processes can be planned, released and documented in the

system. Responsibilities, time windows and status information are logged automatically. This increases traceability and reduces administrative effort.

### Flexible architecture for international structures

Today, Winguard is used at several locations worldwide. The system architecture allows for different operating models – from local installations at individual plants to central control centers or regional security operation centers that monitor multiple sites. According to Klier, this flexibility was a key factor in the system decision. At the same time, he emphasizes that Advancis is prepared to react flexibly to individual requirements and to develop new solutions together. It is precisely this partnership-based cooperation that makes the provider an important part of security management.

The implementation of the platform shows that hazard management systems today go far beyond pure alarm processing. Open integration platforms enable a central overview of the situation, support operational processes and create the basis for cross-location security strategies.



Chemical development  
in Biberach an der Riß

For internationally active companies such as Boehringer Ingelheim, this makes it clear that the integration of technical systems and organizational processes is a crucial building block for efficient and sustainable safety and security management. **GIT**



Advancis Software & Services GmbH  
[www.advancis.net](http://www.advancis.net)

## FOCUS BULGARIA | FIRE SAFETY

# Fire Safety at Scale



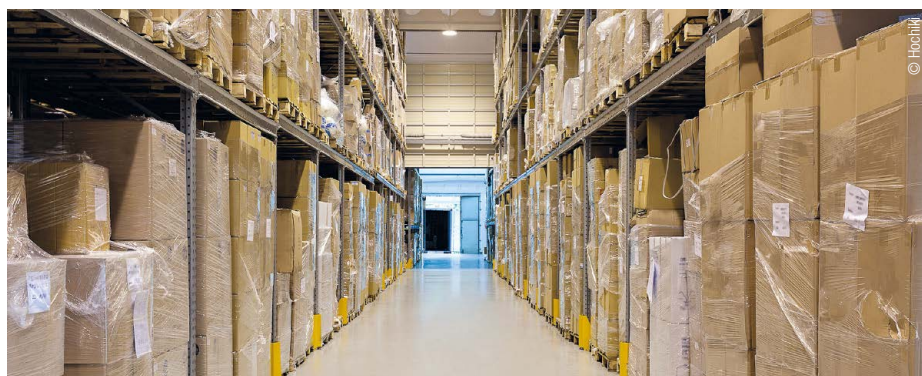
## Hochiki Europe Strengthens Fire Safety Across Bulgaria

From a logistics hub in Radinovo to a landmark tower in central Sofia, Hochiki Europe is supporting fire safety in some of Bulgaria's most demanding environments.

Two recent projects – delivered by partners MCM Engineering and Sectron – demonstrate how flexible detection systems can be adapted to very different risk profiles, from high-density warehouses to complex mixed-use buildings.

At the Bultex 99 logistics centre, a 270,000 sq ft facility storing flammable textiles, 350 ESP intelligent devices were installed alongside a six-loop Latitude fire control panel. Protecting dense racking systems required a targeted approach: FIRE-beam Xtra addressable beam detectors were positioned along aisles to ensure full coverage while limiting false alarms. The open-protocol system enables centralised monitoring and allows for future expansion.

In Sofia, the Smart Tower project presented a different level of complexity. The development combines residential and commercial areas with a multi-storey underground car park. More than 10,000



Hochiki devices were installed across the interconnected buildings. Addressable ESP systems were used in commercial areas, while CDX solutions covered residential units. In the basement car park – where exhaust fumes restrict smoke detection – linear heat detection cables were deployed for reliable monitoring.

Both projects highlight a broader trend in Eastern Europe: system integrators increasingly value not only product quality, but also long-term reliability, open-protocol flexibility and compliance assurance. Scalable

architectures and the integration of multiple detection technologies are becoming key selection criteria.

Hochiki's installations in Bulgaria illustrate how fire protection is evolving towards application-specific solutions – designed to meet distinct risks while remaining adaptable for future requirements. **GIT**



Hochiki Europe UK  
[www.hochikieurope.com](http://www.hochikieurope.com)

## ACCESS CONTROL

# Navigating The New Landscape

**From Perimeter To Core: Why Power, Connectivity and Integration are Becoming the true Drivers of Next-Generation Access Control**



Ronnie Pennington,  
Sales Director of the  
Americas, Altronix

Access control has increasingly become the technology of choice by security professionals as the need to protect employees, visitors, assets and property from new and emerging threats is a rising concern. Just scan the headlines, and it's clear that a new genre of threats have arisen stemming from a variety of external sources including public protests, teen takeovers and even sports victory celebrations have gone awry.

■ All this in addition to the list of long-standing issues like theft, vandalism and workplace violence that are top of mind for security professionals every day. Fortunately, modern electronic access control (EAC) solutions add an immediate layer of protection from threatening events. EAC's ability to monitor and control entry/egress presents the first line of defense organizations need to limit their exposure to potential harm and liabilities.

As facilities become more modernized, so have the variety and complexity of EAC solutions that can be deployed at the very perimeter of a property's "fence line" and migrate to its innermost secured areas. Facility-wide EAC deployments support mission critical business continuity, risk mitigation, and operational resilience, requiring new levels of integration so that system devices can seamlessly talk to one another and remain operational even during power disruptions to ensure protections are always in place. This is ushering in a new generation of modern power and data transmission solutions that represent the foundation of every EAC system solution.

## Modern EAC Power and Access Integration

The best way to prevent unauthorized entry to a facility is with the right combination of electronic access control and secured entry solutions to closely monitor, manage, control and document who has access at the prop-

erty line, to building entrances and secured interior areas. However, traditional access control systems can occupy a significant amount of real estate within facilities where space is typically at a premium and require multiple layers of security. This can require one or more independent distribution frame (IDF) closets located throughout a facility to house the various access controllers, power supplies, networking devices and enclosures required for a multi-layered access system. These IDF closets also require localized power and adequate HVAC to maintain stable environmental conditions for deployed system devices. The bigger the facility, the higher the associated equipment and real estate costs will be.

Modern access control and power integration solutions increase system capacities while reducing both the physical footprint required to install these systems, and their overall costs. This is being accomplished in three fundamental ways:

Minimize access control and power system footprints with densely configured integrated systems

## Leverage 4PPoE (802.3bt) to eliminate the need for localized power at access points

Enable remote power management across multiple devices and locations

Best-in-class access and power integration solutions like TROVE™ from Altronix provide the space saving and installation

efficiencies organizations need to best utilize valuable real estate while increasing system capacities and lowering overall costs. Rack mounted configurations are also ideal for installation in standard server racks to maximize space utilization.

## From Siloed to Networked System Solutions

Network communications play a vital if not essential role in maintaining the highest levels of security. New advanced remote power management platforms allow security personnel to remotely monitor, report and control multiple groups of power and data transmission products driving EAC systems across any number of locations. This provides numerous performance and cost-reduction benefits including expediting the deployment of additional EAC locations and enhancements with new devices, as well as for troubleshooting and maintenance scheduling.

Modern network communications dashboards like Altronix LINQ™ also include the ability to update software on multiple devices simultaneously, and to receive notification when a product's firmware is outdated. Detailed status reporting also provides real-time visibility to monitor current, voltage, internal temperature of access enclosures, battery status, and more. Such powerful network power management solutions significantly increase system reliabil-

ity and ROI, enhancing virtually any access control installation.

### Low Voltage Security Relies on AC Source Power

Even the best low-voltage security system infrastructure requires primary sources of AC power, as do all of the critical environmental systems needed to support and sustain operations. Many facilities today typically have alternate sources of high-voltage power requiring the ability to automatically switch between available sources the moment a power disruption is detected. Altronix devel-

oped Circ as a cost-efficient means of ensuring AC power availability. A high-voltage AC automatic transfer switch, Circ connects two independent AC sources and provides a single redundant power output. In the event that the primary AC power source goes down, Circ™ instantly switches to the secondary source with zero delay, ensuring uninterrupted operations across all critical systems.

Business operations across all industry classifications from manufacturing to health-care and food processing drive our global economy, and there can be no compromises when protecting them. Improving the ROI

on physical security system installations demands the best available power and data transmission solutions. By leveraging modern security technologies, organizations can better mitigate risks, ensure compliance and optimize system performance and reliability to best safeguard their people, property and assets with the highest levels of cost-efficiency. **GIT**



## BIOMETRICS

# Facial Recognition, Responsibly

## Balancing Security, Privacy, and Trust



Thomas Jensen,  
CEO of Milestone  
Systems

■ Facial recognition remains one of the most polarising tools in modern video analytics – caught between fears of mass surveillance and its proven value in solving serious crimes. Thomas Jensen, CEO of Milestone Systems, argues that its future in democratic societies depends on strict limits, transparent governance, and a clear ethical compass.

At the core of public concern lies the risk of indiscriminate monitoring. Continuous tracking of individuals fundamentally conflicts with democratic values and the right to privacy. For Jensen, this makes a compelling case for sharply defined use cases. Facial recognition should only be deployed in clearly justified scenarios, such as matching against narrowly scoped, legally authorised databases like those of Europol or Interpol, or in the search for missing persons with explicit consent from relatives.

Equally critical is the question of data sourcing. Harvesting images from social media without informed consent represents a profound breach of trust and purpose limitation. Without strict controls, any citizen could effectively become a suspect – an unacceptable scenario in open societies.

There are, however, examples of privacy-conscious implementation. Automated

border control systems at airports compare live images solely with passport biometrics, processing data locally and only for the duration of the check. Modern systems increasingly rely on encrypted biometric templates rather than storing raw images, making misuse more difficult. Yet even these safeguards must be reinforced through rigorous encryption, strict access controls, and robust data minimisation principles.

Another major challenge is algorithmic bias. Studies have shown that facial recognition systems can produce uneven results across demographic groups, particularly where training data lacks diversity. Addressing this requires systematic fairness testing, continuous validation with representative datasets, and full transparency about performance metrics.

Regulation plays a decisive role in setting limits. The EU AI Act, for instance, largely prohibits real-time facial recognition in public spaces, allowing exceptions only under narrowly defined conditions such as imminent threats or serious criminal investigations. Importantly, Jensen argues that the real issue is not the technology itself, but the context of its use – whether real-time or retrospective analysis. Both

demand strict oversight and clearly defined watchlists.

Beyond legal compliance, organisations must implement internal governance: clear decision-making processes, the four-eyes principle for validating matches, documented procedures, and defined data retention periods, typically around 30 days unless investigations require otherwise.

Responsibility ultimately lies with both regulators and industry. Technology providers must adopt ethical codes of conduct, communicate system limitations, train users, and be prepared to decline questionable deployments. Close cooperation with policymakers is essential to ensure that regulation keeps pace with technological reality.

Facial recognition, Jensen concludes, should remain a tightly controlled instrument – reserved for high-risk scenarios where its benefits clearly outweigh the risks. When governed by robust rules and ethical standards, it is possible to harness its potential without compromising fundamental freedoms. **GIT**



## TRENDS

# No Security Without Secure Communication

**Bernhard Klinger (Pnev/Germany): Why Secure Communication is Becoming a Key Resource for Resilience and The State's Ability to Act**



We are facing geopolitical, security, economic and climatic challenges that are constantly coming to a head. In these times of acute threats from cyber attacks, military and economic wars and conflicts as well as natural disasters, secure and highly available communication is more important than ever. Politics, business and society are also feeling the effects: the acceptance of investments in security has increased – and this also applies to security-critical communication systems. Civil-military cooperation in the field of interdisciplinary mobile communication is also becoming increasingly important.

■ In today's world, the following is truer than ever: Without secure communication, there is no security. Without reliable and highly available communication networks, there is no resilience. And without resilience, there can be neither a sovereign and effective state nor a productive and efficient economy. Without critical communication, our country would grind to a halt. When it works, we don't even notice it. But when it fails, the decisive factor is missing—for life, for security, for supply, and thus for the functioning of the state. The critical communications sector is therefore not just a technological ecosystem—it is a strategically relevant ecosystem. It strengthens our country's capacity to act and stands for a secure and resilient Europe.

## Digitization

One of the most important technological developments relevant to the industry in recent years is digitalization. As it progresses, software applications are rapidly gaining in importance and data in value. This creates new opportunities for companies in all sectors and also public authorities. At the same time, this increases the need for secure and highly available com-

munication solutions. For example, a 5G campus network is a basic requirement for many new digital processes and applications to increase a company's efficiency, flexibility and security, making it a business-critical component. It must therefore be highly available for the secure digitalization of the economy.

## Three technological megatrends

There are three megatrends in today's technology environment: broadband, cloud and artificial intelligence. These technology trends will also be used in the field of professional mobile communication in the future. They not only offer new possibilities for users, but also new opportunities for attacks. These must be fended off with suitable means. Although voice will remain the dominant service for critical communication for many years to come, data applications will increase – and they will also become critical at a rapid pace. Artificial intelligence will speed up processes, prepare decisions quickly and accurately based on the precise analysis of large volumes of data and also help to compensate for the increasing shortage of skilled workers.

## Multi-technology convergence in critical communication

In the context of critical communication, multi-technology convergence refers to the seamless integration and coordinated interaction of multiple communication technologies to create a uniform, highly available and resilient communication environment – especially for security and mission-critical applications. Multi-technology convergence describes the operation of several radio, IP and network technologies in a common architecture so that users can use them transparently and depending on the situation. Instead of isolated systems („technology silos“), an integrated communication ecosystem is created.

In critical secure communication, multi-technology convergence means intelligently combining several proven and new communication technologies to ensure secure, available and application-optimized communication for vital operations at all times. The benefits of multi-technology convergence (especially in critical communications) can be clearly demonstrated from an operational, technical and strategic perspective. In short, it increases the performance, resilience and future-proofing of communication solutions.

### High-availability communication for KRITIS, industry and business

KRITIS, industry and many other sectors of the economy require highly available communication and viable cybersecurity solutions. Secure and reliable communication is essential for all industries and economic sectors – also in the context of digitalization. In times of increasing cyber attacks and real physical threats, it is more important than ever to think about the security and protection of communication networks. Companies need effective cybersecurity mechanisms to protect themselves from attacks. The resilience of companies and KRITIS must be increased.

### How trends are changing association work

PMeV works towards a secure, resilient and connected Europe by promoting secure

communication solutions. In addition, we support professional users with new technology trends and developments and the associated opportunities and challenges. The political, economic and technological changes require a high degree of flexibility in PMeV's work: new topics are gradually and flexibly taken up by the association and its members as required. A further thematic expansion is planned for 2026.

New working groups will be established on the following topics: User dialog, broadband terminals, 5G campus networks, Internet of Things (IoT), artificial intelligence (AI), satellite communication and civil-military cooperation (ZMZ). In 2024, the association established working groups on cyber security, BOS messenger solutions and crisis and emergency communication, to name but a few.

In parallel to the new topics, the PMeV is continuing its association work on the already established classic topics with progressive innovative concepts, strategies and standardization. In addition to new technical and regulatory topics, the association's work will continue to focus increasingly on raising awareness among politicians, society and users with regard to the requirements for secure, high-availability communication solutions and their indispensability for the security and supply of our society. **GIT**



**Bundesverband Professioneller Mobilfunk e.V. (PMeV)**  
(Federal Association of Professional Mobile Communications)  
[www.pmev.de](http://www.pmev.de)

## Motorola Solutions' Body Cameras Support Berlin's Commitment to Increased Security

Following a European-wide open tender process, Motorola Solutions has been awarded a contract to equip Police Berlin and the Berlin Fire Department with 3,000 body cameras.

The V500 body cameras have been used by police and fire services in Berlin on a daily basis since the end of 2025. With this first joint procurement by a police and fire department, both public safety organisations join a growing network of emergency services across Europe that rely on Motorola Solutions' body cameras.

Last year, approximately 10,000 police officers, firefighters, and other emergency personnel — including members of Police Berlin and Berlin Fire Department — fell victim to violent offenses while on duty in the federal capital. The introduction of body cameras underscores the goal of Berlin's public safety organisations to increase frontline safety, transparency of interactions, as well as capturing evidence.

"Frontline-teams often operate in high-stress environments where their focus must remain entirely on the situation at hand," said Helmut Gaschler, sales director, Central Europe at Motorola Solutions. "Body cameras enable eyes-on-scene for greater clarity as events unfold, while also helping to create a reliable record of critical events. We are proud to be working with Police Berlin and Berlin Fire Service on this important initiative."

The Motorola Solutions V500 body cameras are provided alongside the highly configurable VideoManager evidence management software. This software is integrated directly into the forces' internal IT infrastructure, allowing officers to quickly upload, securely store and efficiently manage video footage as part of their existing daily workflows.

[www.motorolasolutions.com](http://www.motorolasolutions.com)



**3,000 body cameras will enhance officers safety and transparency during interactions**

**Category A: Machine & Plant Safety**

|                 |                                                                             |
|-----------------|-----------------------------------------------------------------------------|
| Bihl+Wiedemann  | ASi-5 Safety PCB Module                                                     |
| E. Dold & Söhne | Innovative RE 6900 Wireless Safety System                                   |
| Euchner         | CKS2 Transponder-Coded Key System                                           |
| K. A. Schmersal | SFB Port Extender for Flexible Safety Architectures                         |
| Mersen          | ProGrid Solutions – Safety Load Disconnect Switch for the Energy Transition |
| Moxa Europe     | NPort 6000-G2 Series – Secure Serial Device Servers                         |
| Murr            | MVK Fusion CIP Safety – 3-in-1 Hybrid Fieldbus Module                       |
| Phoenix Contact | Multifunctional Safety Relay PSR-UNI                                        |
| Sick AG         | Flexi Net Safety Controller – for stationary and mobile machines            |

**Category B: Occupational Safety**

|                    |                                                                                  |
|--------------------|----------------------------------------------------------------------------------|
| Ansell Healthcare  | Acetone-resistant gloves TouchNTuff 93-800                                       |
| Atlas Schuhfabrik  | Max Series – Safety footwear for extreme conditions                              |
| Blaklaeder         | Multinorm long-sleeve shirts 3436/3437                                           |
| Denios             | Real-time Asset Monitoring for Safety Cabinets                                   |
| Dupont             | Chemical Protection with a Focus on Comfort                                      |
| Ejendals           | Tegera Uniform 9078 Protective Gloves                                            |
| Fristads           | Multinorm Green – Protective Clothing with a Transparent Environmental Footprint |
| HB Protective Wear | HB-ArcFlash Pro 4kA and 7kA Softshell Jacket                                     |
| Krause-Werk        | Stabilo 135 XL Step Ladder                                                       |
| Munk Group         | Modular Assembly Platform                                                        |

**Category C: Video Security**

|                      |                                                              |
|----------------------|--------------------------------------------------------------|
| Ajax Systems         | Superior NVR H2D Series – AI-powered network video recorders |
| Axis Communications  | Q6411-LE Bispectral PTZ Camera                               |
| Dallmeier Electronic | Panomera V8 Multifocal Sensor Camera                         |
| Hanwha Vision        | PTZ cameras for harsh environments                           |
| LiveEye              | Digital planning tool for temporary security solutions       |
| Security Robotics    | ACUDA security platform                                      |
| Spectro AI           | Spectro AI: DockWatch Trailer                                |

**Category D: Access Control**

|                        |                                                                      |
|------------------------|----------------------------------------------------------------------|
| Ajax Systems           | Superior MotionCam G3 (PhOD) Jeweller – Wireless PIR Motion Detector |
| ASL-Ademco             | ABAX Door Contact Sensor                                             |
| Aug. Winkhaus          | BlueEvo Electronic Locking System                                    |
| Dom Sicherheitstechnik | Online Mesh for Connecting Digital Locks                             |
| Dormakaba              | ST PRO Green RC3 Automatic Sliding Door                              |
| Hirsch                 | Microsesame Access System                                            |
| Ksenia                 | Conexa is the IP touchscreen keypad                                  |
| MP-Bos                 | BOS-ID digital ID card                                               |
| Portier Global         | Portier Vision 5 locking system software                             |
| Satel                  | Be Wave Hybrid – Security and building automation system             |
| Schmeissner            | Capacitive break-in protection                                       |
| Telenot Electronic     | hiline1 – Transmission device                                        |
| Tell Software          | OPEN.ioting Smart Gate Opener retrofit module                        |

**Category E: Security Management**

|                     |                                                                                |
|---------------------|--------------------------------------------------------------------------------|
| Advancis            | AIM – Advanced Identity Management                                             |
| Ajax Systems        | Superior Hub G3 Jeweller – Wireless hub control center with photo verification |
| Ambient System      | ICO Emergency – Emergency intercom for critical situations                     |
| Axis                | D2122-VE Radar and Axis D2123-VE Radar                                         |
| Chubb               | Connected Services – Networked security services                               |
| Hirsch              | Lumor Fiber Optic Intrusion Detection                                          |
| Hiscout             | GSS – HiScout GRC Suite's secrecy and tamper protection module                 |
| ID-ware             | Software-based management platform PIAM Suite                                  |
| IVMS                | Lynx – Hazard management system                                                |
| KGS Fire & Security | Fusion – Security platform                                                     |
| Octave              | Coda Spatial – 3D security and perimeter monitoring                            |
| Quanergy Solutions  | Q-Shield – LiDAR sensor for intrusion detection                                |
| Security Robotics   | Autonomous mobile security robots (AMSR)                                       |

# Your Vote, Please

[www.security-award.com](http://www.security-award.com)

Detailed information about the products there

Once again our GIT SECURITY AWARD jury has nominated a qualified shortlist of industry products. Now, it is up to you, our readers, to select your favorite product and vote. We will present the nominated products online only – you can vote directly on the presentation platform.

## Reader Prize

Win the reader prize! Select one favourite from each category to take part in the draw for 3 Wiley-branded Ledlenser P7R Work UV.



**GIT**  
**SECURITY**  
**AWARD**  
**FINALISTS**

## Category F: Fire Protection

|                      |                                                                                |
|----------------------|--------------------------------------------------------------------------------|
| Ajax Systems         | EN54 Fire Hub Jeweller – Wireless Fire Alarm Control Panel                     |
| Axis                 | D6310 Air Quality Sensor for safety-critical indoor areas                      |
| Dehn                 | Certified E30 solution for surge protection in the event of a fire             |
| Gekartel             | VdS 6024-certified fire safety tablet                                          |
| Hanwha Vision Europe | Bi-spectrum cameras for early fire detection                                   |
| Inotec               | GMS safety guidance system for evacuation                                      |
| Johnson Controls     | SafeLinc cloud web interface and mobile app                                    |
| Securiton            | SecuriGas – aspirating smoke detector system with highly sensitive gas sensors |
| Krause-Werk          | Stabilo Stufen-Stehleiter 135 XL                                               |
| Munk Group           | Modulare Montageplattform                                                      |

**Voting** will start 1 June  
and will be open until  
**1 September** via  
[www.security-award.com](http://www.security-award.com)





The Priodoor RTX inspection door provides fire-resistant partitioning of cable ducts in data centers.



A Priodoor inspection door provides generously dimensioned access to service ducts.

## DATA CENTERS

# Compliant Duct Access

## The Benefits and Applications of Inspection Catches to Service Ducts in Data Centers

Data centers are highly complex facilities in which large quantities of power and data cables are routed through service ducts. These cables must not only be managed efficiently, but also fire-sealed. At the same time, easy accessibility is essential. Inspection hatches offer an optimal, indeed indispensable, solution for this.

■ Tested and certified fire-rated enclosures with a fire resistance of up to 90 minutes ensure that valuable time is gained in the event of a fire and that safety within the data center is enhanced. At the same time, inspection hatches guarantee optimal accessibility. The strict temperature limits for fire-resistant components are also met in the frame and edge areas ( $\leq 140\text{ K}$  on average /  $\leq 180\text{ K}$  at specific points).

Non-combustible material and a circumferential smoke seal prevent the spread of fire and smoke in the event of a fire. The inspection doors are manufactured to the nearest millimeter – from small to large dimensions, in single or double-leaf designs.

They can be installed in various wall types, such as plasterboard shaft walls or solid walls, and a four-sided or optional three-sided frame allows for installation in both walk-in shafts and raised installations.

### Dust-free installation

Another key advantage is the quick and virtually dust-free installation. The surface of the doors is already finished, so no subsequent painting or plastering work is required. The doors can be repainted if necessary, but this is not essential. Inspection doors are designed so that self-closing is not required. The door remains open whilst access is required for maintenance work or

re-cabling, which makes the work considerably easier.

There is no external handle; the door can only be opened with a special tool or key, thereby minimizing the risk of unauthorized access. Overall, access doors for installation shafts in data centers offer a perfect combination of fire protection, accessibility, flexibility, and aesthetic integration. They are therefore the ideal choice for modern and secure data center infrastructures. **GIT**



Priorit  
www.priorit.de



FOCUS UK | FIRE ALARM

# A Good Turn

## Comelit-PAC Supports the Samaritans with Fire Safety System Upgrade

Leading charity Samaritans has worked in partnership with Comelit-PAC and installer Red Technical Services Ltd to complete an upgrade to the fire safety system at its registered office in Ewell.

■ The Samaritans organization is focused on suicide prevention through human connection, and provides emotional support 24 hours a day, seven days a week. To protect the staff who help make this possible at its central office services, Samaritans has replaced its aging fire alarm with a new LogiFire solution designed to bring reliability, compliance, and reassurance. The charity required a system that could be installed quickly and efficiently, with minimal disruption to its vital operations. Following a detailed review of requirements, Comelit-PAC recommended the LogiFire wireless system, which combines the latest technology with straightforward operation.

Anthony Borrow at Samaritans says: “The safety of our staff and volunteers is always a priority. We needed a fire system upgrade that would bring us peace of mind while also being practical for our office environment. The process was made straightforward through the support of both Comelit-PAC and Red Technical Services, who worked with us from the outset to understand our needs and ensure trouble-free installation.”

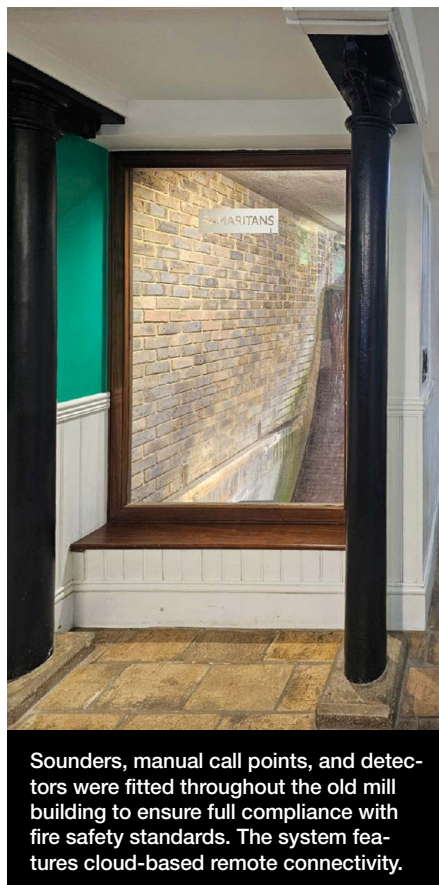
### Cloud Connectivity

At the center of the system is a single LogiFire 118 panel configured as a wireless solution. To extend coverage across the office, the system incorporates four translators and wired interfaces linked with four door access points. Sounders, manual call points, and detectors were fitted throughout the building to ensure full compliance with fire safety standards. The system features cloud-based remote connectivity, enabling Samaritans’ facilities team and Comelit-PAC engineers to monitor and manage the fire safety network in real time from any location. Authorized users can receive instant alerts through a secure online platform, check system status and carry out diagnostics without needing to be on site, ensuring a fast response to any issue.

Steve Hopkins, General Manager from Red Technical Services Ltd, added: “This project required careful planning to keep the office fully operational for their essential work during installation. The wireless design of the LogiFire panel meant that we could phase the work efficiently, avoiding



The Samaritans headquarters in Ewell, UK, has now been equipped with a Comelit-PAC wireless fire alarm system.



Sounders, manual call points, and detectors were fitted throughout the old mill building to ensure full compliance with fire safety standards. The system features cloud-based remote connectivity.

immediately, which reduces maintenance costs and improves ongoing resilience. “

### Close Cooperation

Delivering the upgrade required close collaboration between all parties. Right from the design and specification stage, Comelit-PAC worked alongside Red Technical Services Ltd to map out the system requirements and plan the works program. This included site surveys, identifying the best equipment locations, and agreeing on installation phases to reduce disruption to the charity’s operations.

Mandy Bowden, Comelit-PAC Fire Systems Business Manager – UK & ROI, concluded: “Our priority was to design a fire safety system that delivers reliable protection and can adapt as Samaritans’ requirements change. Through close partnership, we carried out detailed surveys and planning to ensure the system fits the building and its operations precisely. The combination of wireless technology and secure cloud monitoring provides the flexibility to expand coverage, add new devices, or adjust settings as needed, all offering long-term confidence in the safety of staff and volunteers.” **GIT**

intrusive cabling and keeping downtime to an absolute minimum. Remote cloud access now allows engineers to run system checks, update configurations, and respond to alerts



Comelit-PAC

www.comelitgroup.com

© Images:

FOCUS FRANCE | ACCESS CONTROL



# Yesterday's Craft – Today's Talent

## A Monumental Task to the Last Detail

On the evening of 15th April 2019, the world held its breath. Notre-Dame de Paris, the Gothic masterpiece that had inspired faithful hearts for centuries, was ablaze. Flames threatened to erase not just a building but a bedrock of French and European identity.

■ It was a defining moment for Christine Soulier, Responsable Serrurerie Décorative at Maison Fontaine. “The 2019 fire marked a turning point in our relationship with heritage,” she recalls. From that smoldering tragedy has arisen a fascinating tale of renewal, with Europe’s oldest artistic locksmith playing its own small role. With a history stretching back to 1740, Maison Fontaine – today part DOM Security – brought centuries of expertise to Notre-Dame’s restoration. “This exceptional legacy grants us in-depth knowledge of historical styles, ancestral craftsmanship techniques, and heritage conservation requirements,” Christine explains.

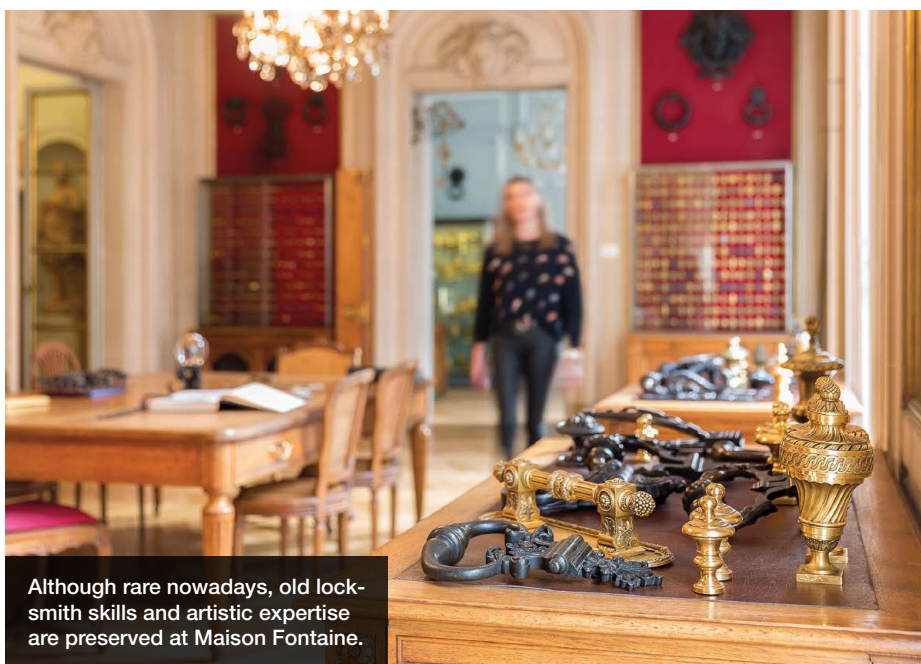
The company’s task was to craft embossed door handles for the cathedral’s sacristy, where clergy prepare before meeting the congregation. Partnering with Art et Technique du Bois from Saint-Brive-Courcelles, they drew inspiration from 19th-century designs. “Together, we designed a custom handle model that remained faithful to the spirit of the site,” she says, “a perfect alliance between tradition and functional precision.”

## A Traditional Approach To A Modern Challenge

Materials selection was equally thoughtful: “We deliberately chose brass – a noble material historically used in decorative ironwork for its malleability, durability, and natural patina that ages gracefully over time,” Christine explained. Using the lost-wax casting method, each handle was molded and then hand-finished, sharpened, chased, and polished to a warm, authentic sheen. “No two handles are ever exactly alike – each one is unique,” she added.

Approved by the Architects of Historic Monuments, these handles were installed for Notre-Dame’s 2024 reopening. “It is with immense pride that Maison Fontaine had the privilege of working alongside the many craftsmen and experts who had been mobilized to restore this emblematic monument,” Christine reflects.





Although rare nowadays, old locksmith skills and artistic expertise are preserved at Maison Fontaine.

### A Lasting Legacy

With its showroom located next to the Louvre on the Rue de Rivoli, Maison Fontaine remains deeply connected to its roots. This historic space, first opened by M. Lavollée and later run by the Fontaine brothers, was long known for its decorative fittings, locks, cylinders, and essential ironmongery. Today, it serves as a showcase of the company's craftsmanship and a meeting place for clients, bridging past and present in the heart of Paris.

Since its inception, Maison Fontaine has contributed to some of Europe's grandest stages: the Palace of Versailles, the Paris Opera, and the Hôtel de Crillon – each carefully crafted piece a testament to its mastery. "Our true strength lies in the fact that we possess the original molds," Christine says. "That allows us to recreate missing or damaged elements in exact detail." But more often their work necessitates breathing new life into original pieces through meticulous restoration that honors the materials' history.

### Tradition Reimagined

Heritage craftsmanship only has meaning for Maison Fontaine if it continues to inspire the present. This philosophy has carried them across borders, from the Ritz Hotel in Paris to Huawei's headquarters in Shenzhen, supplying high-end cremone bolts and espagnolettes that marry traditional techniques with modern design. From time to time, they even collaborate with contemporary artistic designers such as Jean Boggio to keep their craft vibrant.

This range of work rests on Maison Fontaine's maintaining the delicate balance between preservation and innovation.

"For exceptional projects like Versailles, the Louvre, or Notre-Dame, our priority is restoration, far beyond simple reproduction," Christine explains. It is a commitment to historical fidelity and functional durability that is evident in each polished curve and patinated surface.

As a member of DOM security, Maison Fontaine will also collaborate on access control projects such as the recent installation at Igoville town hall in northern France, where they crafted ornate hardware to complement bespoke locks from Déný Security, ensuring the chateau's 18th-century doors retained their period elegance while offering modern security.

### Leveraging History To Look Forward

In this way, Maison Fontaine brings its artistic expertise to a wider mission: helping to preserve not just the buildings but also the stories and values that they represent. Working under the DOM Security umbrella, from sacred cathedrals to civic landmarks, every handle, lock, and escutcheon embodies a shared commitment to excellence, trust, and preservation.

"We engage in a dialogue with history in every project," Christine reflects. "It is how we ensure that decorative locksmithing continues to hold its rightful place in the architecture and technology of tomorrow." **GIT**



Dom Security

[www.dom-security.com](http://www.dom-security.com)



# CLIQ®

## The smart way to digitalize access

Take your access management into the digital era. With CLIQ, you upgrade from mechanical to digital access at your own pace to gain greater control today and adaptability for tomorrow.

**Learn more about making the switch to digital access**



**Download our whitepaper**

# ASSA ABLOY

Advanced biometrics from the Canadian company Invoxium provide enhanced security, productivity, and safety across industries, enterprises, and critical infrastructure.

LIGHTEGE



FOCUS USA | ACCESS CONTROL



# The Biometric Edge

**A High-Security Data Center Standardizes on Biometrics for Touchless Access Control**

Data centers protect the digital backbone of modern business. For LightEdge, a leading cloud and colocation provider trusted by many Fortune 500 companies across the Midwest USA, security must be uncompromising. As their legacy system no longer met that standard, LightEdge sought a modern biometric solution that could strengthen security, improve the user experience, and integrate with their existing systems without disruption.

LightEdge wanted to standardize on biometrics to support a complex security environment serving both employees and visitors. Before modernizing, the company relied on a hand geometry system to activate visitor cards during check-in and to secure sensitive areas such as mantraps. The solution needed to reliably manage access for hundreds of users – including employees, tenants, and visitors – at seven data center locations across Iowa, Missouri, Nebraska, Kansas, Texas, Minnesota, and Arizona while maintaining a consistent and secure experience at every site.

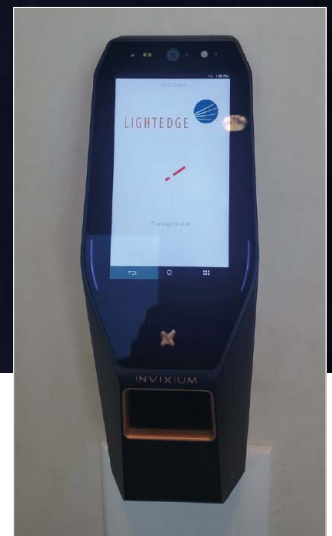
## From Legacy to Leading

LightEdge selected IXM Titan, Invoxium's flagship biometric solution, for its ability to deliver uncompromising security while elevating the user experience. Combining multi-biometric authentication with a sleek, all-aluminum design and a 5-inch LCD screen, the solution brings both precision and sophistication to every access point. Deployed across key locations, IXM Titan replaced legacy systems and transformed how access is managed. Visitor check-ins are faster and more

intuitive, while critical areas such as mantraps are secured through a consistent, streamlined workflow. After years of continuous use, LightEdge continues to benefit from a solution that not only strengthens security but also projects a modern, forward-looking image that aligns with its brand.

## Swift Verification

By replacing traditional credentials with advanced biometric authentication, LightEdge significantly reduces the risk of unauthorized access or credential sharing. Multi-biometric capabilities add an additional layer of assurance, ensuring that only verified individuals can enter sensitive areas, even in high-traffic environments. Touchless facial recognition streamlines access for employees, tenants, and visitors, while authentication is completed in seconds, reducing bottlenecks at entry points and improving overall operational flow. This is especially valuable in data center environments where both security and efficiency must coexist without compromise.



The all-aluminum case and large IPS display contribute to the sleek design of the Invoxium touchless user terminal.



Integration with existing access control systems allowed LightEdge to modernize without overhauling its entire infrastructure. The transition from legacy hand-geometry systems was smooth and minimally disruptive, enabling teams to maintain continuity while quickly realizing the benefits of a more advanced solution. The IXM Titan's all-aluminum construction and large IPS LCD display contribute to a clean, modern aesthetic that aligns with Light Edge's forward-thinking brand. Every interaction with the device reflects precision, quality, and technological leadership, reinforcing trust with customers and visitors alike.

Standardizing on a biometric solution ensures that security protocols and user experiences are uniform across all facilities. This consistency is critical for organizations operating multiple data centers, as it eliminates variability and reduces the risk of enforcement or usability gaps. With a standardized solution in place, LightEdge's IT

and security teams can manage access control more efficiently, reducing administrative overhead and enabling faster response times.

### Healthy Bonus

The platform is designed to scale alongside LightEdge's expansion as new facilities, users, or security requirements are introduced. The solution can adapt without requiring significant reconfiguration or additional complexity. Touchless authentication minimizes physical contact at shared access points, supporting cleaner, more hygienic environments. This is particularly relevant in high-density facilities where reducing touchpoints contributes to the overall workplace. **GIT**



Invixium

[www.invixium.com](http://www.invixium.com)

© Images: Invixium

### Simplifying the Switch to Digital Access with Programmable Keys and Compatible Cylinders

With a key-based digital access management system like Assa Abloy's Cliq solution, it becomes straightforward to grant access rights that are personalized to an individual's precise needs and level of authority. Every access event is logged by the system, so audit trails can be generated with a few clicks in the software control panel – streamlining compliance obligations with regulations such as NIS2 and the CRA. The Cliq ecosystem includes more than 60 different cylinder and padlock types. Smart key systems are the fastest, least disruptive way to switch mechanical security for intelligent digital access. Electronic or electromechanical locking cylinders simply slot into place instead of the legacy mechanical devices, without door damage or wiring. Intuitive software and programmable digital keys issued to authorized site users gives facilities management teams granular control over the movements of staff and contractors.

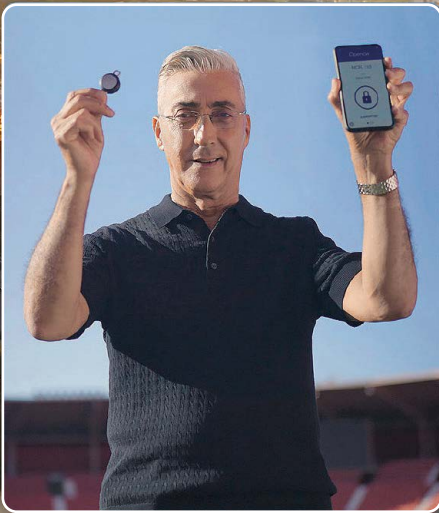
[www.assaabloy.com](http://www.assaabloy.com)



**Fire protection  
solutions for  
data centres**



**Inspection doors for  
installation shafts  
in data centres**



A variety of different credentials can be used with the comprehensive digital access control system at Spanish soccer club UD Almería.

Stadiums require access technology that is versatile, durable, reliable and easily scalable. Finding a single system that meets all these needs and simultaneously has digital devices for all the different types of openings in a typical stadium is not straightforward. In many cases, security managers resort to running two security systems in parallel.

Spanish soccer club UD Almería wanted to transition from traditional mechanical locks to digital access control for a security upgrade at their 18,000-capacity stadium without getting into the situation of having a mix of digital control and mechanical cylinders to administer. They sought a solution that could provide centralized management from a single, intuitive software interface. Ease of installation within the existing stadium infrastructure and the ability to equip heavily used doors were further criteria.

They chose Assa Abloy as their partner to digitize their access control, whose SMARTair digital access system includes wireless locks for many access points and mobile keys or smart cards for user convenience. The team at Almería benefited from technical support provided by Assa Abloy specifiers who have the expertise to work on digital access solutions for complex stadium projects. The final solution also offers centralized management of Assa Abloy eCliq smart keys, electronic cylinders and padlocks, and enables all the different access points in the stadium to be secured digitally.

FOCUS SPAIN | ACCESS CONTROL

## On The Ball

Hybrid Smart Key and Mobile Solution Digitizes Access at a Spanish Soccer Stadium

For added convenience, every smart key also has an RFID chip inside that can be programmed to unlock authorized doors secured with SMARTair devices.

including the police, carry an eCLIQ smart key programmed with individual access permissions.

### Credential Choice

By adding Cliq devices within a SMARTair solution, security managers have total traceability of access events in a single system, saving time and hassle. They can even manage access at remote locations that are equipped with durable Cliq cylinders and programmable keys, all from the familiar user interface. The combination of the two systems gives facilities managers the choice of both mobile credentials and RFID credentials (smart cards, fobs, or badges). Retrofitting existing doors was simple: installers simply replaced the mechanical cylinder with an eCliq cylinder, without wiring or batteries. Power is carried to the cylinder via the user's battery-powered key.

The club security team chose SMARTair for real-time control and oversight of offices, locker rooms and physio suites. Authorized staff use customized RFID cards that double as ID badges or mobile keys in the Openow app. Visitors and external contractors receive time-limited access through mobile keys sent directly to their own app, streamlining convenient visitor management. Alongside this, eCLIQ cylinders protect the technical rooms and interior service zones. Maintenance staff and security personnel,

### One User Interface

Both the electronic and electromechanical cylinders and the out-of-the-box SMARTair system are part of a suite of connected Digital Access Solutions from Assa Abloy. When they are deployed together, security teams can manage even more doors from the usual software interface. They can implement digital access almost anywhere, without drilling or causing damage to the building structure. All user profiles and access points are managed online using SMARTair TS1000 Web software. Installed devices can include i-max escutcheons and knob cylinders for glass doors, as well as integrated wall readers for office turnstiles. These are supplemented with eCliq smart key-operated digital cylinders, Cliq wall PDs and eCliq padlocks for gates and tool cages. This entire digital system operates without cables leading to or laid around any openings: both SMARTair and Cliq devices are wireless and were installed in the stadium quickly between home matches, without invasive structural work. **GIT**



Assa Abloy Opening Systems  
www.assaabloy.com



## KRITIS-Tage 2026 Provide Insights into Security and High Availability for Critical Infrastructure

The successful series of KRITIS-Tage events continues in 2026, with the next event taking place at the Groupama Stadium in Lyon, France on 11 June. It will provide security managers, consultants, planners, and specialist installers with up-to-date expertise on protecting critical infrastructure and NIS-2 entities. The first event already took place in April in Mainz, Germany. Under the motto "Well informed for the future: security and high availability for critical infrastructure", the KRITIS-Tage 2026 will address the current challenges and requirements of technology, legislation, and real-world practice. Experts will provide updates on the current status of legal frameworks – such as the NIS-2 Directive and the German CRITIS Umbrella Act – and offer practical insights into best practices for the physical and digital security of critical infrastructure and NIS-2 entities. [www.kritis-tage.de](http://www.kritis-tage.de)

## Camera to Cloud Connectivity Within a VSaaS Platform

i-PRO have announced that selected cameras now support native camera-to-cloud connectivity within Milestone's Arcules video surveillance-as-a-service platform. The integration enables i-PRO cameras



to connect directly without requiring on-site servers, recorders, or hardware gateways. Organizations can then deploy a simplified, serverless video infrastructure while maintaining high performance, robust cybersecurity protection, and operational flexibility. i-PRO cameras operate as intelligent edge devices that transmit encrypted video and event data directly to the Arcules platform. This delivers centralized cloud video management, including live monitoring, playback, event search, mobile access, alert management, and case handling tools across distributed environments. Embedded edge AI analytics processes people and vehicle detection directly within the camera. Only relevant metadata and event-based footage are transmitted to the cloud, reducing bandwidth consumption while maintaining real-time responsiveness. [www.i-pro.com](http://www.i-pro.com)

## Hybrid Smart Key and Mobile Solution Digitizes Access at a Spanish Football Stadium

Stadiums require access technology that is versatile, durable, reliable and easily scalable. Finding a single system that meets all these needs and simultaneously has digital devices for all the different types of openings in a typical stadium is not straightforward. In many cases, security managers resort to running two security systems in parallel. Spanish football club UD Almería wanted to transition from traditional mechanical locks to digital access control for a security upgrade at their 18,000-capacity stadium. They chose Assa Abloy as their partner to digitize their access. Their SMARTair digital access system includes wireless locks for many access points and mobile keys or smart cards for user convenience. The same solution now also offers centralized management of eCLIQ smart keys, electronic cylinders and padlocks. This combined solution enables the stadium to secure all their different access points digitally. For added convenience, every CLIQ smart key also has an RFID chip inside which can be programmed to unlock authorized doors secured with SMARTair devices. Aligning CLIQ with SMARTair gives facilities managers the choice of mobile credentials or RFID credentials (smart cards, fobs, or badges). Retrofitting existing doors was simple: installers simply replaced the mechanical cylinder with an eCLIQ cylinder, without wiring or batteries. Power is carried to the cylinder via the user's battery-powered key. Both CLIQ electronic and electromechanical cylinders and the SMARTair out-of-the-box system are part of a suite of connected Digital Access Solutions from Assa Abloy. When they are deployed together, security teams can manage even more doors from their SMARTair software interface. They can implement digital access almost anywhere, without drilling or causing damage to the building structure. [www.assaabloy.com](http://www.assaabloy.com)



## Octave Launches New Brand Built Around Unleashing Intelligence at Scale

Octave, the potential software spin-off from Hexagon AB, has unveiled its new brand identity, marking a major step toward its transition into an independent company, comprised of Hexagon's Asset Lifecycle Intelligence and Safety, Infrastructure & Geospatial divisions, alongside the Bricsys, ETQ and Projectmates businesses.

Octave's brand signals a clear vision of purpose and mission to unleash intelligence at scale, and unifies a market-leading portfolio that solves and simplifies complexity across the entire lifecycle. The portfolio is powered by domain-specific artificial intelligence that helps organizations achieve crucial outcomes across the lifecycle that were previously difficult to address. Octave has now announced the acquisition of VXG, a provider of enterprise-grade, cloud-native video management software, that will enable the company to build upon its AI-enhanced cloud capabilities within its physical security portfolio, and further strengthen its software offerings that protect people, places, and assets. [www.octave.com](http://www.octave.com)



Only one Panomera unit is needed to simultaneously deliver both an overview and detailed images

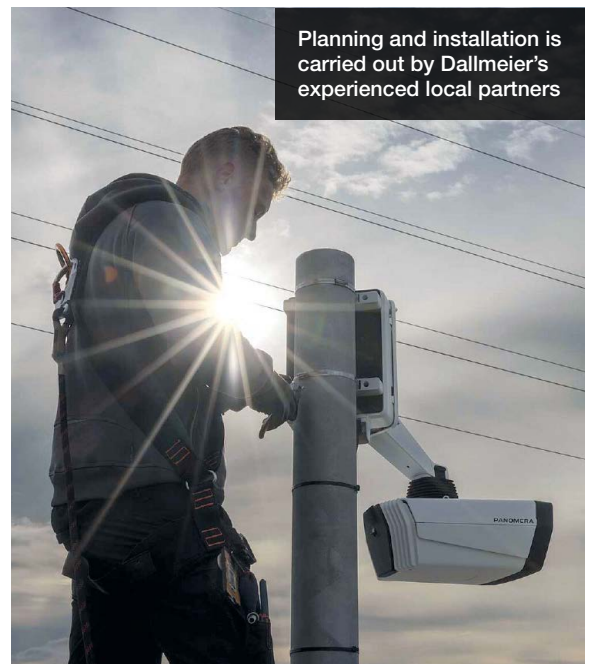


FOCUS SWEDEN | VIDEO

# All In One

## Smart Video Surveillance Provides Seamless Security for a Large Vehicle Fleet

A leading industrial company in the greater Stockholm area faced the challenge of efficiently monitoring a large vehicle yard with hundreds of daily vehicle movements. Existing video technology could offer either an overview or high-detail footage, but not both at the same time. Assisted by security integrator Certego, the company opted for Panomera, the multifocal sensor system from Dallmeier. The solution combines wide-area coverage, detailed resolution, and intelligent video analytics in a single system.



Planning and installation is carried out by Dallmeier's experienced local partners

Conventional surveillance systems were not designed for such large-scale, dynamic environments. Providing full visibility would have required a high number of single-sensor cameras, resulting in significant installation, operation and management costs.

In addition, the overview would often be lost when zooming into a specific area.

The objective was to find a compact yet powerful solution that could deliver both complete situational awareness and precise detail in real time and with continuous recording.

Panomera is a multifocal camera technology developed by the German manufacturer Dallmeier. It is used worldwide in

complex surveillance environments such as industrial sites, logistics hubs, stadiums and urban areas. As Dallmeier's exclusive partner in Scandinavia, Certego offers complete solutions including planning, installation, integration and long-term service. With its modular lens system, each Panomera unit can be tailored precisely to the specific sur-



The Panomera system is of course capable of handling adverse lighting conditions

veillance environment, ensuring maximum visibility with minimal infrastructure.

Multifocal sensor technology merges both an overview and details into one image. The Panomera multifocal sensor system from Dallmeier has multiple lenses of different focal lengths housed in a single unit, which allows simultaneous capture of large areas and high-resolution detail views without switching perspectives or losing the bigger picture. This is especially valuable for security personnel: even when zooming in on an incident, the full scene continues to be recorded all the time, ensuring that no information is lost.

#### Seamless Implementation from an Experienced Partner Network

The project was implemented in close cooperation with Scanview, Certego's sister company in Denmark, which has extensive experience in deploying Panomera systems. This strong partnership ensured smooth planning and installation, and resulted in a solution that had not previously been available on the Swedish market.

"By combining our local presence with Scanview's technical expertise, we were able to deliver a solution that was truly new to the Swedish market," explains Rafael Samuelsson, Certego's CCTV Technical Expert.

Panomera delivers a wide range of technical and operational advantages for the customer, including high-resolution imaging even across long distances and in chal-

lenging lighting conditions, real-time event detection through intelligent, AI-supported video analytics and, importantly for the budget controllers, a reduced camera count thanks to efficient coverage of large areas. The system can be seamlessly integrated into an existing security infrastructure and is a future-proof platform that is scalable to meet additional requirements. "We needed a system that provides a full overview, sharp detail and ease of use. Panomera delivers exactly that," says Samuelsson.

#### Future Ready

The Panomera system has significantly improved the customer's situational awareness and security response capabilities. At the same time, it simplifies day-to-day monitoring and reduces strain on personnel through intuitive operation and targeted alerts. Thanks to its modular, scalable architecture, the system is a future-ready investment that allows straightforward expansion and adaptation to changing needs. **Git**

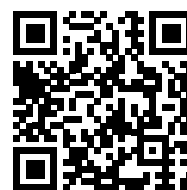


Dallmeier electronic  
GmbH & Co. KG  
[www.dallmeier.com](http://www.dallmeier.com)

# VOTE NOW

CLOSING DATE  
**SEPTEMBER 1<sup>st</sup>, 2026**

**GIT**  
**SECURITY**  
**AWARD**  
FINALISTS



## GIT SECURITY AWARD

Information on the finalists,  
voting and readers' prize:

[www.security-award.com](http://www.security-award.com)



# WILEY



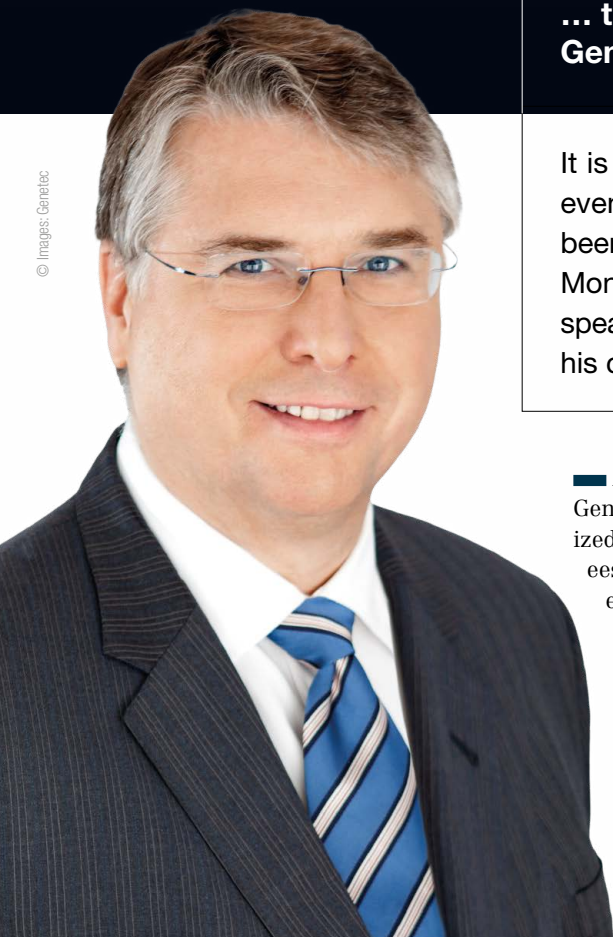
Control room in Mont Royal Shopping Mall in Montréal, equipped with Genetec's video surveillance technology

## COVER STORY

# To AI or not to AI

... that is the Question. An Impression of Genetec's Application of Ai Right from the Source

It is not every day that an invitation to attend an international press event drops into your letterbox. A two-day program of events had been organized in February this year at the Genetec headquarters in Montreal. Matthias Erler from GIT SECURITY took the opportunity to speak with CEO Pierre Racz, founder and President of Genetec, about his company's latest projects.



© Images: Genetec

■ A two-day program of events at the Genetec headquarters had been organized in February this year for the attendees, who had arrived from many different countries. The physical security market is undergoing ever more rapid changes to adapt to developments in the geopolitical world as well as to the significant improvements in the available technology. Andrew Elvish, Vice President Global Marketing at Genetec, reminded the attendees about the current state and probable future of the market from the point of view of Genetec – GIT SECURITY reported earlier this year. In our interview,

Genetec's CEO, Pierre Racz, explained his views, particularly on the role of artificial intelligence in his industry.

**GIT SECURITY:** Mr. Racz, let me start by asking you, what is currently the most important impact of artificial intelligence within your company?

**Pierre Racz:** The first thing to understand is that the term 'AI' has evolved significantly over time. I have personally been working in this field since the 1980s, when AI meant logic programming – Lisp, Prolog, that kind of thing. Later, we moved on to neural networks and support vector machines. We have actu-

ally been using what was considered AI in our products for a long time – since around 2003. With the rise of deep neural networks around 2010, we transitioned to those, and they have been a core part of our systems since 2012. More recently, we have also been experimenting with large language models.

As an engineer, what matters most to me is understanding the strengths and weaknesses of the tools. It is like building a bridge: if you expect heavy loads, you do not use wood, you use steel. Similarly with AI, you need to know where it works well and where it does not. That is why we design our systems so that the impact of failure is minimized. In practice, this means we keep AI out of the final decision-making loop. Humans provide judgment and creativity while machines handle the heavy lifting.

**What does that look like in practice?**

**Pierre Raczy:** AI is particularly good at what you might call ‘fuzzy search’. It can identify patterns and similarities in large datasets, but it is actually quite poor at detecting fine details. This is because it is fundamentally probabilistic. It does not ‘know’ things – it estimates based on patterns. What people often call ‘hallucinations’ are really just the system returning results that are close enough statistically, even if they are not correct.

**You have used the term “impressionism” to describe just that...**

**Pierre Raczy:** Yes, that is a useful analogy. Before photography, painters – and especially realists – aimed to reproduce reality as accurately as possible. But that role became obsolete once photography emerged, so artists adapted. The Impressionists began painting in a more abstract, ‘pixelated’ way – large brush strokes that only form a coherent image when viewed from a distance. You do not see precise detail; you get an impression. AI works in a similar way: it forms an impression based on its training data and projects your question onto that. The result is essentially a guess – sometimes surprisingly accurate, but still a guess.

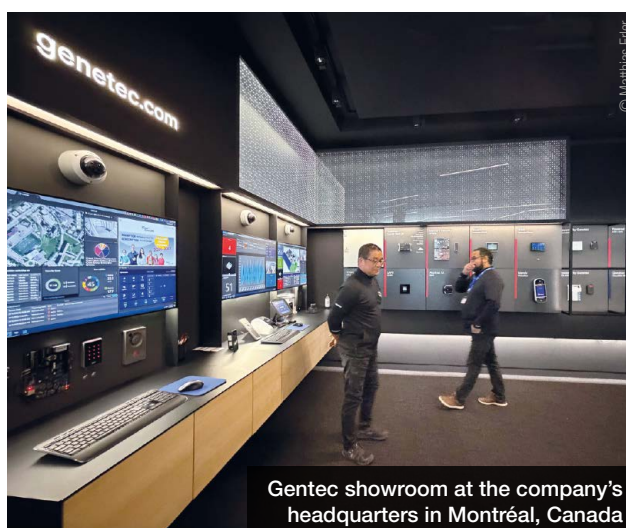
**What do your customers expect from AI today?**

**Pierre Raczy:** Interestingly, many customers have become quite skeptical. At industry events, you see vendors enthusiastically promoting AI, but customers often respond: “Do not give me noise – give me something

useful.” They do not have time to evaluate endless new technologies, and there is a growing awareness that simply labeling something as ‘AI-powered’ does not mean it is valuable. In fact, it can be a red flag. There is even a tendency to use “AI” as shorthand for poorly done work. Some people joke that AI is like a lazy intern with a bad attitude.

**So AI is more of a tool than a solution?**

**Pierre Raczy:** Exactly. It is like a calculator: it does not make you smarter or dumber – it just makes you faster, but only if you know how to use it properly. There is also a growing ability to recognize AI-generated content. Once you have learned the patterns, you start noticing them everywhere – repetitive structures, overused phrasing, and so on. And fundamentally, AI does not innovate – it imitates. It recombines what already exists.



Genetec showroom at the company's headquarters in Montréal, Canada

**Looking ahead, how do you think AI will change the physical security industry over the next five to ten years?**

**Pierre Raczy:** In the short term, I expect problems. We will likely see what I would call ‘sloppy security’ – systems that work well in controlled environments but fail in the real world. This can create a false sense of security, and adversaries will exploit these weaknesses. I think we will see some significant incidents as a result. There is even a term for this: “AI slop”. It refers to low-quality, poorly implemented AI systems.

**Is that already happening?**

**Pierre Raczy:** Yes, it is. It just has not yet led to large-scale, widely reported disasters. Over time, though, we will learn. Every new technology goes through this phase. When electricity was first introduced, people used it for all sorts of absurd applications. It takes

decades to figure out how to use new technology properly.

**You also mentioned that people tend to anthropomorphize AI.**

**Pierre Raczy:** Yes, that is a major issue. Humans naturally project intelligence onto these systems. We saw the same thing decades ago with early chatbots like “Eliza”.

Today’s systems are more sophisticated, but the underlying limitation remains: they do not truly understand. They can also struggle with ambiguity – for example with certain linguistic constructs that humans can easily interpret.

**Let us return to your company. What are your plans for the coming years?**

**Pierre Raczy:** Our focus is on helping customers to achieve greater operational efficiency. Many of them face constraints – budgetary, regulatory, or legal – and they want to know how technology can help them to meet those constraints without compromising their mission. Interestingly, about 50 % of our product features come directly from customer input. The other 50 % are things we anticipate ourselves – though not all of those turn out to be useful. Our approach is essentially exploratory problem-solving. We work closely with customers, test ideas, and iterate – without wasting their resources.

**Are there any current developments you can share?**

**Pierre Raczy:** One key direction is our hybrid approach – bridging the gap between cloud and on-premises systems. Different organizations have very different requirements: some want everything in the cloud, others want minimal cloud involvement, and many need a mix due to regulatory or performance constraints. We have designed our systems to handle this flexibility with a single code base. That allows us to adapt to different environments without forcing customers into a rigid architecture.

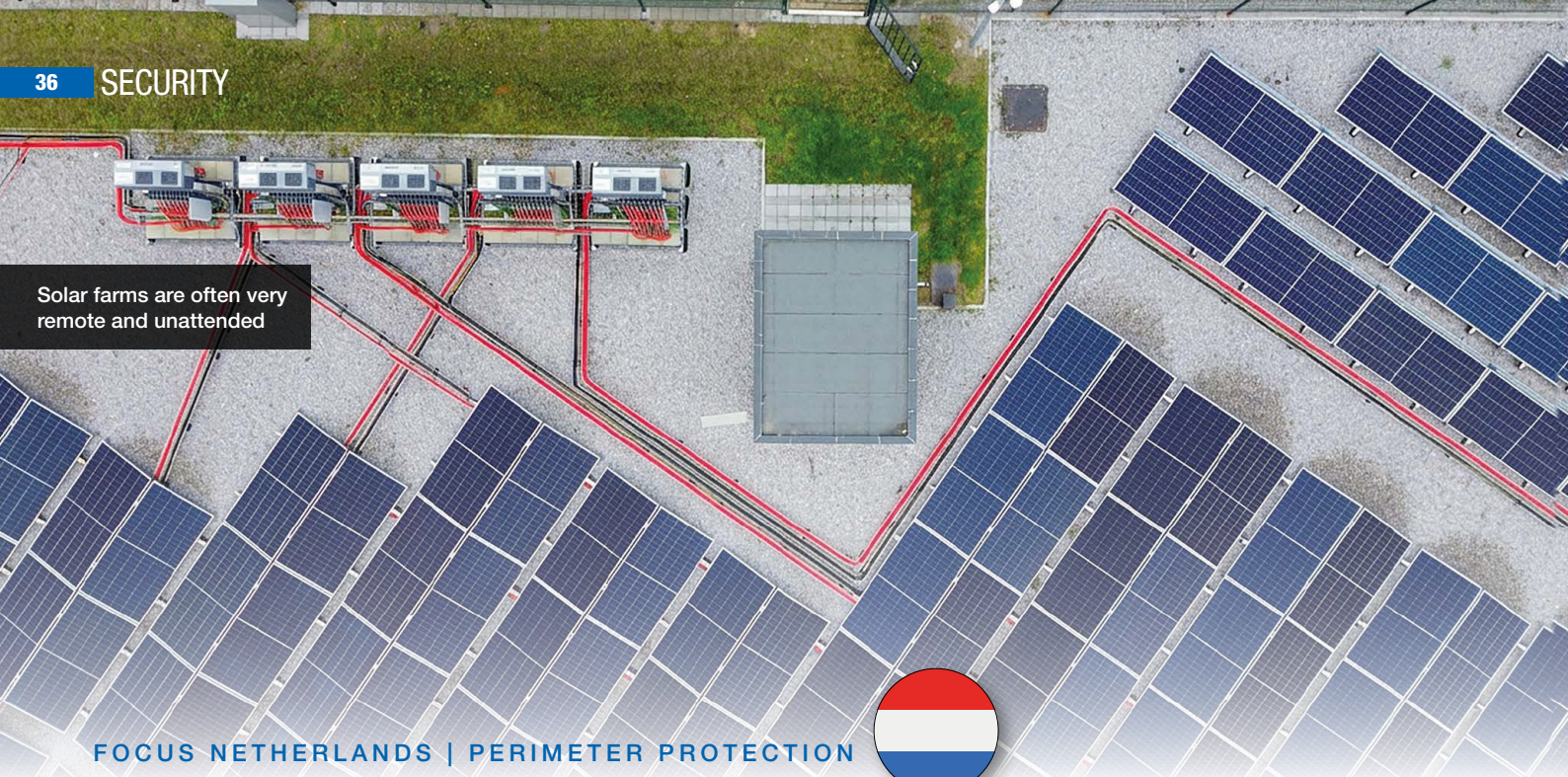
**Thank you very much for your time.**

**Pierre Raczy:** My pleasure. **GIT**



Genetec

www.genetec.com



Solar farms are often very remote and unattended

FOCUS NETHERLANDS | PERIMETER PROTECTION



# Lightfingers In The Dark

## How a Major Solar Farm in the Netherlands Was Made Secure

A large solar farm in Almelo, near the German border in the Netherlands, recently faced a severe challenge: a highly coordinated theft of copper cables by organized criminals. This incident highlighted the growing threat facing renewable energy sites across Europe, where high-value metals and remote locations make solar farms prime targets. The loss of critical infrastructure exposed weaknesses in the site's perimeter security and prompted immediate action to safeguard operations and assets.

Like many solar farms, the Almelo site spans a vast, minimally staffed area, making traditional security measures such as fencing and standard CCTV insufficient. With copper thefts and associated losses rising sharply, UK reports alone show a 93% jump in solar-related crime from 2021 to 2022, site operators are under increasing pressure from both operational and insurance perspectives to fortify their defenses.

Solar installations are uniquely vulnerable to theft and vandalism due to several factors: their remote and expansive locations often span hundreds of acres, with minimal staff presence, providing criminals ample opportunity to act undetected; high-value materials such as copper cabling, inverters, and batteries all carry strong resale value and are easier to transport and offload than large panels; studies indicate that once a site is attacked, there is a high likelihood of future targeting unless security is visibly improved.

Operators have reported incidents of cable theft exceeding 50 kilometers in a single event and more than 5,000 major thefts annually across Europe, demonstrating the

scale and persistence of the problem. These trends underline the insufficiency of traditional passive measures such as fencing or standard CCTV alone, leading many insurers to raise premiums or condition coverage on enhanced security provisions.

### Strategic Security Partnership

To address these vulnerabilities, the Almelo solar farm operator turned to their trusted security partner, Loogisch. Together with distributor SmartSD and technology company Optex, they engineered a new, multi-layered perimeter security system. At the heart of this solution is the award-winning Optex Redscan Lidar (RLS-50100V), selected for its precision, reliability, and long-range detection capabilities.

Redscan Lidar offers several advantages, such as having an extended detection range that covers up to 50×100 meters with a single unit. Flexible zoning provides eight independent detection zones for tailored alarm logic and smart VMS integration. The all-weather capability maintains high performance in rain, fog, and low light, unlike tra-

ditional sensors. Advanced intruder detection will detect slow, low-profile intruders often missed by PIR or microwave sensors.

### Engineering a Robust Solution

The new perimeter system was meticulously designed to overcome some site-specific challenges. Strategic positioning and precise angling of the detectors avoids false alarms from interference, for example from birds perching on panel edges, while custom zone shaping has countered issues from glare and panel reflections. The system was validated under operational conditions for maximum reliability. According to Frank Pikkemaat, Operational Manager at Loogisch, "The combination of long range and flexible zoning made Redscan the clear choice. One detector covered the entire field."

Optex provided expert support with remote configuration, zone tuning, and ongoing performance optimization, ensuring that the system delivered as promised. About the collaboration with Optex, Frank Pikkemaat, Operational Manager at Loogisch, said, "After the skilled help provided

by Optex during the fine-tuning process, we were very content that the system performed exactly as we intended.”

### Proven Results

Since installation, the upgraded security system has achieved zero intrusions: there have been no unauthorized entries since deployment. There has also been a 90%+ reduction in false alarms, with dramatically fewer nuisance alerts, boosting operator confidence and efficiency. Enhanced situational awareness is delivered through integration with Milestone VMS and Domox visualization, which enables real-time monitoring and rapid event verification.

Low maintenance requirements and reliable performance reduce the risk of downtime and support long-term cooperation between the solar farm operator and their partner Loogisch. The positive outcome demonstrates how advanced perimeter detection, and especially lidar-based technology, can transform security outcomes for critical infrastructure.

### The Strategic Value of Advanced Perimeter Protection

The Almelo case is a benchmark for best practice in solar farm security. As theft and vandalism continue to threaten renewa-



ble energy infrastructure across Europe, advanced perimeter detection, especially Lidar-based solutions, are proving essential for the protection of assets, uptime, and future project viability. Operators who invest in layered, professionally designed security solutions not only deter crime but also secure insurance eligibility and safeguard their business continuity.

The deployment of Optex Redscan at the Almelo solar farm has set a new standard

for effective, reliable security in the renewable energy sector. With zero intrusions, a drastic reduction in false alarms, and improved operational confidence, this project demonstrates the strategic value of advanced perimeter protection for critical infrastructure. **GIT**



**Optex Europe B. V.**  
www.optex-europe.com

© Images: Optex Europe

### AI Cameras Introduced

Chroma24 breaks through the limitations of traditional surveillance equipment that typically delivers only black-and-white, blurry images at night. Even in low-light conditions, it outputs clear images with true color and extremely low noise, ensuring sharp details in nighttime footage. In dynamic scenes, the system suppresses motion blur and ghosting, while wide dynamic range technology (WDR Pro) balances bright and dark areas. Using deep search functionality, users can quickly locate key footage by color, person, or vehicle attributes, whether during the day or at night, significantly reducing manpower and time costs. Chroma24 is

well suited for environments with insufficient lighting, large coverage areas, or round-the-clock security needs, such as parks, campuses, suburban roads, and critical infrastructure, including factories, warehouses, energy storage facilities, and solar power plants, and reduces the need for manual patrols.

**www.vivotek.com**



### Multifocal Camera Receives Highest Distinction at the Red Dot Awards

The Panomera V8 from Dallmeier has once again received a prestigious design award at the Red Dot Awards 2026. The multifocal sensor camera was honored with the highest distinction ‘Best of the Best’ in the Product Design category. After already winning the iF Design Award 2026, the camera has now also impressed the jury of the Red Dot Design Award, an internationally renowned competition in the field of design. With the Panomera V8, Dallmeier has developed a camera system that combines state-of-the-art multifocal sensor technology and artificial intelligence into a single system, delivering seamless 180° coverage without blind spots and highly precise analysis, even across large areas.

**www.dallmeier.com**



Gerhard Harand, Geschäftsführer von Wehrhan TPS

## SERIES: TESTING GROUNDS

# Targeting Drones

**Perimeter Security in a Practical Test:  
How the Wehrhan-TPS Urban Test Site  
Makes Real Attack Scenarios Visible**



New series: Testing Grounds put to the test with Markus Piendl and Hannes Dopler – Practice-oriented tests of radar sensors and video management systems on an urban security test site – accompanied by our two independent experts Markus Piendl and Hannes Dopler.

Our new series: No showrooms, no PowerPoint stages – but environments in which security technology has to show what it can really do. Part 1: With Markus Piendl and Hannes Dopler at Wehrhan-TPS.

Perimeter security is becoming increasingly important in view of the growing requirements in urban areas and critical infrastructures. GIT SICHERHEIT took the two experts Markus Piendl and Hannes Dopler to the test site of Wehrhan-TPS Sicherheitstechnik GmbH in Vienna. There, they examined radar sensor technology, system integration and offender profiles under real conditions – and showed the role that practical test environments play in planning, evaluation and decision-making processes.

## A test site in the middle of the city

Wehrhan-TPS Sicherheitstechnik GmbH has a long company history dating back to the 1920 s. Originally operating as a traditional security company with key and lock technology, the company developed into an installation company for access, alarm and video systems after the takeover in 2004. In 2010, the company merged with TPS Technology, Planning, Security GmbH, adding expertise in video and alarm management as well as a wholesale division. Today, the company employs over 20 people who work on a wide range of security technology solutions.

The decision to have its own test site was made for practical reasons: Complex video and perimeter systems can only be assessed to a limited extent in sterile laboratory environments. Realistic conditions are required in order to reliably assess false alarms, shadowing, blind spots or the combination of different sensors. The focus is not only on the technology – human behavior and unconventional movement patterns must also be tested.



From left: Renato Nordera (GPS Italia), Jovan Pajic and Gerhard Harand (both Managing Directors of Wehrhan TPS), and expert Hannes Dopler



Wehrhan TPS Company Grounds: A test site right in the city center – as realistic as at the customer's own premises

detection, the system supports configurable alarm and exclusion zones as well as the definition of crossing lines.

Another focus was on integration into the Milestone video management system. The sensors are connected directly to the event server via a MIP plugin, which enables a central display in the Smart Client including a map view. The installation takes place on the server side and makes it comparatively easy to add further GPS system elements.

please turn page ►

### Trigger: A KRITIS project with special requirements

The visit by our two experts Markus Piendl and Hannes Dopler arose from a specific inquiry from a company in the KRITIS environment, which was brought to Markus Piendl. The task: a perimeter security solution for a challenging urban location with irregular fence lines, walls, access roads and several entrance areas. The end customer has a great deal of technical expertise and wants to test the sensors and system integration personally before placing the order. As Gerhard Harand explains: „Markus Piendl had informed me that a company in the KRITIS environment was looking for a perimeter security solution in an urban location with difficult fence lines, walls and various entrances. A good price-performance ratio was just as important as the fact that this customer wanted to see the sensors and their integration into a video management system for themselves and try them out in person before placing the order.“

### Sensor technology in focus: Radar 077

For the tests, the team is preparing the 077 radar from GPS Italia – a 77 GHz radar system with two operating modes: a 90° wide mode with ranges of up to 40 meters and a narrow „blade“ variant with a distance coverage of around 60 meters. The sensor system uses MIMO technology, machine learning-based classification and allows multiple objects to be tracked simultaneously. In addition to pure

### „Improving the firmware based on the tests“

**GIT SICHERHEIT:** Hannes Dopler, your impression of the test site?

**Hannes Dopler:** I was impressed by the flexibility of the area. We were able to run through different perpetrator profiles in a short space of time and quickly change sensor positions.

**What do you look for in perimeter tests?**

**Hannes Dopler:** The behavior in exceptional situations – slow movements, concealed approaches or atypical ways of moving. These scenarios show how reliably a system really works.

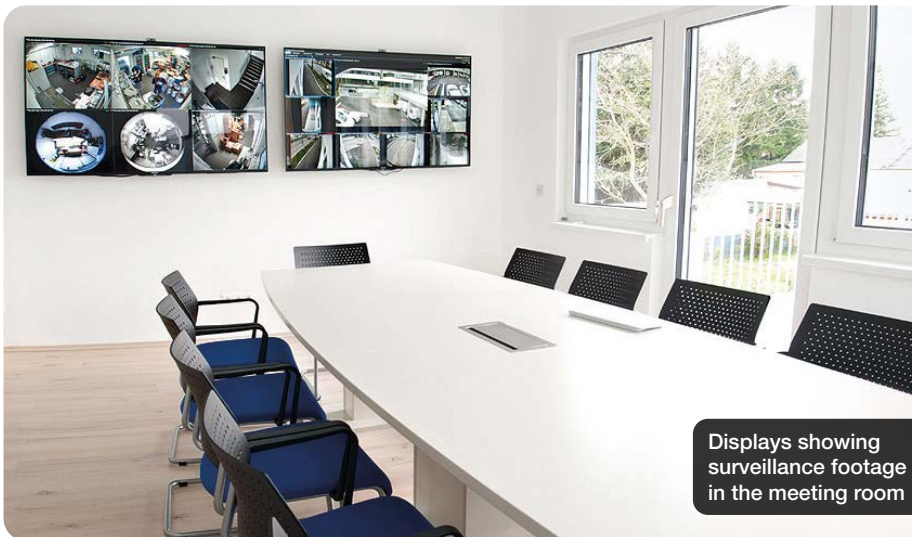
**What is your conclusion – and how did the collaboration with the participants go?**

**Hannes Dopler:** Operating a test site in a large city is of course something special due to the limited space. I was particularly impressed by the wide range of options for installing sensors quickly and easily. We were able to simulate the various perpetrators' actions at short and medium distances without



Hannes Dopler, Sachverständigenbüro Markus Piendl

any problems, for example at delivery entrances, parking lots, office entrances or underground garages – and without being disturbed by third parties. I also really liked the fact that GPS immediately took on board our suggestions for firmware changes.



Displays showing surveillance footage in the meeting room



Rolling in slow motion, expert Hannes Dopler attempts to outwit the safety systems.

### Examination procedure: perpetrators, profiles and manipulations

Up the stairs and into the tests: the test day started in the training room on the second floor of the Wehrhan building. End customers, manufacturer representatives and the

TPS team follow the experts' test sequences on several monitors. Meanwhile, the two experts simulate burglar behavior in various forms – with and without camouflage, slowly, quickly and with the use of aids. The aim: to systematically record the response behavior of the sensor system. And: test,

test, test. Scenarios such as „leopardizing“ and „ocelotizing“ are particularly demanding – crawling and rolling movements that are designed for minimal signature. TPS boss Harand: „A highlight of the intrusion tests was the ocelotting and leopardizing with simultaneous cover from flares, dazzle and confetti grenades as well as attempts to manipulate the sensors in a targeted manner.“ In other words, bang effects included. At the same time, video analysis functions were used to support verification processes.

### Results: Reliable data and concrete optimizations

The important break-in tests were successfully completed. The manufacturer's development department, which was connected remotely, followed the tests live and was able to analyze trigger thresholds and events in real time. Feedback from the experts was immediately incorporated into firmware adjustments and optimizations to the Milestone plug-in. The highlight and a special achievement of the Wehrhan TPS partners: the proposed changes were implemented just a short time later.

Gerhard Harand: „The break-in tests, which are important for the end customer, were passed with flying colors. GPS Italia's development department was connected via a secure internet connection and fol-

## „More than glossy brochures“

**GIT SICHERHEIT:** Gerhard Harand, what role does the proving ground play in your work?

**Gerhard Harand:** It helps us to assess systems as they behave in actual use. Many issues – such as limit ranges or false alarms – can only be evaluated under real conditions.

**How do you benefit from independent tests?**

**Gerhard Harand:** They broaden our perspective. Experts like Mr. Dopler and Mr. Piendl contribute other test methods and provide valuable information for manufacturers and for us as installers. And

that's good for the project, the customer and the operator!

**What significance does this have for the industry?**

**Gerhard Harand:** I hope that many manufacturers and safety installers like us have small, large and test sites. As many of them as possible should be presented in this series at GIT SICHERHEIT! We can learn so much from each other. As we all know, glossy brochures are one thing – but a visit to a test site, including good follow-up work, is clearly preferable.



Ing. Gerhard Harand, MSc,  
CEO Wehrhan TPS

lowed live how well the sensors worked and which trigger thresholds were triggered in real time. We also transmitted a live video stream. The two experts gave GPS and us good tips for improving the sensor firmware during the tampering tests and also contributed good ideas for the Milestone plug-in.

This gave the end customer a clear picture of the functionality, limits and integration capability of the system – and ultimately the decision to implement the project together with Wehrhan-TPS and the selected partners.

### Partner GPS Standard: Solutions for perimeter protection

GPS Standard has been a European provider of perimeter protection solutions for decades and relies on a combination of sensor technology, data fusion and modular security architectures. Headquartered in Italy, the company develops radar systems, fence sensors and ground detection technologies based on various physical principles. This range allows perimeter solutions to be flexibly adapted to terrain, building structures and environmental conditions – an aspect that is just as relevant in the industrial sector as it is in the area of critical infrastructure.

One of the company's main focuses is the continuous further development of its own radar platforms. Systems such as the 77 GHz radar 077 used in the test are based on active detection technology, supplemented by classification algorithms that distinguish between different object types. The products also support integration into higher-level video management and control systems. This openness makes it easier for installers to connect to existing infrastructures and creates standardized alarm and documentation processes.

### Partner Milestone: Solutions for video management

Milestone Systems is one of the established providers of open video management platforms and has been developing software solutions designed for scalability and integration capability since the late 1990 s. Headquartered in Denmark, the company relies on an ecosystem model in which video, audio, sensor technology and analysis tools from different manufacturers can be brought together via standardized interfaces. This approach supports installers, planners and operators in connecting different system

## „Test site makes expertise visible“

**GIT SICHERHEIT:** Markus Piendl, how did the visit help you in your assessment?

**Piendl:** The real-world environment helped us evaluate the systems objectively. That's more meaningful than pure theory.

**What makes the test site stand out?**

**Piendl:** The combination of a training room and a test field is practical. You can see from above what's happening below – that makes evaluation and discussion easier.

**What advice would you give to installers?**

**Piendl:** A test site makes expertise visible. It helps set realistic expectations and select systems responsibly. And specifically regarding Wehrhan TPS here: The logistics are truly unique. The fact that customers can sit comfortably in the training room while sensors are being tested right beneath them – it's simply fantastic. During breaks, both laypeople and experts can try out settings, various intrusion detection systems, IP intercoms and speakers, as well as video and access systems on exhibits and in live operation. I really liked the comparison of the different Milestone versions, including the fully functional GPS plug-in. The integrated approach



Markus Piendl,  
Sachverständigen-  
büro Markus Piendl

and the avoidance of siloed solutions are truly put into practice. Security installers face significant price pressure in many projects: a test site is an excellent way to stand out from the competition. Wehrhan TPS has achieved this brilliantly here in a very small space. Thank you for letting us visit.

landscapes – from small installations to extensive networks.

The core of the portfolio is the XProtect platform, which is available as a basic, mid-range or premium version depending on the size of the project. The software allows the operation of classic monitoring structures as well as the integration of modern analysis methods, including object recognition, motion pattern analysis or event automation. External hardware and sensors – such as the tested Radar 077 – can be connected directly via the Milestone Integration Platform (MIP) SDK. This creates a common event structure that displays both visual and sensor data in a synchronized manner.

### Conclusion: added value for manufacturers, installers and customers

The decisive factor is on the pitch, to quote coaching legend Otto Rehagel. We at GIT SICHERHEIT can only agree with this, because it is precisely in the area of safety

that test sites enable a differentiated view that goes far beyond glossy product brochures. They bring together real conditions, clear opportunities for comparison and comprehensible system reactions.

Our experts also emphasized that installers can create qualitative added value in the face of price pressure and set themselves apart from the competition.

And if, as in this case, good results and the famous safety plus can be achieved for the customer and operator – what more could you want? **GIT**



**Wehrhan TPS**  
Sicherheitstechnik GmbH  
www.Wehrhan-TPS.at

CSO TALK

# Guidelines Do Not Deter Attackers

Deutsche Telekom CSO Warns of AI-Accelerated Cyberattacks



Thomas Tschersich is Global Chief Security Officer (CSO) of Deutsche Telekom and CEO of Telekom Security. In addition to cyber security, he is responsible for the Group's cyber security and operational security issues. He is also Chairman of the Board of „Deutschland sicher im Netz“ and a member of the Cybersecurity Council. In an interview with GIT, Thomas Tschersich talks about the current challenges of his work and how 2,500 experts successfully fend off 76 million attacks every day. We also asked Dr. Tschersich about „OnNet“, a service that automatically integrates security into the network – and about the dangers of AI-supported adversaries that exploit vulnerabilities in seconds.

**GIT:** Mr. Tschersich, cybersecurity is naturally a key issue for Deutsche Telekom. Let's start with the organizational aspects. How is cybersecurity set up and organized within Deutsche Telekom?

**Thomas Tschersich:** Historically, like many companies, we come from a highly distributed structure in terms of the division of responsibilities. IT security was the responsibility of IT, network security was separate from this, corporate security was the responsibility of Group Security and so on. This leads to a structural problem: as the person responsible for security, you are often subordinate to the CIO, who generally pursues a cost-cutting agenda. In cybersecurity, however, you often have to invest, i.e. increase costs. This is a classic conflict of objectives.

We therefore decided around 15 years ago to resolve this conflict and put security on an equal footing with the CIO and CTO. As Global CSO, I am positioned directly

at the same level. We report to the same Executive Board. This means that I can't enforce everything I want – but conversely, the CIO and CTO can't enforce anything against security either. There is an obligation to reach agreement, but no relationship of dependency.

We have also bundled responsibility: Cybersecurity and physical and personnel security belong together. After all, threats are not just digital. To give a simple example, a data center can also be attacked physically – via the cooling system, for example.

This has been emphasized more and more recently. . .

**Thomas Tschersich:** Yes. You need to take a holistic view. Many companies are very documentation-driven when it comes to security. There are policies and guidelines. But no attacker is deterred by a guideline. We therefore pursue a risk-based and impact-oriented approach. The greatest risk receives the most resources. And we

only implement measures that measurably improve security. Documentation is necessary, but not sufficient. For example, instead of asking someone whether a system is securely configured, we let the system itself report the status. We want to measure reality, not self-reporting.

How large is your area within Telekom?

**Thomas Tschersich:** I have a small team of around 20 people at headquarters. In total, Telekom Security has around 2,500 employees. Around 500 work for the Group's internal security and around 2,000 for external customers. This separation is not strict. We consciously use synergies: What we learn within the Group, we pass on to customers – and vice versa. We have around 700 customers in the area of active cyber defense. If something happens at one of them, we can learn from it immediately and adapt the protection mechanisms for all of them.

What kind of external customers do you approach?

**Thomas Tschersich:** They range from large airlines, energy suppliers, banks and other critical infrastructures to small and medium-sized enterprises. Our customers also include very successful SMEs in the automotive sector, global market leaders in various fields, etc. We are also active in the private customer sector, where our main focus is on protection against malware.

Let's take a closer look at your Security Operation Center and the specialized Computer Emergency Response Team (CERT)...

**Thomas Tschersich:** The Security Operations Center is our first line of defense. This is where we monitor log data and systems in order to detect attacks. We are talking about several hundred terabytes of data per day, which are checked against around 2.5 million attack indicators – so-called Indicators of Compromise (IOCs). This is no longer feasible without automation. That's why we rely heavily on machine learning and automation. Around 80 percent of activities are automated, with only 20 percent requiring human intervention.

If an attack is confirmed, the Computer Emergency Response Team takes over. This is the fire department, so to speak. First, the attack is contained – for example, by preventing an attacker from spreading further in the network. It is then removed. In addition, the team processes a large number of vulnerability reports from manufacturers every day. These are evaluated and passed on to the relevant departments so that appropriate measures can be taken.

There is talk of tens of thousands of attacks on telecoms systems every minute. How do you keep up with this?

**Thomas Tschersich:** We operate so-called honeypots worldwide. These are systems that deliberately look like vulnerable real systems. Attackers come across them and try to compromise them. In reality, they are sensors. Thanks to them, we can observe which methods and tools are being used. The majority of these attacks are automated. We have over 2,000 of these sensors in use around the world, including through cooperation with research institutes. This gives us a very good picture of the current threat situation.

We make the processes publicly available on our own website, where you can see, for example, that there have been 51,005 attacks against these sensors in the last 60 seconds – 3.3 million in the last hour. In the last 24 hours, 76 million. These are unimaginably high figures.

They can't all be serious attack attempts...?

**Thomas Tschersich:** No, but they are preparatory actions. You can imagine it like this: If you see someone walking through a high-rise building and looking at every door handle to see if the door might be open and not locked, that's not really a burglary. The break-in only starts when he finds an open door and then goes through it.

AI-supported attacks should take the game to a new level?

**Thomas Tschersich:** First of all, we are currently seeing a massive movement of organized crime towards state actors. In the past, a DDoS attack was followed by an email demanding a ransom. Now the whole thing happens without this ransom component. It's just the attack.

The second change is the speed of the AI. When Microsoft releases an update for a critical vulnerability, it only takes minutes for someone to start scanning the internet for that exact vulnerability. It used to take months. Now it's minutes. There are attack tools that you can use on the darknet that are AI-driven. You no longer need to have attacker know-how, the tool does it all itself. We know of attacks where it only took 70 seconds from the first attempt to successfully penetrating the system.

Mr. Tschersich, Deutsche Telekom's business areas are very diverse. And security requirements play a role everywhere – from product development and network operation to customer service and even Magenta TV. How can security thinking be effectively anchored in this complex world?

**Thomas Tschersich:** We look at three levels: technical systems, physical objects and business processes. The status of technical systems must be known at all times. In the case of physical objects, it's about sabotage or fire risks, and in the case of business processes, it's about their availability. There is also the indirect human factor.

Organizationally, we have clear responsibilities – both technically and geographically. There are people responsible for each

unit. The „security by design“ approach is important. Security is considered right from the start. When new technologies are developed, we are involved right from the start and help shape them. In addition, there is a security acceptance test before commissioning. We prioritize according to risk: high risks require individual checks, for standard cases we fall back on proven blueprints.

The key point here is that we are constantly learning. Every attack – whether within our own Group or at our customers – improves our understanding and our protection mechanisms. This real-time learning is a central component of our security strategy.

The increasing networking of mobile communications, the cloud, IoT and the fixed network is certainly an additional challenge for your security architecture...

**Thomas Tschersich:** The more devices are networked, the more are potentially vulnerable. We have to adapt the level of security measures to this growth. If you visit us in our Cyber Defense Center, you will meet a whole host of smart employees. Instead of handling attacks individually each time, they do it once and then automate these steps. Not out of laziness, but with a view to efficiency and the growing number of attacks.

With „Security OnNet“, you offer protection directly from the network. Is that particularly interesting for smaller companies?

*please turn page ►*



**Thomas Tschersich:** When you do security today, it often involves telling the customer: „You have to install something on your end device, configure it and update it regularly.“ A lot of people are left behind because they don't have the specialist expertise. We therefore asked ourselves the question: why doesn't security come automatically from the network without you having to do anything? Of course, this does not offer a 100 percent security level, but it does go a long way. The idea is to solve the first 80 percent for the customer without them having to do anything. It simply comes as part of the mobile phone tariff in the business customer environment. The customer can switch it on or off – without the need for detailed configuration.

**You report that hundreds of thousands of attacks have been blocked and over a million fraudulent websites have been blocked. Is there presumably no end in sight...?**

**Thomas Tschersich:** Whenever we block something, the attacker goes one step further. It often works like this: you receive a text message – a parcel for you, DHL, DPD.

It contains a link. If you click on it, you are told to install an app – and once you have done so, the attacker takes control of your device. Although we can technically detect and prevent this delivery attempt, we are not allowed to do so because telecommunications secrecy prevents us from doing so. But: When you click on this link, your cell phone establishes access to a website. If we know that it is known to be harmful, we can block it and that is what we do.

**You have just mentioned a regulatory aspect. What is your overall view of the normative situation in this area?**

**Thomas Tschersich:** If you are a critical infrastructure operator, you currently have to report an incident to five authorities in Germany alone, depending on the case: BaFin, the Data Protection Commissioner, the Federal Network Agency, the BSI and the BBK. Five authorities, five completely different reporting channels, five completely different forms, but 95 percent identical content. From the operator's point of view, this means that I am keeping valuable employees, who should actually be solving my problem, busy submitting reports. But that doesn't

solve the problem. I can only start solving the problem once I have finished submitting reports. This is a dangerous path we are on. As long as we are still reporting in order to protect ourselves legally, the attacker has free rein. Of course, we see the legitimate interest of the authorities. But the way the processes are designed, they do not contribute to greater security.

**Is it even possible to keep up with the threat situation?**

**Thomas Tschersich:** There is no way to get out of this situation – but something can be done. You have to secure every system around the clock at all times against all conceivable attacks. The attacker has an advantage because he can choose the target. They determine the attack and the time. You never have equality of arms. But you can stay on it. **GIT**



Deutsche Telekom AG  
www.telekom.de

© Images: Deutsche Telekom AG

## Readers and Updaters for Indoor and Outdoor Access

Readers and updaters for indoor and outdoor use make extending the scope and reach of a Cliq solution even simpler, including to third-party digital access devices. These additions to the product family are compatible with fully electronic eCliq and electromechanical Protec2 Cliq solutions. They simplify both secure unlocking and the transfer of access updates to the keys. All the keyholder needs to do is insert their key and wait for visual confirmation from its inbuilt LED. An optional remote relay unit can add an extra layer of security. Installing and connecting a reader can put a Cliq system in control of user access to doors with electric strikes or motorized locks, automatic revolving doors or sliding glass doors, lift priority and more.

[www.assaabloy.com](http://www.assaabloy.com)



## Synology Underscores Need for Cyber Resilience and AI-Ready Infrastructure in the Middle East

Synology has highlighted the accelerating shift from traditional backup methods to resilience driven strategies among Middle Eastern enterprises during a successful online media briefing it recently hosted. The company emphasized the urgent need for businesses to modernize their data protection strategies as rising cyber risks, accelerating AI adoption, and evolving data sovereignty requirements continue to redefine the region's digital landscape. Recent reports indicate that cyber attacks across the GCC have surged by nearly 40 percent year on year, with the UAE alone experiencing more than 200,000 attempted intrusions per day. This points to the critical need for more robust, adaptive, and forward-looking data protection strategies. Synology suggested the first priority is unlocking value from fragmented and unstructured data through integrated storage, hybrid cloud architectures, and AI-driven capabilities; the second is strengthening digital sovereignty by enabling organizations to retain full control over their data while meeting evolving regulatory and operational requirements.

[www.synology.com](http://www.synology.com)

# SafeLeader

The GIT Talk with the Market Leaders



**GIT** **SECURITY** INTL

**Contact:**  
Miryam.Reubold@Wiley.com

**WILEY**



## DISTRIBUTION

# First Call Partner for Engineers and Integrators

**In Conversation with Connor Doherty: Fast Parts, Clear Data, Powerful Systems – How Digikey Designs Automation Holistically and With a Focus on Safety**

© Digikey

**GIT SICHERHEIT:** What does “automation partner” mean for DigiKey beyond component availability? How is this different from the traditional distributor model in terms of value delivered to OEMs, system integrators, and end users?

**Connor Doherty:** For DigiKey, being an automation partner means we are helping customers reduce friction through their entire automation lifecycle – from concept, design and deployment, through maintenance, repair and operation (MRO). Traditional distributors tend to focus on availability and transactional fulfillment, but at DigiKey, we take pride in our support role that helps enable designs throughout the lifecycle. Our Automation Resource Center, which is designed to provide useful information on topics like protocols, programming, PLCs, robotics and more, offers a partnership level of online support. Finally, as an automation partner, DigiKey provides a high level of operational resilience through fast fulfillment, small lot availability, transparent lead times and a wide breadth of products.

**Which customer problems in automation are your top priorities to solve in 2026–2028?**

**Connor Doherty:** The automation market is rapidly evolving with technology and investments varying across geographical locations. The challenges that stand out to us are threefold:

**Time to deployment pressure:** Our customers are being asked to automate more complex solutions faster with fewer engineering resources. It's our goal to ensure customers are aware of products that can help solve these pressures and get them in their hands quickly.

**System complexity:** Automation systems are increasingly more complex with increased controls, the amount of power, electrical signaling, sensing, connectivity and more. DigiKey offers solution-level support to help customers identify other products they may need to integrate into a complex system, as an extra layer of assistance.

DigiKey is evolving from a pure component supplier to a safety-focused automation partner. Transparent data, fast availability, a system-oriented portfolio, and targeted support for safety standards and certified components make the company the „first call“ for engineers in increasingly complex and safety-critical automation environments. Anke Grytzka-Weinhold, editor-in-chief of our automation trade journal *messtec drives Automation*, spoke with Connor Doherty, Director of Industrial Automation at DigiKey.

**Lifecycle resiliency:** Many automation and warehousing solutions are built on legacy systems, but there is also strong innovation across the industry, requiring new parts. Stocking products to support both new and legacy systems is a balance we aim to strike to ensure availability for all lifecycles.

**How is today's geopolitical environment affecting DigiKey's automation business?**

**Connor Doherty:** Geopolitics reinforce the importance of DigiKey's diversification compliance as we're actively managing multi-region sourcing strategies. With transparency as a key part of our strategy, we provide customers with detailed product information, enabling them to make informed decisions about the country of origin and explore alternative solutions. We also have added a sorting filter to our website for our US-based customers that allows them to search for tariffed and non-tariffed products.

DigiKey will also continue to leverage our Foreign Trade Zone (FTZ) program to mitigate the immediate upfront impact of tariffs and work with our suppliers to ensure that products remain competitively priced.

How is DigiKey addressing the growing demand for safety/security-certified components—such as sensors, relays, and controllers—especially for applications in industrial automation and robotics?

**Connor Doherty:** We have seen safety as a growing topic – so much so that we recently launched safety as an official category on our website to make these products easier to find. This new category includes products like PPE equipment, machine safety like light curtains, relays and controllers, along with safety protocol products like E-Stops, door interlocks, laser safety scanners and more. DigiKey is not only adding more products in this area, but we are also making them easier to find through this isolated category on DigiKey.com, helping to promote it more broadly.

With the rise of IoT and edge computing, what role does DigiKey's portfolio play in enabling secure hardware solutions, and how do you support customers in mitigating cybersecurity risks at the device level?

**Connor Doherty:** The rise of IoT and edge computing has put a much stronger emphasis on security at the hardware level, and DigiKey plays an important supporting role in that ecosystem. Much of the actual cybersecurity functionality at the device level originates within the components that our suppliers design – often embedded as subcomponents inside modules that we ultimately carry and distribute. While we're not developing those security technologies ourselves, we're deeply involved in making them accessible and reliable for customers.

From a portfolio perspective, DigiKey offers a wide range of secureready hardware used in edge and IoT applications. That includes secure microcontrollers, trusted elements, secure connectivity devices, and industrial networking components designed specifically for edge environments. As suppliers continue to invest in R&D to meet evolving cybersecurity requirements, we ensure that these technologies are represented accurately and completely within our portfolio.

How does DigiKey help design engineers navigate global safety and security standards (e. g., IEC 61508, ISO 13849, or IEC 62443) when selecting components for mission-critical systems?

**Connor Doherty:** DigiKey plays a critical role in helping design engineers navigate global safety and security standards—such as IEC 61508, ISO 13849, and IEC 62443—by making the complex world of certifications more transparent and easier to incorporate into early design decisions. While compliance with these standards is ultimately achieved through the extensive certification work performed by component manufacturers, DigiKey ensures that this information is accessible, clear and actionable during the component selection process.

Our suppliers invest significant time and resources to validate that their products meet the necessary functional safety or cybersecurity requirements. DigiKey's value lies in elevating that information so engineers can quickly determine whether a component aligns with the regulatory, safety and application-specific criteria of their mission-critical designs.

A major focus of this effort is the continuous improvement of how certification data is surfaced within our portfolio. This includes more precise product tagging, clearly listed compliance attributes, and direct access to supporting documentation. When a part meets a particular safety integrity level or cybersecurity standard, we work to ensure that this information appears right alongside essential product details, such as datasheets and images, on the DigiKey website.

What is making DigiKey stand out in the automation space?

**Connor Doherty:** We still have the same philosophy that we've had for over 50 years – to get products into customers' hands. We're using all the lessons we've learned over the years in the electronic components space and applying best practices to the automation industry. The same skills that helped us become the largest e-commerce distributor of electronic components are being applied to automation products. **GIT**



DigiKey Electronic  
www.digikey.com

© Images:

## On a Personal Note: Connor Doherty

**Which superhero would you like to be?** Ironman. I think all engineers aspire to be similar to him with his incredible devices and high-tech lab.

**Whose life would you like to swap with for one day?** I would love to swap places with my wife to soak up more time with our nine-month-old baby at home.

**What would you invent if you could?** I think teleportation would be an invaluable invention. Not only would eliminating travel time allow you to go anywhere, it also would give the opportunity for more face time with business partners, family and friends. I would love to experience more of the world and removing travel time would be an incredible way to make it more accessible.

**I've always wanted to...** Build a garden at home. Giving my family access to fresh herbs, vegetables and fruit is something I've been striving to do.

In **GIT Business Partner**, the “Who’s Who of Safety and Security,” you’ll find the most competent providers from all areas of safety and security. The companies listed here look forward to hearing from you.

All presentations, listings, company information, and reports on each company can also be found in the corresponding Company Channel at <https://git-sicherheit.de/de/business-partner> – complete with links to the companies.

Are you one of the leading providers and want to reach more than 25,000 decision-makers directly with every issue? Then contact us for a presentation.



# VIDEO TECHNOLOGY

Video Technology



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

Video Technology



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

Video Technology



i-PRO EMEA B.V.  
Herikerbergweg 292, 1101CT Amsterdam  
Netherlands  
<https://i-pro.com/eu/en>  
High-quality CCTV solutions (IP & analogue),  
Video Automation and IA, Sophisticated technol-  
ogies (FacePro, people masking), Cyber Security  
Protection for GDPR compliance, VMS: Video Insight

Video Technology

[www.luna-hd.de](http://www.luna-hd.de)

Video surveillance • Video door intercom

# SECURITY MANAGEMENT

Security Management



Ksenia Security S.p.A.  
Strada Provinciale Valtresino, 49  
63065 Ripatransone (AP), Italy  
Tel. +39 0735 751646 · Fax +39 0735 652281  
info@kseniasecurity.com · [www.kseniasecurity.com](http://www.kseniasecurity.com)  
Security and Home & Building Automation

# FACILITY SECURITY

Facility Security



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

Security Management



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](http://www.nsc-sicherheit.de)  
CCTV, Fire Alarms, Voice alarm systems

## Be Part of the Section



Just send a mail to  
[miryam.reubold@wiley.com](mailto:miryam.reubold@wiley.com)  
We will be glad to advise you!

# TIME ACCESS

## Time + Access

**AceProx**  
Identifikationssysteme GmbH

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

## Time + Access

**FEIG**

FEIG ELECTRONIC GMBH  
Industriestrasse 1a · 35781 Weilburg  
Tel. +49(0)6471/3109-375 · Fax +49(0)6471/3109-99  
sales@feig.de · [www.feig.de](http://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**

ASSA ABLOY Opening Solutions EMEA  
Digital Access Solutions  
Dukes Court, Dukes Street  
Woking, GU21 5BH · Great Britain  
[www.assaabloy.com](http://www.assaabloy.com)  
Access control, Access management, Wireless locks,  
Electronic Access Control Systems

## Time + Access

**phg**  
Die richtige Verbindung

phg  
Peter Hengstler GmbH + Co. KG  
D-78652 Deißlingen · Tel. +49(0)7420/89-0  
datentechnik@phg.de · [www.phg.de](http://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**

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](http://www.pepperl-fuchs.com)  
Security sensors, inductive, capacitive, opto-  
electronic and ultrasonic sensors, vision sensors,  
identification systems, interface modules

## Time + Access

**DoorBird**  
Technology meets Design.

Bird Home Automation GmbH  
Uhlandstr. 165 · 10719 Berlin  
Tel. +49 30 12084824 · [pr@doorbird.com](mailto: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](http://www.doorbird.com)

## Time + Access

**primion**

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](http://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**  
**cryptin** **STOLBERG**  
Intelligente Zutrittskontrolle

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](http://www.cryptin.de)  
Operational data collection, time recording,  
access control

## Time + Access

**STid**

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



**Register for our  
free Newsletter**

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

**NOW**

**e-Issue  
included!**



**WILEY**

# THE VIP LOUNGE



© Airbus Defence and Space

## Sven Dawson

Head of Corporate Security,  
Airbus Defence and Space

**What was your career ambition at the age of 20?** At that time, I was already committed to the German Armed Forces. I had the desire to pursue something both engaging and meaningful – something that, in essence, has stayed with me to this day.

**What motivated you to take on a role in security?** Curiosity and the vision that security would become increasingly important. That prediction has certainly come true.

**Which security policy decision or project, in your opinion, should have been implemented long ago?** European countries should commit far more strongly to cooperation instead of continuing to prioritise national interests. This vulnerability is something external actors are increasingly drawing attention to.

**What do you consider the most significant invention in the field of safety and security?** In my view, the most impactful innovations in security follow three fundamental principles: protecting information, controlling access, and detecting threats early. Cryptography forms the foundation of digital security; mechanical and electronic access systems safeguard physical spaces and critical infrastructure; and technologies such as radar introduced early-warning capabilities against threats. Together, these principles form the core architecture of modern security and resilience systems across government, industry, and defence.

**A recent success of yours was ...** We were able to successfully evacuate employees from a critical situation and bring them home safely. Unfortunately, such situations are becoming more frequent.

**Who, in your view, deserves recognition?** My favourite podcast host, Paul Ronzheimer. He manages not only to cover topics in a highly professional manner but also to keep key issues relevant and up to date in the daily news cycle.

**How do you relax?** DIY projects, gardening, and outdoor activities in general.

**Which travel destinations would you recommend?** Cities: Singapore, New York, Boston. Countries: the United States.

**Which magazines do you read regularly?** The German news magazine "Der Spiegel".

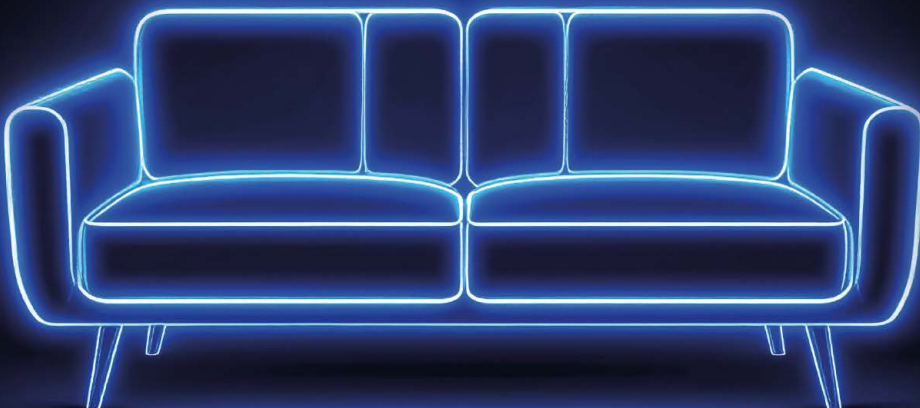
**GIT magazine is important to me because ...** it provides a platform where key decision-makers in the security industry can regularly share their perspectives.

**What book have you read recently?** "Shitbürgerturn" by Ulf Poschardt and, prior to that, "If Russia Wins: A Scenario" by Carlo Masala.

**What kind of music do you prefer?** I don't have a fixed preference – it depends on the mood.

**What motivates you?** Driving change together with a committed and motivated team, and moving things forward with purpose. In today's world, security is no longer just a cost factor for companies – it is a prerequisite for doing business at all.

**What concerns you – and what gives you confidence?** As a country, we still have not fully understood the extent to which we need to transform and reinvent ourselves. We are too slow and cumbersome, and our public sector is too large and costly. We need to take more risks and present ourselves more confidently on the global stage. What gives me confidence is that these issues are increasingly being discussed – hopefully accelerating the pace of change.



# This month at GIT-SECURITY.com

SECURITY 51

## 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@vuserice.de  
Our service is available for you from  
Monday to Friday 8 am – 5 pm CET

### Production

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

### Bank Account

J.P. Morgan AG, Frankfurt  
Account No.: 6161517443  
Routing No.: 501 108 00  
BIC: CHAS DE FX  
IBAN: DE5501108006161517443

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 possi-  
ble 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 respec-  
tive owners.



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

WILEY



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



Register  
here

NEWS LATEST ARTICLES PRODUCTS MAGAZINE BUSINESS PARTNER EVENTS DE IN

**GIT SECURITY** INTERNET

MANAGEMENT SECURITY FIRE PROTECTION IT-SECURITY SAFETY

Read the latest issue online  
GIT SECURITY International for download

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

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

**SECURITY**

**Perimeter Security in a Practical Test: How the Wehrhan-TPS urban test site makes real attack scenarios visible**

NEW SERIES: TEST SITE UNDER TEST: Perimeter security with radar and video management on the premises of Wehrhan-TPS

**MANAGEMENT**

**Drones instead of trackside routes: DB plans automated monitoring to prevent tampering and disruptions**

**SECURITY**

**Perimeter Security in a Practical Test: How the Wehrhan-TPS urban test site makes real attack scenarios visible**

ADVERTISEMENT

**CLIQ®**  
The smart way to digitalize access  
**ASSA ABLOY**

Learn more

NEWS

**Hallmeier and Elso Show Solutions at SicherheitsExpo 2026**

**Standards Can Drive Innovation in Physical Security**

**Gunscho Group Reports Gains in Diversity, Renewable Energy and Supply Chain Standards**

**Setting the Standard for Multi Licence Narcotics Storage in Canada**

**Kesinfinity Group Accelerates Transformation and Introduces Simplified Management Structure**

LATEST ARTICLES

**TOPSTORIES • SECURITY**

**Perimeter Security in a Practical Test: How the Wehrhan-TPS urban test site makes real attack scenarios visible**

NEW SERIES: TEST SITE UNDER TEST: Perimeter security with radar and video management on the Wehrhan-TPS urban test site

**TOPSTORIES • SECURITY**

**Winguard from Advancis: How Boehringer Ingelheim is modernizing its global risk management**

Boehringer Ingelheim optimizes global safety management with the Winguard open threat platform from Advancis

**TOPSTORIES • SECURITY**

**Trust, Not Surveillance: How Facial Recognition Can Be Used Responsibly in Democratic Societies**

Facial recognition is among the most controversial topics in modern video analytics.

**TOPSTORIES • MANAGEMENT**

**Drones instead of trackside routes: DB plans automated monitoring to prevent tampering and disruptions**

DB CEO Hennies: How AI, drones & bodycams are revolutionizing rail security. A look at the new strategy

ADVERTISEMENT

**WILEY**

Simplify your marketing plan  
2026 media planning starts here  
VIEW MEDIA KIT

CORPORATE SECURITY GSA CORPORATE SECURITY

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

**GIT SECURITY AWARD Winners**  
The current winners in all categories.

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

PRODUCTS

**Hanwha Vision: BI-spectrum early fire detection cameras (GSA27-60)**

**Inotec: Guidance Marking System GMS (GSA27-57)**

**Johnson Controls: SafeLink cloud internet interface and mobile app (GSA27-64)**

**Ajax Systems: EN54 Fire Hub Jeweller - Fire Alarm System (GSA27-64)**

**Gekartel AG: Fire-resistant tablet computer (GSA27-57)**

EVENTS FIRE PROTECTION

www.GIT-SECURITY.com



## conexa

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



**Find out more!**  
[www.kseniasecurity.com](http://www.kseniasecurity.com)