

GIT SECURITY

MAGAZINE FOR SAFETY AND SECURITY

Subscribe to GIT-SECURITY Newsletter
Now for free



© Swiss Südostbahn AG / Thomas Kessler



GIT SECURITY AWARD p 11

FIRE PROTECTION p 16

BIOMETRICS IN SECURITY p 27

CRITICAL INFRASTRUCTURE p 34

**SECURITY FOR
PORTS & AIRPORTS** p 38

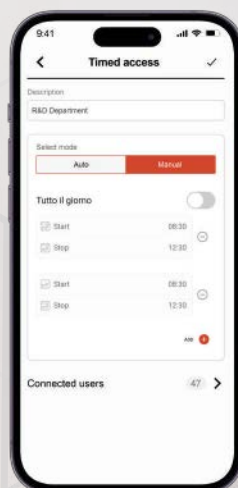
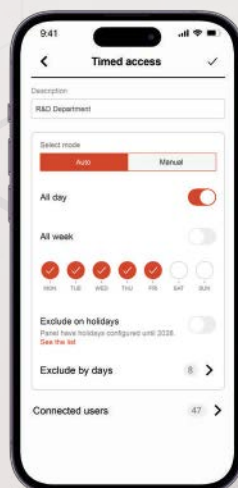
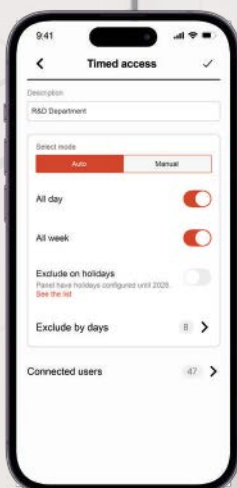
COVER: Providing Innovative Fire
Protection Solutions for Railway
Vehicles: **WAGNER Rail** p 16

WILEY

ACCESS CONTROL



intro



Dear readers

It's a big hello from me and a temporary farewell to Lisa Holland, our long-term Deputy Editor in Chief, who headed off on maternity leave last month. We wish her and her husband all the best for a safe and happy arrival.

I caught up with about 50 of you at The Security Event at the NEC in Birmingham a couple of weeks back, which was a fantastic reintroduction to the industry. It felt like I was on cloud nine, as all the talk at the show was of the cloud and its impact on security in 2024.

It's fitting therefore that we cover the issue of biometrics in our special focus. It's a fascinating read and brings us bang up-to-date with what's going on ... even down to behavioural biometrics and DNA capture!

Stories from Milestone and Hikvision show how AI and smart video technology are being used in practice to make the ports of the world safer and better places to work. We also feature stories on airport security. And three experts give their opinions on critical infrastructure security developments.

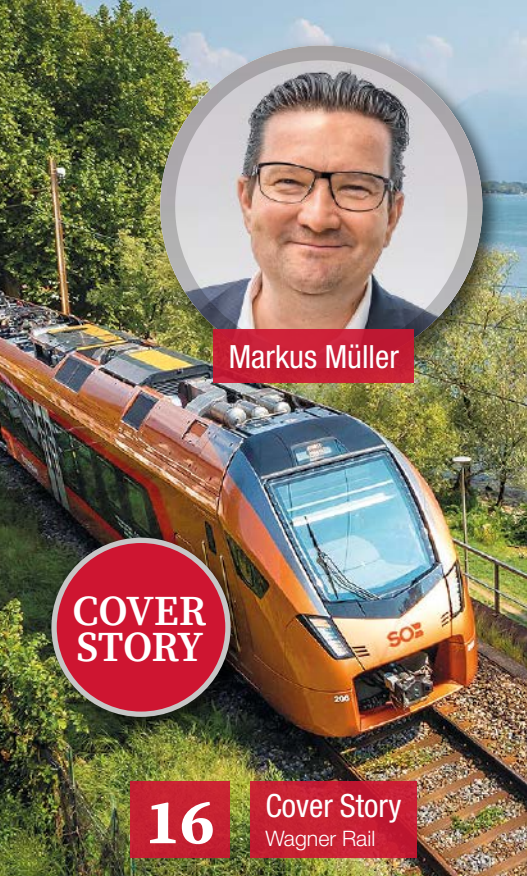
Our cover story from Wagner Rail by contrast tracks the evolution of passenger safety from fires on the railways over the past 30 years. We also cover heat-resistant drones for firefighting and weatherproof fire sensors for a new fruit processing plant.

First up is the story of the task of securing the 2024 Paris Olympics, which start on 26 July, told through the lens of French perimeter security manufacturer Sorhea.

And finally, please remember to register your votes for our GIT SECURITY Award 2025 finalists. There are seven categories to vote in, and you can cast them any time from 1 June to 1 September. Three lucky readers will win Wiley-branded Ledlenser P7R Work UV cameras.

Good luck and happy reading!





Markus Müller

COVER
STORY

16

Cover Story
Wagner Rail



30

Jamie Barnfield
Idis Europe



32

Christian Heller
Frogblue

GIT
SECURITY
AWARD
2025
FINALISTS



**Vote
Now!**
for the next
winners

WILEY

MANAGEMENT

- 3 Editorial**
Mark Triggs
- 8 Paris Goes for Gold...**
Making the Olympic Games 2024 in the French capital safe involves not only securing the sporting event locations but also the sightseeing attractions, and above all the masses of people who are expected to attend

GIT SECURITY AWARD

- 11 Your Vote, Please**
Select your favorite product and vote

FIRE PROTECTION

- COVER STORY**
- 16 The Evolution of Passenger Safety**
30 Years of Fire Protection in Trains

- FIRE PROTECTION**
- 19 Hot and Steamy**
An Approved Fire Alarm System and Weatherproof Devices Secure New Food Production Facility

- FIREFIGHTING**
- 20 Fire Drones**
Heat-Resistant Drones for Firefighting

SAFETY

- SURGE PROTECTION**
- 23 Well Protected**
System Protection for Building Technology and Measuring and Control Systems

Welcome to the knowledge age

Wiley builds on its 200-year heritage by partnering with universities, businesses, research institutions, societies and individuals to develop digital content, learning, assessment and certification tools.

Wiley continues to share and deliver the answers to the world's challenges helping you to further your mission.





Stefan Blohm
Raytec

Christian Bömmel
Innosent

Nick Smith
Genetec

34

3x3 Questions
Critical Infrastructure



38

Rahul Yadav
Milestone Systems



44

Stefan Olf
Advancis

■ SECURITY

VIDEO SURVEILLANCE

- 24** Video Syncs with Giant EV Charging Park
Rail Station Pioneers Smart Car Park Protection

VIDEO SECURITY

- 26** Alert-to-Action
A Security Solution for Banks and Financial Institutions

BIOMETRIC SYSTEMS

- 27** My Oh My!
The State of the Art in Physiological Biometric Security Methods

SPECIAL FOCUS

VIDEO SURVEILLANCE

- 30** Repeat After Me – New Branch
Smarter Video Solutions for Retail

ACCESS | DOOR INTERCOM

- 32** Simple, Secure, Smart
The Frogblue Door Station for Professional Building Automation and Access Control

3 X 3 QUESTIONS

- 34** Critical Infrastructure

SPECIAL FOCUS

■ SECURITY

RADAR

- 36** It's Critical to Play It Safe
Radar is Vital in Security Design

VIDEO ANALYSIS

- 38** Only Dummies Will Do
AI Project to Keep Danish Ports Safe

KEY MANAGEMENT

- 40** Secure and Transparent
An Access Solution for Building Keys and Assets at Munich Airport

AIRPORT SECURITY

- 41** Smooth Operators
The Critical Importance of Complete Airport Security

VIDEO SURVEILLANCE

- 42** Wang Enjoys Long-Awaited Comforts
Qingdao Port Improves Efficiency Threefold

INTERVIEW

- 44** Representative Security
Middle East: Smart Cities and Other Future Projects

CONTROL PANELS

- 46** Everything Under Control
A Smart Platform to Aggregate Multiple System Controls

■ SECTIONS

- 06** News
22 Fire Protection and Safety Products
48 Security Products
49 BusinessPartner
51 Company Index | Imprint



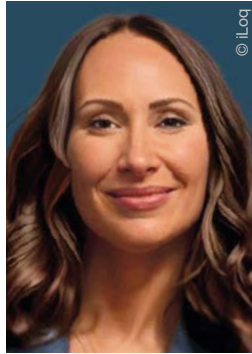
Comfortably read
your e-Issue of
GIT SECURITY on
your sofa: Register here



Michelle Rodgers Joins iLoq

Michelle Rodgers has been appointed as Country Manager, United Kingdom, as of February 1, 2024. She is a seasoned commercial leader with a distinguished background in driving revenue growth across diverse industries, including telecoms, utilities, security, and technology. With over two decades of strategic leadership, she excels in optimizing business operations, building robust teams and forging impactful partnerships. Her commitment to aligning growth strategies with a collaborative organizational culture aligns with iLoq's vision and values, fostering sustainable growth and success within the UK market. "I am delighted that Michelle is joining the iLoq UK team," said Ferry Nekkers. "I am confident, with her experience and background, that iLoq UK will grow successfully in the coming years. I wish Michelle success in her new role."

www.ilq.com



Salto Systems Announces Transformation for Future Growth

Salto Systems has announced a significant transformation to adapt to the evolving landscape and to position the company for continued success. The group has unveiled its new identity as Salto Wecosystem, symbolizing a comprehensive evolution, embracing a holistic approach, reflecting the company's commitment to innovation and the integration of brands, companies and cutting-edge technologies.

Three independent core brands have been established under the Salto Wecosystem brand umbrella with Marc Gómez as CEO to harness the strengths of each entity: Gantner, Salto and Vintia. Each core brand will play a pivotal role in contributing to the overall success and growth of the organization while maintaining its unique identity and focus. The revamped organization will have four global teams: sales and marketing, technology and innovation, people and global services, and cybersecurity.

Marc Gómez,
CEO of Salto Wecosystem



www.saltosystems.com

Fingerprint Recognition Algorithm Embedded in Samsung Galaxy S24 Series

Suprema has announced the supply of the latest version of the under-display ultrasonic fingerprint recognition algorithm, BioSign, to the Samsung Galaxy S24 series supported by the Qualcomm 3D Sonic Sensor Gen 2. Since 2019, starting with the Samsung Galaxy S10, Suprema has continuously incorporated its fingerprint recognition algorithm into numerous Galaxy S series, earning recognition for its world-class technological capabilities. The BioSign 6.0 version featured in the Samsung Galaxy S24 has received acclaim in the market for its significantly upgraded fingerprint recognition speed and security. Compared to its predecessor, BioSign 5.0, BioSign 6.0 has achieved a technological innovation that simultaneously enhances speed and accuracy. It provides an improvement in accuracy and a faster response time, to greatly enhance user convenience.

www.supremainc.com



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



Vitaprotech Group Goes Global with Identiv Buy for \$145m

Leading European electronic security group Vitaprotech has signalled its global aspirations with the signing of a stock and asset purchase agreement with Identiv to acquire its security business for \$145m. Vitaprotech will acquire the physical security, access card and identity reader operations and assets of Identiv, a global digital security and identification leader in the IoT, with the support of Seven2 and BPIFrance. The acquisition materially expands the group's access to the North American market, delivering on the strategic objective to further expand outside of Europe. Identiv's security business – which employs more than 200 across the US, Canada, Germany and India – provides an industry-leading high-security platform that has been trusted by government agencies and commercial organisations worldwide.

www.vitaprotech.com

Dahua Subsidiary Launches into Fire Protection

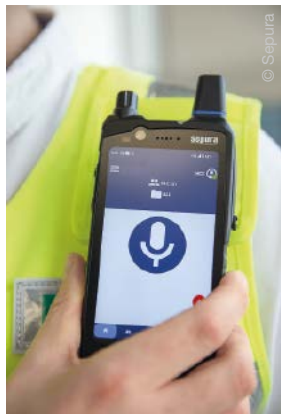
A Dahua subsidiary has launched a new range of quality-driven and innovative smoke, heat, CO and environmental alarms into the UK and Ireland. WisuAlarm has designed its BSI-certificated range to provide advanced fire and environmental protection. The devices are manufactured under quality-controlled precision manufacturing conditions and take full advantage of Dahua's expertise in video analysis, cloud computing, big data and smart IoT. The range of alarms features split-spectrum sensors, which result in fewer false alarms from environmental factors such as dust and steam. Professional installers in private homes and social housing are the target for the initial offering from WisuAlarm. The range is suitable for grades D1, D2, F1 and F2 and categories LD3, LD2 and LD1 under BS 5839-6, and includes smoke, heat and CO alarms and environmental sensors to detect damp and mould and to monitor air quality.

www.wisualarm.com | www.dahuasecurity.com



Sepura Launches Mission Critical Broadband Hand-Portable Device

Sepura has launched the SCL3, a rugged broadband hand-portable device, at this week's BAPCO Annual Event. Complementing the SCU3 Hybrid Broadband Vehicle Device, the SCL3 reinforces Sepura's commitment to invest in the future of critical communications and reduce the risk and costs of migrating to Mission Critical Services (MCX) by providing hybrid solutions to help bridge the transition. The new SCL3 device has the flexibility to be deployed as LTE only or as hybrid Tetra and 4G/5G, providing a powerful device to enable the migration to mission-critical broadband communication. Supporting the best of both worlds, the SCL3 is the link to future MCX communications using its optional Tetra module to provide a migration path from existing Tetra communications to MCX services. Start today with Tetra TMO voice and LTE data and migrate to MCX voice and Tetra DMO for Device-to-Device (D2D) services. www.sepura.com



Secutech Thailand 2024 Confirms Dates

Organisers of Secutech Thailand have confirmed that the 2024 edition will return to the Bangkok International Trade & Exhibition Centre (BITEC), Bangkok, from 30 October to 1 November 2024. Thailand's leading fair for security and fire safety for commercial and industrial premises announced the dates to over 80 local industry players, who discussed the industry's development and upcoming market trends. Key suppliers signed up include Axis, Blazecut Co Ltd, DNAKE Thailand, Hikvision, HIP, Security Systems Services, Secom and Siemens. Industry associations are involved too, such as The Building Inspectors Association, Genthai, Thai IoT, Drone Association of Thailand, National Cyber Security Agency, Thai Intelligent CCTV Association, Thai Security Association, Baramizi Group, Innovator X, Municipal League of Thailand, The Consulting Engineers Association of Thailand, Thailand Productivity Institute, Department of Industrial Works and Amata. www.secutechthailand.com | www.messefrankfurt.com



LEED is one of several green building certifications where Assa Abloy's expert support can help

Collaboration Helps Achieve LEED Gold Certification

As experts in industrial design and construction, Polish Company GBPPB Projprzem were engaged by multinational Phillips-Medisize to create and execute the concept for a major new facility outside Katowice in southern Poland. Part of the project brief was to gain LEED certification for this new manufacturing plant. To help achieve this goal, they sought specialist BIM and specification support from the early design phase right through to project completion – including for the building's door, security and access solutions which also impact the award process. Expertise in relevant materials and the documentation required to receive LEED credits was critical: "We knew that Assa Abloy had the knowledge and the access and security solutions dedicated to sustainable buildings," explains Wojciech Szmyd at GBPPB Projprzem.

The company partnered with Assa Abloy Opening Solutions over the course of the project. This collaboration formed part of a BIM approach which GBPPB have long used to connect architects, civil engineers and installers within one transparent environment – to enable fast, accurate, cost-efficient project delivery. A dedicated BIM consultant at Assa Abloy helped ensure the entire door specification process was efficient and effective. One key collaboration tool was the Openings Studio software plugin for Revit, which enabled specification changes to quickly and accurately populate the evolving building design.


The same tool also enabled transparent communication between the project coordinators and other stakeholders. Everyone was always working with accurate, up-to-date information. The vast portfolio of available Assa Abloy door and access solutions was another major benefit. The company supplied a broad range of products and solutions including around 180 ALPE doors for various specialist applications around the facility; effeff electric strikes; rack-and-pinion door closers; mechanical security locks and more. The availability of these varied solutions, as well as documentation, such as detailed Environmental Product Declarations (EPDs), is supporting Phillips-Medisize throughout their application process for the targeted LEED award of Gold.

www.assaabloy.com

SECURITY SITUATION IN FRANCE

Paris Goes for Gold...

Making the Olympic Games 2024 in the French capital safe involves not only securing the sporting event locations but also the sightseeing attractions, and above all the masses of people who are expected to attend.



Increased security at monuments such as the Eiffel Tower has become necessary because of the expected number of visitors during the Olympics in Paris

The 2024 Summer Olympic Games will be held from 26 July to 11 August in the French capital, Paris. This is the third time after 1900 and 1924 that the city will host the event. The effort required to secure the event locations, the athletes' and their support personnel's accommodation, also the tourist attractions of all the visitors outside the Games, is a Herculean task for all those involved.

■ The French company Sorhea, as a manufacturer of perimeter security systems in their home market of France and one of the European market leaders, has already been involved in securing the Olympic Games properties for a number of years with its products. The building sites and also the material storage depots for the athletes' village have been protected using various technological security solutions.

The Eiffel Tower and the Stade de France: A Metropolis with Differing Security Aspects

Not only are numerous government and public buildings in the Paris region being protected but also various sports arenas and prestigious sightseeing venues. The customer list of Sorhea includes the Stade de France, by far the largest stadium in the country, as well as the Eiffel Tower, the tallest building and icon of the city of Paris recognized worldwide.

Understandably, no information can be given about the security measures that have been implemented so far for the 2024 Olympic Games because of the current threat level. It is possible, however, to provide some general information on the typical challenges that confront physical security and perimeter protection providers for such a large international sporting event.

The Olympics are faced with these security challenges:

■ **Terrorist threats:** High visibility events, such as the Olympic Games, are potential targets for terrorist organizations. French authorities have to plan and implement robust security measures to counter this threat. These can include the activation of additional policing authorities, the exchange of information and the observation of potential threats.

■ **Security of the event locations:** Ensuring the security of the various Olympic event locations is a mammoth operation. It involves access control, checking the par-

ticipants and their possessions, as well as ensuring that only authorized personnel and vehicles have access to restricted areas.

■ **Crowd control:** Controlling large numbers of people during the games is a complex task. Measures must be taken to prevent overfilling and to be able to react to medical emergencies or to initiate evacuation procedures that ensure the safety of spectators, the athletes and the staff.

■ **Cybersecurity:** The dependence on technology for event management and communication means that cybersecurity can be a problem. Protecting the systems against cyberattacks is fundamentally important to avoid interruptions and potential threats to IT security.

■ **Transport security:** The transport infrastructure used by the athletes, staff and spectators is a potential target. Making the airports, railway stations and other transport nodes secure is just as important as ensuring the security of the public transport that moves the people to and from the event locations.

■ **Coordination and information exchange:** Effective communication and cooperation between various different security authorities at home and abroad is very important. The exchange of information and joint operations is essential to identify potential threats and to react to them.

■ **Protests and demonstrations:** There can be protests and demonstrations at large events, some of which represent a security problem. The authorities must strike a balance between peaceful protest and the maintenance of order and security.



Sorhea has secured the building site since the start of work on the athletes' village

■ **Emergency response:** Preparation for and response to emergencies, such as natural catastrophes or medical crises, is highly important. Preparation includes ensuring that medical equipment and sufficient personnel are always available.

■ **Insider threats:** Security personnel and event personnel must be thoroughly checked in advance in order to minimize the threat of insider attacks. Background checks and continuous surveillance are two elements of this.

It is important to realize that the security measures for the Olympic Games are normally confidential for operational reasons. The organizers work closely with local, national and international security authorities to develop comprehensive security plans to react to potential threats and minimize risks. Security aspects are taken very seriously and significant resources are

applied to ensure the security of participants and spectators. The actual security challenges for the 2024 Olympic Games in France will be dependent upon the geopolitical situation and the security situation at that point in time.

The Current Danger Level in France

The French government raised its Vigipirate security warning system to the highest level of 'Emergency Attack' (Urgence Attentat) on 13 October after a terrorist knife attack in the town of Arras in which a French teacher was killed. As a result, the population of the whole of France as well as visitors were met with increased security measures in public areas, including the airports, public transport, places of worship, sightseeing locations, schools, large sports arenas and in large shopping plazas.

turn page ►

Dallmeier

BECOME A PANOMERA® PARTNER NOW.

- Fewer systems
- Less infrastructure
- Lower overall cost
- Satisfied customers

ONVIF | M S T

Integrated in **advancis** **Genetec** **milestone**

MADE IN GERMANY



LEARN
MORE



The entrances to the stadiums are already critical areas, even without a sporting event taking place. The Stade de France is therefore a particularly sensitive site for surveillance



Sorhea is significantly involved in the security around the Eiffel Tower

There have recently been numerous bomb threats at airports, schools and tourist locations, such as the Palace of Versailles and the Louvre, and the French Executive has warned of 'importing' the Middle East conflict to Europe and France.

The ambassadors of various countries have reminded their citizens to be watchful around them, to take suitable measures to increase their personal security, and to avoid demonstrations and areas with increased police activity. Always be careful when near large gatherings or protests, and leave the area immediately if demonstrators clash with the police or damage property. Always follow the directions of the police and rescue services.

The French authorities are actively monitoring terrorist threats by organized groups and radicalized individuals. Attacks can take place with little or no warning and be aimed at tourist locations, large sport and cultural events, as well as other public venues that attract a large number of people. Visitors to crowded and popular tourist attractions should take particular care.

France's Rules on Video Surveillance and AI in Public Areas

The French decree to regulate the use of algorithms during the Olympic Games in Paris was finally published at the end of August 2023. Tenders have been issued by the Depafi (French Department of the Interior) for the supply, installation and maintenance of a 'video protection solution with artificial intelligence'.

In the decree it states that: "In a test phase and until 31 March 2025, [...] the images that are obtained with the help of video protection systems [...] and cameras installed in aircraft [...] or places where sporting events, leisure or cultural events take place", in particular where people may be exposed to the danger of terror acts or

severe attacks on people's security and their environment, as well as in vehicles and preferential public transport and on the roads that may help because of their presence or their situation, can be subjected to algorithmic processing.

The decree contains a list of 'previously defined events' that might be subject to algorithmic processing:

- the presence of unattended items in protected areas
- the presence or use of weapons
- the non-observance of traffic rules by a person or a vehicle
- the presence or traversing of a person or a vehicle in a prohibited or sensitive area
- the presence of a person on the ground after falling
- mass movements of people
- an increased concentration of people
- or the outbreak of a fire.

A further clarification about the use of AI in video surveillance in public areas in France deserves a mention: The decree states, "Only algorithmic processing may be used that has been developed by or for the state, or has a certificate of conformity issued by the French Department of the Interior."

EU-Discussion about the Use of AI

The not yet final list for the approval of AI in public areas to forbid intrusive and discriminatory use, created by the European Union Members of Parliament and currently being discussed, involves among other matters:

- biometric remote identification systems in 'real time' in publicly accessible spaces
- 'subsequent' biometric remote identification systems, with the exception of the criminal investigation of severe crimes and upon the approval of a judge
- biometric identification systems using sensitive features (such as gender, race,

ethnic origin, nationality status, religion or political orientation)

- predictive police systems (based on profiling, location or previous criminal behavior)

- emotion recognition systems that are used for law enforcement in border management, at work and in training establishments

- the general gathering of facial images from the internet or CCTV recordings to feed face recognition databases (which is a violation of human rights and the right to privacy).

Newest Technology and the Oldest Aspiration: Security for Groups of People

Flying taxis, autonomous shuttles, assisting robots – technology will be at the center of the 2024 Olympic Games in Paris. A gigantic laboratory in which artificial intelligence will be used, and in particular in security applications, is a first at national level. The security challenges that the event generates are giving the authorities some headaches, especially the one hundred thousand people who are expected for the opening ceremony along the Seine River. The French cities are hoping that the new technology can be smoothly integrated into the security plans and will deliver decisive security benefits. Paris, in particular, is acutely aware of the mammoth task because, apart from the Olympic arena, the masses of people at sightseeing locations and tourist attractions as well as the monuments must be protected. ■



Sorhea GmbH
www.sorhea.com

Your Vote, Please

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 with the advantage that you can vote directly on the presentation platform. New special category for this year is Safety & Security Partnerships & Safety/Security Management.

GIT SECURITY AWARD categories

We have asked security and safety product vendors to submit their best products in the following categories:

- A – Machine & Plant Safety
- B – Occupational Safety and Health & Explosion Protection
- C – Video Security Systems & Video Management
- D – Access Control & Intruder Alarm
- E – Building Safety & Perimeter
- F – Fire Protection
- S – Special Category: Safety/Security Partnerships & Management

Voting

We present the nominated products as listed on the next pages. All readers can vote directly via the voting tool online on www.security-award.com. An easy way to do this is to scan the QR code in this article. To ensure fairness, companies cannot vote for their own product. Moreover, you will have to vote with your company address. Private persons are not entitled to vote. Therefore, a business address is essential. Please select one product in each category. Vote now – Voting is possible from 1 June to 1 September, 2024 on www.security-award.com

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.



Reader
Prize

**GIT
SECURITY
AWARD
2025
FINALISTS**

**Voting will start 1 June
and will be open until
1 September via
www.security-award.com**



WILEY

Category A: Machine & Plant Safety

ABB Stotz-Kontakt	Mobile two-hand control unit: Type JSD-TD25P-320700
Bihl+Wiedemann	ASi-5 Safety Muting Modul BWU4411
Dina Elektronik	Small control system – SAFELINE VARIO
Euchner	Electronic-Key-System EKS2
K.A. Schmersal	Field bus gateway SDG for serial diagnostics
Keba Industrial Automation	KeTop "Safe Wireless" handheld control unit with operation area monitoring
Moxa Europe	UC-8200: World's First IEC 62443-4-2 Certified Industrial Computer
Phoenix Contact Deutschland	AXL E PS IOLS4/4 IO-Link Safety Master
Pilz	PSEnlock Mini
Pizzato Elettrica	NX series RFID safety switch with lock
SSP	Simplifier Gateway – Profisafe

Category B: Occupational Safety and Health & Explosion Protection

Asecos	ION-LINE ULTRA
Dräger	INARA - digital service concept
Ejendals	Tegera 8846 – class F cut protection glove
Gore-Tex Professional Fabrics	EXTRAGUARD upper technology
Helly Hansen Workwear	HH Connect Concept
Krause-Werk	KRAUSE Telescopic step ladders
Ledlenser	EXC6R – ATEX LED Right-Angle Light
SharpEagle	Explosion-Proof Camera

Shortlist

Category A: Machine & Plant Safety**K.A. Schmersal: Field Bus Gateway SDG**
Field Bus Gateway for Serial Diagnostics

Electronic safety sensors and solenoid interlocks with SD interface can transmit comprehensive diagnostic data to a higher-level machine control system. The data from the series-connected safety switching devices (up to 31 devices) is sent to the SDG fieldbus gateway via the SD bus and from there to the machine control system via the fieldbus. For example, error messages can be forwarded. Advantages: improved fault diagnosis, minimisation of down-

times, increased productivity, lean wiring, extensive additional functions via integrated web server and long-term storage of log messages via microSD card. The SDG fieldbus gateway has a web server and a microSD memory card and therefore offers the following features: Event logs can be evaluated in real time via the web interface; Complete diagnostic data from all safety switchgear devices are displayed in plain text; Devices, such as interlocks and control panels, can be controlled directly via the web interface; microSD card allows event logs to be exported for evaluation and long-term storage.

**Category C: Video Security & Video Management****Eagle Eye Networks: Eagle Eye Camera Direct**
Direct Camera Installation and Cloud Synchronization

Eagle Eye Camera Direct offers simple installation and high performance, perfect for small setups or remote locations. Cameras, including Eagle Eye and others, sync directly to the cloud for full cloud management. Live and recorded video is accessible globally, with AI and camera settings configurable via the cloud. Utilizing Eagle Eye Connect, it securely links cameras to the cloud without risky network setups. ONVIF compatibility ensures seamless integration with any camera featuring the relevant API. Innovative features are: Cloud syncing functionality (even if the camera is stolen or damaged, videos are retained); QR scanning to auto-populate the MAC Address through the Eagle Eye Mobile App for fast setup; no on-premise bridge required; Open solution that can be integrated with a broad range of ONVIF cameras.



Category C: Video Security & Video Management

AG Neovo	TTN series, safe security monitors
Ajax Systems	NVR – Network video recorder
Bosch Building Technologies	IVA Pro PPE video analytics software
Eagle Eye Networks	Eagle Eye Camera Direct
Eizo	4K UHD IP Decoding Box
Genetec	Security Center SaaS
Hanwha	PNV-A6081R-E1T and PNV-A6081R-E2T SolidEDGE video cameras
Hikvision	4 MP DeepinView Multi-Sensor Bullet Network Camera
i-Pro	i-PRO X-series: AI On-site Learning Camera Series
Raytec	VARIO2 IP Hybrid illuminators
Videor	SOL-VICAM-MOBILE-LTE Mobile Video Surveillance Solution

Category D: Access Control & Intruder Alarm

Acre Security	Acre Access Control
Advancis	Advanced Identity Manager (abbreviated “AIM”) – Software Platform
Ajax Systems	KeyPad TouchScreen Jeweller – Wireless keypad
Aug. Winkhaus	blueEvo – Electronic Access Control
Bird Home	IP Video Door Stations D21x series
BSS	HELIH security and automation radio window handle
Carrier Fire	ATS3700-MM – AXON Security Panel
Dormakaba	MATRIX as a Service – cloud-based access control
Essentry	Access Management with Identity Verification
Evva	EMZY – Electronic motorised cylinder
Frogblue	frogTerminal – SIP-based video access control station
Ksenia	intro Door Controller Module
Optex	REDSAN mini-Pro LiDAR
PCS	DEXIOS – web-based access control software
Salto	XS4 Mini Metal – electronic door lock
Wilka	easySmart – cloud-based access control from a distance

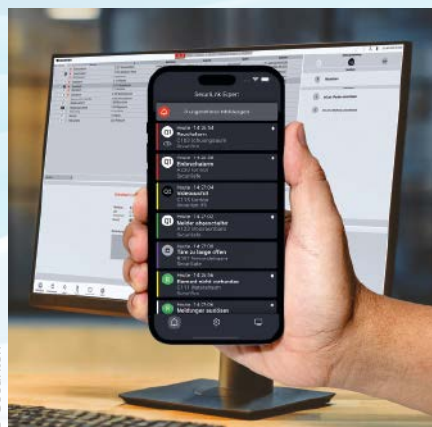
Highlights

Category E: Building Safety & Perimeter Protection**Securiton: SecuriLink MobileControl****Mobile Operation of Security Management Systems**

SecuriLink MobileControl is a digital application in the SecuriCloud landscape and enables remote mobile operation of a SecuriLink Expert security management system.

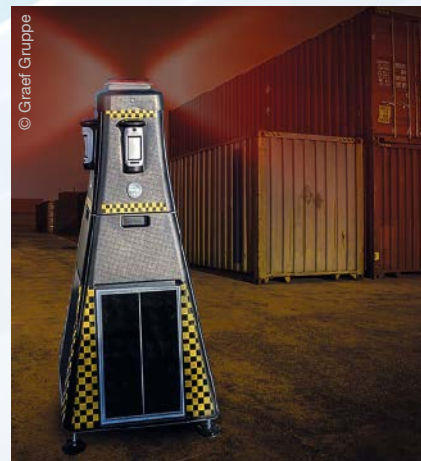
In the event of an incident, users are notified via SecuriLink MobileControl (push notification). With a brief touch, the user accesses the app's user interface. They can process the notification in the prioritised notification list – in the same way as on their familiar SecuriLink Expert security management system. An event is always processed in the same simple way, regardless of the source – whether the reporting system is from Securiton or a third-party manufacturer.

With SecuriLink MobilControl, Securiton's development engineers have succeeded in bringing together all system status and alarm messages from integrated security or building technologies in one app. This is a pioneering step for companies and organisations that are increasingly relying on digital solutions to optimise their security systems and their organisation and to benefit from the possibilities of multi-site message control.

**Category E: Building Safety & Perimeter Protection****Graef Gruppe: NARRAD****Video alarm tower**

Graef Gruppe has developed the autonomous NARRAD video alarm tower, specifically conceived for the effective protection of construction sites and remote areas. By integrating solar modules, this solution ensures complete grid independence, making it operational in environments lacking electrical power. At the core of this security system lies advanced sensor technology that reliably detects unauthorized access through precise motion detection. Coupled with cutting-edge alarm technology, NARRAD provides seamless protection. Its straightforward installation and operation make this video alarm tower an effective and user-friendly solution for a wide range of security requirements.

NARRAD stands out through the combination of autonomy, mobility and advanced sensor technology. Independent of external power supply and with its lightweight, modular design, it allows for swift and versatile deployment. Its sensors utilise intelligent algorithms for precise detection with minimised false alarms, leading to efficient monitoring with low operational costs. With NARRAD, a new standard is set for monitoring unattended areas.



Category E: Building Safety & Perimeter Protection

Blickfeld	QbProtect – Smart 3D Security LiDAR
Bosch Building Technologies	IP-based Horn Loudspeakers with Amp Module
Graef Gruppe	NARRAD Video alarm tower
Hanwha	TNO-C3012TRA/22TRA/32TRA and TNO-C3010TRA/20TRA/30TRA – AI-based radiometric thermal cameras
Ledlenser	XP30R – high-end spotlight
Optex	EchoPoint Distributed Acoustic Sensors (DAS)
Salto	BLUEnet – Wireless Door Controller
Securiton	SecuriLink MobileControl – Mobile operation of security management systems
Senstar	MultiSensor – AI-Powered Detection System

Category F: Fire Protection

AP Sensing	Fiber-optic Linear Heat Detector N45 LHD series
Axis	P1468-XLE – Explosion-Protected Bullet Camera
Bosch Building Technologies	Avioteq 8000i IR – video-based fire detection solution
Denios	Lithium-ion battery transport box XL
Detectomat	CONUS II – Sounder-Flasher addressable alarm device
Hekatron	155 F – wireless system for hold-open systems
Kentix	MultiSensor-TI with 4-factor early fire detection
Labor Strauss	Fire Detection Control Panel BC08
Meister Automation	multialert 30
Munk	SafeCaddy® – mobile safety system
Novar	NOTIFIER Self-Test Detector

Shortlist



© AP Sensing

Category F: Fire Protection**AP Sensing: N45 LHD series**
Fiber optic Linear Heat Detectors

The N45 LHD series of fiber optic Linear Heat Detectors (FO-LHD) can achieve a measuring range of up to 16km per channel with up to 4 independent sensor channels. Each measuring channel can be divided into up to 2,000 zones with up to 5 individual alarm criteria per zone. Commissioning via standard web browser has been significantly simplified by assistance programs. The N45 LHD series communicates via various network protocols; furthermore, up to 98 output relays can be integrated. The 4mm sensor cables have two independent fiber-optic fibers that enable fully redundant monitoring of customers' assets. Due to the large number of approvals (EN (VdS), FM, UL, SIL2, EX), the new N45 LHD series is already valued in many projects globally. Measurement ranges have been extended from 10 to 16km per channel with a significant reduction in measurement times from 10 to 5 seconds and less. This series can be used for very long-range monitoring in very long tunnel systems and storage facilities, e.g. floating roof tank farms.

Category F: Fire Protection**Meister Automation: Multialert 30**
Simultaneous Extinguishing for Control Cabinet Installations

Fires break out in companies somewhere every five minutes. A defective electrical system is a frequent cause of fires. This is where the Multialert 30 comes in, a further development of the Multialert mini that won third prize in the 2024 GIT Security Awards. Together with the AMFE mini fire extinguishers, the Multialert 30 can protect several areas and control cabinets at the same time. It is supplied with 230 volts and operated independently of the control cabinets. Depending on the situation, it can combine up to 30 mini fire extinguishers and smoke detectors, and can be integrated into existing fire protection systems. It is already used to protect the Würth Airport in Schwäbisch Hall, one of the busiest commercial airfields in Germany. The Multialert 30 can connect up to 30 fire extinguishers to trigger serial extinguishing. If the situation at a site requires it, the Multialert 30 can operate both R-AMFE mini fire extinguishers and smoke detectors.



© Meister Automation

Category S – Special Category: Safety/Security Partnerships & Safety/Security Management

BVSW + TH Deggendorf	Partnership between BVSW, Technische Hochschule Deggendorf, and Bavarian Police
Mobotix + Kepler	c71 NurseAssist – powered by Kepler Vision Technologies
Salto	WECOSYSTEM – unites Salto, Gantner and Vintia Access and Identity Control Management
Schuberth + Twiceme	F300 with Twiceme Integration
Wanzl + Astrum IT	Digital Wanzl & ASTRUM IT visitor management with E-Reception
Wibu	AxProtector for CTP – Compile Time Protection (CTP)



Now it's up to you!
Vote for the
next winners



www.security-award.com

Highlights

Category S: Safety/Security Partnerships

Schuberth: F300 with Twiceme Integration Firefighting Helmet

Schuberth's helmet F300 is a firefighting helmet using Twiceme HTH technology. This technology protects professionals both before and after an accident. Before an accident, Twiceme helps by keeping track of equipment through inspections and self-checks. After an accident, the technology provides quick access to important information about a person such as name, identification characteristics, medical info, allergies to medicines, pre-existing medical conditions, emergency phone numbers and more. Twiceme's technology is already being used in the sports and construction industries but Schuberth is the world's first PPE producer to leverage Twiceme's digital innovation for the increased protection of firefighters.



Category S: Safety/Security Management

Wibu-Systems: Ax Protector CTP Software Protection Solution against Reverse Engineering

Ax Protector Compile Time Protection (CTP) is a software protection solution in the global market combining licensing and obfuscation while achieving security on par with encryption-based tools. It obfuscates program code and data during compilation, increases complexity with the insertion of additional blocks and hiding of logical links within the code, encrypts the control flow and optionally adds integrity verification measures to fend off reverse engineering attacks. Leveraging the LLVM compiler, it can practically support any available frontend language and backend platforms. Ax Protector CTP offers comprehensive security enhancements that are crucial for the development and deployment of safety-critical software applications. By ensuring the integrity and security of software used in systems for fire prevention, video surveillance, access control, and workplace safety, Ax Protector CTP helps companies safeguard their intellectual property and comply with stringent security standards, ultimately contributing to the overall safety and security of the environments they are designed to protect.



Wagner Rail ensures ideal fire protection in the Swiss Südostbahn's Traverso with a customised solution consisting of water mist technology and fire detection

COVER STORY

The Evolution of Passenger Safety

30 Years of Advanced Fire Protection in Trains

The railways are becoming increasingly important as an efficient and sustainable transportation solution in light of challenges posed by climate change and traffic congestion. In spite of the COVID hit, rail passenger transport has been increasing for years and is a central pillar of the desired transport mix across Europe. A reliable fire protection is essential for the optimum safety of passengers and rail vehicles.

■ According to the German Allianz pro Schiene e.V., an association of 16 non-profit organisations and 29 commercial enterprises, rail is by far the safest means of transport. In order to ensure the safety of passengers, trains and infrastructure, adequate fire protection measures are an important and indispensable aspect of rail traffic management.

Fortunately, fires on trains are rare – but when they do occur, they can endanger human life and cause major economic and ecological damage. Heat, smoke and flames themselves can maim and even kill, as can panic reactions by passengers caught in the fire.

Fire Protection Prevents Damage

Fires endanger human lives, cause material damage to trains and infrastructure, disruption to operations and can provoke significant environmental damage. Fire protection solutions that aim to prevent or

quickly extinguish fires are therefore crucial for passenger and rail vehicle safety, and for protecting the environment.

Dr. Markus Müller, Managing Director of Wagner Rail, says: “If we want to promote the safety of passengers, rail vehicles and rail infrastructure, manufacturers and operators of rail vehicles must focus on holistic fire protection solutions. We are doing everything we can to improve rail safety. Detecting fires as early as possible is one of the keys to our success.”

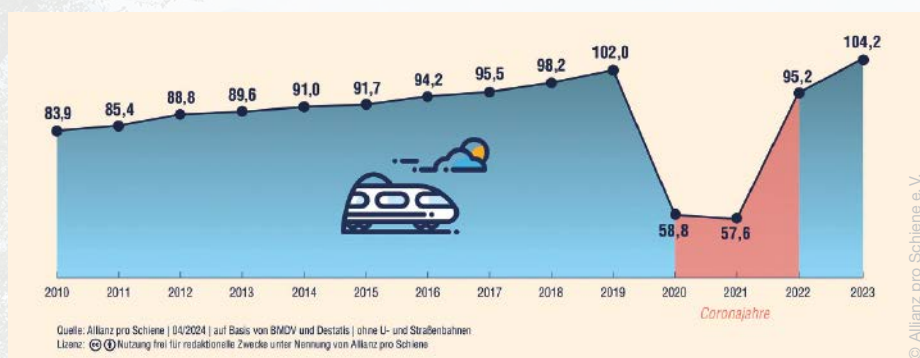
Wagner offers holistic fire protection solutions designed to ensure the safety of people travelling by rail, including aspirating smoke detectors (ASDs), which have been deployed on trains for over 30 years.

Effective and Reliable Fire Detection

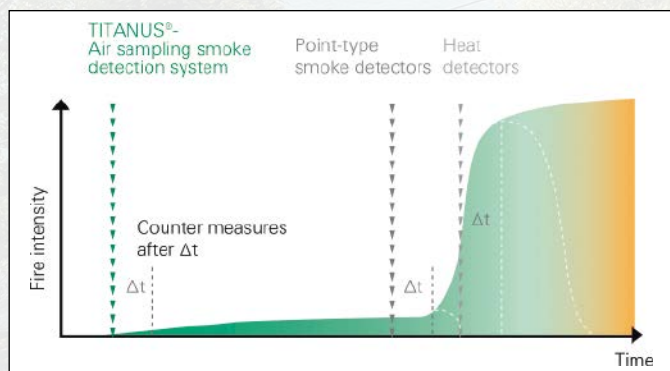
Identifying potential fire hazards and detecting fires as soon as they occur allows emergency services to evacuate, and put the fire out as quickly as possible.

Dr. Müller says: “Reliable and rapid fire detection is particularly important on trains for two reasons: firstly, to raise the alarm quickly and protect people in the event of an emergency; and secondly, to keep fire damage to the trains and the infrastructure to a minimum. We recommend our wide range of automatic detectors – ASDs, optical detectors or multi-sensor fire detectors – to monitor the protected areas for smoke as a fire indicator.

“State-of-the-art systems for spotting fires early detect smoke particles in the pyrolysis phase, i.e., the early stage of a fire before open flames develop. For technical areas where smoke detection is unsuitable due to the ambient conditions on site, the temperature parameter is used as an alarm trigger. Here, we use linear or heat detectors, which can be integrated into the ring bus in combination with a fire alarm control panel (FACP) or used as a stand-alone solution.”



The growth of passenger rail traffic in Germany, shown in billions of passenger kilometres, recovering in the aftermath of the COVID pandemic



Development of a fire and response time of different fire detection systems



The air sampling points of the Titanus aspirating smoke detector are discreetly integrated into the car and are virtually invisible

Protected from False Alarms

Especially when used in train passenger areas, detectors must be highly resistant to false alarms, so that unclean air, such as cigarette smoke from unauthorised smoking in toilets, does not trigger an alarm that causes unnecessary emergency stops.

For early fire detection in trains, ASDs are often the chosen solution. They continuously take air samples from the monitored area via a connected pipe system. Air filters remove foreign substances that are not required for fire detection. This precise and continuous monitoring of airflow enables the detection of even the finest fire smoke particles. Fire alarm control panels record the messages and issue alarm and status messages via the specified information media.

Three Decades of ASDs

Fire detection solutions with aspirating smoke detectors have been used for three decades to improve the safety of rail transport. Dr. Müller says: "Our records show ASDs being used in 1994 in locomotives in service in Switzerland, Scandinavia and India – and most of them are still in service today."

"ASDs marked Wagner's entry into the railway market, and today our systems are mainly found in passenger compartments, control cabinets, supply, exhaust

and recirculation air systems, underfloor areas, engine rooms and in air conditioning ducts. Today, our ASDs are highly resistant to false alarms, so that it does not lead to faulty and costly service interruptions. So it's fitting to celebrate the 30th anniversary of fire protection with this technology."

Titanus devices from Wagner offer further advantages. For a defined area, i. e., a passenger carriage, only a single ASD is required. The heart of the system, consisting of pipes, a detector module and a filter, is located behind the ceiling or wall panels. Passengers can only discover the air sampling points, which are just a few millimetres in size, when they look very closely.

In contrast to the usual point detectors, they are protected against vandalism – as what is not visible and does not protrude as a mounted device is not exposed to vandalism and cannot be accidentally damaged.

Invisible Fire Detection

Train designers can discreetly integrate the system into the existing interior design. They can choose the number and positioning of the air sampling points to suit each specific interior, ensuring optimum safety even when the airflow is affected by room elements or air conditioning systems.

Wagner Rail also offers smoke switches primarily for applications without a perma-

nent presence of passengers and with only selective monitoring of individual objects, such as control cabinets, containers, and the driver's cab. They provide a sensible alternative to ASDs as stand-alone solutions without the need for an FACP.

Water Mist Systems Protect People

Automatic fire extinguishing and firefighting systems are increasingly installed in addition to fire detection systems in response to operator demands and the latest industry standards and guidelines. These are now typical in passenger compartments, sleeper or couchette cars and all staff areas. Water mist systems are deployed to limit the spread of a fire until the next available stop and contain the smoke so that passengers can escape to safety.

Dr. Müller explains: "Our engineers developed special water mist systems, sprayed from small nozzles in very fine droplets, so that a large amount of energy can be absorbed with a small amount of water. The fine droplets also wash out the resulting smoke gases." This technology allows the water supply tanks to be adapted to the carriages, making optimum use of available space and eliminating the need for conventional pressure tanks or high-pressure lines. If a compressed air supply is available, it can be used to generate the water mist. Alternatively, the water mist



**Wagner Titanus Micro Sens
Aspirating Smoke Detector**



**Wagner Rail fire protection solutions are
used in many countries around the world**



**Dr. Markus Müller,
Managing Director
of Wagner Rail**

system can be combined with the existing toilet tank to save space and weight.

To protect technical areas in containers on or under the train and in technical cabinets, today's standards and guidelines require the installation of automatic extinguishing systems, depending on the fire risk. The aim is to extinguish a fire as soon as it starts. These systems are becoming increasingly important in commuter and metro trains as well as in underground trains.

Fire Protection for Technical Areas in Rail Vehicles

The Wagner portfolio has included gas extinguishing technology for many years, using natural extinguishing agents for sealed-off, closed areas, such as control and switch cabinets as well as electrical equipment in underfloor areas and locomotives.

Gas extinguishing systems introduce natural extinguishing gases, such as nitrogen, into the protected area, reducing the oxygen concentration and so extinguishing all types of fires by depriving them of the 'air to breathe'. They are modular and can easily be adapted to the size of the areas being protected. Combined with a fast and reliable fire detection system, the use of gas extinguishing technology allows an incipient fire to be safely extinguished without leaving any residue. This prevents the extinguishing agent from becoming a hazard to electrical systems.

Energy-independent extinguishing systems are also in use. These autonomous, stand-alone systems are connected directly to the train control management system (TCMS). They are an effective solution for new trains and potentially for retrofit in existing vehicles. These autonomous fire protection systems are in all types of rail vehicles, such as trams, light rail vehicles and elevated trains, high-speed trains, passenger coaches and people movers.

Aerosol Solution for Effective Extinguishing

Technical areas such as transformers, power converters or diesel engines are often equipped with several non-closable openings for ventilation. The motion of the train creates air currents in these areas, making it difficult to extinguish the fire. Normally, the train has to slow down or stop completely in order to extinguish the fire safely – with corresponding consequences for rail logistics.

As an important milestone in railroad safety, Wagner Rail has introduced an aerosol system to meet this challenge. It is used where gas extinguishing systems with containers in the housing are too complex or openings in the protected areas are too large for reliable extinguishing using gas. The aerosol extinguishing system contains a defined quantity of extinguishing agent in a cartridge. The system initiates the extinguishing process when electrically activated after a fire alarm or by self-activation at a temperature of 300°C.

The controlled burning of the extinguishing agent in the generator creates aerosols that flow out into the protected area. The extinguishing effect is based on the interaction of the flames with the aerosol: the chemical extinguishing effect can intervene in the chain reaction of the fire and interrupt the combustion process. At the same time, the physical extinguishing effect cools the source of the fire. In this way, a fire can be safely extinguished in a confined area. The flooding of the extinguishing area is practically pressureless, so that no special pressure relief measures are required.

Wagner did extensive prior research in cooperation with German technical inspection association TÜV Süd Rail and in compliance with the German ARGE Guideline Part 2 'Firefighting in railway vehicles'. They carried out tests with fire scenarios

under various ventilation situations to perfect the technology. They successfully extinguished fires completely in ventilated technical rooms even while the train was exceeding speeds of 100 kmh using aerosol extinguishing agent cartridges.

Passenger Safety Around the World

FACPs issue fire protection messages and controls, such as raising the alarm, triggering extinguishing or controlling things like selectively switching off the air conditioning or closing fire doors. All fire detectors and other devices are connected to the FACP via a ring bus. This ensures that if a wire breaks, all devices are still connected to the control panel and none will fail. The integrated ethernet connection allows the FACPs to be connected to the train bus interfaces.

Passenger safety is a top priority around the world. This is why manufacturers and operators of rail vehicles rely on high-quality, reliable and efficient systems. Wagner fire protection systems are fitted in countries from A-Z worldwide, on tourist attractions, on mountains and in deserts.

Dr. Müller says: "We have so many exciting projects that it is difficult to single out individual ones; but I call to mind the world record train in Switzerland, our projects in India with no less than 5,000 cars, the Transrapid in Shanghai, the Talgo high-speed train for Saudi Arabia, the Caltrain in the USA, the ÖBB Railjet in Austria and even cable cars like the Wurzeralmbahn, which takes skiers and hikers safely up the mountain to an altitude of 1,400 meters." ■



Wagner Rail

<https://rail.wagnergroup.com>

FIRE PROTECTION

Hot and Steamy

An Approved Fire Alarm System and Weatherproof Devices Secure New Food Production Facility

Installers JTI Brandbeveiliging were contracted to help make safety a number one priority at a leading food manufacturer in the Netherlands. They achieved this by choosing Hochiki Europe's Latitude fire detection system, alongside weatherproof devices from the ESP range. This comprehensive solution ensures the highest level of fire protection throughout the facility, giving the food manufacturer peace of mind and allowing them to focus on what they do best – producing delicious food.



Boasting many important international regulatory approvals, the versatile Latitude fire detection system is ideal for many different installation environments

■ Kervo is a specialist in the high quality cultivation and processing of fruit in the Netherlands. Morello cherries have been grown in the Vossen family's orchards in Roggel, the Netherlands since 1980. The family were one of the first growers in the region to use mechanical harvesting in the 80s. Fast forward 43 years and Kervo now runs operations across Europe and the UK and is proud of its reputation for offering the finest quality fruit to bakeries and fresh food processors.

Complexities

JTI Brandbeveiliging was founded in 2009 and is trusted by its customers for advice, installations, repairs, and the maintenance of fire protection systems across the region. The team, led by Luciën van Eldijk, was commissioned in 2022 to design and fit the fire safety system that would be integrated into Kervo's new manufacturing plant in Neer. One of the complexities of this project was that during food production, and particularly during the cleaning processes, significant amounts of steam are generated, leading to false alarms.

Luciën van Eldijk explains how he and the team navigated this issue: "In food production sites like this, it is essential for the machinery to remain clean throughout the entire process. This means there is a lot of steam and water present, which unfortunately can trigger false alarms. We needed to install devices that could negate this issue; Hochiki's weatherproof call points, sounders and sensors were the perfect solution, and they work seamlessly with the Latitude fire safety system."

Huge Capacity

Latitude, which is BOSEC approved – a requirement for fire detection devices and systems in the Netherlands – has a powerful network-wide cause and effect capability. The system has the capacity to support 5,000 entries, with up to 20,000 inputs and 20,000 outputs across the network. The new building at Kervo is a huge facility; at over 40 meters in height, it required over 2.5km of cabling and hundreds of fire detection devices to secure the building, making the Latitude system the best solution.

Van Eldijk says: "Due to the nature of this project, there have been some technical aspects where we have needed to seek advice, but the team at Hochiki have been very helpful in working with us to create the best solution for our customer. We choose Hochiki products and systems because they are reliable, easy to install, and most importantly meet the high standards and regulations required by the laws of the Netherlands – we would recommend Hochiki products for this reason."

Hochiki's analog addressable range (ESP intelligent) together with the Latitude system are EN 54 Part 13 certified and, with the BOSEC certification also in place, they provide the best complete and compliant fire detection system for businesses across the Belgium region as well as bordering countries, such as Luxembourg, the Netherlands and Germany. ■





FIREFIGHTING

Fire Drones

Heat-Resistant Drones for Firefighting

Researchers at Empa and the Imperial College London have developed a heat-resistant drone to support firefighters. The drone can take a close look at the center of building or forest fires. This helps firefighters to choose the right tactics before entering the danger zone.

Where others run out, they have to go in: firefighters put themselves at risk with each call-out – sometimes in a sea of flames. Last year, the Swiss fire brigade fought more than 12,000 fires. Every unnecessary risk must be avoided because deadly temperatures of more than 1,000 degrees Celsius can be encountered in burning buildings. Drones can assist in such scenarios: researchers at Empa and the Imperial College London are developing a heat-resistant drone that can deliver initial information about the danger situation. This enables the men and women of the brigade to adjust their strategy before they attack the inferno.

“The firefighters don’t know what they will encounter and what difficulties they will face before they enter the danger zone,” says Mirko Kovač, head of the ‘Sustainability Robotics Lab’ at Empa as well as the ‘Aerial Robotics Lab’ at Imperial College London. Drones equipped with cameras and CO₂ detectors (carbon dioxide) can provide valuable information about the extent of the fire, unexpected dangers or trapped people.

Too Hot for Normal Drones

Drones are already being used for firefighting to take aerial pictures, to lift hoses onto high buildings or to drop extinguishant in remote areas, to stop the spread of forest fires for example – but always at a safe distance from the actual fire. “The extreme heat of a fire is too much for nor-

mal drones to be able to fly closer,” says David Häusermann of the Sustainability Robotics Lab at Empa. The frame would melt and the electronics would fail close to the fire. “Conventional drones can only provide aerial images of the fire from a safe distance,” adds David Häusermann. It was therefore the aim of the robotics researcher to develop a drone that could withstand the heat and quickly provide precise info about the center of the fire.

Ultralight and Tough

Together with firefighters, David Häusermann established the requirements for a drone that would be used close to fires and set about finding a material that could surround and protect the core of the drone – the motors, batteries, sensors and the electronics. He found the answer with his colleagues from the Empa Building Energy Materials and Components Lab: the team of researchers working with Shanyu Zhao and Wim Malfait were able to create an isolating material that could withstand high temperatures and thereby make the drone more resistant to fire. They were inspired in the design of the ‘fire drone’ from nature, or more exactly, from animals like penguins, the polar fox, and certain beetles that all live at extreme temperatures. All these animals have corresponding layers of fat, fur, or produce their own protective layers from a temperature-regulating material that allows them to survive under extreme conditions.

Suitable for Space Suits

This is an aerogel, an ultra-light material that consists almost completely of air-filled pores that are covered by a skin of a polymer substance. In this case, the material researchers used an aerogel on the basis of a polyamide plastic. Polyamide aerogels are also being researched by NASA, among other reasons for insulation in space suits. Shanyu Zhao not only used polyamide for the creation of this aerogel: the composite material consists of polyamide and silica and is also strengthened with glass fibers. “Laboratory analysis has shown that this comparatively fire resistant material is particularly well-suited for use in drones,” says aerogel researcher Shanyu Zhao.

Flight into the Inferno

The prototype of the ‘FireDrone’ already did well during the first tests in the flight arena at Empa in Dübendorf. The flying characteristics and control of the approx. 50 centimeter drone were excellent, even when fitted with the aerogel insulation jacket and an additional cooling system as well as aluminum wrapping to reflect heat. The design that the researchers published in the “Advanced Intelligent Systems” news-sheet was impressive during the ‘dry run’. Whether the drone would survive a real fire had to be tested under realistic conditions. The Empa team were able to experience such a ‘real life’ scenario on the grounds of the training center in Andelfingen. Stefan Keller, training coordinator of the fire



Glass fiber-reinforced aerogel surrounds the heart of the drone and protects the power supply and the electronics from heat

brigade for building safety in the canton of Zurich, together with the training center logistics crew, built a gas fire in an enormous metal dish, and the drone pilots flew their device into the middle of the inferno.

The result: the FireDrone prototype survived numerous test flights. A happy David Häusermann summarized: "Even

after numerous flights, the electronics, the thermal camera and the CO₂ sensors of the FireDrone were undamaged and ready for further tests. The next step will be to test the FireDrone in a fire that in contrast to the relatively 'clean' gas flame contains a lot of smoke particles." The fire brigade expert Stefan Keller was impressed

with the results: "If a drone can make a first assessment of the situation, we don't have to send firefighters into the danger zone immediately. This is an enormously interesting step forward for us."

The FireDrone could also be used in extremely cold environments, such as in polar regions and on glaciers. The team also tested the drone in a glacier tunnel in Switzerland to see how the system behaved in very cold temperatures. Discussions are already underway with potential commercial partners on developing the prototype further. "The use of drones has so far been limited by environmental factors such as extreme temperatures," says Mirko Kovač. "The FireDrone has demonstrated a way to considerably extend their application in the future under extreme conditions." ■

Original Publication:

D. Häusermann, S. Bodry, F. Wiesemüller, A. Miriyev, S. Siegrist, F. Fu, S. Gaan, M.M. Koebel, W.J. Malfait, S. Zhao, M. Kovač; FireDrone: Multi-Environment Thermally Agnostic Aerial Robot; Advanced Intelligent Systems (2023); doi: 10.1002/aisy.202300101



Empa
www.empa.ch

© Images: Empa/newsimage/dw

PYROsmart®

Intelligent fire prevention for large outdoor areas

PYROsmart® detects fire hazards before they start.

The infrared system offers the decisive advantage: reliable early detection of critical temperatures and precise control of automatic extinguishing attacks for cooling.

Find out more? Visit: www.orglmeister.de/en



Orglmeister
Infrarot-Systeme



- Monitors large outdoor areas, ports, halls, etc.
- Hundreds of systems in use worldwide
- Quick overview thanks to video and infrared panorama



Geared up to Display Comprehensive Fire Safety Solutions at Fire Safety 2024

Renowned life safety equipment manufacturer Hochiki Europe geared up to display its comprehensive solutions at the Fire Safety Event 2024, which took place at the NEC Birmingham from the 30 April to 2 May 2024. Visitors to Hall 5, Stand E35 experienced firsthand Hochiki Europe's commitment to innovative technology and its most advanced fire safety solutions yet. Attendees engaged with interactive demonstrations of the Latitude Life Safety Platform, the Ekho Hybrid Wireless Fire Detection, the FIREscape Nepto self-monitoring system, the ESP Intelligent Range, and the CDX Conventional Detection, as well as the specialist detection portfolio of detectors designed to address unique fire hazards in challenging environments. Visitors exchanged knowledge on critical themes, such as the latest fire safety regulations and best practices, or how installers can optimize fire safety solutions for different building types and the power of integrated life safety platforms. www.hochikieurope.com

Artificial Intelligence Protects Aachen Cathedral

Since the end of last year, Bosch's artificial intelligence has been safeguarding the world-renowned Aachen Cathedral, which is more than 1,200 years old. Germany's first UNESCO World Heritage site was equipped by Bosch Building Technologies and the engineering firm planning with an intelligent video solution that protects it against a multitude of potential threats. Fires in particular can be devastating for such a historic building of inestimable intangible value. Over 50 Aviotec cameras from Bosch in 16 rooms use intelligent video analytics to detect smoke and flames visually, directly at their source. AI algorithms can also differentiate candlelight from a developing fire, reducing the likelihood of false alarms. The cameras respond much earlier than conventional ceiling-mounted fire detectors, which require smoke to rise to them.

www.boschbuildingtechnologies.com



Synergies

Cias announced a new integration with Avigilon, the brand that addresses security challenges for organizations of all types, offering end-to-end security solutions, VMS & video analytics, video surveillance, and access control. Together, the companies have integrated Cias' sensor data collection software IB-System-IP with the Avigilon Control Center (ACC) VMS system. The two systems communicate synergistically so that, in the event of an intrusion attempt detected by Cias sensors, the IB-System-IP software sends signals of Alarm, Pre-Alarm, Tampering, or Fault to the Avigilon ACC system, thereby enhancing the protection of the sensitive site. This integration marks a significant step forward in their mission to provide comprehensive and integrated security solutions for their clients. www.cias.it

Shortlisted

Advanced has been shortlisted for three FSM (Fire and Security Matters) awards in 2024. The nominations include Fire Safety Innovation of the Year for the company's Advanced Live solution, Fire Safety Manufacturer of the Year, and ESG Company of the Year for the work the company is doing to become a more sustainable organisation. The winners will be revealed at a gala dinner on 12 June at the CBS Arena in Coventry. These nominations follow the company's previous successes at the FSM Awards in 2022, where it was recognized as Fire Safety Systems Manufacturer of the Year and received recognition in the Fire Innovation of the Year category for the BS 8629-compliant evacuation alert system, EvacGo. www.advancedco.com

Standards-Compliant Surge Protection for Industry

The DEHNventil ACI M TNS 264 FM has the electrical and mechanical parameters to fulfil the requirements of IEC 60364-5-53 with SPDs installed as close as possible to the service entrance of the electrical installation. The reliability of switchgear in, for example, industrial plants, data centers, hospitals and large administrative buildings is critical, which makes surge protection essential. However, the replacement of the surge protection module should not influence system availability. The Dehn device has no backup fuse and, in the event of a fault, the protection module is safely disconnected and can be quickly removed from either side or the front. The touch-safe design allows the protection module to be replaced without system downtime. The device has various mechanical mounting options (DIN rail, mounting plate/switchgear cabinet wall and PE busbar via M8 screw) with simultaneous impulse current-tested contacting of the PE connection. www.dehn.de

Video Flexibility and Availability Beyond the Control Room

Qognify has launched version 7.4 of its VMS, which brings greater operational flexibility and video availability, inside and outside the control room. The new Qognify Web Client

places exceptional live viewing, playback, and investigation capabilities in the hands of the people who need it, whether they are on patrol, off-site, or in the control room. Its highly secure, modern user interface can be accessed via standard browsers on various platforms. Improvements to the forensic search tool QogniFinder now support metadata streams from Axis and Bosch cameras, as well as through a new suite of AI-based video analytics. Available for purchase alongside VMS 7.4, these include perimeter security, counting, object detection, fire/smoke detection, face recognition and gender/age analysis. Qognify VMS 7.4 is now available worldwide. www.qognify.com



SURGE PROTECTION

Well Protected

System Protection for Building Technology and Measuring and Control Systems

Technical building equipment and measuring and control systems (MCS) must function reliably and signal paths must be designed to be fail-safe. Surge protection plays an important role in this context. Arresters from the Blitzductorconnect and Dehnpatch product families protect MCS circuits, the DC mains supply, Ethernet infrastructure as well as bus and telecommunication interfaces against damage in the event of lightning and surges.

■ Permanent monitoring of both product families by Dehnrecord IRCM enables the fast detection and notification of arrester failure and faults. If an arrester fails, a remote signal is automatically sent so that the module concerned can be replaced without delay.

The combined lightning current and surge arresters of the Blitzductorconnect family protect both measuring circuits and bus systems. Specially approved product variants for intrinsically safe signaling circuits are also available. The fail-open function ensures that normal operation continues even if an arrester needs to be

replaced. Overloaded components are disconnected from the signaling circuit and the system circuit remains available. The arrester can be replaced during operation with all production processes up and running. Thanks to an integrated status indication with a matching remote signaling unit and the predefined failure behavior of the arrester, the operator is always aware of the status.

The Blitzductorconnect protective devices are available in a compact or modular design. Both variants have a width of just 6 mm. Functions such as the secure release buttons (secR) and the push-in

terminals also help to optimize installation and maintenance work. The arrester itself has a simple disconnection function. Plugging the arrester module in the other way around interrupts the signal circuit – giving a time advantage when performing measurements.

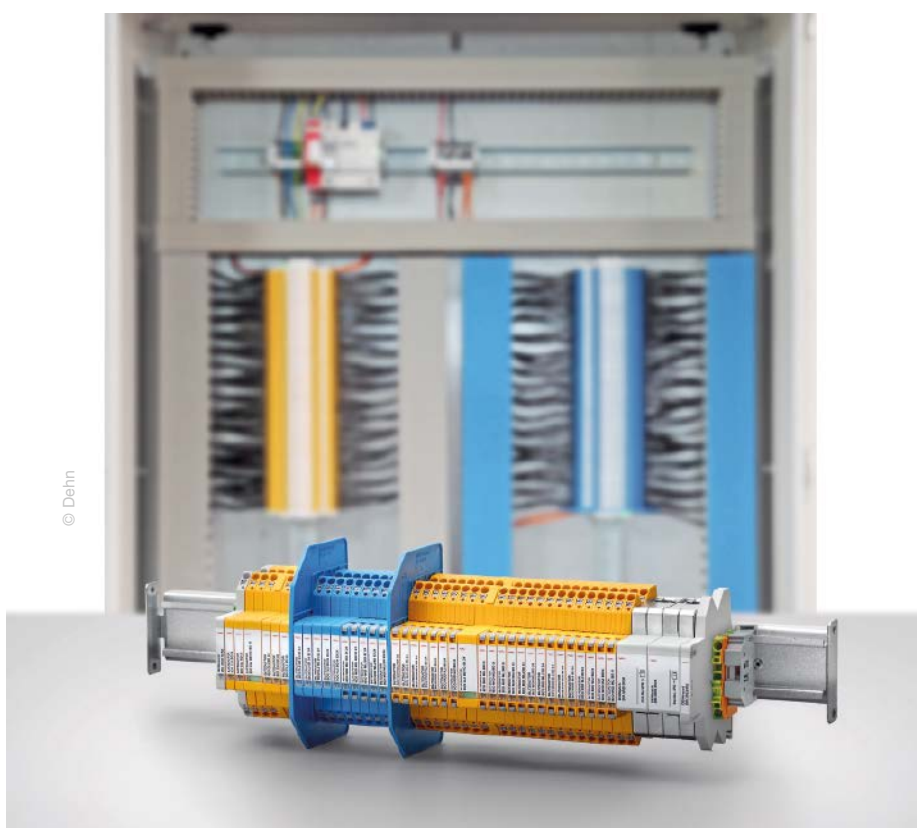
Safety First

Advancing digitalization demands an ever faster supply of data: high transmission volumes and ever improving bandwidths are a prerequisite here. Structured cabling is an important component of today's network topology for information and data technology. In this context, safety is a multifaceted topic in which lightning current and surge arresters play an important role.

The Dehnpatch DPA CL8 EA 4PPOE arrester is designed for use in a switch-gear cabinet or data distributor and can handle data rates of up to 10 GBit/s. With Power over Ethernet (up to 4 PPOE with a power transmission of up to 100W), class EA transmission standard (max. 500 MHz), status indication, and the possibility of remote signaling, the Dehnpatch is equipped for modern applications. Dehnpatch has the GHMT-approved seal of quality which affirms that the arrester has met the normative requirements and standards for high-performance networks of data technology.

Well Informed

The Dehnrecord IRCM condition monitoring unit, a DIN rail device set with a visual transmitter/receiver and a visual reverse unit, enables condition-based monitoring of Blitzductorconnect and Dehnpatch arresters in a single system solution. It is a visual monitoring principle – resistant to extraneous light. The arrester status is signaled quickly and easily via an LED group display combined with a remote signaling contact. ■



System protection for building technology and MCS



Dehn SE
www.dehn.de

VIDEO SURVEILLANCE

Video Syncs with Giant EV Charging Park

Rail Station Pioneers Smart Car Park Protection

A German train station has installed smart video analytics to protect the largest Electric Vehicle (EV) charging car park in the world. Merklingen train station, between the cities of Stuttgart and Ulm, boasts an impressive 259 charging points powered by locally generated solar power to charge vehicles. It was inaugurated in December 2022.

■ The new train station serves 1,000 to 1,300 passengers daily. It has benefitted local hospitality, retail, and tourism since it opened with the state Ministry of Transport calculating that it will eventually generate an annual economic benefit of €4.8 million for the region.

As a transport hub for the local municipality of Merklingen, it is vital that visitors feel safe and operations run smoothly. Because of this, the management team of the Zweckverband Schwäbische Alb (ZSA) contacted Reif GmbH looking for a new, intuitive video system that was future-proofed and could support the management of the station's innovative EV charging park.

Existing systems on the market did not meet the customer's requirements, specifically National Defense Authorization Act (NDAA) compliance which was important from a GDPR perspective. NDAA compliance confirms systems are fit for use with US military and other critical defence priorities, ensuring troops have the training, equipment and resources they need to carry out their missions. The ZSA team also wanted an easy-to-use video management system (VMS) to help daily operations and with investigation of any incidents.

VMS Linked with Parking Management

Hanwha Vision was chosen thanks to its intuitive Wave VMS, NDAA compliance, open platform and camera features. As a Diamond Partner, Reif GmbH was also able to offer a 5-year warranty on the Hanwha Vision cameras.

In total, 37 cameras are installed around the station's car park along with Wave VMS enabling continuous monitoring of the building and surrounding locations. The cameras include the QNO-8080R, a 5MP Network IR Bullet Camera, a TID-600R Intercom and the XNO-9082R, a 4K IR Bullet Camera with the Wisenet7 chipset and powerful video analytics including directional detection, audio detection, shock detection, and face/upper body detection. Maintenance staff can access the on-site server in the event of an emergency or malfunction due to the

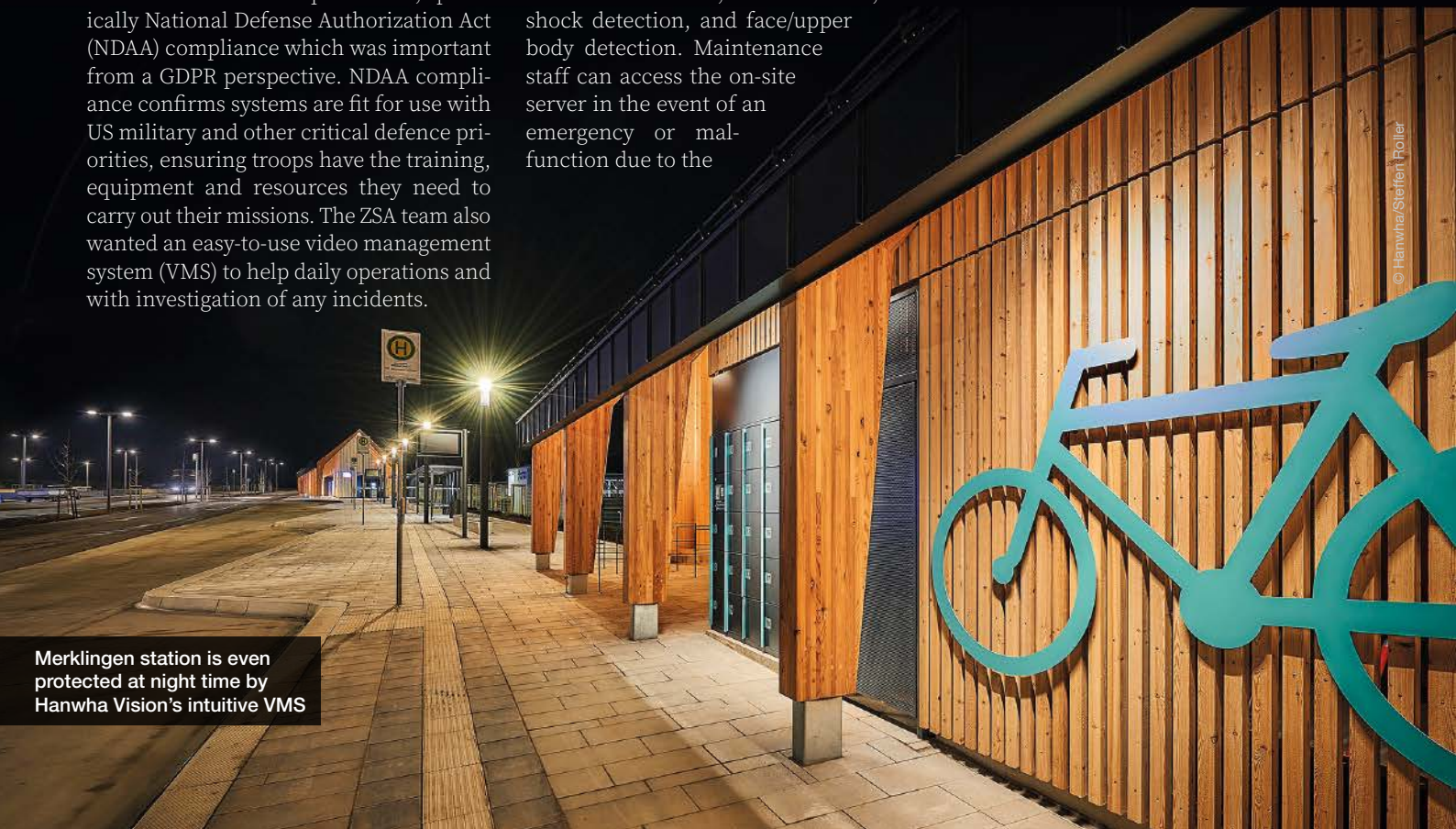
Wave VMS, with remote access through Wave Mobile.

Andreas Baumann, Managing Director at Reif GmbH, said: "The performance and quality of Hanwha Vision cameras, along with the open Wave VMS that works with the in-house AI parking management system, made it the logical choice for the Merklingen station project."

Advanced Video Analytics Promote Safety

Advanced video analytics to improve the passenger experience and safety across the rail network is increasingly accessible thanks to a wide range of cameras that sup-

Merklingen station is even protected at night time by Hanwha Vision's intuitive VMS



port analytics, such as loitering detection, audio detection of shouting, screams and broken glass, motion detection and more. Such analytics can alert operators to potential trespassing in restricted areas such as control rooms or level crossings. Shouting or screaming can alert to an unwell passenger, someone fallen on the tracks, or another emergency.

Some cameras can detect crowd formation to help station security proactively deter anti-social behaviour, while occupancy monitoring can also be used to manage queues and waiting room occupancy. Integration with access control, bodycam devices, digital signage, and equipment monitors can further expand the alerts and automation supporting the control room.

Benefits of an Open System

Hanwha Vision's open platform offered the flexibility and futureproofing needed by the operator team, notably in supporting an integration with a custom in-house AI parking control system that was developed in partnership with a regional software company. This system automates parking management removing the need for personnel to issue access, exit, and parking fees for the station car park. The open platform also supports future expansion of the station video surveillance if needed, or additional features and uses.

Crucial Evidence and Insights

The cameras work with the in-house parking management system to prevent unauthorised vehicles from entering the premises. They have also captured footage that was later used to investigate damage to property, helping operators to resolve such cases clearly and effectively with the video evidence.

The XNO-9082R shows excellent performance in different lighting conditions thanks to Wisenet7, delivering clear images back to operators to help with situational awareness day and night. IK10 water and vandal protection was another selling point for the station team, as the cameras are all situated outdoors.

Installing cameras with advanced video analytics can create new efficiencies and a better visitor experience, extending the value of surveillance beyond traditional security applications. For instance, barriers can be automatically raised for pre-authorised vehicles based on licence plate recognition, or drivers can be directed to vacant parking bays with integration between cameras and sensors monitoring the bays and digital signage for directions.

Fees can also be automatically issued when a vehicle is detected leaving a car park. Automating some aspects of parking



37 cameras protect the largest EV charging car park in the world

© Hanwha/Steffen Roller

management frees up operator time to work on other tasks, improving team efficiency and reducing time-consuming, repetitive work.

Meeting GDPR Requirements

Hanwha Vision cameras are NDAA compliant, meeting the GDPR requirements for the station. No productive data is passed on to external third parties and the system can be operated completely on-site to meet data protection regulations. Only explicitly authorised individuals can view data.

Critical infrastructure, such as the rail network, is vital to keeping countries running smoothly and, as such, can be an obvious target for malicious actors that want to cause disruption. A high level of cybersecurity is paramount to safeguarding against attacks and video surveillance must not be a weak link in cyber-defences. Insecure video cameras can be hacked, along with other connected devices, to access the

valuable data collected by them, or as a gateway to a larger attack. Partnering with a manufacturer that puts cybersecurity and data privacy at the core of every product will give operators and passengers peace-of-mind that the video system in use is as secure as possible.

GDPR compliance is another consideration, as is NDAA. Looking for compliance with such requirements can be a clear confidence signal that a manufacturer is taking cybersecurity seriously. Other 'trust marks' include having dedicated resources, such as a cybersecurity team, to keep updated with the latest threats and vulnerabilities, and a commitment to sharing best practices and knowledge with the wider industry and customers. ■



Hanwha Vision Ltd.
www.hanwhavision.eu



The VMS links with the in-house parking system to automate parking management



To display video streams by integrated IP decoding without using a computer: the FDF2712W-IP 27" Full HD IP decoder monitor from Eizo

VIDEO SECURITY

Alert-to-Action

A Security Solution for Banks and Financial Institutions

Banks and credit institutions are responsible for managing billions of dollars in investments, income and savings, as well as an enormous amount of private information. As such, they are often the target of crime. Securing financial assets around the clock depends on security personnel and bank employees having critical information at their fingertips to prevent criminal activity and to protect customer assets. A solution from Eizo called Alert-to-Action can provide bank staff with increased visual awareness through the integrated use of video analytics or facial recognition.

■ The safety of branch employees is a high priority due to the sensitive nature of working in a bank. Securing the premises before opening or closing is crucial to prevent incidents and to ensure the safety of employees. It is vital that security personnel, such as those deployed via an intermediary security service, develop a high level of situational awareness of the environment to ensure the safety of bank employees and customers.

When integrated with video management systems (VMS), video analytics or other security systems, operators can visually confirm the security of the premises around the clock and be notified in real time if something is amiss. The monitor or IP decoder box can provide visual indicators when suspicious activity occurs in the area and immediately initiate the measures necessary to maintain a secure environment. Alert-to-Action can also provide bank staff with increased visual awareness

through the use of video analytics or facial recognition. This can alert tellers to suspicious behavior, identify known suspects or detect fraud attempts and protect assets.

Securing Access to Protect Assets

Financial institutions grant their employees varying degrees of access to sensitive areas such as vaults, cash drawers and rooms where cash reserves and other valuables required for day-to-day operations are stored. In addition, managing cash balances to support customer transactions requires that cash transporters and maintenance technicians also have access authorization to certain areas. These highly sensitive areas can quickly become the target of internal theft if thorough security measures are not in place. Proactively monitoring these areas using real-time notifications can help identify if an employee has breached protocol, preventing losses before they occur.

With the Alert-to-Action function, the IP decoder monitor or IP decoder box can send an alert if the connected access control system detects a deviation from certain protocols. For example, if two employees are required to be present to open a safe or access a cash drawer, but only one employee is present or attempts to enter the area, an alert can be sent to on-site security personnel so they can respond immediately.

Customizable Event Response

The web API of Eizo's IP decoder solutions supports customized integration with the local security systems and devices to enable communication with and response to alarms over the network. When an event occurs and an alarm is sent from IP cameras, access control, hazard detection, a VMS or other system, the Eizo solution responds with a predefined action, such as layout adjustment, a message display, audio activation, camera adjustment, masking, or other actions. Implementing an intelligent visual communication system into the workflow is a step forward in supporting the transformation of banks through timely alerts while enhancing the security of high-value assets and sensitive information managed by financial institutions. ■



BIOMETRIC SYSTEMS

My Oh My!

The State of the Art in Physiological Biometric Security Methods

‘Something you know’, and ‘something you have’: these are the traditional items necessary for two-factor authentication (2FA) security. The combination of a physical authentication token of some sort as well as an item of knowledge that, hopefully, nobody else knows ensures that access is granted only if both can be presented.

SPECIAL
FOCUS

■ The ‘have’ is nowadays increasingly biometric and we investigate some of the current techniques more closely in this article. But a third element is now becoming more frequently used for identity verification: ‘something you are’.

Let us look first of all at some of the possible biological ‘haves’. There are many aspects of each to be considered when constructing a security system tailored to the particular circumstances of an organisation or company.

High on the list is user acceptance of their introduction, helped by an education campaign to dispel any false information, rumours or downright lies about the effect of taking scans of body parts. We know with certainty meanwhile that your hand will not be burned, you will not go blind, and you will almost certainly not develop an allergy by using biometric security devices!

Quick and Reliable Fingerprints

When they are dirty, wet, swollen or damaged through injury, fingerprints cannot be used as identity verification. The rest of the time, which is most of the time, they provide a quick and reliable method of proving someone’s identity.

Contactless fingerprint scanners are rapidly becoming widespread, reducing hygiene concerns and making the process

more convenient. Modern scanners look at the finger in question at different optical wavelengths or using ultrasound to build up an accurate digital model and also to check if there is blood flowing – a good sign that someone is alive and not just a severed finger has been offered up.

TBS in Switzerland have a wide range of scanners for the job in hand ... sorry for the pun. Aratek also have a palette of products and solutions that are available in most regions of the world.

Facial Scans Have Their Limits

While the stuff of science fiction movies in the 1960s, facial scanning has become an everyday technique to identify people. It has its limits though, and can be confused by beard growth, changes in makeup, some temporary skin ailments, or even just people getting older. Early primitive systems could even be overcome by holding up a photograph of someone’s face.

Nowadays, a 3D grid map provides a far more accurate 3D model made up of 30,000 data points or more. With that, it is also possible to tell whether someone is awake and responsive, or drugged, or even still alive.

However, even these facial recognition algorithms working in the background often struggle with people from some ethnic minorities and produce inconsistent

results, a situation already experienced by police, border forces and some universities. Someone’s face is often freely available on their social media accounts, the website of their football club and the local school PTA, so it’s easy to obtain ‘fake faces’.

You might like to contact Oosto to find out about their facial scanning solutions that avoid such scams. Alternatively, the Luna range of terminals is manufactured by Vision Labs in Amsterdam. Summary: face scanning is ideal for a great many situations but not perfect.

Retina and Iris Scans and Vein Pattern Recognition

The invention and introduction of facial recognition has caused a heap of political discussion, as well as regulation, for fear of racial discrimination or the intrusion of privacy. Neatly overcoming that problem are scans of other body parts.

Everybody’s eyes have a unique pattern of shapes and blood vessels that can be scanned using infrared light to generate a totally individual record. The scans look at the colourful part of the eye, and the distinctive patterns of the iris or the retina, and refer to a database for highly secure identity verification.

Also unique are the patterns of blood vessels in your hand. Under infrared light



they can be compared against a biometric template in a database. Either fingers or palms can be analysed, both of which provide a highly secure method of identification.

A spinoff benefit of highly accurate retina scanning is exposing so-called 'deep fakes' that are otherwise totally convincing. NEC have patented the method of iris recognition and capture used in their terminals, while terminals from Secunet are in a trial phase at Frankfurt airport.

Link Voice Recognition with Biometry

Computer software can be trained to recognise patterns in spoken words or in continuous free speech. The duration of speech necessary to achieve a satisfactory identification has continuously come down, and is currently under a minute.

Again, a number of factors can lower the useability of voice recognition as a unique identifier, among them variations in one's voice caused by illness or background noise. Most critically, and as we are now hearing almost every day, the development of voice recognition has been matched by voice generation, which has now become so advanced that fake audio (and video) clips of outstanding quality are relatively easy to produce, and already overcome anti-spoofing methods.

Voice authentication can only be used in combination with other, preferably biometric, methods of identity verification for secure environments.

DNA Matching on the Way

Yes, a physical sample of your body can of course be a unique identifier. The processing of DNA samples still takes too long to be generally used as an access control method, but it is highly secure, and the technology that will make a DNA test a quick process is developing rapidly.

Antier are working hard to advance the technology into everyday life and applica-

tion in a number of security-related scenarios.

Behavioural Biometrics as You Type

Not physiological but behavioural analysis to identify people is much less known generally, but has already been subtly in use for many years. This cannot (yet) be used alone for rapid access control, but if this has already been breached somehow, then the behaviour of an imposter will certainly give them away.

Most commonly, the way in which we interact with the input devices of our PCs will allow us to be uniquely identified. We all have our own favourite way of using the shift key, our own individual time gaps between characters, even our own most common spelling mistakes. The benefit of this type of analysis is that it can be continuously done while you work.

The algorithms running in the background build up a profile of your particular behavioural traits over time and gradually narrow down the leeway of doing things differently so that any sudden deviation from 'normal' behaviour is flagged up. So the accuracy of behavioural biometrics naturally increases as time goes on.

"This Won't Hurt a Bit, James ..."

Fans of old science fiction or James Bond movies such as Casino Royale might have already thought of combining the 'what you are' and 'what you have' by inserting a (micro)chip subcutaneously into your body somewhere.

James is not alone: Today there is a growing five-figure number of people among us with microchips under their skin. They are currently used predominantly for cashless payment, access control and storing emergency medical information. They also offer a very convenient method of granting access to those people who are mobility challenged. Apart from that, they are, of course, a highly secure method of identity verification. Go and visit Bioteq's website if you want to join the secret service, or have other ambitions.

Can You Fool the System?

Of course, every security system is only safe until it is cracked ... and biometric systems, although far more challenging, are no exception.

What might sound like a poor April Fools' Day prank is actually already true: An application called PrintListener can capture the 'sound' of fingerprints when they pass over a surface and scarily reproduce them on demand.

While the technique is not perfect, its current 9% accuracy is climbing quickly and already poses a real threat today. The surface in question is the screen of your smart phone, while its built-in microphone is easily sensitive enough to pick up the unique 'scratching' noise that your fingers make. So wiping across the screen should only be done with the microphone disabled. Check now which apps installed on your phone have access to the microphone and camera and disable those that do not need access for their basic operation.

So-called 'presentation attacks' involve downloading, printing or generating a person's photo, using a fake silicone fingerprint, or using a 3D mask. Needless to say, this primitive form of trying to fool a biometric terminal will nowadays rarely, if ever, be successful because of 'liveness' tests.

SOC2 Baseline for Data Security Compliance

While all this capturing of highly individual and person-related data is going on, that highly personal data has to be available and referenced when required. It is almost needless to say that it is essential to capture and store biometric data in strict compliance with national applicable regulations, preferably to a standard some way beyond that legally required and also just local to the verifying terminal; SOC2 could be a very good starting point.

When implementing security upgrades with a biometric element, collecting all the biometric scan data for a large number of users will be time consuming and labour intensive. Staff may even be required to visit off-site locations to have the necessary scans done. The time and effort invested, however, will be rewarded with the satisfying peace of mind that yet another barrier has been put in place against fraud, theft, and blackmail.

The gathered data must then enjoy the highest of security levels and only ever be transmitted in encrypted form between biometric terminals and a remote reference database. Administrative access to the management of any centrally-stored data is also best covered by a 'four-eyes' principle, with those eyes themselves being a part of biometric personnel validation too.

In a strategic partnership with Veridos, Innovatrics is developing DNA-based security database solutions, while iProov pay rigorous attention to achieving, and indeed exceeding, the highest security certification for their range of products.

Unifying Authentication Standards

With all these scanning devices from different manufacturers popping up that are look-

ing at hundreds of body parts every second, there is great potential for manufacturers' proprietary island solutions to develop that lock a user into just one supplier.

The well-established FIDO Alliance is working to combat this risk and advocates an open communication specification and exchange of data between edge devices

and centralised management and databases. Their Biometric Component Certification Program allows manufacturers of IoT and other terminal devices to submit their products once for performance and compliance certification to be acceptable right across a massive potential customer base without further testing.

Suppliers

Antier | www.antiersolutions.com

Aratek | www.aratek.co

Bioteq | www.bioteq.co.uk

FIDO Alliance | www.fidoalliance.org

Innovatrics | www.innovatrics.com

iProov | www.iproov.com

NEC | www.nec.com

Oosto | www.oosto.com

Secunet | www.secunet.com

TBS | www.tbs-biometrics.com

Veridos | www.veridos.com

Vision Labs | www.visionlabs.ai

Ensuring Access Is Universal

EU Guideline 2019/882, more easily referred to as the European Accessibility Act (EAA) (Barrierefreiheitsstärkungsgesetz or BFSG in Germany), will apply to digital customer onboarding using identification methods as of the middle of 2025.

It applies to service providers with at least ten employees and an annual turnover or a balance sheet total of more than two million euros, as well as to all manufacturers of identification devices, biometric or otherwise. It aims to ensure that people with restricted mobility or physical impediments are not excluded from using general verification methods.

A simple example of this would be a face scanner at an entrance that must also be able to be used by someone in a wheelchair; there are of course many other situations. Suffice to say, biometric terminal manufacturers must think broad and long before introducing new techniques to ensure that, firstly, they will work reliably for all valid users, and equally reliably keep out the invalid ones. ■



**PROTECTION.
EXACTLY WHERE
IT IS NEEDED.**

Highly precise detection and surveillance with REDSCAN mini-Pro

The new REDSCAN mini-Pro sensor series provides highly accurate and reliable short-range detection of intruders and moving objects within a 20m x 20m range. Providing an extra layer of security intelligence, the REDSCAN mini-Pro features an integrated infrared camera for instant verification, while simultaneously recording and saving images for post-event analysis. Designed to work in both indoor and outdoor environments, the sensors can be mounted horizontally to protect roofs and skylights and vertically to create virtual detection walls to protect narrow spaces and high-value assets.



www.optex-europe.com

Onvif® | **S**
ONVIF is a trademark of Onvif, Inc.

INTRUSION DETECTION | VISUAL VERIFICATION
TAILGATING DETECTION | VEHICLE DETECTION
PEOPLE COUNTING



VIDEO SURVEILLANCE

Repeat After Me – New Branch

Smarter Video Solutions for Retail

Multi-branch retailers are gaining multiple benefits from advanced integrated video management solutions (VMSs) that are easily repeatable. These include better security, reduced losses and valuable business intelligence on customer behaviour, seasonal trends and staff performance. One Idis client has a single IT manager for 50 stores, delegating day-to-day security functions to the branches.

■ **Repeatability** – developing a successful offering then replicating the model at new branches – is critical to retail chains. They must keep operations manageable as they grow, maintaining control, and keeping costs down.

Increasingly, video surveillance technology plays its part. Camera systems no longer simply detect theft and reduce losses. They now boost profits and enable better strategic decision making by improving remote management oversight and delivering business intelligence. This stems from advances in AI and easier integration with retailers' ERP/POS systems.

Vendors and systems integrators are working with retailers to deliver VMS solutions that are sustainable long term, and that will help them to compete in changing circumstances.

AI-enhanced camera systems that can be replicated store-by-store have become affordable over the past year. Retailers benefit from better security and reduced losses and making it easier to add and manage new branches. They also get valuable business intelligence around footfall, customer behaviour, seasonal trends and staff performance. And they support flexible management styles too, facilitating the monitoring

and maintenance of uniform processes throughout dispersed branch networks, while supporting a degree of autonomy and decision-making at local branch level.

Cut Losses and Reduce Risks for Small Shops

The rise of affordable, intuitive and accurate AI-enabled video analytics has led to their installation, not just in multi-floor department stores, but in shops as small as 50 to 100 m². Previously these retailers could only justify a new system based on how quickly it would cut shrinkage and 'pay for itself'.

Idis DV-1304
AI Box

Until recently, mid-range retail businesses relied on manual, time-consuming methods for branch-by-branch people counting, or door sensors that were cheap but a blunt tool for data-capture. Store owners needed multiple software applications and specialist IT services to analyse sales, footfall and related metrics and view video footage alongside point of sale data – and that came at a cost.

Now, video analytics deliver more accurate and useful data, allowing retail management to focus on other critical areas such as staffing levels, customer service, staff training, store location, promotional activity and stock handling. Supported by at-a-glance dashboards and targeted reporting, they can identify areas that are performing best and build on them.

One of the key enablers for these new solutions is easier and more affordable integration of video data with retailers' ERP software – those systems which underpin the management of the business, including inventory management, purchasing and supplier management, POS, payments and order processing.

Turnkey Solutions Deployed Easily

Separate software from different vendors is no longer necessary to operate video, analytics for people counting and queue monitoring, ERP software and the integration itself. This simplifies VMS deployment and avoids compatibility issues, reducing costs and removing complexity. Retailers can now buy a single off-the-shelf all-in-one VMS solution with cameras and all the key

analytics they need linked seamlessly with their ERP software.

The result is click-and-connect functionality that can be replicated across multiple outlets, particularly where those outlets share a common layout. The retailer benefits from VMSs that are easy to install, maintain and use, and that allow centralised monitoring with delegation of responsibility to local managers for certain functions. This empowers in-store staff to boost sales by adjusting store layouts and promotions based on data, supporting more flexible and responsive local management rather than adherence to promotions pushed down from distant head offices.

In addition, overlaying video with POS transaction data allows managers to investigate suspicious check-out activity to detect fraudulent activity by staff or customers, using something as simple as a VGA/HDMI encoder. It's a neat and powerful piece of kit that avoids tech clutter at check-outs and cash desks, and once experienced becomes a must-have. Simple time synchronisation of cameras across stores also enables managers to quickly identify suspicious activity such as sweethearting.

Mobile video surveillance apps allow managers and operations teams to work more flexibly, from home, office, retail outlets or on the go. They even allow footage playback in the same high definition that operators and managers get in control rooms with live streaming on remote mobile devices enabled – high image quality in H.264/MJPEG and H.265 formats, and in most environments without any noticeable latency.

Reduce Workloads: Focus on the Job

Notifications generated by edge AI make it easy to investigate incidents or suspicious behaviour. More efficient investigations allow fraudulent activity to be spotted sooner. Better fraud spotting not only reduces losses but also builds a positive culture throughout the business, confirming crime will be detected and prosecuted.

Modern VMSs make it easy for local managers to retrieve video evidence for police in support of investigations, reducing workloads for central loss prevention. One retailer using Idis solutions has a single IT manager covering almost 50 stores. They have delegated day-to-day security functions to the branches, leaving more senior time for analysis and comparing performance by store.

Some VMS options sufficient for many of these applications are available free. They allow recording in store with central monitoring and include the essential functions these applications need: easy camera management, trouble-free integration, a simple dashboard and powerful reporting tools. It's also easy to upgrade to an enterprise VMS with the same user interface, should the business needs change. ■

Author:
Jamie Barnfield
Senior Sales Director
Idis Europe



Idis Europe
www.idisglobal.com

ACCESS | DOOR INTERCOM

Simple, Secure, Smart

The Frogblue Door Station for Professional Building Automation and Access Control

The Frogblue 'frogTerminal' video door station was one of the highlights at the Light+Building exhibition in Frankfurt. GIT SECURITY took a closer look: Here is our interview with Christian Heller, Sales Director (CSO) at Frogblue, where we talked about the company, its ambitions in security and especially in door stations.

■ The Frogblue company from Kaiserslautern has concentrated on the development of wireless, Bluetooth-based electrical installation solutions for professionals since 2016. 'Made in Germany' is just that – the company only manufactures in Germany. The overriding principle of the really innovative technology is that switch functions and their connections can be easily configured or adapted to new situations via an app. The benefit: It makes Frogblue products compatible with every existing switch range – users can then easily perform various different functions with just an everyday light switch.

A particular highlight in Frogblue's portfolio is the professional video door station – the 'frogTerminal' – that supports the worldwide SIP telephone standard and is thereby multi-party capable. It provides a decentralized access solution with an integrated RFID reader and PIN keypad that allows up to three-factor authentication.

GIT SECURITY: Mr. Heller, what does Frogblue have to offer, and how do you define building technology, security, access control?

Christian Heller: At Frogblue we view security and security technology as matters of universal relevance, regardless of commercial conditions or external influences. That is why we focus on the integration of security technology and building automation. With the help of the SIP standard, our terminals can help to provide really efficient building automation. I would go so far as to say that they have completely redefined building technology through their versatile, reliable and secure connections to door communication, access control and building control. Our frogTerminal provides a decentralized access solution that is perfectly suited both to private houses and to comprehensive industrial environments.

Ideally, everything has to go quickly and easily these days. What can you tell us about the installation of the terminals?

Christian Heller: Our priority with the frogTerminal was actually to ensure simple installation and commissioning. We know very well that electricians and installers are often under immense time pressure. We have therefore included a setup wizard in our system that makes it possible to rapidly commission a frogTerminal within just three minutes. By using standard technology such as Bluetooth, Dali, and SIP, we have been able to greatly simplify the installation process and integration into existing infrastructure. In addition, the terminal also provides access control using RFID, which enables decentralized access control without the system having to be connected to a network. This opens up lots of potential applications for single buildings as well as for complex building networks at different locations worldwide.

What security measures does the door station have on board?

Christian Heller: The video SIP door intercom system can provide complete surveillance and recording of events within buildings, for example, with the option to directly raise alarms on one or multiple smart phones. One striking



ing feature of our solution, which has been developed and is manufactured completely in Germany, is its versatility in integrating door communication, access control and building management without any control cables or cabinets being necessary. Based on the integrated SIP world standard, the video door station supports simple multi-party scenarios up to widely distributed properties, whereby multiple SIP telephone systems and SIP servers can be simultaneously incorporated.

IP video door station with additional functionalities: multiple telephone systems; direct SIP call and smart phone calls; 8MP hemispherical camera; three-factor authentication



© Frogblue

Christian Heller: Exactly. At the heart of our system are the so-called Frogs – intelligent control modules that enable installation without additional cables. By using Bluetooth mesh to build redundant and highly secure communication, the system provides a high level of security. Even if one element fails, the redundancy of the mesh network still ensures reliable communication. Individual validity-restricted PIN numbers for access can be used on the frogSIP terminals within a multi-party system, thereby signif-

know everything about the systems – major companies such as Valeo IT, Neteye, ADS System, or Uniserve, for example.

How does the pricing of Frogblue products compare to other systems?

Christian Heller: Our products have an excellent price-performance ratio and are an attractive alternative to systems, such as those that you mentioned before from Siedle. The modular system design allows our



© Wiley | GIT SICHERHEIT

The ideal solution is available for every application and installation environment: different versions of the frogTerminal

The integrated 8-megapixel camera gives a 180° view, while the audio transmission remains clear even in loud environments. The video logbook records calls at the door as well as the opening of the door using a PIN or RFID. Incidentally, we will soon be developing and manufacturing security cameras ourselves – watch this space!

We are already keen to see the security cameras – that sounds very interesting. But back to the door station for a moment: How is Frogblue positioned with regard to existing systems? Let's take Siedle as an example ...

Christian Heller: If required, we are able to replace existing door stations one-to-one by incorporating our equipment into existing infrastructure. This allows us to seamlessly integrate our solutions into existing systems – and to modernize the building's communication in the process. We are also open to cooperation with other manufacturers so that we can offer tailored solutions that meet the needs of all our customers.

We looked at the heart of the Frogblue system (see QR code) in the GIT interview with Dr. Ralf and René Hinkel some time ago. Are they still the basis?

icantly reducing the risk of unauthorized access codes. The integrated Mifare DESFire EV2 reader provides two-factor authentication. You can choose the required level of security; automatic call verification and three-factor authentication are options.

Who will be particularly interested in the Frogblue door station and your other products?

Christian Heller: Commerce, industry, public authorities, home associations, even doctors' surgeries or chemical plants – everyone who lives in a building or uses it for commercial purposes will be pleased with all the features that our frogTerminal offers. We can see a lot of potential in the modernization of existing properties. The versatile and scalable technology allows us to offer tailor-made solutions for a wide range of applications, from access control to building automation. Our products are of course interesting for integrators, installers, planners, and architects who are looking for innovative security and building automation solutions. We work together with selected distributors under our 'frogblue competence center' scheme to ensure that our products are ideally placed and supported. There are currently ten such competence centers in the DACH area who are all well trained and

customers to choose exactly the functions that they need without having to pay for unnecessary extras. And apart from that, you can find features in the frogTerminal for a list price of €1748 that are not even available in most systems for €3000 and more.

Where are you going with the frogs, and what vision of the future is Frogblue following?

Christian Heller: Our frogs, the technology behind them, and other frog products will help us to become a leading brand in security and building automation – and make our products available worldwide. We are already a good way along the route as there are already 50 international value-added distributors – that is, Frogblue competence centers. We will continue to invest in innovative technology and work closely together with our partners to develop tailor-made solutions for our partners and customers. ■

More on the topic:
Link to the interview with
Dr. Ralf and René Hinkel



Frogblue
www.frogblue.com

3x3

Questions

Critical Infrastructure

1. The development of solutions for critical infrastructures is characterised by a constant process of adaptation to evolving threats and new technologies. A key part of Raytec's strategy is the integration of hybrid lamps, which enable seamless switching from infra-red to white-light in the event of an incident. This flexibility is crucial in order to be able to react quickly and effectively to different situations. Raytec also attaches great importance to the safety of its products. The IPPOE lamps are equipped with TLS (Transport Layer Security) encryption to protect data transmission and minimise potential points of attack. To ensure the effectiveness of these security measures, various on-site penetration tests were successfully passed. The tests serve to uncover potential vulnerabilities and ensure that our products meet the highest security standards.

2. Managing the unique nature of critical infrastructure sites while ensuring tight security is a paramount concern for our operations. With years of experience working on critical infrastructure projects in England, where standards have traditionally been stringent, we have developed a deep understanding of the challenges and requirements involved. Raytec has a proven track record of delivering



Stefan Blohm

Business Development
Manager for DACH
regions, Raytec

www.raytecled.com

secure solutions for CI, and this is reflected in our successful compliance with rigorous inspections and standards. Our commitment to security is ingrained in our processes, from initial design to implementation and ongoing maintenance. Furthermore, our employees who work in this area undergo rigorous training and certification to ensure they understand the unique security needs of CI sites. This combination of experience, expertise and dedication enables us to effectively manage the unique challenges of CI while maintaining the highest standards of security and reliability.

3. While we have successfully implemented numerous projects in the field of electricity within critical infrastructure, unfortunately, due to the stringent safety and security protocols surrounding these projects, we are not permitted to disclose specific information or case studies. However, I can assure you that our products and solutions have been instrumental in enhancing the reliability, efficiency and security of various critical infrastructure projects. Our commitment to excellence and our track record of delivering innovative and reliable solutions speak to the trust placed in us by clients in the CI sector.

1. Right from the start, in addition to our standard products, we also develop individual radar solutions in close cooperation with our customers. We are in constant communication with the industry in order to test radar monitoring in real and individual scenarios and to optimise it for the user. The changing dangers, tasks and locations of use concern not only our customers but also our radar experts in product development. Innosent is strongly committed to research projects and also develops sensors for other industries. These findings are then incorporated directly into our existing and new radar solutions. Examples of this include the use of AI and advancements in chip technology that allow us to achieve even better performance.

2. The performance of the products is particularly important for critical infrastructure. False or missing alerts can have dire consequences. We set extremely high standards for our sensor solutions for the security sector in terms of quality, accuracy and reliability. This specifically means that our products have filter functions for wind, rain or small animals, detect attempts at manipulation and are insensitive to contamination. We are also conscious of using multiple technologies to ensure watertight protection. That's why



Christian Bömmel

Chief Business Unit Officer
Automotive & Industrial,
Innosent

www.innosent.de

our radar systems can also be combined with camera technology. We thereby create synergies that make security monitoring even better. One challenge is to avoid interference between numerous radars being used, but we achieve this through the availability of different frequency channels. Regular updates and new product solutions that use the latest technical developments and materials are a matter of course for us as technology drivers.

3. Most of our radar systems perform very classic tasks: they trigger an alarm signal as soon as people or objects are within the monitored zone. We install them on CI sites, such as energy production, refineries, water production etc. The radar systems for perimeter protection either monitor a specific zone on the premises or detect movements outside in order to protect against intruders. Radar barriers often come into play, which detect people, animals or objects that pass through a kind of invisible 'radar fence'. You will also find our sensors on critical infrastructure. For example, traffic management systems use our radar to control traffic lights, or our level radar determines flood levels. Our distance measuring systems generally support the manoeuvring of objects at ports and airports. Radar is a technology that can be used in many ways.

1. How are you developing your critical infrastructure solutions in response to evolving threats and emerging technologies?
2. How do you cope with the very specific and individual nature of critical infrastructure sites and the criticality of their security being watertight?
3. Please describe an exemplary case study where your products and solutions are used on a critical infrastructure project.



Nick Smith

Business Development
Manager at Genetec

www.genetec.com

1. Critical infrastructure facilities can be large, so protecting them is a complex challenge that demands multifaceted solutions. Our unified security platform configures, monitors and controls all third party security systems and devices such as surveillance cameras and door controllers within one interface. We are constantly innovating this platform to help security operators within CI organisations to gain a better understanding of their environment. We're also putting a big focus on Security Center SaaS, our unified, enterprise-grade security-as-a-service solution. This newly announced offering brings together access

control, video management and many other advanced security capabilities in the cloud. It's a particularly good fit for CI organisations who are finding they aren't well served by other options on the market. Proprietary solutions hold customers hostage, while standalone VSaaS/ACaaS solutions offered by emerging players are too simple to address their complex needs.

2. We empower our partners and end users to address the very specific and individual needs of critical infrastructure sites by providing them with an open platform, unified software solution which can tap into a constantly evolving ecosystem of technologies and support thousands of industry-leading security devices. Organisations are free to choose the most appropriate devices for them at that specific time. As threats evolve, they can swap out or add new technologies to address emerging challenges without starting from scratch. We prioritise the cybersecurity of these solutions to safeguard the integrity of critical infrastructure sites and the sensitive data they hold. This commitment is evidenced by several certifications we have obtained, including ISO 27001, ISO 20017, CAPSS, ANSSI and SOC2 Type 2. This signifies that internal controls at Genetec are built on the best industry practices and aligned with industry standards to secure CI organisations.

3. Énergir, the main natural gas distributor in Quebec, Canada, employs over 1,500 people and has over \$8 billion in assets. To keep its people and properties safe, the company upgraded to Genetec Security Center. Faced with outdated technology, Énergir recognised the need for a unified platform to optimise processes and enhance site security. Since upgrading to Security Center, Énergir has been able to enhance operational and response efficiencies tenfold. That's because the team now manages security across its sites from one single platform. Within Security Center, the team can also monitor live or recorded video using the Omnicast video surveillance system and manage cardholders and doors using the Synergis access control system. The energy company has also implemented the AutoVu automatic number plate recognition (ANPR) system to reinforce perimeter security. This has allowed Énergir to minimise traffic congestion and improve the flow of vehicles at site entrances and exits.



ASSA ABLOY
Opening Solutions

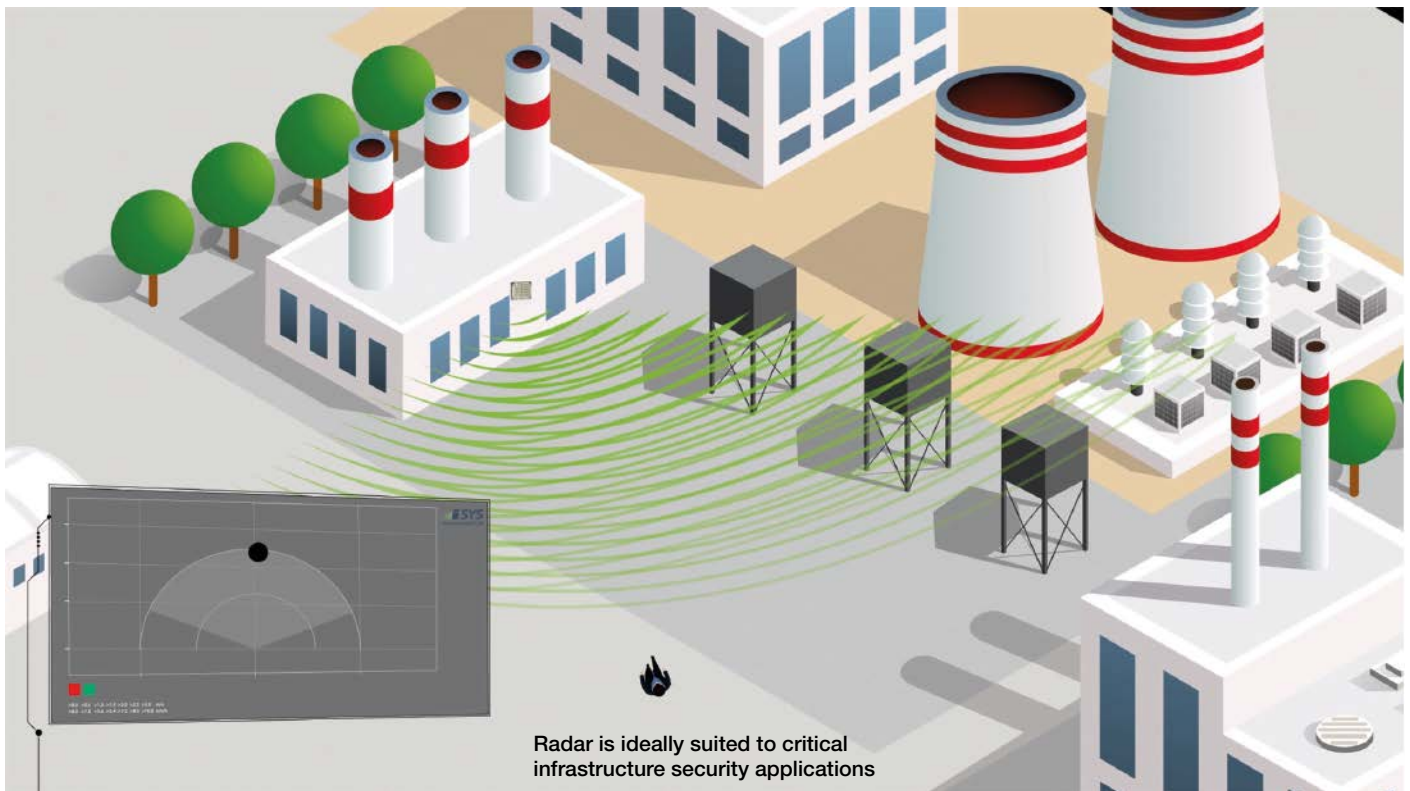
Make your
access ready for
what's ahead

We are experts in access.
**With us, you digitalize
with confidence.**



Learn
more

Experience a safer
and more open world



RADAR

It's Critical to Play It Safe

Radar is Vital in Security Design

Radar has been applied for demanding applications right from the start. It was originally used by the military and to help with airplane and ship navigation. These applications already set high standards for radar devices when it comes to reliability and precision.

■ As the technology evolved, it became available to other markets. But it is still preferred for use in challenging environments and high-value or complex applications. Because in these cases, the precise and reliable measurement that radar brings with it is usually the crucial point. Therefore, radar plays an important role in security technology. It is an almost indispensable part of security system design, especially in critical infrastructure.

What Radar Systems Do

Radar systems can detect static and moving objects. They deliver not only presence information like PIR, but they also provide information on speed, distance and angle to the object. With this information, it is possible to locate and monitor any moving person or object within the radar field of view.

Robustness is in most cases the clincher in favour of radar. It simply performs more

reliably compared to other technologies such as PIR or cameras, which suffer performance issues due to environmental factors.

Why Radar Works for Critical Infrastructure

Radar works in any light and weather conditions. It also comes with impressive temperature tolerances, both extreme heat and penetrating cold. So, the technology is extremely reliably and robust and works perfectly for outdoor applications.

- Resistance to tampering – blocking, spraying or dirt build-up – does not disrupt the performance.
- Radar devices require no maintenance.
- Radar detects various materials depending on their radar cross-section (RCS). From car to human, radar systems notice every movement.

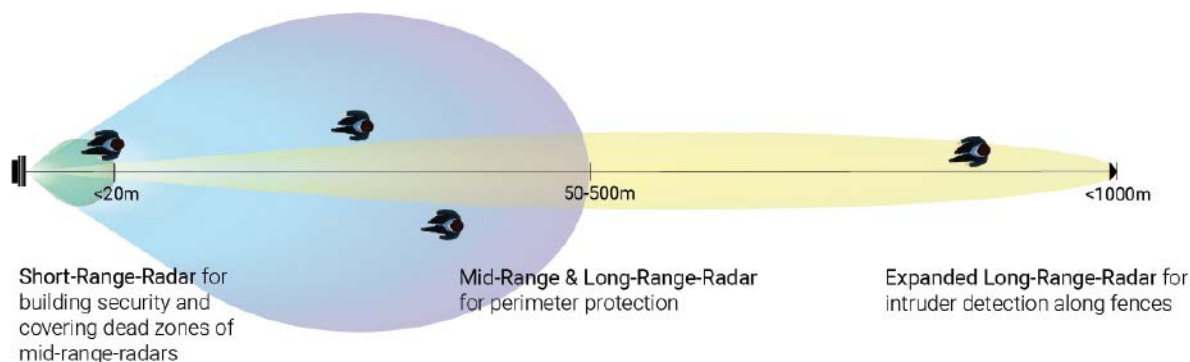
■ Large areas can be monitored as radar has a wide range.

■ Numerous data can be obtained through the radar measurement, which is helpful for security personnel to assess security incidents. The data is anonymous because the technology does not output an image.

24 GHz Radars Are Typical

The combination of these benefits lets the performance of radar sensors technically stand out for critical infrastructure. Since the dawn of radar use in security applications, the products have developed significantly. Advances in signal evaluation and antenna design not only make radar devices more user-friendly, but also offer more functionality that is tailored to the needs of the application. System solutions which are easy to integrate or ready-to-use are trending.

For critical infrastructure such as industrial parks, 24 GHz radars are typical. Here,



Pick the appropriate radar for the range you want to detect, even up to one kilometre

the developers achieve an optimum relationship between detection range and resolution that meets the requirements of the security industry. Radar is mostly used for detecting approaching objects from far off or as a radar barrier alongside fences.

Beside the large range and high resolution, advanced systems offer additional features to meet the requirements of the application. For example, they monitor multiple targets simultaneously. To increase the efficiency of the detection, it's also possible to adapt the detection to the local conditions by setting limits to the detection range.

Trigger Responses in Specified Zones

Even individual zones can be set. These can be used to set aside specific 'alarm' or 'ignore' areas. Or they can be set to trigger by a combination of different security measures. For example, a motion detection some way off triggers first switching on lights and perhaps a camera, too. When the moving object gets closer and enters the next defined detection zone, the acoustic alarm could sound, or the guarding team be informed to monitor the potential intrusion.

Another highlight of modern radar systems is the tracking feature. It follows and visualises the movement of people and

objects over time. Operators can track the motion history for a better risk evaluation and to see where the intruder emerged from. This history won't be lost, even if the slow-moving object or person stands still for a short time because radar also detects static objects.

Premium radar systems with advanced digital signal processing and high radar resolution are also able to classify a detected target. So, you will know if a car or a person is entering the critical zone. The extended measurement functionality also outputs more data about the target, such as speed of motion or RCS.

User-friendly configuration options enable operators to set filters to improve the performance efficiency. For instance, they can filter detections by RCS or speed individually according to their needs. In order to reduce false alarms, it is possible to filter out small animals or other irrelevant detections through the filter settings.

New Tech Promises Future Advances

The future still holds a lot of potential for further development for radar systems. Advances in chip technology, software development, antenna design and other industries are promising and will influence the evolution of radar devices. It is to be

expected that they will improve further in performance, design and customisation, which promises much for critical infrastructure security applications.

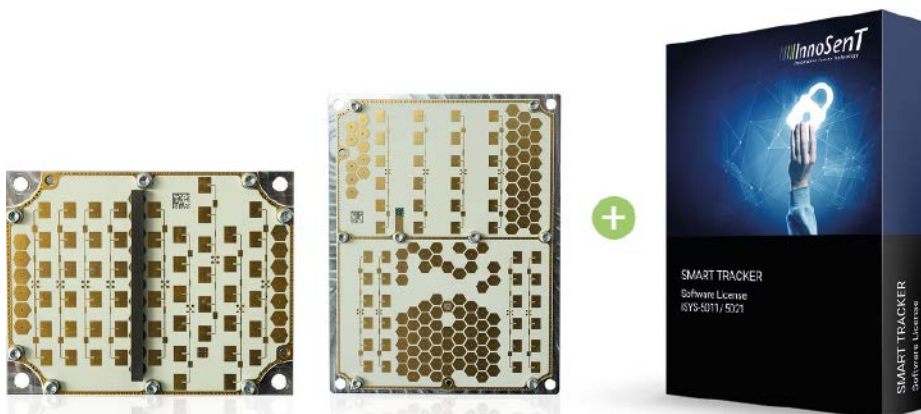
Innosent has 25 years' experience in developing and manufacturing radar sensors and systems. As one of the leading radar technology firms, the company drives the innovation process forward and sets new standards for the market. Its security product portfolio covers a large range of applications. For area surveillance and perimeter protection, the iSYS-5021 and iSYS-5011 24 GHz 4D MIMO radar systems bring in advanced features like smart tracking and multi-target-detection. ■

Author:
Christian Bömmel
Chief Business Unit
Officer Automotive &
Industrial, Innosent



Innosent GmbH
www.innosent.de/en

© Images: Innosent



The Innosent iSYS-5011 (left) + the Innosent iSYS 5021 Smart Tracker radar system

VIDEO ANALYSIS

Only Dummies Will Do

AI Project to Keep Danish Ports Safe



The team set out to cut the 1,650 deaths in 15 years in Danish waters. Their biggest challenge was training the AI system to detect when a person falls into the harbour using test dummies

Despite their beauty and functionality, Danish harbours have unfortunately witnessed numerous drownings over recent years. From 2001 to 2015, a staggering 1,647 people died in Danish waters, with a quarter of these tragedies occurring within the ports themselves. An innovative solution was needed to combat this alarming trend.

■ That's when a remarkable team of innovators in video technology, including Actas, a Milestone technology partner, and Aalborg University (AAU) in northern Denmark, came together.

With sponsorship from the Danish Tryk Fonden, they embarked on a ground-breaking project to combine artificial intelligence (AI) with video technology to enhance safety significantly in the Port of Aalborg – one of Denmark's busiest ports.

Transforming Tragedy into Progress

At the heart of the project was the development of the AAU/Milestone thermal dataset, comprising the largest published collection of annotated thermal images. By training AI models on this dataset, the goal is to create an advanced video analytics solution that will be able to promptly detect and alert rescue teams when a person falls into the harbour. This article explores the

ground-breaking collaboration that has the potential to redefine safety standards in ports, ultimately saving countless lives in years to come.

The primary challenge faced by the team was training the AI system to identify instances when a person falls into the harbour. Training an AI system is akin to teaching a child to recognise objects or comprehend language. We show the child numerous pictures of dogs, enabling them to learn the defining characteristics of a dog.

Similarly, when training AI, we provide it with abundant data, in this case videos of people falling, enabling it to identify patterns associated with falls. The more data we provide, the more accurate the AI becomes in recognising falls. Unlike a child, an AI system necessitates thousands or even millions of data points and images to learn effectively.

Volunteers Take a Dip into Danger

To train the AI in detecting individuals falling into the harbour, volunteers initially simulated falls for analysis. However, due to safety concerns, they could not ask volunteers to actually fall. Instead, they were asked to jump, which is a different pattern of motion. It is important to note that genuine falls involve sudden and involuntary movements that were not captured in this data, rendering it less effective for AI training.

An AI model requires a diverse dataset to detect different types of falls consistently across various conditions and seasons. For example, a fall in winter may present unique challenges due to the individual wearing bulky clothing. However, the potential risks associated with volunteers jumping into the freezing water of winter were too great, so an alternative approach was needed.

Test Dummies, a Safer Way to Train AI

Using a test dummy proved to be a safer and more effective method of collecting data. Instead of putting human lives at risk, researchers used a test dummy filled with warm water, making it detectable by thermal cameras, to simulate multiple falls into the harbour. This allowed the team to simulate many different types of falls, resulting in a more comprehensive dataset.

However, this approach also had its limitations. The dummy could only imitate human movements to a certain extent and lacked the complexity of a real person falling into the harbour. Additionally, gathering a large amount of data was unfeasible as simulating a person falling into the water many times with slight variations was not a viable option.

Scaling up with Synthetic Data

Initially, the team used thermal cameras to capture real images over eight months to create a thermal dataset. The resulting dataset is the largest collection of annotated thermal images ever published, with approximately 8 million bounding box annotations.

It covers four classes: person, bicycle, motorcycle and vehicle; however, luckily it

does not include many examples of abnormal behaviours – including falls. Using synthetic data, the goal was to expand the thermal dataset by including many abnormal behaviours and incidents.

Synthetic data is a technique to provide additional data for an AI's comprehension and identification of real-world events, such as when an individual falls into a harbour. At AAU, it originated as a student project aimed at generating an artificial depiction of a person falling. However, the initial simulation was simplistic, and it soon became evident that these examples were inadequate.

Innovative Partnership to Save Lives

Recognising the need for an advanced dataset, Milestone Systems' research department joined forces with AAU to extend the synthetic dataset. The drive for better and more precise synthetic data was not solely focused on improving an AI algorithm; it was about saving lives.

The training data was enhanced to simulate scenarios with more intricate behaviours, such as falls from wheelchairs, skating and biking. Each enhancement to the data had the potential to increase the system's ability to detect real-life falls swiftly and accurately.

The innovative partnership between Milestone Systems and AAU has harnessed the power of synthetic data and AI to tackle the significant issue of drowning in Danish harbours. The team's objective was to develop a comprehensive dataset capable of training an AI system to detect a wide range of hazardous situations.

The development of the AAU/Milestone thermal dataset represents a ground-breaking step forward in video technology. Ultimately, the goal is to help rescue teams respond faster and potentially reduce future drowning incidents.

Autor:
Rahul Yadav
CTO Milestone Systems



Milestone Systems A/S
www.milestonesys.com

© Images: Milestone Systems

The AAU/Milestone research team took real images with thermal imaging cameras over an eight-month period in the port to create the largest collection of annotated thermal images ever published



KEY MANAGEMENT

Secure and Transparent

An Access Solution for Building Keys and Assets at Munich Airport

More than 6,000 employees at Munich airport obtain access to building keys and important assets through solutions from Kemas. Around 4,200 depots are in daily use there. Markus Schaurer, Advisor for Security Technology at Munich airport, explains how the logistics of key and tool management at Germany's second largest airport is kept under control.

Markus Schaurer is a security technology advisor at Munich airport and responsible for the planning and coordination of new installations and modifications to existing security-related systems

■ GIT SECURITY: Mr. Schaurer, how important is the Kemas solution in the internal processes of the company, and how was it handled before?

Markus Schaurer: The solution is important for all of us as a functioning airport because we can trace the complete content of the systems at any time, by both time and personnel. Keys and tools that numerous people need to use can also be kept centrally and made available without any contact. We used to have 'analog' key cabinets here at Munich airport with a book to document who has the keys, or some people kept keys of certain categories in their desk.

What was the trigger to look for a new solution?

Markus Schaurer: The inspiration for the acquisition of Kemas systems was the requirement to mechanically store keys and other operational tools securely, and at the same time also to implement electronic supervision with alarms. Our expectations were to be able to manage keys at various central locations, have consistent documentation of the status of the content of all systems, and, for example, also to receive an alarm when a pre-defined usage time has been exceeded. Access management according to a matrix was also essential. As our department is responsible for the entire security technology at Munich airport, we have to ensure the highest availability of

the systems for all the other departments, also that of the Kemas systems.

How did you learn about this supplier?

Markus Schaurer: Our company fire brigade found out about Kemas in 2004 at the Security event in Essen and bought the first system shortly afterwards. The central lock administration of our company security division established the system throughout the entire airport campus, and the number of systems increased significantly over the years. This was made possible through the continuous and smooth cooperation of the company security and security technology departments at Munich airport with Kemas as a reliable supplier.

What is the solution comprised of and how many terminals are in use today?

Markus Schaurer: There are currently 53 systems in use. We use key and storage boxes with RFID monitoring as well as other containers, making a total of around 4,200 depots. As well as keys, we also store radios and laptops/tablets in them. Some of them are equipped to charge the devices while they are being stored. More than 6,000 personnel now have access to the systems that are spread all around the airport. There are also interfaces to the airport fire brigade and our central lock system administration over which various information is transmitted.

After being in use for so long, what has improved or changed? Could your original expectations be fulfilled?

Markus Schaurer: The initial expectations were fulfilled. We ourselves had to improve because of the continuous growth of the systems and developments in technology and IT. The cooperation between the airport and Kemas runs very smoothly, and acceptance by the employees is also very high. New users are instructed directly on one of the system's operating terminals, but people who are authorized to assign rights to others through the administration software, so-called key box administrators, receive separate internal training and reference documentation.

What are the next elements that will be implemented?

Markus Schaurer: We will be introducing a new interface to the company security department and to the fire brigade to improve the flow of information. We also strive to keep the system up-to-date, which involves carrying out software updates or server and database upgrades, as well as hardware adaptations that become necessary because of the growth of the system and technological developments. ■



Kemas GmbH
www.kemas.de

AIRPORT SECURITY

Smooth Operators

The Critical Importance of Complete Airport Security

■ Several notable recent security breaches made headlines, including when passengers bypassed security and boarded a plane at London Gatwick and the Hamburg Airport hostage drama in November 2023.

The efficient operation of an airport can be significantly disrupted when individuals gain unauthorised entry to runways or airside areas, whether for illegal entry into the country, theft, vandalism, or acts of terrorism targeting aircraft or on-site infrastructure. While certainly not everyday events, they do happen, which is why getting airport security right is critical.

Securing the Perimeter

One of the major challenges airports face is effectively monitoring and protecting extensive perimeters. Additionally, the presence of multiple entry points, such as vehicular, pedestrian and cargo, further compound the task of maintaining robust security infrastructure.

Safeguarding runways, public areas and controlled access areas requires a combination of different technologies to meet the specific needs of each airport. Different environments, from snowy Switzerland to sunny Spain, demand versatility in the type of security solutions specified. Perimeter fences can be hundreds of kilometres long and punctuated with CCTV cameras and video surveillance. Building a reliable security system requires detection technologies that can distinguish genuine intrusions and accurately identify the precise location of an intrusion as it is taking place and subsequently.

Tracking an Intruder's Progress

Indeed, being able to detect and track an intruder from an initial point of entry is increasingly important and can allow a quick response to security threats. Fibre optic perimeter intrusion detection systems can be buried, mounted directly onto the fence line or in a hybrid installation and can identify the precise location of anyone even before the perimeter is breached. They can detect anyone attempting to jump over, cut through or even crash into the fence using a vehicle, with instant alerts sent to the control centre.

Light Detection And Ranging (LiDAR) is a remote sensing technology that uses light in the form of a pulsed laser to determine distances by targeting an object or a surface with a laser and measuring the time for the reflected light to return to the receiver. This too can provide highly accurate and reliable detection of a target up to 100m away, further enhancing security particularly at vulnerable entry points.

Protecting Rooftops and Solar Panels

Areas between the outer fences and the main airport buildings are a hive of activity, with vehicles, luggage and people constantly moving between aircraft hangers, warehouses, control towers and data centres. LiDAR technology is again useful for detecting unauthorised access while not disrupting the operations and traffic in these busy areas. It is perfect for detecting people or vehicles as they approach a prohibited area, allowing more time for an appropriate response to be actioned.

Rooftops are often overlooked, but are critical areas that require protection. They can often prove vulnerable to intruders tampering with or trying to steal lead flashing or solar panels, for example, or attempting to gain access through a skylight. Mounted horizontally, LiDAR creates a virtual detection plane to add an extra line of security.

Invisible LiDAR Calms Nervous Flyers

Airport operators are keen to create an open, relaxing space, particularly for nervous flyers. Also, with airport shopping generating huge revenue, detection systems need to be discrete and in keeping with airport aesthetics.

LiDAR is invisible to passengers and creates virtual internal barriers, which, when crossed, will alert security and provide the perpetrator's exact location. It can be programmed to match the opening and closing times of every individual shop, and can also be used to detect people trying to gain unauthorised access into the country by jumping the escalators.

Objects being thrown airside or landside are another challenge for airports to deal

The airline industry's profitability relies on keeping planes in the sky. Any disruption to the flow of air traffic in and out of an airport can have a major impact on its economy and reputation.

with. One European airport recently discovered passengers were discarding their passports as they approached passport control, so that they arrived undocumented. Optex's LIDAR technology creates an invisible ceiling over the security checks to prevent this from happening. There have also been instances of personal documentation being thrown between passengers to enable illegal entry into a country. Again, LiDAR can provide the answer, programmed to detect any object with its highly precise sensing analytics providing security with the exact location of the incident as it occurs.

Even Flying Clubs Are a Target

There are various types of airports, from international and national to regional and military, each with their own distinct security requirements. Smaller local airports and flying clubs are often targeted by intruders seeking to steal expensive parts for private planes or valuable materials, such as copper cabling and lead from roofs. While these facilities may not require the same level of sophistication as large as military airport security, they could benefit from more modern and adaptable technologies.

From bustling international hubs to regional airstrips, combining multiple technologies to create a multi-layered approach to security that is highly reliable and ensures minimal false alarms is essential for our airports to remain safe and efficient spaces for all. ■

Author:

Mark Cosgrave
Divisional Director
Western Europe, Optex



© Optex



Optex Europe Ltd.
www.optex-europe.com

VIDEO SURVEILLANCE

Wang Enjoys Long-Awaited Comforts

Qingdao Port Improves Efficiency Threefold



A gruelling job exposed to the harshest weather conditions is set to become more bearable with the innovative use of video technology. The Port of Qingdao has partnered with Hikvision to roll out an intelligent tally system at cranes across the port.

■ Qingdao is one of the 10 busiest ports in the world and is located on the Yellow Sea in the Shandong Province of China. Qingdao Port consists of four areas, which are often themselves referred to as ports due to their size: Dagang port area, Qianwan port area, Huangdau port for oil tankers and Dongjiakou port area, 40 kilometres south of Qingdao city. Hikvision has installed its intelligent tally system at 84 cranes across the port to improve working conditions for its tally clerks.

Improving Employees' Lives with Video Tech

The smart solution – which uses AI technology to recognise container and trailer ID numbers and to make them electronically 'readable' – allows tally clerks to perform the majority of their daily tasks

remotely from the comfort of a temperature-controlled operations room. The system streams video footage and sends container and trailer ID numbers to monitors in the tally operations room in real time. ID numbers are also cross-referenced with port records automatically to ensure consistency with shipping bills.

If everything is present and correct, the tally is completed automatically, and the loading process is initiated. Otherwise, the tally clerk receives an automated alarm, allowing them to respond quickly and appropriately to resolve the issue. Chen He, Transportation Industry Manager, Hikvision, says: "Wang Xianpeng, a tally clerk at Qingdao Port in China has worked on the docks for 18 years, exposing him to extreme temperatures and other health and safety risks. Now, Wang and his colleagues can conduct their daily work

from the comfort of a temperature-controlled room, thanks to latest-generation smart video technology from Hikvision."

Port Makes 200 % Efficiency Gains

As well as making tally operations safer and more comfortable for Wang and the tally team, the Hikvision solution has also helped the port to increase loading efficiency by 200 %. He says: "With our previous manual approach to tally operations, each clerk managed a single 'line'. Now, we can work three lines simultaneously with less effort and less risk, which has increased overall loading efficiency by 200 %."

The intelligent tally solution is also helping the port to evolve its services and optimise customer experiences. This is enabled by innovative capabilities, such as

◀ Wang Xianpeng, a tally clerk at Qingdao Port in China, has worked on the docks for 18 years – exposing him to extreme temperatures and other health and safety risks

tally information queries, and cargo status tracking, which allows customers to review the status of their shipments as they pass through the port.

The Role of a Tally Clerk

A tally clerk's role is to record proper and accurate tallies of cargoes discharged from or loaded on to vessels and record them onto a tally sheet, such as date and shift, ship name, shed or berth number, etc. This includes all details of the packages and containers loaded or discharged and reporting if there are any delays or idling of the ships.

At ports around the world, tally clerks work tirelessly to monitor the flow of trailers and containers based on shipping logs and other documentation. By matching container ID numbers with port records, they create an auditable record of all goods entering and leaving the facility – allowing customs controls to be implemented and ensuring that logistics operations run smoothly.

Wang's Story – Tough Working Conditions All Year

Tough working conditions, occupational challenges and hazards have long affected Wang Xianpeng, a tally clerk at Qingdao Port. For the last 18 years, he has been tallying containers and trailers as they move through the port, working outside in all weathers to keep logistics operations on track.

"In the summer, the temperatures on the dock reach 50 degrees Celsius, which makes it very difficult to stay cool and hydrated," says Wang. "Then, in the winter, it can be minus 10 degrees Celsius, and I remember occasions when I've stopped for a moment to warm up my hands on a light bulb."

With the new smart system, Wang and his colleagues in the tally team are no longer exposed to physical risks on the docks. What's more, they can now carry out their daily work comfortably in a temperature-controlled environment.

"It's like a spring day in the operations room, and we no longer deal with extreme temperatures and weather in the summer and wintertime," says Wang. "The new technology has also reduced our safety risks and overall workloads, which is a very welcome change."

As well as being fast-paced and mentally demanding, the work of a tally clerk is often highly physical. Clerks are often exposed to extreme weather conditions, from ice and snow in the winter, to intense sun and soaring temperatures in the summertime.

In addition to these challenges, working on port docks can be dangerous, largely due to risks posed by moving equipment and vehicles and falling containers. The chal-

lenges of the port environment require tally clerks to be aware of their surroundings at all times, and to wear protective clothing, such as steel-capped boots. ■



Hikvision
www.hikvision.com

Qingdao Port's 84 cranes now boast an intelligent tally system from Hikvision



Stefan Olf is now
General Manager
for Advancis Middle
East operations

INTERVIEW

Representative Security

Middle East: Smart Cities and Other Future Projects

Advancis has appointed Stefan Olf as General Manager for its Middle East company in Abu Dhabi in the United Arab Emirates. In coordination with the Board of Advancis, he will be growing the business of the software supplier. The company will thereby strengthen and grow its already successful activity in a particularly dynamic growth market. GIT SECURITY spoke with Stefan Olf.

■ GIT SECURITY:
Mr. Olf, you have just taken over the leadership of the Advancis subsidiary in Abu Dhabi. Could you tell us a little about your background?

Stefan Olf: I studied Electro-Information Technology in Darmstadt. Since then I have been selling enterprise software solutions, SaaS, and cloud solutions for more than 20 years. Before I started with Advancis, I was Sales Director for Central Europe at Planon, a leading provider of facility management and real estate software solutions from the Netherlands. At Advancis, I was director of sales operations for more than two and a half years before now moving to Abu Dhabi.

Then let us talk about the Middle East subsidiary. How is it set up?

Stefan Olf: Advancis is one of the international market leaders in vendor-neutral security and building management systems. We have a very experienced team here – and that is a big plus. It consists of a service team that supports our partners and our end users with the implementation of our software solutions. It is led by our long-serving technical director Mohammed Zubaidi. I'm responsible for the sales team and the entire company as General Manager.

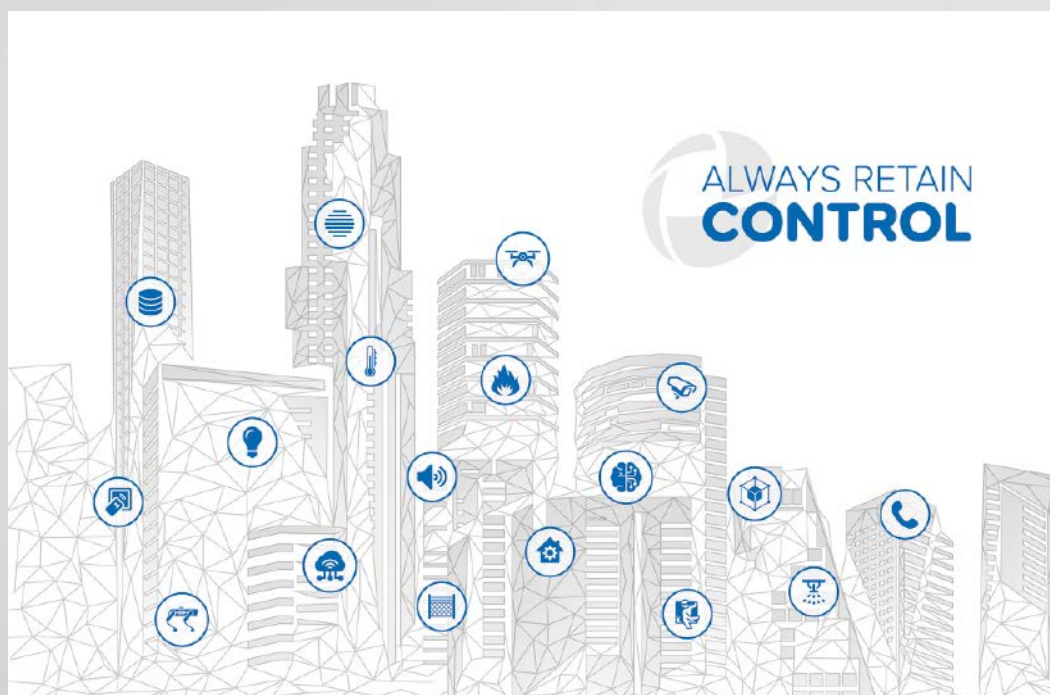
We have additional resources in Saudi Arabia. We are also supported by our col-

leagues from the global services division that are located either at our head office in Langen near Frankfurt or our office in Ireland. Our partners and customers in the Middle East also benefit from this global and holistic approach. The close networking allows us to advise both partners and customers by using the local and global experience and thereby implementing projects in the best way.

Where do you see the most important tasks and aims for Advancis in the Middle East?

Stefan Olf: We have successfully operated here since 2010 and already serve a broad customer base. Our AIM and WinGuard solutions are used wherever a high level of security is imperative. Our Middle East customers are, among others, in the United Arab Emirates, Bahrain, Oman, Kuwait and Saudi Arabia, mostly in the petrochemicals and energy supply industries, the military, and public administration.

Advancis is well known in the region, so we are often on the shortlist for new projects with our solutions. One of my tasks is to further expand this strong position. In addition to that, I will be building new strategic partnerships in the region. This will help us further expand our network and reach in the Middle East, as well as intensify our relations with partners and customers. At the same time, we want to drive the integration of the Advancis Middle East processes into the global Advancis structures. My work at the Advancis HQ over the last two and a half years will be of help here.



The WinGuard X5 open platform integrates the entire security, building, and communication systems, as well as the IT infrastructure

Where do you see the greatest opportunities for Advancis to grow business in the Middle East?

Stefan Olf: Large projects are carried out here that just don't exist on that scale in Europe. Saudi Arabia's 'Vision 2030' project covers multiple smart cities that will be built from the ground up. These include many opportunities for providers of innovative security solutions such as us. In addition to that comes the fact that security here in the Middle East is placed very high on the list of priorities. Abu Dhabi is not one of the safest cities in the world for nothing.

All this opens up big opportunities for us. Open security platforms will be required all over the place that can meet the most varied requirements. We offer the perfect solution to providing effective

and efficient security management with our WinGuard X5 open integration platform, which enables the overarching integration of the entire security, building, and communication systems, as well as the IT infrastructure.

The clocks tick a little differently in the Middle East compared to Europe or the USA. How do you perceive the cultural differences of the region?

Stefan Olf: You have to be flexible, particularly in the sales and business processes. Information and decisions are expected quickly – but even with all that speed, things can be delayed. Our experienced team here has the big advantage that it consists of Arabic-speaking colleagues, some of whom have always lived here,

and from whom I can always get some good advice.

What are your first projects and plans?

Stefan Olf: It is particularly important for me to get to know our existing customers and partners, and to get to know them personally in order to best support them with their projects. Intersec in January in Dubai was very helpful for this, and I was able to meet many existing and also potential customers and partners at our stand. I was able to establish the first contacts, which has been very valuable for me. ■

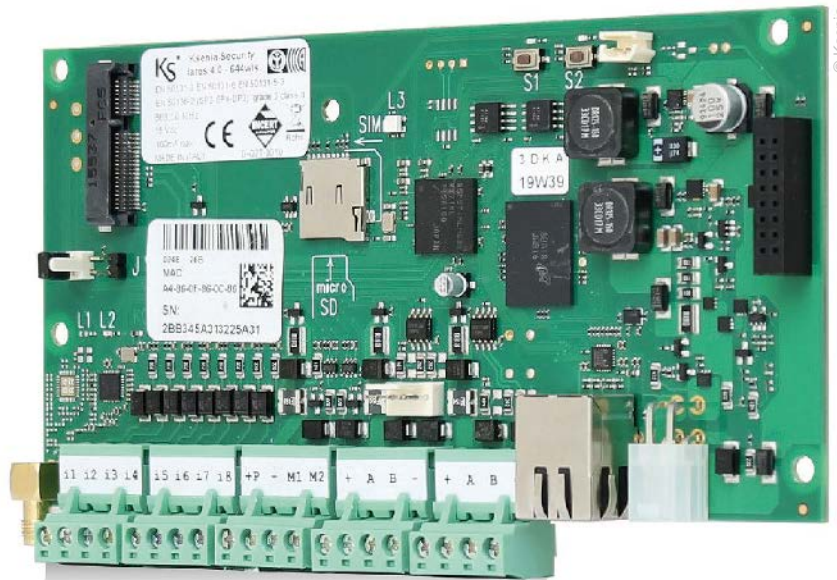


Advancis Middle East
www.advancis.net

© Images: Advancis

The company's AIM and WinGuard solutions are already used extensively wherever a high level of security is imperative





A multifunctional control platform with a simple to use app

CONTROL PANELS

Everything Under Control

A Smart Platform to Aggregate Multiple System Controls

The term “lares” derives from the Latin according to which the Lares in ancient Rome represented the deities who protected the domus, the house, and therefore also the family. If you are a security professional, you probably already know of lares 4.0, the IoT platform from Ksenia Security. This article explores some of the benefits of the system and some of its features.

■ The lares 4.0 control panel has many advantages, offering installers the ability to create professional, easily programmable, and customizable systems according to customer requirements. Lares 4.0 is designed to adapt perfectly to any type of installation. It is equipped with an ethernet connection with a 4G back-up, and can be remotely configured by connecting to the Ksenia SecureWeb cloud. It is an innovative and reliable control panel to manage security, video verification, smart home, and access control functions from a single platform. It is available in five versions, in six hybrid, wired and wireless variants as

well as an all-in-one version with lares 4.0 wls 96. The system is extremely versatile and suitable for different applications in residential, commercial and industrial contexts, including sensitive environments, such as banks, museums and government institutions that require maximum security. It is also scalable over time, allowing easy adaptation of the system to meet customers' changing needs.

Talk to Everyone

The programming does not require any specific software; lares 4.0 can be configured remotely through the intuitive Ksenia

SecureWeb cloud platform or via a smartphone, thanks to the Ksenia Pro app, which enables all the installations to be centralized and geolocated, providing maximum convenience for the end customer. Another distinctive feature is the ability to integrate with major brands in the automation, surveillance and access sectors, such as Google Home, Amazon Alexa, Creston, Control4, Milestone, Avigilon and Dormakaba. In addition, it can integrate with third-party IP devices thanks to the ‘porta IoT’ – the http gateway of Ksenia Security that allows direct communication between the devices and the control panel, without necessarily

using an SDK, thanks to the use of http strings.

Lares 4.0 has been designed to make the installers' work easier by offering a series of features that have revolutionized the way systems are configured. Each lares 4.0 control panel is equipped with the same number of inputs and outputs to manage lights, climate, irrigation, roller shutters and any other type of automation. As a flexible and scalable system, the number of inputs and outputs can be expanded up to a maximum of 644 for large environments, such as large industries and warehouses.

Zoned In

Ksenia Security has implemented IP zone functionality within lares 4.0. By configuring IP zones with a compatible IP camera, it is possible to use a single device to detect the movement of an intruder, activate the alarm and access the associated screenshots from the lares 4.0 user app. This implementation is not limited to the association of cameras but allows the integration of any device capable of sending an http request to the system.

All the panels have a KS-BUS interface to connect Ksenia peripherals that expand the capabilities and functionalities of the control panel. Lares 4.0 has a 4 GB eMMC memory to save programming data, event logs, updated device firmware, IP camera

and screenshots. In addition, the installers have three ways to save their programs: either in the internal memory of the control panel, locally on their PC, or via the cloud thanks to the free automatic backup service, activated directly from the SecureWeb programming platform.

Lares 4.0 monitors both the external supply voltage and the battery voltage, reporting any faults. In case of prolonged power failures, it has a battery disconnection function to prevent deep discharge. It has an integrated ethernet port that allows local connection to the web server to perform programming, maintenance and diagnostics, software updates of the control panel and its peripherals. In addition, it can send emails, synchronize the clock via the NTP protocol, and send the events via the SIA DC009 protocol without using any additional hardware or licenses. The control panel periodically checks for updated firmware on SecureWeb and, if it finds available updates, automatically downloads them into memory, visible to the user.

Voice from Above

All descriptions and events can be converted into automatically-generated audio files thanks to the Loquendo license. For example, it is possible to program the reproduction of a voice message on the

vox-M outdoor siren in case of an alarm or attempted sabotage, and acting as an acoustic deterrent. Programmable logics link the system's events while AND/OR conditions only perform actions in specific situations, allowing even the most unusual or complex customer requirements to be satisfied.

Lares 4.0 can manage over a thousand access control users. A PIN can be assigned to Ksenia keypads or RFID tags by the administrator through the lares 4.0 app, who can interact with a system having up to 64 interfaces to manage each gate. Each user can be assigned to one of the seven different access levels.

In conclusion, lares 4.0 is the control panel designed for the installer, with its many advantages and outstanding features. The ability to expand the system over the years, its innate versatility, and the ability to integrate with other systems allow the creation of a professional system that fully meets the needs of the user. A true and reliable ally for installers and end users, lares 4.0 increases the level of safety and comfort in a wide range of applications, whether in residential, commercial, industrial, or even critical environments. ■



Ksenia Security S.p.A.
www.kseniasecurity.com



The Most Comprehensive Compound Coverage for Confident MS Analysis

The Wiley Registry/NIST Mass Spectral Library combines the power of two of the most comprehensive and trusted spectral reference databases, making it the clear choice for unknown compound identification.

Ask for the combined Wiley/NIST library with your instrument for the best results!



Thermal Camera Packages

Flir A6701 thermal camera packages dedicated to electronic applications can add significant value. Thermal imaging is critical to efficient electronic design and verification testing, providing precise temperature data to troubleshoot potential problems, to optimize thermal efficiencies and even to identify counterfeit components. Infrared thermography is therefore gaining popularity during the development phase as it can identify hot spots indicative of failure points. Central to Flir's cost-effective packages for the testing of electronics is the A6700 MWIR mid-wave infrared (MWIR) thermal camera, which operates in the 3.0–5.0 μm waveband (1.0–5.0 μm broadband option) and produces finely detailed, 327,680 (640x512) pixel images. While gigabit ethernet and analogue video are active simultaneously, the A6700 offers independent control of each for greater flexibility when recording.

www.flir.co.uk

Cutting-Edge Access and Intercom Solutions

The Hikvision Value Series access terminal with a 4.3" LCD touch screen enables touch-free, secure entry and exit with a capacity for up to 1,500 faces and 3,000 cards. The vandal-proof DS-K1T502DBWX-C terminal is great for seamless access control for multi-unit residential applications requiring a more robust, vandal-proof device. The cost-competitive device is IP65 (vandal-proof) and IK09 (waterproof) protection rated and reinforced with rugged zinc alloy materials. Already well known for their video security camera technology, the company also offers comprehensive security systems that integrate video and authorized access, sophisticated IP and 2-wire intercom kits and intelligent biometric terminals, managed centrally with HikCentral software.

www.hikvision.com

Security at Passenger Terminal

Gunnebo Entrance Control exhibited at Passenger Terminal Expo 2024 from 16-18 April in Frankfurt am Main at booth E340 to debut its latest airport entrance systems alongside new advancements



in security technology. There were live demonstrations of the company's latest systems, offering intelligent passenger flow management for all stages of the airport journey. These include PreSec, which operates as a self-service boarding pass check before security, and LoungeSec with biometric capability and facial data capture to ensure controlled access for authorized customers to lounge areas. BoardSec was presented as an automated self-boarding eGate to accelerate the whole boarding process alongside ImmSec to maximize resources with efficient verification of passengers at border control. The company also debuted an innovative new airport entrance control system.

www.gunneboentrancecontrol.com

Enhanced Cybersecurity Transparency

Milestone Systems has partnered with the Common Vulnerability and Exposures Program as a CVE Numbering Authority (CNA). The aim of the program is to find, describe, and catalog known cybersecurity issues. Organizations worldwide that work with the program find and share these vulnerabilities. They publish CVE Records with clear details about the issues to help IT and cybersecurity experts talk about the same problem and work together to fix it. Thomas Jensen, CEO of Milestone Systems, said: "As Responsible Technology becomes a license to operate, we believe that people have the right to feel safe knowing that they can trust video technology. Publishing mitigated vulnerabilities to the wider community will allow Milestone to coordinate and address potential issues even more effectively. This will further enhance our cybersecurity and continue to build trust in our XProtect open platform video management software."

www.milestonesys.com



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



The Hidden Costs of Video Analytics

While there is a general awareness that the software and video cameras needed for analytics can be expensive, video management software (VMS) solutions such as the Milestone XProtect can perform analytics, for example forensic search on the server side of things and making the most of metadata. When working with third-party analytics like facial recognition, the hardware requirements of XProtect are almost always lower than alternative options. Because it is an open-platform VMS, XProtect allows analytics from different camera brands to be combined at no additional cost. Open platforms are also useful for server-side analytics. Advanced server-side analytics often come with high storage costs as well as specific processor and RAM requirements. The 'teaching part' of machine learning requires a lot of human involvement in identifying mistakes (i.e., false alarms), finding out the cause of the mistakes and making adjustments. The good news is that the costs can be minimized by choosing the right VMS.

www.milestonesys.com

SECURITY MANAGEMENT

Security Management



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

Security Management



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

FACILITY SECURITY

Facility Security



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

Facility Security



frogblue · Smart Building Technology
Luxemburger Straße 6 · 67657 Kaiserslautern
Tel: +49-631-520829-0
info@frogblue.com · www.frogblue.com/de

Frogblue ist führend in der Entwicklung von drahtlosen,
auf Bluetooth® basierenden Elektroinstallationslösungen für
den professionellen Einsatz, die vollständig in Deutschland
produziert werden. (Sicherheit, SmartHome, energieeffiziente
Gebäudetechnik, Zutrittskontrolle)

Facility Security



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

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

Facility Security



Walter Wurster GmbH
Heckenrosenstraße 38-40
D-70771 Leinfelden-Echterdingen
Tel. +49 (0) 711/949 62-0
kontakt@wurster-online.de · www.wurster-online.de

Money handover systems fire resistant up to F90 and bullet resistant up to FB7, cash trays, cash-drawers and facade counters to pass through money, valuables, documents and for installation in high-security areas, banks, petrol-stations, pharmacies, sports – and cultural sites indoors and outdoors.

VIDEO TECHNOLOGY

Video Technology



BURG-GUARD GmbH
Wormgermühle · 58540 Meinerzhagen/Germany
Tel. +49 2358/905 490 · Fax +49 2358/905 499
Burg-Guard@burg.biz · www.burg-guard.com
Video security · analogue & IP cameras
AI video analysis · network recorder · BURGcam APP
project planning · Service & Support · network accessories

Video Technology



Dallmeier electronic GmbH & Co. KG
Bahnhofstrasse 16 · 93047 Regensburg
Tel. +49(0)941/8700-0 · Fax +49(0)941/8700-180
info@dallmeier.com · www.dallmeier.com

Video security technology made in Germany:
multifocal sensor technology Panomera®,
IP cameras, recording servers, intelligent video
analysis, video management software

Video Technology



EIZO Europe GmbH
Belgrader Straße 2 · 41069 Mönchengladbach
Tel.: +49 2161 8210 0

kontakt@eizo.de · www.eizo.de
Professional monitors and solutions for 24/7 use in
video surveillance, IP decoding solutions with easy
installation and computerless operation.

Video Technology



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

Video Technology



Video surveillance • Video door intercom

TIME ACCESS

Time + Access



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

Time + Access



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

Time + Access



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

Time + Access



ELATEC GmbH
Zeppelinstrasse 1 · 82178 Puchheim, Germany
Tel.: +49 89 552 9961 0
info-rfid@elatec.com · www.elatec.com
Provider of user authentication and identification solutions. Driving the digital transformation of customers and partners with the combination of universal multifrequency readers and advanced authentication software, service, and support.

Time + Access



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

FIRE PROTECTION

Time + Access



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

Time + Access



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

Be Part of the Section



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

We will be glad to advise you!

Time + Access



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

Time + Access



sesamsec GmbH
Finsternbachstrasse 1 · 86504 Merching, Germany
Tel.: +49 8233 79445-0 · Fax: +49 8233 79445-20
info@sesamsec.com · www.sesamsec.com
Provider of access control systems, from single-door solutions to smart campus systems. Hardware and innovative software solutions such as Physical Access Control-as-a-Service (PACaaS).

PLANT SAFETY

Time + Access



PCS Systemtechnik GmbH
Pfälzer-Wald-Straße 36 · 81539 München
Tel. +49(0)89/68004-0 · Fax +49(0)89/68004-555
intus@pcs.com · www.pcs.com
Time recording, building security, access control, Biometrics, Video, Visitor Management, SAP, Hand Vein Recognition

Time + Access



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

Plant Safety



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

Company Index

ABB Stotz-Kontakt 12	Denios. 14	InnoSenT. 34, 36	Pilz 12
Advanced Electronics 22	Detectomat 14	Innovatrics. 27	Pizzato 12
Advancis 13, 44	Dina 12	i-Pro 13	Qognify 22
AG Neovo 13	Dormakaba 13	iProov 27	Raytec. 13, 34
Ajax Systems. 13	Dräger. 12	K.A. Schmersal 12	Salto 6, 13, 14, 15
Altronix Outside Back Cover	Eagle Eye Networks 12, 13	Keba 12	Schuberth 15
Antier 27	Eizo. 13, 26	Kemas. 40	Secunet. 27
AP Sensing 14	Ejendals 12	Kentix 14	Securiton. 13, 14
Aratek. 27	Empa 20	Kepler 15	Senstar 14
Asecos 12	Essentry 13	Krause 12	Sapura 7
Assa Abloy. 7, 35	Euchner. 12	Ksenia. . Inside Front Cover, 13, 46	SharpEagle 12
Astrum 15	Evva 13	Labor Strauss 14	Sorhea 8
Aug. Winkhaus. 13	FIDO Alliance. 27	Ledlenser 12, 14	SSP. 12
Axis. 14	Flir 48	Meister Automation 14	Suprema 6
Bihl+Wiedemann 12	Frogblue 13, 32	Messe Frankfurt 7	TBS. 27
Bioteq. 27	Genetec 13, 34	Milestone 38, 48	TH Deggendorf 15
Bird Home 13	Gore 12	Mobotix. 15	Twiceme 15
Blickfeld 14	Graef Gruppe. 13, 14	Moxa. 12	Vanderbilt 13
Bosch. 13, 14, 22	Gunnebo 48	Munk Group 14	Veridos 27
BSS 13	Hanwha. 13, 14, 24	NEC 27	Video 13
BVSW 15	Hekatron. 14	Novar 14	Vision Labs 27
Carrier. 13	Helly Hansen 12	Oosto 27	Vitaprotech 6
Cias 22	Hikvision 13, 42, 48	Optex 13, 14, 29, 41	Wagner Group . . . Front Cover, 16
Dahua. 6	Hochiki 19, 22	Orglmeister 21	Wanzl 15
Dallmeier. 9	Idis 30	PCS 13	Wibu. 15
Dehn. 22, 23	iLoq 6	Phoenix Contact. 12	Wilka. 13

Imprint

Published by

Wiley-VCH GmbH
A Company of John Wiley & Sons, Inc
Boschstrasse 12 · 69469 Weinheim
GERMANY
Tel.: +49 (0) 6201 606-0 · Fax: -791
www.GIT-SECURITY.com
GIT-GS@wiley.com

Managing Directors

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

Wiley GIT Reader Service

65341 Eitville / 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

Editorial

- Matthias Erlar
+49 (0) 6129 5025300
matthias.erlar@wiley.com
- Eva Kukatzki
Tel.: +49 (0) 6201/606-761
eva.kukatzki@wiley.com
- Mark Triggs
+44 (0)7966 037011
mark@abadee.co.uk

Editorial Assistant

- Stormy Faust
Tel.: +49 (0) 6201/606-125
stormy.faust@wiley.com

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 is published
4 times per year.

Subscription 2024

4 issues 55.00 €, single copy 16.30 € plus postage. Pupils and Students receive a discount of 50 % at sight of a valid certificate. Subscription orders valid until cancelled, notices 6 weeks before end of the year. Subscription orders can be revoked within 1 week in writing. Dispatch complaints are possible only within 4 weeks after publishing date.

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

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



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

WILEY



eFlow™
Enhanced Fire
Power Solutions

FireSwitch™
Network Managed
NAC Power

CommBatt™
BDA Power
& Backup

**YOU
DESERVE
BETTER**

A | Altronix®

Protecting People, Property and Assets

Altronix delivers world-class power and peripherals for fire alarm detection, signaling and emergency egress. We now provide back-up power for emergency communications systems, ensuring that first responders are always connected. Our products save lives.

We've got it all covered.

altronix.com

