

GIT SECURITY EMEA

MAGAZINE FOR SAFETY AND SECURITY



© diegograndi - stock.adobe.com

- Mobile Access
- Security for Public Transportation
- Intrusion Prevention
- Special Focus Retail
- Video Surveillance

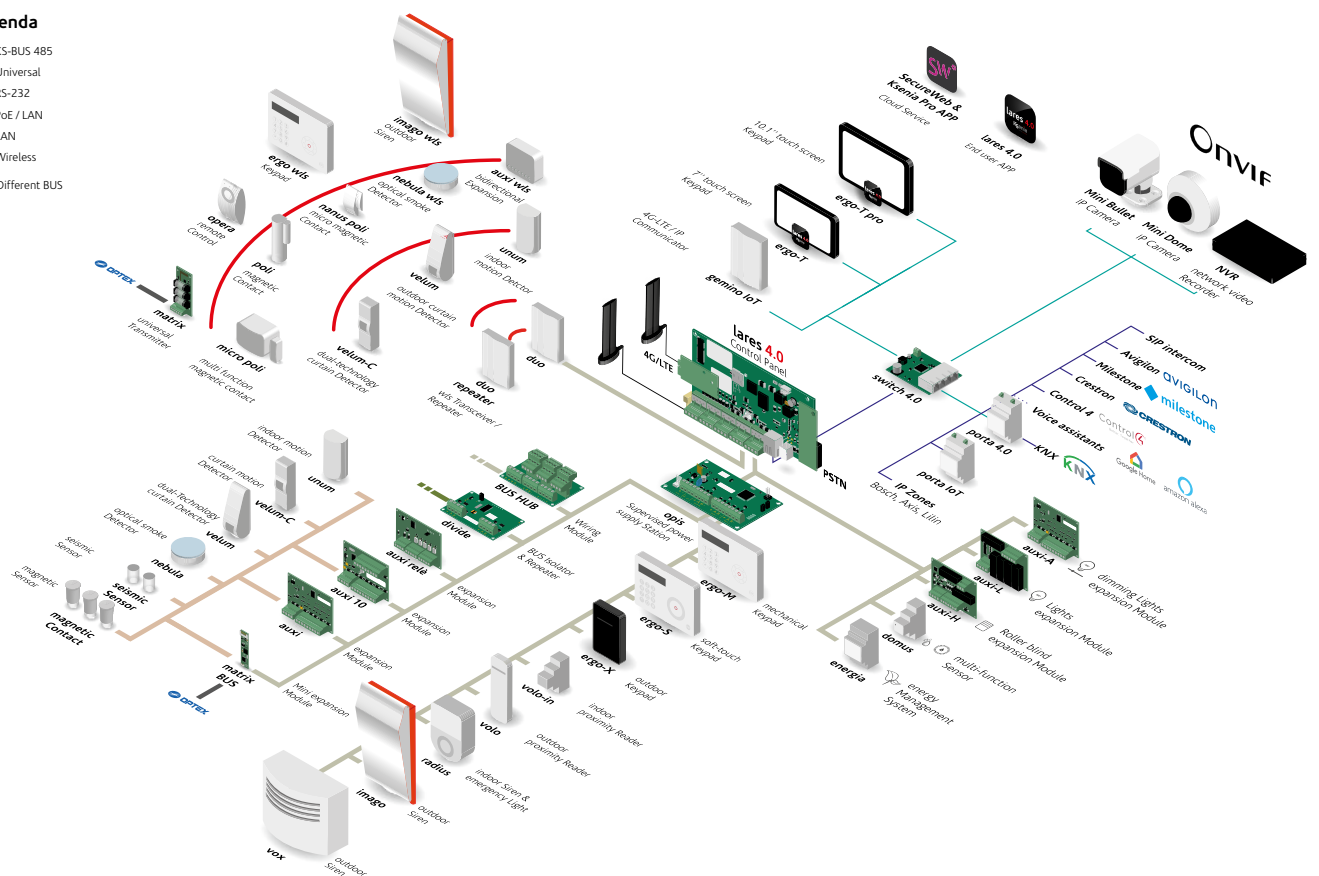
COVER: Bosch Building Technologies
Rolling AI – Interview with Andreas Mauer, Chief Architect

WILEY

SOLUTIONS RANGE

Legenda

- KS-BUS 485
- Universal
- RS-232
- PoE / LAN
- LAN
- Wireless
- Different BUS



THE MOST INNOVATIVE IoT SOLUTION FOR SECURITY AND HOME & BUILDING AUTOMATION



Design

Innovation

Made in Italy

Eco-sustainability

FIND OUT MORE



Proof of Concept

To secure an enterprise it is recommended to go for a multi-layer approach, meaning to install several layers of security. In such an approach, perimeter security is a crucial element of almost every security concept. It is the first line of defence to protect your assets, information, and people. The perimeter security system is designed to keep away unauthorized intrusion in your property and more and more people are deploying state-of-the-art security solutions to make unauthorized intrusion practically inconceivable. The solution you may want to install solely depends on the possible threats and what it is that you wish to protect.

In this issue, you will find several articles about perimeter protection and intrusion detection: On page 40 we start our special focus on airport security and you will get valuable insights on how to secure an airport perimeter. On the following pages we show perimeter protection best practise. Successful installations are the best proof of concept, but in this sensible area we are often not allowed to go into details when we describe solutions. This is one of the reasons why we invented our own system testing series last year to give vendors and security solution providers the opportunity to give the industry a proof of concept for their perimeter protection offering. In 2023, we will add another GIT System Test Video Analytics and extend the range of tested systems beyond video analytics with the GIT System Test Perimeter Protection (GSTPP).

Finally, a little reminder for all of our readers. To promote product development, every year we recognize the best products with GIT SECURITY AWARD. Starting on page 9 we present the nominated products for GIT SECURITY AWARD 2014, carefully chosen by our jury. Please have a look at the products and vote for your favourites. The voting tool opens June 1st.

Stay safe and enjoy reading this issue!



Heiko Baumgartner
For Wiley's Safety and Security team



COVER STORY

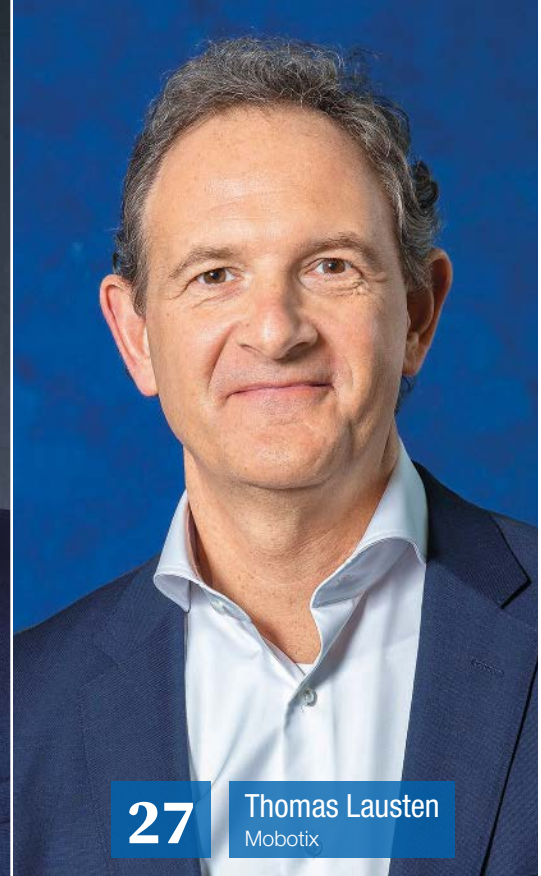
22

Cover story
Bosch Building Technologies



26

Vincent Dupart
STid



27

Thomas Lausten
Mobotix

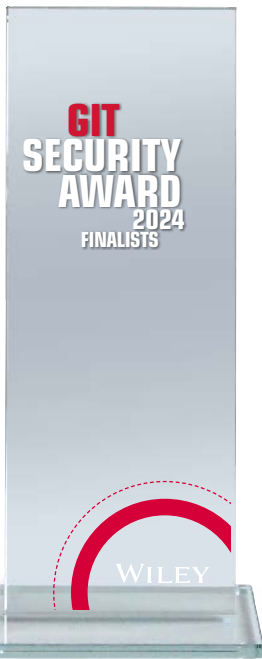
MANAGEMENT

COVER STORY

- 22** When AI Starts to Roll...
More Than Just Smart:
Artificial Intelligence in
Building Control

COVER STORY

- 9** **GIT SECURITY AWARD**
The Nominees
Readers can vote for their
favorite product from June 1st



INTERVIEW

- 26** High Security Experience
Combining Flawless Security
With Intuitiveness

BUSINESS MANAGEMENT

- 27** Opportunities Seized
In Conversation with
Thomas Lausten, CEO Mobotix

- 28** Time for a Triple
i-PRO, Mobotix and Konica Minolta
Strengthen Strategic Collaboration

PSIM

- 30** Security Management Best Practice
Securing Companies and Managing
Resources with Software

SECURITY

POWER SUPPLY

- 32** Power Wherever You Need It
Answering the Call for More Power,
Access Capacity, and Cost Efficiency

ACCESS CONTROL

- 34** Going to the Office Today?
The Role of Access Control in Making
Work More Flexible

4X3 QUESTIONS

- 36** Mobile Access Control

ALARM SYSTEMS

- 38** Ajax Protects Banksy's
Works in Ukraine
Motion Detectors and Opening Detectors by
Ajax Protect the Objects Against Attempts
to Damage or Approach the Artwork

AIRPORT SECURITY

- 40** Inside, Around, and Above
A Plethora of Security Solutions
Helps to Keep Airports Safe

SPECIAL FOCUS

CRITICAL INFRASTRUCTURE

- 42** Greatest Challenges in
Critical Infrastructure
What Providers Need to Know and
Do to Safeguard Premises

SPECIAL FOCUS



Joachim Mahlstedt
ASSA ABLOY



Clément Menviel
STid



Michael Rumpf
Senstar



Borja Ganzarain
Salto Systems



Sanjit Bardhan
HID PACS



48 **John Rosenbusch**
Senstar

36

SECURITY MANAGEMENT

- 46 Attack to the Core**
Threats to and the Protection of Critical Infrastructure

PERIMETER PROTECTION

- 48 Sensors, KRITIS and AI**
Sensor and Information Management Systems for the Protection of Infrastructure and Assets

ADVERTORIAL

- 51 Full Color at Low Light**
Hikvision Unveils Next Generation ColorVu Technology With Enhanced Low Light Imaging Using Super Confocal and Smart Hybrid Light Innovations

VIDEO SURVEILLANCE

- 52 Every Meter Perimeter**
Tailored Video Security Technology From Dallmeier Provides Perimeter Security and Workplace Safety

SAFETY

MACHINE AND SYSTEM SAFETY

- 54 Creation of Safety-Related Application Software**
Practical Examples for Familiarization with Handling

SECTIONS

- 06 Security News**
- 57 BusinessPartner**
- 59 Imprint | Company Index**

www.GIT-SECURITY.com

REGISTER NOW
for our free
NEWSLETTER



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.



AMG Expands North America Sales and Marketing Team

AMG Systems of the United Kingdom and USA are strengthening their North American sales and marketing effort by adding three key industry veterans to lead the push into the Americas Market: Dave Sinise is now AMG Vice President of Sales for the east region; Dan Anderson for the west region; and Frank (Skip) Haight, now Americas Marketing Manager. All three come from what was ComNet. Dave Sinise is an electrical engineer and led ComNet ITS and Security Sales for the east region since ComNet started in 2008. Dan Anderson, who acquired his degree from Texas Tech, comes to AMG from his former role as Director of Sales for ComNet. Skip (Frank) Haight, recently retired ComNet Global Vice President of Marketing, established the marketing acumen, strategy, and tactics that took ComNet from an unknown startup to the highest profile, most successful company leading to the Acre acquisition. www.amgsystems.com



Secure Tetra Communication

The Munich Security Conference is the world's leading forum for debating international security policy. Held annually at the Hotel Bayerischer Hof, the main conference brings together a good 450 high-ranking decision makers and prominent opinion leaders from all over the world, including heads of state, ministers, leaders of international organizations and non-governmental organizations, as well as leading representatives from business, the media, research and civil society. The requirements for ensuring the safety of all participants are correspondingly high. ESG Elektroniksystem und Logistik was commissioned with the implementation of secure Tetra communication for the 59th Munich Security Conference in February this year, as well as for the following main conferences until 2025. Two Tetra base stations were installed at the Hotel Bayerischer Hof and integrated into the overall Munich city Tetra network. www.esg.de

Smiths Detection and Grasp Innovations to Collaborate on Technology Integration

Smiths Detection has announced a collaboration with Grasp Innovations, a solutions provider for aviation security optimization, to allow the integration of their sensor technology into Smiths Detection's security checkpoints. The collaboration is part of the Ada Initiative that seeks to enable hardware, software and algorithms from different product suppliers to be plugged together using open architecture. Grasp Innovations uses strategically placed sensors to provide data on passenger flows that allow for better resource allocation and will result in an improved passenger experience and operational efficiency. The two companies will jointly pursue opportunities within the industry and interact with existing customers to prove the potential benefit of this partnership. www.smithsdetection.com



Sicurezza and the Milan International Building Alliance

Four events – the GEE-Global Elevator Exhibition, the ME-MADE expo, the Smart Building Expo, and Sicurezza – are all scheduled for November 2023 at Fiera Milano from 15 to 18 November 2023. The “quad-event” will show the synergy between fundamental elements of design, construction, and the requalification of buildings. Sicurezza (15–17 November) is not only the reference event in Italy dedicated to security and fire and offers a comprehensive overview of video surveillance, access control, intrusion detection and fire-fighting systems but also of the new frontiers of cyber security. In its 2023 edition, Sicurezza is giving space to current trends: digitalization, integrated systems and customized solutions, and also to new skills and professionalism. www.fieramilano.it

Idis to Acquire Costar Technologies

Idis and Costar Technologies announced the execution of a definitive agreement and plan of merger pursuant to which Costar will be acquired by Idis in a merger transaction. The agreement has been unanimously approved by the boards of directors both of Idis and Costar. Stockholders collectively holding approximately 45% of the outstanding shares of Costar common stock have entered into voting and support agreements pursuant to which they have agreed to vote their shares of Costar common stock in favor of the merger transaction. The merger is expected to close during the second quarter of 2023. Idis CEO, Mr. Kim Young-Dal, said, “Leveraging Costar's established distribution networks and sales channels in the U.S. gives a significant boost to Idis' growth strategy, which is founded on building long-term relationships with systems integrators. With this acquisition, Idis will diversify and synergize its presence in the government sector and intelligent transportation systems.” www.costartechologies.com

Integrated Security Management Platform

Pacom welcomed visitors to the Security Event at the NEC, Birmingham, to preview its next generation cloud-based platform. The solution is a centrally controlled integrated security management platform that is intelligent, user friendly and highly cost effective. It also extends its functionality beyond security by acting as an interface with the internet of things (IoT). By accessing, storing and processing data from the smart IoT sensors found in intrusion detection, access control, audio, video, and building management systems, it is able to deliver valuable business intelligence, operational insights and efficiencies.

www.pacom.com

VMS, Video Intelligence and Incident Management

Qognify showed its video management software (VMS) and enterprise incident management (EIM) solutions at ISC West in Las Vegas, Nevada last month. The VMS combines the powerful core of an enterprise-class system with advanced ecosystem integrations, integrated video analytics capabilities, cloud storage options, low total costs of ownership and business process support that adds value beyond physical security. The latest version 7.2 of Qognify VMS introduces body-worn video integration, faster access to cameras, maps and views, and enhanced vehicle recognition capabilities. A new addition, QogniFinder, significantly speeds up investigations by enabling recordings to be searched for persons or vehicles according to specific physical attributes such as age, color of clothing, glasses, etc. and helps to locate persons or vehicles of interest as well as to retrace their steps during post-incident investigations. www.qognify.com

Radar-Activated Drone Security

Magos Systems has collaborated with robotic aerial security company Nightingale Security to provide a fully autonomous radar-activated drone solution for perimeter security. The solution combines Magos ground-based radar detection and classification with the Blackbird autonomous drone. The radars work in conjunction with PTZ cameras and the Magos MASS+AI software to classify targets as wildlife, vehicles, persons, etc. to reduce nuisance alarms and categorize potential threats. Once the radar solution detects a potential target, the Blackbird drone is automatically dispatched from its base station to the alarm location, streaming live video to the security team, serving as a mobile PTZ. The combined solution is ideal for facilities with large perimeters, rough terrain for officers to traverse, or in remote locations where traditional camera perimeter installations are cost-prohibitive or difficult to install. www.magosys.com

Video Management Solution

UK-based integrated security manufacturer Tdsi unveiled its new VMS solution as well as display its Gardis App and a raft of new updates to the software platform at The Security Event 2023, which took place from 25 to 27 April at the NEC Birmingham, UK. Appearing on Stand 4/G40, Tdsi will also show the new app in action, which enables security operators to securely control many different access control options from anywhere using a compatible iOS or Android device. Gardisvu is a major project for Tdsi and provides integration between the company's software platform and the cloud-computing engine and CCTV system from fellow Vitaprotech Group member Recas. Based on the powerful Foxstream video analytics engine, it will be replacing the previous Vugarde solution with a cloud-based alternative that fully embraces the flexibility and convenience of this approach.

www.tdsi.co.uk

Complex Multi-Site Perimeter

In combination with the Micro-Ray barrier with microwave rays, used both to defend the gates and in anti-climbing mode, the Sioux Pro2 Mems detection system from Cias was the product most used in various critical infrastructure sites to protect fences. All the Mems cables and sensors were laid in sturdy TAZ metal tubes and boxes to prevent any voluntary or involuntary damage. Those critical infrastructures of national importance, such as hydro-electric and gas generation plants, transformer stations, recycling stations and waste-to-energy plants, are scattered throughout the territory with more than 10 km of fences, walls, and supply pipes protected. Extremely reliable digital fuzzy logic devices were selected along with a mix of technologies, such as 'linear' microwave, fence-mounted Mems sensors and FSK radar. Such applications demonstrate that sophisticated electronic technologies like Mems fence-sensors and microwave barriers can work perfectly even close to electrical conductors up to 150kV.



www.cias.it

CPD Seminars

Amthal has delivered its first dedicated Continuing Professional Development (CPD) seminar on fire technology to a leading integrated property consultancy. In partnership with Honeywell Gent and Motorola Avigilon, the CPD entitled "Comply, Stay Alive!" highlighted the importance of fire safety. As a highly interactive and eye-opening event, its aim was to introduce a real-life application of dedicated fire technology and how it has made a real difference. Amthal offers a complete portfolio of CPD courses with leaders in fire safety and security including Honeywell Gent and Assa Abloy. Covering all aspects of the fire detection and security industry, including legislation, building regulations and standards, each seminar aims to provide a better understanding of the key considerations surrounding a particular subject area.

www.amthal.co.uk

Halma Acquires FirePro for €150 million

Halma has acquired FirePro. Headquartered in Limassol, Cyprus, FirePro is a manufacturer of aerosol fire suppression systems that protect people, critical infrastructure and equipment using a non-pressurized, condensed aerosol technology that does not contain ozone-depleting substances or fluorinated greenhouse gases, and extinguishes fire without causing damage to the environment. FirePro's products, for which it holds several patents, have been installed in over 110 countries across a broad range of industries and applications, and have listings and approvals with certified bodies around the world. The acquisition is part of Halma's growth strategy to acquire businesses aligned with growing a safer, cleaner, healthier future for everyone every day. Halma has completed seven acquisitions so far this financial year – FirePro broadens the range of fire safety technologies within Halma's safety sector.

www.halma.com

Civil Defense Day Fire Fighting Challenge

The Fire Fighting Challenge took place 28 February to 2 March as part of the Civil Defense Day celebrations in Abu Dhabi, and benefited from the support of Intersec to bring the event to the United Arab Emirates. As Diamond sponsors, Intersec supported the challenge as part of its 25th anniversary celebrations ahead of its Silver Jubilee edition in January 2024. The Fire Fighting Challenge has been developed by organizers 911 Challenge Events Management to draw attention to the requirements of firefighting, both physical and mental. Competitors demonstrate their real-life actions through a series of challenges, allowing visitors to see equipment in action, as well as witness the extraordinary levels of fitness required of firefighters. As the Middle East's premier exhibition for the safety, security and fire protection industries, Intersec works closely with Civil Defense to drive the industry forward in the region and beyond.

intersec.ae.messefrankfurt.com

Electromobility Fire Risk Conference

Electromobility is intrinsically linked to the storage of electric power, which increasingly is being delivered by renewable energy sources. Many new aspects and challenges have arisen, with the changing fire risk being of particular interest and requiring new solutions. The Eusas conference on 10 and 11 May entitled "Addressing the Fire Risks of Electromobility" will provide an up-to-date overview of the hazards from different perspectives, and also provide a look at technologies, politics and law. Three conference sessions will be hosted on the first day by the ZVEI in Niederrad, near Frankfurt am Main, with presentations from Dutch and UK fire safety bodies, manufacturers and component suppliers of electric vehicles, as well as research institutes looking at the causes and propagation of battery fires. Further research presentations will start the second day, which will be rounded off with a look at detection and suppression strategies. Registration is via the "Events" page of the EUSAS website.

www.eusas.org

AI-Boosted Video Analytics

PureTech Systems has announced its integration with Intel's OpenVino to deliver its AI-boosted video analytics on edge devices with lower cost, lower power consumption, and at a smaller size. OpenVino is a powerful toolkit developed by Intel that allows developers to deploy their computer vision applications on a variety of hardware platforms, including edge devices. By integrating this, the AI-boosted video analytics can now run on edge devices without the need for discreet GPU cards, which are expensive and power hungry. This new integration emphasizes the company's commitment to delivering cutting-edge technology. By leveraging its AI-boosted video analytics capabilities, the company is well positioned to drive technological innovation for critical infrastructure protection, and to create long-term value for its customers.

www.puretechsystems.com

25k Conformant Products

Onvif has met the dual milestones of surpassing 25,000 conformant products and celebrating fifteen years as the de facto industry standard for interoperability. Since its inception in 2008, products that conform to Onvif profiles have consistently grown in number and scope, beginning with core products, such as IP cameras, video management software, and network video recording solutions. Today's database of conformant products now encompasses intercoms, license plate recognition cameras, and can also include drones, and services, such as video surveillance as a service (VSaaS), a reflection of both the growing value of video and the advantages of using cloud solutions. To support the industry in these key areas of video analytics and integration with IoT systems is the Onvif Profile M specification, which standardizes the handling of metadata and analytics events.

www.onvif.org

Energy Performance and Fire Safety of Buildings

Euralarm welcomes the position adopted by the European Parliament's Committee on Industry, Research and Energy (ITRE) on the revision of the Energy Performance of Buildings Directive (EPBD) after long and difficult negotiations. The compromise amendments contain significant changes and Euralarm especially welcomes recommendations to better address the fire safety of buildings. Better performing buildings implies new technology – such as battery energy storage systems – that can increase the fire risk, so significant changes in fire safety and security requirements are required. Beyond the recommendations proposed by the ITRE Committee, we call on EU decision makers and member states to create incentives for all renovated buildings to be fitted with the latest fire safety and security technology. Euralarm has full confidence in the European political institutions to take the right decisions that will [...] ensure a sustainable future for all citizens, be it in terms of environment, energy, the use of natural resources as well as safety and security.

www.euralarm.org

Our Finalists for GIT SECURITY AWARD 2024

GIT SECURITY team is proud to report that the award jury voted digitally on their favorite industry products. Now is your turn, dear reader, to select your favorite product and vote. In the following pages, we will display all the finalists of each category.

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
- Special Category: Sustainability

Voting

To have fair voting, 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. Select one product in each category.

Reader Prize

Win the reader prize! Select one favourite from each category to take part in the draw for the camera. We will have a price draw for 5 Wiley-branded Ledlenser P7R Work UV.



Reader
Prize

GIT SECURITY AWARD 2024 FINALISTS

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



This year, we had
in-person meetings
with most of the jury
members and hybrid
meetings for some of
the discussions



Category A • Machine & Plant Safety



Meister Automation: Multialert mini

Fire Protection Control for Control Cabinets and Machine Plants

Fires break out in companies in Germany every 5 minutes. A defective electrical system is a frequent cause of fires. AMFE, the VdS-approved mini fire extinguisher, detects and extinguishes fires in control cabinets. For larger or multiple control cabinets, several AMFE extinguishers are required that are triggered simultaneously. This is handled by the Multialert mini control unit. The Multialert mini is operated directly inside the control cabinet at 24 volts, and will integrate into the fire detection systems on site. Depending on the requirements, it combines AMFEs and smoke detectors. In addition, it can use audio-visual signals to draw attention to the fire and report it to superordinate systems. After triggering, the system itself is ready for use again via an integrated reset.



Moxa: EDR-G9010 + MXsecurity

Firewall with Optional IDS/IPS Module

To preempt ever-present cyberthreats, Moxa combines OT-centric firewall capabilities (EDR-G9010 Series) with MXsecurity management to help detect cyberthreats and prevent them, ensuring secure and continuous operations (Modbus TCP/UDP, DNP3, IEC 60870-5-104, and IEC 61850 MMS traffic filtering). The 10-port full Gigabit secure router of the EDR-9010 Series is capable of firewall/NAT/VPN/switch/IPS functions, extends deep packet inspection to more OT protocols, contains the latest security intelligence, and supports virtual patching to mitigate identified threats. MXsecurity helps track network defense using real-time dashboards. The software translates OT-specific threat intelligence into visible defense intelligence and security management for better protection, detection, and reaction to cyberthreats.



Jury Members

of Category A:

Birgit Sellmeier, VDMA,
Dr. Markus Winzenick, ZVEI,
and Dr. Timo Gimbel, Wiley



VOTE NOW FOR THE NEXT WINNERS

WWW.SECURITY-AWARD.COM

Pizzato Elettrica: P-KUBE

Smart Safety Handle

The P-KUBE Smart safety handle, combined with RFID safety sensors, allows to create an effective interlock system for all guards on machines without inertia. The handle integrates an orientable block with an RFID TAG that can be detected by the sensor as a normal actuator. The block can always be correctly oriented toward the sensor, thus making the handle suitable for any installation (hinged or sliding doors, horizontal or vertical etc.). The front band of the grip is available in satin chrome or backlit white finishes, with the option of integrating a control button to interact with the machinery. The RGB LEDs in the backlit grip allow local signalling of the guard status using different colours and fully customisable sequences. These features give to machine manufacturers the chance to optimise the cost of components by eliminating peripheral control boxes and illuminated signalling columns.



SICK: safeVisionary2**3D Time-of-Flight Camera with Safety Certification**

One of the first 3D time-of-flight camera with Performance Level c safety certification increases the safety and efficiency of AGVs/AMRs and collaborative robots through safe three-dimensional environment detection. In addition, the camera also reliably solves automation tasks thanks to precise 3D measurement data, saving the need for additional hardware components. safeVisionary2 has a compact, robust design and can be used in a versatile and reliable manner in everyday industrial applications. In addition, the user benefits from a high level of user-friendliness. This saves considerable time during installation and configuration.

**TXOne Networks: TMPS3 Pro****High-Performing Malware Scanning Tool**

TMPS3 Pro is a portable security device designed to scan for and clean up malware on isolated industrial control systems (ICS), as well as to provide secure storage and data transfer. TMPS3 Pro looks like a USB flash drive, combining malware scanning and removal with 64GB of secure storage equipped with AES-256 hardware encryption. It enables IT, OT or security teams to securely transfer important files or patches to offline systems and isolated networks and also to perform on-demand malware scans on any system without the need of software installation. The built-in notification LEDs display the status of the malware scan, making operation quick and convenient.

Category B • Occupational Safety and Health & Explosion Protection

Cemo: Li-Safe**Battery Safety Storage and Charging Cabinet**

The battery storage and charging cabinet Li-Safe stands for comprehensive protection against burning lithium-ion batteries. For the first time, the cabinet offers not only fire protection but also explosion protection, tested according to the latest/highest test standard of the TÜV Nord Cert. It thus ensures greater safety during operation – e. g. when storing and charging batteries for power tools or e-bikes. Thanks to an innovative integrated pressure relief system, it can be ruled out that the doors of a typical gas explosion open unintentionally, what will invalidate any protective function of the cabinet. So far, fire resistance alone was considered as enough. Nevertheless, an MPA-tested fire resistance of 60 minutes (inside to outside) and fire tests with e-bike batteries form the basis. 3-fold stackable, compactness for quick evacuation and electrical alarm systems are also standard. Two cabinet sizes, each with 4 equipment variants, offer solutions ranging from entry-level requirements to professional applications with SMS alarm to cell phone.

**Linde: Linde Motion Detection****Forklift Assistance System**

Many work-related accidents in warehouse environments occur when counterbalance trucks are reversing. Pedestrians often rely on being seen by the operator of the truck. Due to the blind spot, it is often not possible for the forklift driver to see the entire area behind the truck. The result are collisions between the truck and pedestrians or between two trucks. This is where the assistance system Linde Motion Detection comes in. Mounted on counterbalanced trucks, the system detects movements behind the stationary vehicle and prevents it from reversing. At the same time, the driver is warned by the display and pedestrians and other forklift drivers are warned by an acoustic signal. Active intervention by the driver is not required; the use of this assistance system prevents operating or human error.

Hoffmann Group: New Service in Cooperation with GetSteps**Orthopedic Insole Service**

A new service from the Hoffmann Group in cooperation with orthopedic shoemaker GetSteps GmbH enables companies to quickly and easily obtain DGUV 112-191 -compliant orthopedic insoles for more than 2500 safety shoe models. As a result, the Hoffmann Group is able to supply individually manufactured insoles for a wide range of safety shoes from various brands. For companies with higher orthotic needs, Hoffmann Group and GetSteps offer on-site 3D scan foot measurement. For companies that only want to supply employees with previously diagnosed foot problems, there is the option to procure custom orthopedic insoles remotely. After ordering from the Hoffmann Group, employees then receive from GetSteps a footprint set certified as a medical device, which they use to take their own footprints. This means that even smaller companies can offer a professional supply of insoles without complications.





Munk: GRP Stepladders TRBS-Compliant GRP Stepladders

The new GRP stepladders are the first on the market to be made in Germany and developed in accordance with the new TRBS 2121 Part 2. They are made of insulating glass-fibre reinforced plastic (GRP) and provide the necessary plus in work safety not only in the electrical trade when working near live parts. They are tested for voltages up to 60,000 volts. (DIN EN 61478:2002 +A1 (2004), 6.5.1 category 2). The innovations also score points when exposed to cold and chemical substances. Thanks to their consistent equipment with 80 mm deep steps, they fulfil all current TRBS specifications and can also be used for longer lasting work on the ladder without further accessories. As standard, the GRP stepladders are also equipped with nivello ladder shoes for extra secure footing.

Raytec: Spartan Linear High Output Ex Linear Luminaires

Raytec has recently launched a new High Output variant of their Spartan Linear LED luminaire which is certified for use in Zone 1 and Zone 2 hazardous areas. The new variants offer a significant increase in power and performance which represent a step-change in the way Linear luminaires can be deployed. Delivering up to 14,000lm and 144lm/W, Linear High Output can be used to replace larger fluorescent fittings to deliver large cost savings, or deployed as a cost-effective alternative to traditional bay luminaires. End-users can replace a 2x36W (or larger) fluorescent fitting, with a 2ft LED luminaire that delivers an upgrade in performance and significantly reduced running costs. At the same time, the Linear High Output can be used as a cost-effective replacement for conventional bay-style fittings and is also available with emergency battery backup and a secondary optics for focusing the light.



Phoenix Contact: Mini Analog Pro Compact Ex i-signal Conditioners with SIL 3

The intrinsically safe variants of the well-known Mini Analog Pro 6.2 mm signal conditioner-family set new standards in miniaturization: The products offer reliable signal transmission, intrinsically safe (Ex i) explosion protection and functional safety in a unique compactness of overall width and height. The products are consistently rated to the highest safety level, SIL 3 one out of one. Despite the small design, the user benefits from particularly user-friendly housing and operating concept, a wide range of parameterization options and consistent digitization (via App, clipX Engineer or DIP-switches). Due to the wide operating temperature range from -40°C to 70°C and a documented altitude application range of up to 5000 meters, Mini Analog Pro can also be used under extreme environmental conditions.

GIT SECURITY AWARD 2024

Uvex: Pronamic Alpine Mips Safety Helmet with Mips Safety System



To significantly improve safety, Uvex has developed the Uvex pronamic alpine Mips, a new safety helmet in cooperation with the Swedish company Mips. The Mips technology integrated into the helmet makes a decisive contribution to reducing rotational forces when objects hit the helmet off-center or at an angle, and thus the strain on the brain. As a result, concussion or even brain damage can be significantly reduced. The Uvex pronamic alpine Mips is also certified according to EN397 (industry) and EN12492 (construction sites). A clear development goal was also to integrate all functional elements (ventilation, Mips safety system) into the helmet design in a form-fitting manner. Wearing comfort was also a decisive factor in the development, so that the helmet can be optimally adjusted to the respective head geometry (size range from 51 to 63cm).

Category C • Video Security Systems & Video Management

AG Neovo: TBX-2201

Visual Safety for Public Transport

This specialized 22" monitor in a metal housing was developed by AG Neovo especially for public transport applications e.g. in busses. As usual with AG Neovo, very long product life cycles can be expected with this series. In addition to AG Neovo's unique selling points such as very robust NeoVTM protective and filter glass and the consistent 24/7 design, the cable management, the 8-36VDC power supply and the e-certification will inspire. The unique "NeoTransPro Installation Suite" ensures stress-free installation, runtime and maintenance of multiple on-board displays for IP video security and passenger information without additional accessories. Brilliant images over long distances are thus realized for public transport.



Axis: Q1656-DLE Radar-Video Fusion Camera

The Axis Q1656-DLE Radar-Video Fusion Camera offers you a wide-area intrusion protection and reliable 24/7 detection with a fusion of two powerful technologies: video and radar. This unique device provides state-of-the-art deep learning-powered object classification for next-level detection and visualization. This innovative device brings video and radar analytics together in Axis Object Analytics to deliver next-level detection and visualization. Video analytics provide precise localization and object classification powered by deep learning.



Dallmeier: PlanD Camera Planning Tool

The camera planning tool PlanD takes an approach that is unique in the industry: With PlanD, installers, partners and even end customers can create professional camera plans independently, playfully and without 3D software knowledge. In just a few minutes, users can draw in buildings, place cameras, detect shadows and also

adjust fields of view intuitively and live thanks to 3D Camera View. In this way, PlanD revolutionizes the planning process: a completely new user experience is created and customers can be involved live in the planning process. The intuitive user guidance, interactive collaboration and direct feedback significantly accelerate the planning phase of an entire project.

Eagle Eye Networks: Smart Video Search AI-based Search for Video Surveillance

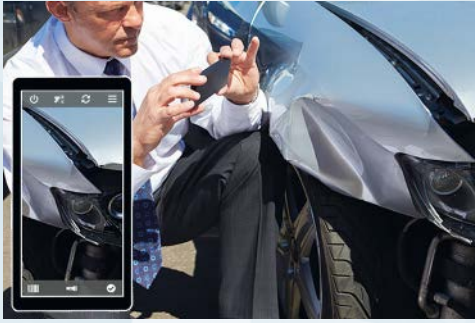
Smart Video Search is a global, AI-based solution for video surveillance that lets users search for people, vehicles or objects across cameras in all sites, saving time and money. It has a unique architecture that adds intelligence to standard cameras and is scalable. The AI is cloud-native, so no new AI camera or appliance is required. Continuously improving AI-based image models process key images and video in real-time when motion is detected, creating searchable metadata in the Eagle Eye VMS dashboard. Users can search with natural language, and advanced functionality includes incident explorer, location-based grouping and show nearby cameras.



Bosch Building Technologies: Autodome 7100i (IR) Cameras Deep Learning Video Analytics for City Surveillance and Traffic Monitoring

Autodome 7100i (IR) cameras are high performance 40x PTZ cameras with excellent starlight imaging technology and high dynamic range. Built-in IVA Pro brings highly reliable deep-learning based detection of persons and vehicles to scenes ranging from sterile zones to crowded and congested. They are a highly accurate and reliable solution thanks to a closed-loop drive platform. The cameras feature IVA Pro, an expert suite of application-specific video analytics offering reliable, precise classification for city surveillance, traffic monitoring and long-distance perimeter detection.





Geutebruck: SmartphoneConnect

Smartphone Integration to Video Management

The app from Geutebruck turns smartphones into security cameras. The smartphone is integrated into the video management system like a permanently installed camera. Images and optionally audio are transmitted via mobile network or WLAN. Scan codes in various formats can also be captured. App users can generate events, trigger alarms with live image feed or record comments on images. Data protection is also taken into account: The image transmission is fully encrypted and are only cached locally for offline use and deleted after transmission to the VMS. Smartphone users have no access to memory images, which guarantees data security even if the smartphone is lost.

Hikvision: TandemVu PTZ Cameras

Dual PTZ Camera

The TandemVu technology features Hikvision's next-generation camera design that integrates multiple lenses into one device. Detected events in the overview camera are transferred to the PTZ camera by the Smart Linkage function and displayed in detail. The user can see details and gets an overall view at all time. This is possible by combining two camera types in one housing: An overview camera with up to 180° viewing angle and a PTZ camera that focuses on important details. The system reduces installation time and effort and is available for Darkfighter, Acusense and ColorVu technology.



VOTE NOW FOR THE NEXT WINNERS

WWW.SECURITY-AWARD.COM



i-PRO: WV-X86531-Z2 / WV-X86530-Z2

AI-enabled Multi-directional and PTZ Cameras

The WV-X86531-Z2 and WV-X86530-Z2 are small and lightweight AI enabled outdoor multi-directional and PTZ cameras with either four or three 5MP multi-sensors and an integrated 2MP PTZ sensor. At just 3.8 kg and 250 x 195 mm, the cameras are the smallest and lightest outdoor multi-directional and PTZ of its kind in the industry, ensuring a discreet look in any environment. Each camera has powerful Ambarella AI processors on board: two processors manage the camera functionalities and two processors manage the on-board AI applications. AI-based object recognition enables a seamless hand-off from the multi-directional lenses to the PTZ while AI auto-tracking ensures the PTZ doesn't lose view of the traced subject.

Motorola Solutions: Avigilon H5A

Multisensor Camera

The Avigilon H5A Multisensor camera incorporates AI-powered analytics with up to four adjustable sensors to cover a site from all angles, with one camera. The camera leverages the latest in AI-powered video analytics to detect and persistently track more objects – whether stationary or moving – with greater accuracy even in crowded scenes, detect unusual activity in a scene autonomously. It adjusts the width of the infrared beam and the illumination to increase the image quality. These advanced capabilities help provide detailed information on what is happening that users can detect potentially critical security events faster and take responsive action.





Raytec: Vario2

Lighting for Seeing Through Windcreens

Delivering world leading power and illumination distances, Vario2 next generation illuminators can improve the performance of any video surveillance system at night. Vario2 730nm illuminators have been specifically designed for intelligent transport systems looking to identify occupants inside the vehicle, such as mobile phone detections system, HOV lanes and many more. Seeing inside the vehicle is notoriously difficult, as modern windcreens filter out certain wavelengths of light to protect occupants and keep the cabin cool. Raytec's Vario2 Far-Red illuminators help to overcome many of these issues and provide the best results for occupant detection.

Senstar: Senstar Symphony

Sensor Fusion

The Senstar Symphony Common Operating Platform with Sensor Fusion is not only an open, highly scalable video management system with integrated video analytics, but it also includes full-featured modules for access control and perimeter detection system support. In short, the Senstar Symphony Common Operating Platform with Sensor Fusion is a fully comprehensive modular solution for security management and data intelligence. The newly developed sensor fusion engine adds a module to the Symphony platform that makes it possible to link perimeter detection systems and video cameras at an unprecedented level. Sensor fusion makes intruder detection enormously accurate. Processing unnecessary false alarms is now a thing of the past.



Category D • Access Control & Intruder Alarm

Assa Abloy: i-minimal

Battery-Powered Mortise Lock

The new i-minimal is a robust, battery-powered mortise lock which works almost completely out of sight. The electronics and mechanics are embedded entirely within the door leaf, so only the reader module on one side, and a privacy button on the other, are visible. This low-profile, elegant aesthetic complements any décor or architecture without compromises on door security. The i-minimal works with multiple DIN handle designs and any Tesa Hotel management system, whether simple, flexible Update on Card, in real time with Wireless Online, or with Openwork mobile access management. Standard batteries power the lock, which consumes much less energy than an equivalent wired solution. The i-minimal combines robust electromechanical engineering – built to secure the busiest doors like guest or office rooms – with intelligent access control and an almost invisible footprint.



Astrum IT: Visit

Visitor Management System

The Visit software solution is used to (fully automatically) manage external persons – visitors, external companies and suppliers – and to map the entire visit and logistics process. Visit offers many features to ensure security on the company and plant premises: assigning and managing access rights, multi-level approval workflows, authenticity check and comparison of ID documents with logon data, dedicated security briefings according to visit type and requirement, as well as document management and verification. Visit is scalable – making it the perfect solution for small businesses as well as enterprises. It is available as an on-premise or SaaS solution, GDPR-compliant and IT security (ISO 27001) according to the latest standards.



Bosch Building Technologies: Mobile Access

Mobile Access Solution

Bosch Mobile Access facilitates the use of the smartphone as a digital access medium to replace the classic access card or to be used as an alternative form of identification. It allows users to pre-assign access rights to visitors, guests, employees, or service providers, enhancing security using the smartphone. With its compatibility and ease of integration, Mobile Access offers a smooth transition to a modernized access control setup. Mobile Access works together with premium access control readers, using Bluetooth Low Energy (BLE). When using Mobile Access there is no need to place the smartphone in close proximity to a card reader. Users can even leave the phone in their pocket or bag. Bosch Mobile Access is completely integrated into Bosch access and visitor management, offering easy installation and low maintenance.



Brivo: Brivo Access

Unified Access Control Platform

Brivo Access is a Software as a Service (SaaS) platform for cloud-based access control. The adaptable solution provides a unified dashboard that can be accessed from any device, anywhere, with complete visibility into every property under management, whether that is a single property or hundreds of facilities. Brivo Access supports proactive planning and innovation to maintain control, and limit total building access through their data visualization tool. This tool provides deep insight into security requirements through real-time visualizations of the patterns and trends in the movement in and around a property. Brivo Access is the only unified security platform with embedded business intelligence functionality built from the inside out. Their ground-breaking data visualization tool empowers security teams with easily customized and visualized access control data.

Genetec: Axis Powered by Genetec

Controller with Access Software

Axis Powered by Genetec combines a powerful hardware access controller and Synergis access control software into one product. Normally, information about who is requesting access is routed through the access control system from a card reader. It goes through multiple levels of controllers to a central server. With Axis Powered by Genetec, software is already pre-installed on the controller. It matches the request with the list of authorizations and then access is either granted or denied. Axis Powered by Genetec doesn't require local PC hardware to store access permissions. The controller can be connected via the network to a central computer at any location.



Evva: Emzy

Motor Cylinder

The Evva Emzy is a motorized cylinder that makes it possible to automatically lock and unlock certain exterior and interior doors to sensitive areas as well as shared offices or medical practices. The motor cylinder is attached to the inside of the door with a motor knob and can be operated from the outside via a wall reader, biometrics or code entry. From the inside, it is unlocked via the Emzy button. It can be easily connected to third-party systems such as fire and alarm systems as well as building management and escape systems via the Emzy interface. Wherever the Emzy is used, it stands for reliable security and visual elegance. Whether in shared offices, in a doctor's office, or on doors to particularly sensitive areas, the Emzy locks and unlocks automatically whenever you want it to. It adapts to third-party electronic systems, Evva's own electronic and mechanical systems, to different profile shapes and to any locking process thanks to its adaptive torque. The Emzy is easy to install and wire. It is therefore also well suited for retrofitting in surface or flush mounting.

GIT SECURITY AWARD 2024



HID: HID Mobile Access

Mobile Access Solution

The mobile access solution from HID allows digital employee badges to be stored in Apple Wallet. Users of iPhones or Apple Watches can store the badge in the digital wallet and gain access to their workplace as soon as they hold their device up to an NFC-enabled reader. The technology reduces the waiting time for physical cards and improves the

user experience. The first user of the new access solution is the office tower "22 Bishopsgate", the second largest skyscraper in London. Smart Spaces, a provider of intelligent building technology, and HID have already been responsible for access control in the building since 2020 and have now jointly introduced seamless employee access via Apple Wallet.

Johnson Controls: Emerald

Multi-functional Access Terminal

With the Emerald access control terminal, Johnson Controls supplies a solution combined in one product. With its sleek design and state of the art 4.3" LCD touch screen, the emerald range offers card reader and controller functionality, scramble keypad for PIN security, fully integrated Voice over IP (VoIP) intercom and optional fingerprint biometric security, all in one powerful touch screen terminal. Emerald also uniquely enables data normally only available on the AC2000 client PC to be accessed locally at the door (Remote Applications) for functions including reader maintenance, room bookings, display of advertisements, visitor information and much more.



Ksenia: micro poli**Wireless Multifunction Sensor**

The product micro poli is a wireless multifunction sensor for burglary protection, designed and developed by Ksenia Security. It implements the wireless bidirectional 868 MHz protocol used by all models of lares 4.0 control panels. The two Reed contacts inside the transmitter make the installation of the sensor extremely easy permitting to choose which of the two magnets to use. Thanks to the embedded 3-axis accelerometer based on MEMs technology, micro poli is also an inertial sensor to detect vibrations and breaking of glass and windows. Finally, by using magnetic anti-masking, it is able to identify the inclination of the frame it protects, allowing the management of any type of window opening.

**Salto Systems: Neoxx Electronic Padlock**

Salto Neoxx electronic padlock is a particularly resistant electronic padlock, which is certified according to EN 16864:2018 Grade 1144-D34. Therefore it is proven to withstand extreme environmental and weather conditions. At the same time, it is equipped with extensive access management features. The IP66/68-certified Salto Neoxx works in parallel with both RFID credentials and mobile access. This differentiates it from competing products that usually handle either Mobile Access or RFID, but not both at the same time. It also works with the Salto Virtual Network (SVN) as standard and with wireless networking technology Salto Bluenet if required. The Salto Neoxx is fully compatible with the Salto Space system platform and the Salto KS cloud access control solution. This allows access points to be integrated into a unified access control system that cannot be equipped with electronic locks, standard electronic cylinders or wall readers. In this way, users gain control over all relevant access points of their properties.

Telenot: histar Dual 1012**Infrared Microwave Motion Detector**

The histar Dual 1012 infrared microwave motion detector is designed for monitoring indoor areas for intrusion. It detects infrared heat radiation via its mirror optics and also has an integrated microwave sensor. At 12 meters, the monitoring range of the histar Dual is 20 percent larger than comparable detector types for room monitoring. The detector is approved for VdS class B, as well as EN50131:grade 2 or in the AM version with additional cover and undervoltage monitoring incl. wall breakaway protection according to VdS class C or EN50131:grade 3. The histar Dual detectors can be used in all current Telenot intrusion detection systems. The shapely design blends inconspicuously into the room design. The detector uses innovative microprocessor-controlled signal processing with new Snap technology (Selective neuron algorithm with power management) in combination with a hitherto unique digital pyroelement. This enables excellent false alarm security and outstanding detection characteristics.

**TIL Technologies: Tillys Cube****Multifunctional Access Control Centre**

The Tillys Cube is a multifunctional access control centre for various trades and part of the "Microsesame Cube" system from TIL Technologies. Up to 24 doors, 24 sirens, 256 inputs or 128 outputs per bus and 32 detector groups can be connected to three RS-485 buses. Up to 48 expansion modules can be connected for access control, burglar alarm technology and building management systems. The Tillys Cube supports various protocols and identification techniques for access control, manages up to 600,000 IDs and stores up to 10,000 events. It also offers protection mechanisms such as an integrated firewall against DoS attacks and holds TLS-V1.3 certificates. Thanks to a ANSSI certification, it is well suited for security-sensitive locations. Further advantages: Very low energy consumption and at least 10 years support guarantee.



**VOTE NOW FOR THE
NEXT WINNERS**

WWW.SECURITY-AWARD.COM

Category E • Building Safety & Perimeter

Advancis: WinGuard X5

Open Integration Platform

The open integration platform WinGuard X5 controls all security, building management and information technology systems via a unified user interface. Dynamic workflows (SOPs) support the operator in event processing. X5 is based on the new Advancis Open Platform (AOP) – a software platform allowing to easily create modular as well as scalable applications. With AOP and a modern API, i.e. a programming interface, the user can extend the system with own functionalities, interfaces as well as individual user interface (UI) elements. Thus, there are hardly any limits to the use of own components in WinGuard.



Capra: iBoom

Combination Fence & Video

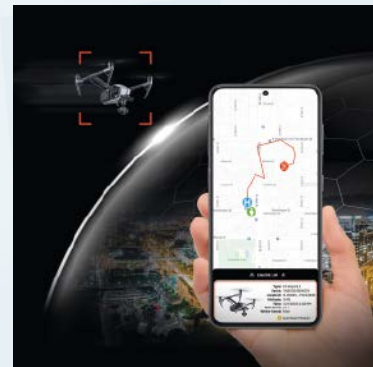
The product iBoom is a mobile security fence with integrated video surveillance used for critical security applications. It consists of a concrete block (810 kg) with patented interlocking system (high mechanical strength) and integrated cable tray for sabotage free cable routing. Integrated Secotec S1 Video-Alarmssystem. 24/7 Live Video Surveillance by VOC with Audio Alarmssystem.



Dedrone: DedroneCity

City-Wide Drone Detection

Drones are getting faster, cheaper and able to carry bigger payloads. As a consequence, traditional perimeter security, while essential, no longer suffices to keep people, airports and critical infrastructure safe. Dedrone's City-Wide Drone Detection Service solves this issue in an easy to implement manner. Both public and private entities can easily access and use DedroneCity, which monitors drones across wide geographical areas to provide real-time notification drones with a pilot's GPS location and drone data, when alert zones are breached. Dedrone-City requires no additional equipment nor installation, and already exists in 40 major cities around the world including New York City, Los Angeles, and Barcelona.



Dormakaba: Argus V60

Sensor Barrier

The compact Argus V60 sensor barrier offers safety, elegance and efficiency, and does so with a unique dimension in the smallest of spaces. Equipped with state-of-the-art sensor technology, it offers users and planners a wide range of possible applications that conventional sensor barriers can only fulfill to a limited extent. Especially in entrance areas of existing buildings, in combination with elevator systems, in open-plan offices for the regulation of area accesses, this compact unit finds its application. In addition to the clear signal effect as a control point for employees, the high detection accuracy is a good source for any room balancing access management. With its dimensions of 240 x 180mm, the Argus V60 proves to be the smallest fully-fledged sensor barrier on the market.



GIT SECURITY AWARD 2024

Hikvision: Stand Alone Thermal Camera**Solar Powered Camera**

Hikvision's solar-powered thermal cameras are designed for use in areas where power and network cables cannot reach. The features: Thermal camera and AI enable reliable person and vehicle detection. Power and network independent – with solar panel, battery and 4G modem for flexible installation. Intelligent power management – monitoring in 24/7 continuous operation or power saving mode. It comes with a robust and weatherproof housing – water (IP67) and wind (Beaufort scale up to 12).

**Navtech Radar: AdvanceGuard Monitoring Solution for Airports**

AdvanceGuard is an innovative, wide-area radar surveillance solution for airports providing fully automatic continuous surveillance inside and outside the perimeter. Easy to scale and integrate with other systems, the system can distinguish threats from normal activity, minimizing nuisance alarms, and warn of incursion before it happens. Automatically detects and tracks unlimited targets in all weather and light conditions. Radars scan 360° and up to 3 km for site-wide situational awareness and real-time threat analysis. Custom options, including critical part monitoring, friend or foe detection, ADS-B, drone detection and surface movement radar, can create a dashboard for airside operations. Proven in airports worldwide, performance guaranteed.

**Securiton: SecuriDrone Fortress Smart Mobile Drone Detection and Defence**

SecuriDrone Fortress Smart is a discreet way of detecting and taking control of drones on a mobile basis and in ad hoc use – even covertly. The system is very easy to install, for example in a car, and can be exchanged between different vehicles within 5 minutes if necessary. This solution is therefore perfect for personal or event protection, among other things. The associated magnetic omnidirectional antennas enable a detection range of up to 3.2 km (depending on the environment and the speed of the vehicle). The system is completely smart and is easily controlled via smartphone or tablet – no matter from where in the world. Control and management via a web suite is also possible.

**Siemens: Building X Security Manager Cloud Solution for All Security Systems**

The Security Manager brings together the data from all security systems on a cloud platform and displays it clearly on a dashboard. Recurring workflows can be merged into unified, automated workflows. Security operations and incidents can be managed centrally and across systems via the dashboard. 3rd party systems and IoT protocols, such as MQTT, can be integrated to serve company-specific use cases. By analyzing the system data, anomalies are detected at an early stage and the systems are optimized as required. The Security Manager is available as a hybrid and cloud variant and thus supports the individual digitization strategy of the company.

Wanzl: Galaxy Gate 1.1**Fully Automated Access Gate**

The fully automated Galaxy Gate 1.1 access gate from Wanzl facilitates intelligent access management using modern sensor technology. Depending on the authentication, the gate's swivel arms open at a reduced passage width or the full extent, e.g. for wheelchair users or suppliers. This sensor system detects straight away if a person is attempting to gain unauthorised access. The complete digital gate can be flexibly configured and equipped with customer-specific readers and accessories such as facial recognition or thermal imaging cameras. The access gates are controlled using the "Wanzl Access Manager", which manages all events and status displays in real time.



Category F • Fire Protection



Ajax: Ajax FireProtect 2 Fire Detector

The detector FireProtect 2 has a dust-proof smoke chamber, a dual-spectrum optical smoke sensor, two A1R thermistors and a CO chemical sensor, and versions with sealed (10 years) and replaceable batteries (up to 7 years). Interconnect feature allows all fire detectors at the facility to activate sirens as one of them detects a threat. The detector is configured in an app and complies with EN 14604, EN 50291, and Q mark. A circulation mechanism provides the optical sensor with an unobstructed field to quickly identify products of combustion in the air. Also, the smoke chamber does not require regular cleaning, which simplifies the detector's maintenance.



Gloria: VR Fire Trainer Virtual Fire Fighting Training

The VR Fire Trainer enables a new kind of firefighting training in the virtual world. The product consists of a virtual reality headset and a dummy fire extinguisher. Using the VR headset, users enter different virtual environments and are guided through realistic exercises that simulate various fire scenarios. Additional functions such as fire spread, smoke development and material deflammability enable an unprecedented degree of reality. Both the deployment and the use of the VR Fire Trainer require no prior technical knowledge or time-consuming instruction. The exercises are designed to be almost intuitive and feedback is generated immediately after the training. No fire extinguishing agents are used. This makes the VR Fire Trainer a sustainable option.

G+H Isolierung: Fire protection app Digital Product Compass

The digital product compass from G+H brings planners and fabricators quickly and easily to the goal of their construction requirements. With just a few clicks, you can find the right solution for pipe penetration seals with Pyrostat-Uni. With the free app, planners and fabricators can quickly find the right pipe penetration seal solution to suit the requirements in just four steps. Just enter the classification (approval range and fire resistance) as well as the component and pipe properties and the insulation material. Then you immediately receive a list of solution variants. In addition, users are offered further important information and documents for their selected solution for download, such as usability certificates, installation diagrams, declarations of conformity and tender templates.



Mobotix: M73 Thermal Camera with App Fire Early Warning System

Especially in the waste management/recycling and logistics sectors, large outdoor areas with bulk materials or halls with high ceilings make fire protection difficult. Mobotix thermal imaging technology detects fire sources without contact by capturing critical temperature thresholds – often before a fire even starts. The weatherproof M73 camera can be upgraded to a thermal image-based fire early warning system without the need for an additional server by adding an easy-to-install VGA thermal sensor module and activating the Thermal Validation App already integrated in the camera firmware. Where fire detection systems such as smoke extraction systems or linear heat detectors may reach their physical limits, the Mobotix thermal imaging system shows its strengths.



Siemens: Cloud-based Services Operational Reliability for Fire Alarm Systems

With new software and hardware, the cloud-based services ensure maximum transparency, operational reliability and convenient operation – thanks to data-based analyses and cloud-based connectivity: The eLogbook enables automatic recording and documentation of fire alarm system events. By recording the data, faults or deviations can be derived and evaluated with the help of various reports. This ensures predictive, fault-free operation and thus increased system availability. Sinteso Connect also ensures mobile access via smartphone and tablet to all information of the fire alarm system – at any time and regardless of location.



Dallmeier Components: Camera Mast Sustainable In Full Length

The Dallmeier Components 6th generation camera mast not only convinces with its special features for perimeter protection, but also with its sustainability. The camera mast is made of 100% aluminum and therefore weighs two thirds less than a camera mast made of galvanised steel. The lighter weight reduces carbon emissions and saves energy during transport and installation. The light metal's resistance to corrosion means it lasts longer and requires less maintenance, reducing resource consumption and environmental impact. The camera mast is also 100% recyclable, as it is 100% remelted and the aluminum can be reused without any loss of quality. This reduces the need for valuable raw materials.

GIT
SECURITY
AWARD
2024

Siemens: Security Manager Cloud Application With People Counting

Flexible working models cause the following problem for canteens: irregular attendance makes it difficult to plan portions. Consequence: too much food is prepared and wasted. The Siemens cloud-supported security solution provides a remedy. An access control solution registers when someone gains access to the building complex. This event serves as the basis for people counting and can also be stored on the cloud. A canteen staff member can access this information in Security Manager on an easy-to-understand real-time dashboard at any time and thus see how many people are on the premises. This allows for better estimation of portions to prevent food waste.



www.security-award.com



Special Category • Sustainability



Salto: SDGs by United Nations Commitment to Sustainability

Salto Systems has committed to helping achieve the 17 Sustainable Development Goals (SDGs) as defined by the United Nations (U.N.) General Assembly. The manufacturer of electronic access control solutions is doing several things to help achieve these SDG goals. Many of the goals are specific to environmental sustainability, such as climate change, sustainable operations, responsible consumption, and product eco-design. Salto takes this very seriously and has achieved ISO 14001 certification (since 2011) and becoming 100% carbon neutral (since 2020) – a significant step in making keyless smart access technology sustainable.



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

COVER STORY

When AI Starts to Roll...

More Than Just Smart: Artificial Intelligence in Building Control

The digitalization of buildings of all sizes promises to deliver significant benefits for their owners, operators, and the individual users. It already made the automation of system controls possible using smart technology a long time ago – but when confronted by increasing complexity, artificial intelligence makes its welcome appearance. First of all, you build a digital twin of the building, such as Bosch Building Technologies does. This provides the most transparent view of all the elements of the building's technology – and shows their most efficient way of working together. GIT SECURITY spoke about the subject with Andreas Mauer, Chief Architect at Bosch Building Technologies.

Artificial intelligence is revolutionizing building control through the use of a 'digital twin' of the building

GIT SECURITY: Mr. Mauer, a home loan bank once said in its advertising that it is human nature to want to build a house. Where did your personal interest in buildings come from?

Andreas Mauer: It's actually linked to my family history. We had a structural engineering business, so we had architects and bricklayers in the family. From an early age, I used to sit next to my grandfather in the excavator. The plan would have been for me to take over the business at some point, but instead I was drawn to the world of IT. I put that down to my enthusiasm for planning and building something from nothing.

But that background presumably gave you more of an aptitude for technology?

Andreas Mauer: I certainly felt an affinity for it early on – repairing trucks or excavators, for instance. I wanted to know who switches off the light in the refrigerator, and I played with experimental building kits. My professional passion was actually ignited during my apprenticeship at the VW plant in Wolfsburg. It was there I first encountered production lines and industrial robots, and all the automation and information technology. That fostered my interest in the relationship between operational technology and IT. I went on to work in that very field for a number of years in Sweden and the USA, and I then spent eleven years in consulting before joining Bosch.

For centuries, a building has been more than just walls with doors, windows, and a roof. In more recent times, the

digitalization of building functions and building management has been bringing about huge changes. To get straight to the crux of the matter, what does your vision of a digital building look like?

Andreas Mauer: Bosch Building Technologies focuses on commercial buildings, such as office buildings, shopping malls, airports, or factories. One aspect of digitalizing such buildings is understanding the processes that take place within them. Examples of areas we are working on include parking space management and the extent to which meeting rooms or elevators are being used. Then we have to consider the conclusions that need to be drawn from this in the interests of our customers, and what these mean for the building occupants, such as chefs, canteen staff, office employees, and janitors. Essentially, it is about understanding the building as a whole, being able to manage and operate it effectively, and asking how digitalization can help with this.

That suggests a shift away from a building managed by us toward an intelligent building that largely manages itself, doesn't it?

Andreas Mauer: In the first instance, a shift toward intelligent systems means the building can, as it were, reveal itself to us, depicting the physical reality in the form of digital representations. We obtain transparency regarding the performance of the heating, lighting, and cooling systems, which we obviously want to work as efficiently together as possible.

What is driving this desire to digitalize buildings in practical terms?

Andreas Mauer: Here too it's all about the major and important issue of sustainability, to which the building sector can also make a particularly positive contribution. As I've already mentioned, the prerequisite for operating buildings in as eco-friendly and efficient a way as possible is to obtain transparency of all processes in the respective building. Service engineers play a key role here given that they are responsible for operating the building technology. To detect inefficiencies, map them out, and optimize the situation, service engineers require transparency of all processes in the building so they can take appropriate action. This is only possible when based on reliable data – and that is what we at Bosch Building Technologies can make available to building owners, operators, and occupants in the form of certain IoT services.

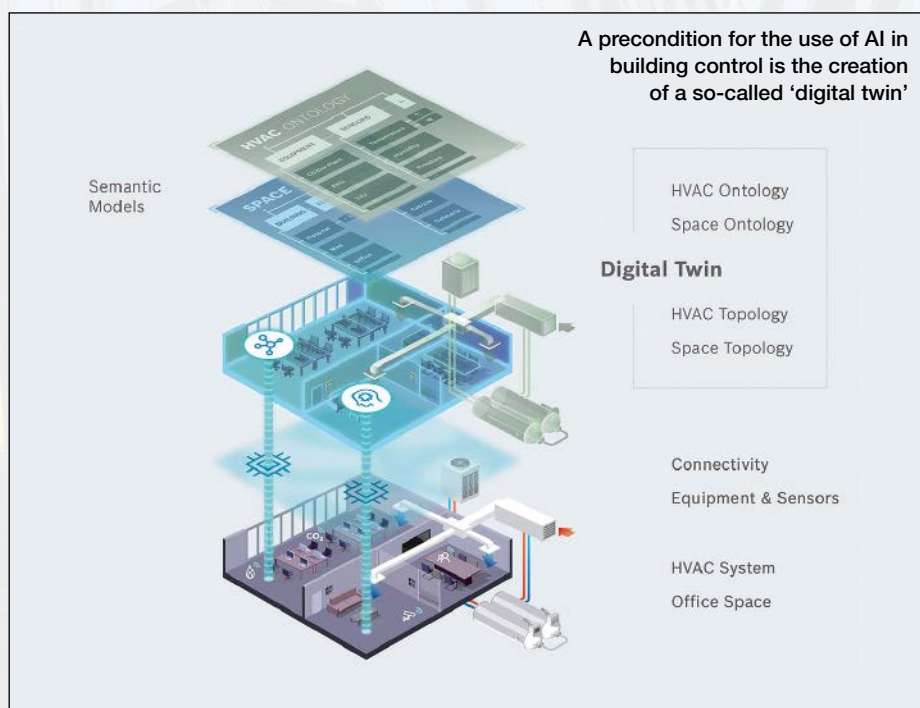
Besides this growing environmental awareness, there are also the increasing ESG reporting obligations that require building owners to provide information about the sustainability of their buildings. Added to that are the rising energy costs that are bringing us an ever greater number of orders. In other words, practices geared toward efficiency and the environment have gone from being 'nice to have' to an absolute must in the building sector.

In terms of digitalization, what role does artificial intelligence (AI) play in this context and how does it differ from smart technology?

Andreas Mauer: In a nutshell, the use of AI becomes an attractive option at the very point where smart technology reaches its limits due to the complexity involved. I would describe smart technology as expert know-how and test results that have been converted into rules for the control automation of building technology – things like automatically switching off the lights under certain circumstances, etc.

However, these relatively simple rules are no longer adequate to deal with the complexity resulting from the combinatorial analysis of different building areas and systems in a large, modern building. This extends from the lighting in the entrance area and access management through to heating, ventilation, and air conditioning. If AI is to be used in building management, it is first necessary to create what is referred to as a digital twin.

Our approach at Bosch Building Technologies is to transfer relevant systems in a building and the topology of the building itself into semantic models called digital



ontologies that the AI can subsequently evaluate. It is then possible to obtain answers to important questions, such as which rooms here at the Grasbrunn location have a temperature that deviates by two degrees from the required level and why that is. That's a quick way to establish whether everything is working as it should, or whether maintenance or repair work is required to optimize the existing technology. This benefits the environment and also saves money. The results from all our digital twin's measuring points are recorded, so we can also incorporate past results into the analysis of optimization potential and obtain a more comprehensive and accurate picture.

So AI can answer complex questions relating to building operation?

Andreas Mauer: That's right. In our digital twin, AI can detect issues, such as system anomalies, and ascertain, for instance, that certain room temperatures are abnormal for the relevant time of year. To use the technical jargon, we project domain knowledge into ontologies that we turn into a digital agent in a digital execution context, thereby creating a learning system that uses deep reinforcement learning. In other words, we convert today's expert knowledge into a digitally executable format with a futuristic master of optimization. This is where AI really starts to roll and deliver transparent benefits.

Bosch launched its Nexospace digital service suite a while back. To what extent does it already match your vision?

Andreas Mauer: Nexospace is based on a whole series of digital building blocks, including the building's connectivity with its systems, which then results in system integration in the relevant project context. Using the building's digital twin, this integration can be standardized and relevant domains can be viewed together at any time. That means we can continuously monitor, learn, predict, analyze, and – in the future – also simulate.

As I see it, there's a good chance of enhancing the technology in a way that will enable us to successfully model scenarios such as the following one: If the state premier were to announce a visit to a company the next day, accompanied by a hundred people, it would be possible to simulate in advance what the requirements would be in terms of tables, catering, heating, ventilation, and air conditioning. That would



Andreas Mauer, Chief Architect at Bosch Building Technologies

involve everything from management of the building technology to proactively procuring spare parts and arranging the availability of a service engineer with the shortest possible distance to travel.

Suppose you receive an order from a bank building in Frankfurt, how long would it take to create a digital twin?

Andreas Mauer: That depends. If the customer is already using building information modeling – BIM for short – a process that produces a digital representation of a building, our tools can create the digital twin very easily on this basis. The whole procedure is then highly automated. It's a whole different matter if the building plans are on paper. At present, formats of this kind still

have to be laboriously converted into formats that the machine understands. In the future, it is envisaged that AI will help with this 'onboarding', using cognitive models that obtain the relevant information from PDF files or scans of paper documents. We are currently working on an 'onboarding co-pilot' into which we are incorporating artificial intelligence to provide this transfer service. That will be particularly useful, because BIM is still not in widespread use and, even where it is used, security and safety technology is often not included.

Physical reality in the form of digital images – and with them, transparency of the performance of all the systems that should work as efficiently as possible together ►

Things are far more advanced in Scandinavia and the UK where all new planning must be compatible with BIM.

Can you give us an idea of the benefits of these innovations for individual users?

Andreas Mauer: In this context, we make a distinction between the three big Os – that is to say the owner, the operator, and the actual occupants in their different roles in the building. Owners want an attractive property in their real estate portfolio. They are keen to retain as many tenants as possible and obtain many new ones. Also related to this is the incentive of being able to plan their investment, in other words, determining where they should invest, where they should build something new – preferably, planned or renovated in a sustainable way based on ESG criteria. For operators, the important matter is whether something might be broken, whether it's too warm or too cold, etc. They must also regularly carry out maintenance work on equipment, such as fire detectors, and ultimately ensure the occupants are happy. Things such as accessibility, intelligence, how easy it is to book a meeting room, and whether this can be done via an app, are especially important to young people working in a building. Connectivity is also a key factor for them.

With our Nexospace digital service suite, we have made a start on winning over all three of these groups. A digital building has a motivating effect on the occupants and makes things more convenient, efficient, and sustainable for owners and operators. We can achieve all that if we take a holistic approach to the concept, transparently

modeling the processes followed by the occupants and the interaction between the systems, and all the while evaluating the physical reality digitally. This applies equally to everything from a small school building to an office skyscraper.

We're conducting this interview in the form of a video meeting and I'm certainly not at the office. Do you think these issues have become less relevant, especially in the case of office and administrative buildings, as a result of the Covid-19 pandemic and the increased number of people working from home, working remotely, etc.?

Andreas Mauer: The world of work has indeed been completely transformed. Hybrid working and the use of smart and intelligent systems are making it possible for areas of buildings to be used more flexibly. For example, you can decide to rent individual building areas as required. The considerations when it comes to investing in buildings for commercial use, in particular, are therefore changing a great deal. That also has implications for security and safety technology, as more flexible usage also changes the security and safety requirements. We want to reflect all that at our new headquarters in Munich too, which we will provisionally be moving into at the end of this year. Given that we will be working there on a carbon-neutral basis, we are also acknowledging our corporate social responsibility.

How much progress have German speaking countries made with regard to the digitalization of buildings? No doubt the USA and China are well ahead?

Andreas Mauer: In the USA, although not everywhere there either, there are areas where people are more ready to experiment, especially when it comes to IoT. The same applies to certain centers in China that have lighthouse projects. Overall, it has to be said that the commercial building sector has tended to adopt a conservative approach. However, a great deal is currently happening in the building sector due to the desire for sustainability, which is a strong driving force.

In Europe, incidentally, the Dutch, the British, and especially the Scandinavians are more active in this regard than German speaking countries. In Germany, Austria, and Switzerland there is still a relatively large amount of skepticism, particularly regarding the question of whether an investment is still beneficial for the actual building owner – or occupants who arrive later on. This means that in those countries we are under more pressure to provide evidence of the benefits.

We've spoken a great deal about the vision. How far into the future do your plans extend, what major steps will you be embarking on next, and with what kind of timescale?

Andreas Mauer: All the issues we've discussed are absolutely core elements of our strategy at Bosch Building Technologies. We want to build more and more perfectly integrated intelligent systems. We are always looking ahead, building things up with our customers bit by bit. The pursuit of sustainability lends more weight to the claim that environments must change to serve their purpose.



CONTACT

Bosch Building Technologies
 Grasbrunn, Germany
 Tel.: +49 89 6290 0
 info.service@de.bosch.com
 www.boschbuildingtechnologies.com

INTERVIEW

High Security Experience

Combining Flawless Security With Intuitiveness

French specialist in identification solutions STid is definitely on an impressive growth curve. For many years in a row the company has shown increases in sales volumes and financial results. A clear vision on market needs and an ambitious and matching innovation strategy are major drivers behind this success. GIT SECURITY has asked Vincent Dupart, CEO of STid, about their success story and the upcoming IFSEC event, where STid will be present.

GIT SECURITY: How do you explain STid's success?

Vincent Dupart: STid is growing at a record pace with 120% growth over the last two years. We are present in more than 60 countries on 5 continents. Our vision on security apparently fully meets the expectations of the market, the need for freedom of choice with open technologies in particular. We guarantee organizations independent

and autonomous management of their security. This freedom is vital for STid: Our customers are not locked into a solution or restricted by proprietary technologies. We are also known for our high security standards. We provide end-to-end security between the card and the reader (with Mifare Desfire EV2/ EV3 technologies and Vcards of STid Mobile ID), and between the reader and the controller/LPU with systems capable of supporting OSDP and SSCP protocols.

Innovation plays a key role in this growth. What is your vision?

Vincent Dupart: We have always believed in releasing technological solutions that support our users in doing their jobs or live their lives. The QR code or four advanced function buttons with our OSDP touch screen reader are good examples. We never release any product without seriously considering both usability aspects and security aspects. Security technology should not be in the way of people and people should feel supported by the technology.

When we released STid Mobile ID, it was not just a solution that would allow you to use your phone as an access control credential, but it would offer a new experience of identification and authentication. All you need is to tap your phone, or use it hands-free or you authenticate your identity by biometrics. Our customers can decide how to best adapt the solution to their needs and requirements, related both to usability and security. Indeed, our solutions have always combined two contradictory needs: The necessity of a seamless user experience and the require-

ment for flawless security by the security departments. And, of course, we always made sure our high security solutions are scalable, future-proofed and can easily adapt to the continuous evolution of customer needs.

So what do you showcase at IFSEC this year?

Vincent Dupart: Our approach is focused on user needs and on the benefits that the user can get from high security. At this year's IFSEC, various areas of demonstrations will highlight the challenges of security departments: How do you ensure that the access control solution deployed is secure? What level of security should I choose? What exactly do we mean by simplified access management?

Visitors will experience live demos of high security identification, based on the power of our STid Mobile ID platform, the comprehensive range of scalable and high security Architect readers and the performance of our Spectre range. We will also demonstrate why our identification solutions are scalable and how we support the migration towards intuitive and secure solutions with our 125kHz module. I think visitors will see great demonstrations of combining flawless security with intuitiveness.

IFSEC · ExCeL London, May 16–18
Booth IF.2820

CONTACT

STid
Greasque, France
Tel.: +33 442 126 060
www.stid-security.com/en

BUSINESS MANAGEMENT

Opportunities Seized

In Conversation with
Thomas Lausten, CEO Mobotix



Thomas Lausten,
CEO Mobotix

Konica Minolta has been a majority shareholder in Mobotix since 2016. The two companies have used this connection to work more closely together and to jointly develop solutions. Mobotix solutions are offered by the Japanese company worldwide, and Mobotix CEO Thomas Lausten sees a “fantastic opportunity” for his company to attain long-term growth. GIT SECURITY spoke with him about the development of the cooperation of both companies.

GIT SECURITY: Mr. Lausten, Konica Minolta invested in Mobotix in 2016. How would you sum up the past six years of belonging to this Japanese optical, medical and office technology company?

Thomas Lausten: We have built up a close cooperation with Konica Minolta over the past six years. It is spread across numerous activities – for example, the joint development of AI-based video solutions that can be sold by both partners of Konica Minolta as well as Mobotix partners. They are aimed above all at our industrial, healthcare, and retail customers but also those in other industries.

In addition, we have also started a partnership with Konica Minolta that allows them to offer Mobotix solutions to their customers worldwide. This was carefully tailored to our sales channel and partner strategy to avoid any conflicts. That is a fantastic opportunity for Mobotix to secure long-term growth and allow further investment in research and development.

How is the integration of Mobotix and Konica Minolta solutions going?

Thomas Lausten: We have analyzed the market developments and trends for the coming year in detail. The heightened

concentration on quality, cybersecurity and artificial intelligence matches our vision of developing video solutions to standards that exceed the capabilities of human sight. Our new product strategy allows us to offer complete video solutions that align with our well-known focus on decentralized technology – but that also work together with centralized solutions, our hub platform for example. In general, we select our developments to meet the specific needs of our customers in selected vertical markets.

In your opinion, what are the next technology trends going to be in the near future – and what innovations can we expect from Mobotix and Konica Minolta?

Thomas Lausten: We estimate that the global trends will be determined by further optimization of image quality, edge computing and AI solutions, whereby user friendliness and data quality will be foremost. Vaxtor is a good example of this trend. Data is precisely read, even when it originates from a moving vehicle. Video surveillance solutions in general will expand beyond just classic security solutions to being a key tool, for example for customer analysis in the context of production processes, preventative analysis

purposes, etc. The ‘Forxai’ platform from Konica will provide further developments in these sectors – and the R&D at Mobotix is concentrating on this too.

Are there already special solutions in which the products of Mobotix and Konica Minolta are mutually integrated?

Thomas Lausten: Yes. We began a number of joint development projects during the last few years – in particular in relation to the P7 camera platform and ‘Activity Sensor AI’ object recognition. On the whole we like to take new approaches to innovation in selected vertical market and developments, for example for industry, the public sector, the energy and healthcare markets. Our business development managers work closely with customers in these sectors and feed their ideas directly to our R&D teams in Langmeil and Madrid where they can be further developed. We want to further strengthen this type of communication.

CONTACT

Mobotix AG

Langmeil, Germany
Tel.: +49 6302 9816 0
info@mobotix.com
www.mobotix.com

BUSINESS MANAGEMENT

Time for a Triple

i-PRO, Mobotix and Konica Minolta Strengthen Strategic Collaboration

i-PRO, Mobotix and Konica Minolta announce that they will strengthen their strategic collaboration by combining their products. This collaboration will allow the companies to mutually leverage the strengths of the portfolio offering of i-PRO and Mobotix, both specialists in imaging and sensing technologies, and combine their products with Forxai, a cutting-edge imaging IoT platform of Konica Minolta.



© Wilm Ihlenfeld - stock.adobe.com

i-PRO offers a wide range of video surveillance products incorporating edge AI technology. Together with the renowned reliability and durability of Japanese products, that has enabled the company to increase its presence in the global market. On the other hand, Mobotix offers decentralized processing (edge computing) IP cameras worldwide, which satisfy the rigorous durability standards

required for made-in-Germany products. With their high-end thermal imaging cameras, they have the critical ability to accurately detect temperature anomalies and variations.

What Kind of Products Can Be Expected?

Mobotix, i-PRO, and Konica Minolta jointly developed a system by visual and thermal

cameras in 2020. The new strategic cooperation says that Mobotix will use selected high-performance i-PRO camera hardware. Combined with unique Mobotix DNA feature sets on an ODM/JDM (Original Design Manufacturing/Joint Development Manufacturing) basis, with the first product scheduled to be launched in 2023, the hardware will be compatible with the existing Mobotix and Konica Minolta system landscape.



GIT SECURITY exclusively asked Gerard Figols, Senior Vice President, EMEA Region, at i-PRO how the partnership came about:

Gerard Figols: “We’re proud to see other market leaders in image-based intelligent services relying on i-PRO products and give EMEA customers access to value-adding usage of video technology for data insights. The partnership first started during the pandemic, when all three companies worked on a joint approach, leveraging their strength to provide measurements for ‘infection risk reduction’. Now we are seeing this initial initiative expand into other areas where i-PRO products can be incorporated into market opportunities for solutions utilising AI sensor technology.

This makes the strategic collaboration a clear example of i-PRO’s open policy and the move of the surveillance and video market towards powerful edge AI applications. i-PRO is a hardware manufacturer focusing on the development of powerful edge-AI cameras, our field of expertise. Different to our legacy from Panasonic when the approach was to develop and maintain the whole vertical solution, since the establishment of i-PRO we have actively endeavoured to rebuild partnerships. This reorientation towards our open policy has become the major driving force for our market growth, enabling i-PRO EMEA to grow roughly three times faster than the overall CCTV market. Together with Mobotix and Konica Minolta, we look forward to giving more customers access to this rapid business growth, and i-PRO’s high quality open edge-AI hardware.”

The collaboration will strengthen solution offerings for the vertical markets – e.g. industry & production, government, healthcare, logistics – in a targeted manner with performant end-to-end solutions. It enables customers to meet their needs in terms of improved processes, higher profits, and support more social safety and security in society.

AI in Video Surveillance: Detection, Analysis, and Prediction

The surveillance and video solutions market now demands much more than video monitoring and post-event verification. Detection, analysis, and prediction using AI, and the provision of data services that leverage it, are increasingly coming into focus as new growth areas.

Connecting i-PRO and Mobotix systems with Konica Minolta's Forxai imaging IoT platform opens up integrating and using various other devices and systems through open partnerships. Thus, the companies hope to develop unique solutions based on Konica Minolta's state-of-the-art imaging AI technology, integrate the technologies

of Forxai partner companies, expand their customer base, and continuously utilize customer data.

Shohei Ozaki, COO of i-PRO, said, "Since its establishment in 2019, i-PRO has been building collaborative relationships with partners around the world, and in 2020, entered into a partnership with Konica Minolta and Mobotix. Konica Minolta, Mobotix, and i-PRO are pioneers in image-based intelligent services and are reputed for the quality and reliability of their products. I believe that this partnership will help our extensive lineup of products incorporating edge AI technology contribute to solving a wider range of social issues."

"Mobotix and i-PRO share many common values and have matching quality standards, especially regarding performance and cybersecurity. Together with Konica Minolta, we can bundle our competencies and offer innovative solutions including thermal technology and AI for our central vertical markets," said Thomas Lausten, CEO of Mobotix. "The focus of video technology on data usage is a common starting point for the cooperation partners. Intelligent video technology is much more than delivering safety. It is

about effective operations, increasing sales, and making people's lives easier."

Toshiya Eguchi, Konica Minolta's Executive Vice President and Executive Officer Responsible for Technologies and Imaging-IoT Solution Business, commented as follows. "We are looking forward to this intensive partnership. Through this collaboration among Konica Minolta's imaging IoT platform Forxai, Mobotix and i-PRO, we are confident that their competencies, high-quality standards, and strengths complement each other perfectly. The cooperation will be a win-win-win for the three companies. The biggest winners, by far, will be our customers and users."

CONTACT

i-PRO EMEA

Amsterdam, The Netherlands
<https://i-pro.com/eu/en>

Mobotix AG

Langmeil, Germany
Tel.: +49 6302 9816 0
info@mobotix.com
www.mobotix.com



PROTECTION FROM EVERY SIDE

Long range detection with REDSCAN PRO

The award-winning OPTEX REDSCAN LiDAR series just went one better, with a new detector featuring its longest range yet. The REDSCAN PRO can accurately detect intruders and moving objects up to 50 x 100m away – making it particularly well suited for those responsible for protecting the highest security sites. And by creating rectangular, high resolution detection patterns, there are no 'gaps', so everything from facades to fences, ceilings to roofs can be covered. For the installer, the sensor's intelligent multiple zones logic means each detection zone can be independently configured, while its camera module brings visual assistance for configuration and post-alarm analysis. The alarms and video stream can all be configured via ONVIF.



www.optex-europe.com

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

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



Gemos 5 is BKS's centerpiece in security management

PSIM

Security Management Best Practice

Securing Companies and Managing Resources with Software

In an interview last January, we introduced Gretsch-Unitas and BKS, including a closer look at the role of the Gemos building and security management system. GIT SECURITY has now spoken again with Fedja Vehabovic, Head of Sales International Business at BKS, about the new Gemos 5, the company's centerpiece in the security management sector.

GIT SECURITY: Can you briefly summarize for us again what role Gemos can play in the security architecture of companies?

Fedja Vehabovic: The new Gemos 5 has interfaces to almost all security systems available on the market and can network these systems, as well as all GU Group products, with the building management system. It is of central importance for us, our customers and the implementation of projects. Last year we introduced two advanced modules, Gemos advanced PSIM and Gemos Access, both of which work as independent systems and function as individual independent security systems. However, they can also be operated as one security system with the PSIM and access control fully integrated. Both systems share the same database and provide a logical, system-integrated solution with PSIM and access control system architecture. Even though they operate separately, both platforms

can be synchronized into one system at any time by adding a single software license. This flexibility makes the systems unique.

What has been improved in the latest update of the Gemos 5 PSIM?

Fedja Vehabovic: Both systems are web-based and Gemos 5 advanced PSIM and Gemos access are now 100% integrated with each other. With the HTML5-based module, we are future-proof and technology-independent in video. The HTML5-based module is the basis for the new video module solution. It provides an interconnectivity platform for all types of video management systems, regardless of whether the VMS supports new formats or not. For cybersecurity, end-to-end encryption according to TLS 1.3 -AES256 and the BSI specifications is important and that we work with the next generation of SQL databases. The Enterprise

Edition of the new Gemos 5 PSIM also offers technically mature and proven redundancy features and real-time synchronization of alarms and event messages across multiple enterprise sites.

What measures did you take in the meantime to open up even more possibilities for users?

Fedja Vehabovic: In the last interview, we already indicated that the requirements of Smart City and Smart Buildings are showing us the way. As you can now see very nicely via our newly designed Graphic User Interface, we have succeeded in integrating further data from the building control system into Gemos 5 via BacNet or IoT connections. The BACnet network protocol was developed specifically for building automation and control systems communication for applications such as heating, ventilation and air conditioning control, fire protection and security systems. Through integration, we make information accessible that goes beyond traditional security information such as alarms and video information. At the BAU trade show in Munich, we will demonstrate how we integrate IoT signals and information from building technology and automation into the management system. Using the example of a hotel, you can see there how we make this data usable. We can draw on experience in the Arab region, where we have implemented several projects in which integration via BacNet or IoT also works well for larger building complexes. The focus there is also on energy optimization, among other things. The information comes together in the FM Expert module, a dashboard for statistics and analysis. You can see all the evaluations there and, for example, analyze and visualize power consumption. With these BacNet and IoT integrations, we have put together a package that puts us in a very good position with Gemos for smart city and smart home applications and, in addition to the tasks directly relevant to security, we can also offer solutions for building and facility management.



Fedja Vehabovic,
Head of Sales
International Business
at BKS

One of the classic security tasks is video integration. Some manufacturers of video management systems and PSIM find it difficult to integrate video systems from Chinese manufacturers, either from a technical point of view or due to political considerations. You do offer your customers a deep integration of Hikvision's HIK Central and also Dahua's DSS video management system.

Fedja Vehabovic: Yes, we have invested in a good technical integration of these two systems and offer our customers to use our new software drivers for these systems if they wish. We offer a vendor-neutral management system and we are guided by the wishes of our customers and in this context we have already had project requests for the integration of Chinese systems. The decision for or against a certain video system is usually made by our customers before they approach us.

In audio and telecommunication systems, communication runs via special protocols from leading providers. Why is the integration of such systems important and helpful?

Fedja Vehabovic: The most important integrations for PSIM include the integration of fire alarm systems, video management systems, intrusion detection systems and access control systems, plus usually perimeter protection systems and, as already discussed, building technology systems. In my view, however, some systems lack a clean integration of telecommunications, with the exception of classic public address systems like Schneider Intercom or Commend. In the event of an alarm, a call to a responsible person or a whole series of people may be necessary, usually via a Voice-over-IP system. With the new connection options of Gemos 5, a call can be automatically initiated in the event of an alarm, and this is done via a so-called Generic SIP protocol from Cisco. Cisco is the market leader in this area and their protocol is also understood by many other vendors. We have worked with Cisco and worked out an integration. By integrating their Generic SIP protocol into Gemos, we now ensure that everyone can be reached via the phone to help in the event of an alarm and we document that they receive the right message.

So you can say that with management systems, in addition to an evaluation of the classic functions, the user interface is becoming more important and the use of the systems for neighboring disciplines is becoming more important?

Fedja Vehabovic: Yes, customers are asking for ease of use because it's no longer just classic security personnel accessing the systems, they no longer want silos with multiple separate systems, and they want to solve more and more tasks with the systems they have. For us, solving security tasks is the duty, but we need to add value in building management, communication and energy saving. In summary, I see today's building management systems not only as a central element for alarms and their processing, but also as an open platform where customer wishes for action plans or the design of the interface can be implemented independently of the system. In addition, the modern connection of building control systems and IoT peripherals enables the PSIM of today to make a significant contribution to the topics of smart city, smart home, energy savings, energy monitoring and cost reduction with the evaluations described.

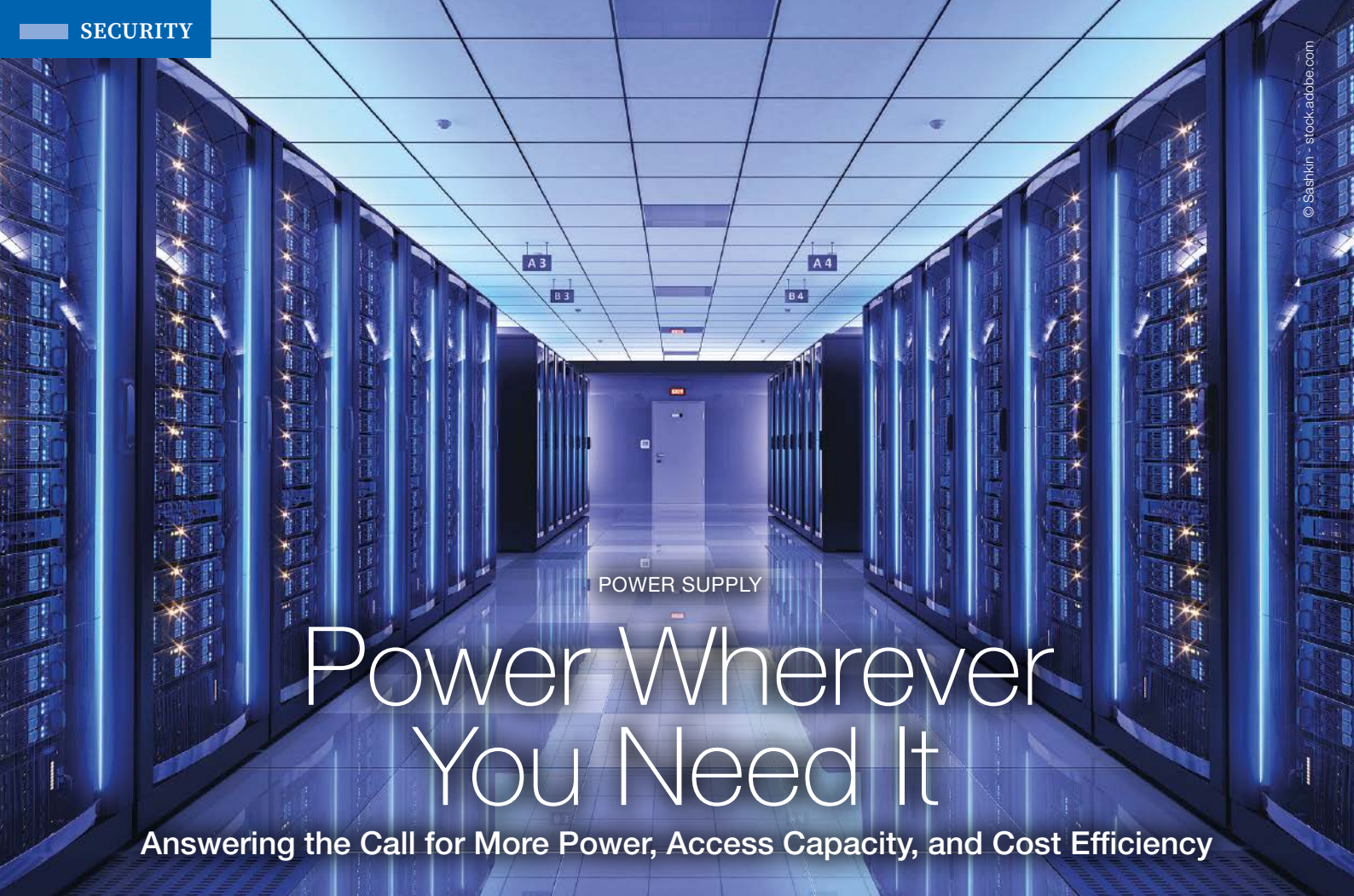
CONTACT

BKS GmbH

Velbert, Germany

Tel.: +49 2051 201 0

info@bks.de · www.g-u.com



Power Wherever You Need It

Answering the Call for More Power, Access Capacity, and Cost Efficiency

There's an interesting confluence of trends in today's security market, whereby security professionals are pressured to do more with less, while management pushes them for better ways to protect people, property and assets, and mitigate risks. The development of new and improved ways to distribute more power, and design and deploy high-capacity, integrated system solutions is helping both security integrators and end users address these new challenges, while lowering costs and increasing overall security.

Cost savings attributed to these new power and integration solutions are largely due to reductions in the amount of time and labor required to configure, assemble, and bench test new systems, as well as the time required to install and implement systems on-site. Power solutions, like 802.3bt PoE, have the ability to be converted and deliver power for physical security system deployments, and new maximum density access and power integration solutions require much less wall and rack space, conserving valuable real estate while increasing system capacity. Let's explore the benefits of both...

More Power Wherever You Need It

Venues that occupy expansive amounts of space, such as warehouses, airports, malls, multi-housing units, and campuses, often require the installation of equipment closets in remote locations where AC power is not always readily available. With 802.3bt PoE, system integrators can leverage low voltage installation and wiring methods to

effectively eliminate the need for dedicated AC power circuits and related expenses. Instead, security devices can be powered over standard cabling without the need to run dedicated electrical wiring.

This latest PoE standard, 802.3bt PoE – also known as 4PPoE or 4-Pair PoE – is truly a game changer for the security market, enabling system installers to install power hungry IP devices easily and cost-efficiently. Simply put, 802.3bt PoE uses all four pairs of conductors to provide up to 90W per port, which is a substantial increase in the maximum power over previous PoE standards. Power management is achieved using communication between the devices over the same connection cable. 802.3bt is also backward compatible, allowing users to upgrade their power source to this newer standard while using existing PoE devices, providing additional savings over the total cost of ownership (TCO).

By eliminating the need for high voltage inside the enclosure, 802.3bt PoE also does away with the cost of electrical permits,

cabling, and dedicated conduit. The low voltage cable used for power can run in the same cable trays and paths as other network cabling which, for service and maintenance, eliminates the need for regulatory safety precautions, such as lock-out tag-out.

Another important feature of 802.3bt PoE is that there is no voltage present on the cable until it is plugged into a powered device and a handshake occurs. Unplugging the ethernet cable from the PoE-driven power supply is safe. Once the cable is plugged back in, the handshake is performed with the power source and PoE is delivered to a powered device.

The ability to use CAT6 cable to distribute both power and bi-directional data represents another significant cost-saving advantage. First, it allows the use of existing CAT6 infrastructure, which is now typically a mainstay of all new and/or renovated structures, without incurring the cost and labor of pulling new cabling. It also allows system designers and installers

to install access, video, and other security devices wherever there is a cable feed, enabling fast and easy scalability when and if the need arises.

Using 802.3bt as an input to a power supply/regulator can simultaneously provide multiple output voltages, giving installers more flexibility when selecting and deploying devices. These new PoE driven power supplychargers deliver a combination of voltage outputs, such as 12V DC and 24V DC simultaneously, to power a wide range of access, video, security, and fire devices.

Enhanced system troubleshooting is another important benefit of advanced 802.3bt PoE power supplychargers. Products that report diagnostics via network communications can help determine the cause of a system failure. This information can effectively reduce system downtime, eliminate service calls, and provide faster response times to help keep security systems up and running. Advanced power and transmission solutions with network communications can also provide early detection of potentially failing devices, permitting service providers to take proactive measures to avoid system interruption.

The combination of faster design, installation and system troubleshooting and servicing translates into greater ROI for integrators, as installation labor costs and off-site service visits can be significantly reduced – and lower TCO for end users.

More Access and Power Integration

Access control is the new security imperative as organizations cope with changing work schedules, increases in crime, and heightened potential liabilities. It's the perfect environment for the new genera-

tion of maximum density access and power integration solutions, which accommodate more access control hardware from leading providers with or without power. Available in high-capacity wall and rackmount models, these integration solutions dramatically increase access system capacities while lowering costs.

The simple yet pragmatic design of pre-configured or customizable access and power integration solutions makes an otherwise arduous task faster, easier, and extremely cost-efficient – all of which are tangible benefits for both end users and installers. Online configurator tools make the design process even easier, if not all but foolproof. Plus, the ability to test systems prior to deployment greatly reduces installation time and overall costs.

Space saving is a significant benefit provided by maximum density access and power integration solutions. In the past, multiple enclosures or racks were typically installed to house access control equipment, power supplies, and accessories. This requires a significant amount of valuable wall or rack space, versus an all-in-one access and power solution that provides ample room for all the required access and power products, and backup batteries.

Applications for maximum density access and power integration solutions include large venues with multiple doors commonly found in large commercial/industrial venues, hospitals, and multi-use properties. The deployment of these systems can greatly reduce the number of enclosures and space needed to provide the necessary access control to secure a facility.

Let's compare a conventional 240-door access system with access control hardware in one enclosure and power in another, versus using a new maximum density access and power integration solution. The conventional system would require up to 30 enclosures employing 8-door access controllers and another 15 enclosures for power – totaling 45 enclosures. A maximum density access and power integration solution that accommodates up to 24 doors with power per enclosure reduces the number of enclosures to 10. This saves significant time, labor, and installation space, and makes servicing the system much easier by combining power and access control in far fewer enclosures.

In this new age of security where more is expected for less, it's easy to see why new power and distribution solutions, combined with next generation maximum density access and power integration solutions, are finding favor with system designers and installers, and the end users they aim to please.

Author

Ronnie Pennington
Director of Sales
for the Americas



CONTACT

Altronix Corporation
Brooklyn, NY USA
Tel.: +1 718 567 8181
info@altronix.com
www.altronix.com



ASSA ABLOY
Opening Solutions

Unlock savings of
up to 80% with Aperio®
wireless access control*

Cut your costs – and do your
bit without doing a lot.

*See the full calculation and
Download our free Solution Guide:



Experience a safer
and more open world

ACCESS CONTROL

Going to the Office Today?

The Role of Access Control in Making Work More Flexible

Office-based working, telecommuting, work-from-home (WFH), co-working spaces and hot-desking: all these habits and schedules are now part of the mix, almost everywhere. As the fixed 'working day' declines, people come and go at different times, with changing schedules, irregular patterns, and a mix of different places where they work. This presents a challenge which many existing access control systems and workflows were not built to meet.

Many of the old certainties are replaced by questions. How can I now ensure the right people – and only the right people – get seamless access when they need to? How do I foster a sense of comfort and safety among workplace users, and peace of mind for the facility managers, even as people come and go in less predictable day-to-day patterns?

Same Demands, New Challenges

Access control has always been critical for building security. Changing work patterns, however, mean monitoring and filtering who can go where and at what times is becoming even more essential. This control ensures staff and visitors move safely

A recent Future Forum survey found that 58% of knowledge workers already follow a hybrid work pattern: “Flexibility is the expectation – and increasingly the norm,” the report concludes.* (See QR code in box.) Further growth in flexible working is a certainty. These changing work patterns make flexibility in security even more critical. Choosing the right access control solution makes a big difference.



Wireless electronic locks provide reliable security, even with ever changing working hours and irregular staff attendance patterns

* Make your work-space ready for a new generation:



** Download your free copy of “Modernizing facilities management” today:



*** To learn more about how access control can support flexible working, a solution guide from Assa Abloy can be downloaded at:



and conveniently into and around the workplace.

Mechanical lock-and-key security has established centuries of trust. It works, but it is neither flexible nor intelligent enough to meet these new challenges. Electronic access control, on the other hand, has this flexibility. And the quickest way to implement it – to make a fast, efficient move to secure hybrid working – is wirelessly.

The Wireless Advantage

The control enabled by wireless, battery-powered door locks managed by intuitive software gives facility managers the power to issue more fine-grained access permissions. Employees, contractors, cleaners, event attendees and visitors can all get

the access they need – no more and no less. Credentials may be programmed to unlock doors during specific timeframes, so staff enter only when scheduled, for example. Facility managers can regulate daily access to keep building occupancy within capacity.

Last-minute or emergency changes to access rights are no problem, because credentials have flexibility that mechanical keys do not. With remote management functionality, office managers can perform any operation even if they are away from the premises. In case of an emergency, they could lock or open doors remotely, for example.

Mobile credentials offer even more: they can update over the air in an instant,

via software which can provide control in real time, from anywhere and around the clock. “An access system which offers this degree of control is much easier to adopt than many business owners and managers imagine,” says Mikel Gaztañaga at Assa Abloy Opening Solutions. “It can provide the backbone for more efficient management of people and their security as work becomes more flexible. The right solution should also integrate with important flexible office services like support ticketing, room bookings and more.”

Wireless, battery-powered devices are fast to install and run without any mains connection. They are easy to retrofit without damaging walls and consume little energy during use, unlike equivalent wired doors. Their cost effectiveness enables them to be fitted at many more doors than would be feasible with any alternative solution.

Flexibility for a Flexible Co-Working Space

Flexible access to offices is a priority in the co-working sector. As ‘fixed’ space rented by corporations begins to fall, co-working spaces are expected to keep growing. In one recent survey, 69% of large companies “identified flexible office space as the most in-demand amenity of the future.”**

To stand out from the competition, the founders of ULab in Alicante wanted the latest in security, accessibility and design to create their 21st-century business center.** Flexible and wire-free, a SMARTair system gives ULab real-time access control via credentials that are easy to program and reprogram. ULab managers chose Openow, the mobile key solution for SMARTair. It gives workspace residents an option to carry virtual keys on their smartphone. It is slick, efficient and gives users and managers even more flexibility. The software manages access for 100 daily users. They also have the flexibility to welcome many more visitors when the event space is full. “In addition to regular daily traffic, weekly traffic can almost multiply by ten if an event is held,” says Enrique Burgos Pérez, Director at ULab. “We needed an access control system as flexible and convenient as SMARTair.”

CONTACT

Assa Abloy Opening Solutions EMEA

Tel.: +49 30 8106 2970

Thomas.Schulz@assaabloy.com

www.assaabloyopeningsolutions.com

Exoskeletons: Tomorrow's Ergonomic Tools at A+A 2023

Exoskeletons focus on the two body zones suffering most from pain caused by physical work: the back and the shoulders. The market for exoskeletons is growing: The market for industrial exoskeletons is expected to grow by more than 40% over the coming years and reach over \$400m by 2025. These physical assistants have become very versatile: Diverse pain points and risk zones are relieved or supported by exoskeletons and soft suits; active systems are also equipped with data interfaces. There are also products for thumbs, wrists and elbows, applying well-established orthotic care principles. These and other products will be at A+A from 24 to 27 October 2023 in Düsseldorf, Germany. The “ExoPark” will be waiting in Hall 5 to see and even personally try out many different systems on realistic job tasks. The WearRAcon Europe Conference 2023 will also be held at A+A.



www.aplusa.de

Edge-Computing Facial Recognition Camera

Vivotek has released its first-ever facial recognition camera that integrates edge computing to help enterprises quickly identify the gender and age of people in the video at the edge, as well as those who are wearing masks. The camera has a built-in memory card with facial data storage of up to 10,000 profiles and achieves a 99% accuracy rate of detection. The camera can also target specific images for real-time alarming and its software and hardware meet the standards of the U.S. National Defense Authorization Act. Built into the software of the FD9387-FR-v2 camera is the SAFR Inside AI facial recognition platform developed by SAFR from RealNetworks, which is combined with the camera's powerful edge-computing capability to significantly enhance the efficiency of analysis. The camera's functions include real-time facial detection and tracking, early warning of strange faces, and image privacy mode for sensitive areas, avoiding sharing of the video with a third party.

www.vivotek.com

Large Camera Count Bridges

Eagle Eye Networks has launched two new bridges, models 901 and 701, that can connect up to 300 cameras to the cloud. These are suitable for customers with sophisticated networks who need large camera deployments at a single location. The bridge connects the customer's existing or newly installed cameras to the Eagle Eye Cloud, providing them full SaaS for video surveillance. Equipped with powerful processing, the bridges can perform video analytics, AI, and license plate recognition. They dramatically reduce the number of components required for large deployments, with the 901 supporting up to 300 4-MP IP cameras and 10 LPR streams, and the 701 supporting up to 150 4-MP IP cameras and 10 LPR streams. Designed for simple installation and reliability, the new bridges are 1U rack mounted and will be available starting April 30.



www.een.com

4x3

Special Focus

Mobile Access Control

1. Why do you consider mobile access control superior to other methods and what benefits can a user derive from the system?
2. Is mobile access now widely accepted in the security industry or are there still concerns about the use of the technology?
3. Please describe a success case where one of your mobile access control solutions was used for a high security or critical infrastructure project.



Joachim Mahlstedt

Commercial Director DAS
at ASSA ABLOY Opening
Solutions EMEA

www.assaabloy.de

1. The convenience benefits are clear. Identical benefits have already brought a mobile-first ethos to banking, travel booking, food delivery and many more sectors. From a business perspective, too, the option for facilities managers to use their own smart device to issue, amend or revoke an employee's mobile key brings added flexibility. It frees security staff from their desk and its admin PC. As work patterns become increasingly fluid – IBM estimates the number of mobile workers at 1.87 billion – the ability to get a job done efficiently from anywhere is becoming essential. This is exactly what a smartphone does.

2. No solution is perfect, of course. Over 17% of respondents to one survey admitted to losing their RFID card or fob in the previous 12 months, for example, which presents an obvious danger. Mobile credentials offer compelling security enhancements over cards. Firstly, the value of the credential itself: How quickly would you notice a missing plastic card? Not as quickly as a lost phone, for sure. In

addition, security managers react faster when credentials are mobile. Access permissions can be cancelled or amended over the air, for example. Plus almost every device has a built-in failsafe: Biometrics, fingerprint or face ID screen locks stop a casual thief from using mobile keys.

3. To thrive in the competitive build-to-rent, multi-family residential sector, businesses must reassure residents that their property is safe. At a major new Becorp development in Barcelona, homes are secured by SMARTair wireless devices, which residents unlock with secure mobile keys in their own Openow app. There's no key, physical card, fob or badge. The app enables easy locking by deadbolt projection: After presenting their phone, a resident simply moves the handle upwards to lock a door securely. At the same time, facilities staff stay in control using their own Openow app: Credentials can be created, sent and cancelled from anywhere, with no metal keys to worry about.



Clément Menviel

Group Communications
Director STid

www.stid.com

1. The management of physical access cards can be a real headache (manually issuing access badges, the security risk of lost badges, etc.) With a mobile access solution, users present their smartphone, a personal device, to the reader to get access to buildings or other secured zones. Virtual credentials greatly reduce the time required for access management. The creation, distribution and revocation can be executed immediately, at any time and at any location in the world. Moreover, the cost of a virtual badge is two to five times less than that of a physical badge: no more consumables, printing and personalization costs, recycling costs or expenses related to loss or damage.

2. The mobile access control solutions in our industry have matured and are now considered a valuable asset to any access control deployment. Security managers better understand the value of allowing people to use their phone converted into an access control key, resulting in improved operational effec-

tiveness and intuitiveness. Users may be reluctant to share their personal data. With STid Mobile ID you are always in full control of your security – no personal information is stored. When applying any security technologies, it is always important to understand the benefits, like user-friendliness, security, scalability and interoperability. STid Mobile ID meets all these requirements.

3. In collaboration with Nedap and Alvem we recently secured the Tour and Taxis building in Brussels, owned by Nextensa. We greatly enhanced and improved the user experience by removing the constraints related to conventional identification technology to better accommodate the 1500 employees, 40 tenants and 400 visitors that Tour & Taxis welcomes daily. The results live up to expectations with the reuse of existing cabling, the set-up of a standardised and futureproof physical access control system, and the transfer of registration responsibilities to tenants.

1. Mobile access delivers convenient, instant, and safe access. There is no need for multiple old-school keys. Mobile access is available for all user types in any build application – from residents, visitors, and staff via a mobile app, empowering any users with more control over their doors and spaces. Mobile access provides a high level of security, including advanced encryption and provides users with a secure and seamless keyless and mobile experience. Systems operators and facility managers can give, change, and remove users' keys remotely, denying or cancelling lost/stolen smartphone digital access instantly. The digital key technology and mobile access (NFC & Bluetooth LE) is fully compatible with the users' own smartphones (iOS and Android devices), even Apple Wallet. It is one access solution for all areas.

2. It is no surprise the demand for mobile access is on the rise. Users want seamless access to their areas, whether workplace, gym, or home, without having to manage multiple keys. Salto first revolutionized smart access control in the hospitality and commercial industries, then education to smart corporate buildings, and now Salto has adapted these core technologies to suit the residential industry. Leveraging credentials embedded on smartphones provides

end users with a number of benefits. It is an entirely new digital key ecosystem that offers Salto mobile smart credentials, making the digital key technology a mainstream choice for many organizations looking to improve access control. The Salto JustIN mobile access technology gives easy keyless access to every lock you need access to. With this technology life is a little easier. Unlock and receive your key instantly, even if your smart keycard isn't with you.

3. Salto is continuously working on technologies that will bring us closer to a more connected living and keyless experience. Salto access control solutions and mobile access technology are in use worldwide in a never ending range of challenging and unique applications and facilities. We worked with Cardinia Shire Council based in Australia to set up over 2500 access points. Salto smart and mobile access technology provides services to this population through 220 council owned sites and buildings – including child-care centres, recreation facilities, community centres, halls, public toilets, and council offices. Moreover, we successfully implemented integrated cloud-based Salto KS smart access solutions for IWG and we help over 8 million people work the hybrid way in thousands of regions and locations worldwide.



Borja Ganzarain

Brand Communications &
Content Marketing at
Salto Systems

www.saltosystems.com

1. If I were to sum it up in one sentence, it would be that HID Mobile Access provides you with convenience and operational efficiency, without compromising on security. The user benefits through the convenience of multiple credentials in their smart device and the reduced risk of lost or stolen cards. This improves operational efficiency as organizations don't have to keep issuing plastic credentials, with the associated processes and costs. Further, through full-circle digital management, credentials can be instantly issued, revoked or re-issued through the cloud – making it quicker and easier, with reduced operational logistics such as shipping, storage and management of plastic credentials. Finally, our Mobile Access solution also provides customers with the dual modality of utilizing either NFC or Bluetooth, given them a wider choice of technologies to use with their handsets.

2. Mobile access is growing at an exponential rate and we've a product to lead this industry transformation globally. Bear in mind, HID introduced Mobile Access way back in 2014 and since then we have continued to innovate with new features, for example, we were the first company in the world

to offer credentials in Apple Wallet. We also support over 500+ smart phones and wearables and are constantly expanding this number – all individually tested and validated. With a legacy of over 30 years of innovating in the access control industry, customers are also assured of reaping the full return on their investment in Mobile Access, as we continually expand features and functionality.

3. Whilst we can't detail high security projects for obvious reasons, our Mobile Access customer base spans over 100 countries and this number continues to grow – from banking and finance institutions, government, global retail chains and of course, a wide array of enterprises. Part of our success is our unique ability to address the various mobile access use cases that our customers have, in the simplest of ways. We're also seeing strong growth in the commercial real estate sector, where employee or tenant experience apps have integrated Mobile Access into their solutions to offer even greater convenience to users. Further, many of these customers, including critical infrastructure institutions, implement our Mobile Access solutions for use cases that go far beyond just opening doors.



Sanjit Bardhan

Vice President & Head of
Mobile, HID PACS (Physical
Access Control Solutions)

www.hidglobal.com



ALARM SYSTEMS

Ajax Protects Banksy's Works in Ukraine

Motion Detectors and Opening Detectors by Ajax Protect the Objects Against Attempts to Damage or Approach the Artwork

Ajax guards Banksy's symbols of resilience in the Kyiv region with opening detectors to protect the objects against attempts to damage or approach the artwork. They were installed on four Banksy paintings in Borodyanka, Irpin, and Horenka.

Ajax Systems has delivered a solution for protecting the works of world-famous artist Banksy in the

Kyiv region. The project was developed on the initiative of the Kyiv regional military administration and local administration.

Ajax wireless security systems were installed on four Banksy paintings in Borodyanka, Irpin, and Horenka. The art objects are protected against potential vandalism and weather conditions, and are monitored 24/7 by the Sheriff security company. The rapid security team will instantly respond to stealing or damaging attempts. The paintings will be protected until delivered to the museum.

"Banksy's works have cultural and historical value for the country as a reminder that light will win over darkness. It is important to resist possible vandalism attempts that have already happened. We are grateful to our partners and security engineers. They have found and delivered a successful solution in a challenging environment," says Oleh Torkunov, the deputy head of the Kyiv Regional Military Administration.





Transparent polycarbonate walls protect the artworks from the external environment



Motion detectors and opening detectors by Ajax protect the objects against attempts to damage or to approach the artwork. The built-in sensors react to shocks and vibrations

Transparent Walls and Humidity Monitoring

Motion detectors and opening detectors by Ajax protect the objects against attempts to damage or to approach the artwork. The built-in sensors react to shocks and vibrations. In case of an alarm, the siren activates, and the rapid response team arrives. Transparent polycarbonate walls protect the artworks from the external environment. The picture of a judoka in Borodyanka also has a temporary protective structure with a smart air quality monitor inside. It monitors CO₂, temperature, and humidity levels. The WallSwitch relay helps maintain the microclimate conditions to keep the painting safe.

“We are grateful to Ajax Systems for fast responding and protecting the paintings. These art objects are war artifacts that we must preserve for Ukrainians. Our cities have suffered from significant destruction, and these art objects represent an unbreakable belief that life will definitely win,” says

Heorhii Yerko, acting head of the village council of Borodyanka.

20 Detectors and Four Control Panels

The security system includes 20 detectors and 4 control panels (hubs). The detectors do not depend on a constant power supply. The control panel can be located in a remote room. The hub maintains communication with the devices at a distance of up to 1,700 meters and transfers alarms in less than 0.15 seconds.

“Protecting such objects is a challenge for any security system or installer. There were many obstacles: from destroyed buildings with paintings to no power supply. But with the assistance of the Kyiv Regional Administration and the Ministry, we were able to find and bring necessary solutions to life. We are happy to see Ajax products protect culture, even in such challenging times,” says Valentine Hrytsenko, CMO at Ajax Systems.

Banksy's Art Appeared in 2022: There Was an Attempt to Steal One of the Paintings

In the autumn of 2022, Banksy's art objects appeared in Ukrainian cities and became one of the symbols of support for Ukraine. In December 2022, an attempt was made to steal one of the paintings. Then the project was initiated.

This is not the first Ajax Systems initiative to protect art and cultural monuments in Ukraine and abroad. In 2021, the original Constitution of Pylyp Orlyk was under the constant monitoring of the Ajax system in the historical building of the St. Sophia Cathedral. That same year, the Ajax security system was installed in the Parkhomivka Museum, named after A. F. Lunov. In addition, Ajax protects a UNESCO World Heritage site in Norway – the wooden architecture of Bergen city.

CONTACT

Ajax Systems, Kyiv, Ukraine
support@ajax.systems · www.ajax.systems

ASSA ABLOY
Opening Solutions

Access control in the Cloud

Incedo™ Cloud is the flexible solution for your business

Download the Solution Guide:



Experience a safer and more open world

SPECIAL FOCUS AIRPORT SECURITY

Inside, Around, and Above

A Plethora of Security Solutions
Helps to Keep Airports Safe



SPECIAL
FOCUS

You may have heard on the news in November and December of last year that climate activists belonging to the “Last Generation” group succeeded in gaining access to the apron of both the new Berlin airport and also the airport in Munich, and then glueing themselves to the tarmac. These serious security breaches caused chaos for thousands of people, with the consequences lasting several days while causing significant direct and indirect costs for passengers, airline companies and their suppliers, as well as the airport operators themselves. Just when we thought we had perimeter security covered, these troublemakers – very easily – proved us wrong, so GIT SECURITY has taken a quick look at some of the latest technology available to help keep airports secure, inside and outside.

Eight unauthorized people managed to enter the security area of Berlin airport simply by cutting a hole in the perimeter fence. Even though security personnel were quick to respond, their response still lasted around an hour before order was restored. The Interior Minister of Brandenburg, Michael Stübgen, quickly demanded a rapid improvement in the security of the airport compound by federal police and the airport operators, and expressed his surprise at how easy it apparently was to gain illegal entry with just a pair of wire cutters.

In an unusual display of unity, politicians across the spectrum, including the Green party and the far right AfD, criticized the intrusion. The “Last Generation” (“Letzte Generation” in German) stated that their members had been able to cross the area on bicycles. The alarm in Berlin closed the airport for 90 minutes, during which 15 incoming flights were diverted to Leipzig, Dresden and Düsseldorf.

Five flights were unable to depart, while other incoming flights were sent in the holding pattern. Luckily, no aircraft were damaged or endangered and no one was injured during this incursion ... this time.

The (W)Hole Solution

So there are a number of solutions to rapidly detect tampering with a boundary fence. RBTec of Maryland, USA, offers a range of products worldwide that employ different techniques to detect – and importantly to accurately locate – intrusion attempts on perimeter fencing. Using either buried cabling to detect vibrations nearby, or a fiberoptic cable attached to the middle of a boundary fence, their systems can be finely calibrated to ignore regular, “safe” sounds and weather induced signals while responding immediately to the typical vibrations caused by destructive actions. The mid-fence solution is, of course, very quick to

install or retrofit and requires no power at distant locations.

Senstar's product range includes mesh-connected lighting units that respond to any physical contact with a fence and report activity to other security systems. Their fiber solutions can pinpoint tampering activity down to within four meters (13 ft.) Haverkamp provides a security fence monitoring solution for new or existing fences using quiescent current or vibration monitoring that will detect tampering or damage, also combined with ground sensors, if necessary.

A second line of defense for the perimeter fence can be provided by invisible beams along the inside being broken: Infrared, microwave and radar are the most commonly used techniques, and have had their algorithms refined over the years to easily disregard wildlife interruptions, such as by foxes or birds. The Italian company Cias can provide any of these types to meet the needs of any site, domestic or commercial.

In February 2021, GIT SECURITY featured a system by Sorhea that uses a dynamic radio mesh network between its Solaris infrared beam columns to transmit alarm information. The only infrastructure require along the perimeter is a concrete block every 100 meters or so. Stateside, you might like to contact Southwest Microwave, who employs their Intrepid microwave sensors to build a volumetric security zone where any human movement will trigger the alarm.

The Automatic Eye

Security on the landside areas of airports already starts on the approach roads and urban transport platforms, with video surveillance supported by intelligent algorithms taking the eye strain out of monitoring dozens and potentially hundreds of cameras. A digital infrastructure and a highly featured VMS is essential to provide the coverage necessary to meet the needs of various stakeholders: the airport security team and operational management, the police, immigration and border security staff, medical personnel, vehicle rental companies and, last but by no means least, the airlines themselves.

At the core of Vivotek's Smart VCA image analysis is a deep-learning AI engine that can detect loitering, missing or unattended objects, line crossing and other behavioral activities according to the given event rules. With an extremely versatile range of video surveillance products and interaction with third-party devices guaranteed by the ONVIF compatibility of all components, Dallmeier can provide a customized solution internationally to match the specific needs of major projects while complying with local data protection regulations.

Can't Fool Us

Walk-through scanners with red and green lights have been providing elementary metal detection for decades at the interface between landside and airside, with many comic sketches being based on the process of ensuring that passengers and airside staff are "OK". But metal detection alone is no longer sufficient because 3D-printed devices, explosives and drugs have increasingly been found in carry-on items. L3Harris manufactures the Provision range of people-screening devices that ensure untoward substances or devices are found, and conform with privacy

expectations if necessary without providing an image to be studied by security staff. They use safe, millimeter wave radio frequency technology. The TH1800 imaging system from security scanning multitalent Nutech is a stand-off people screening solution to detect objects concealed under clothing, such as metal/non-metal weapons, IEDs, liquids, narcotics, or explosive belts. A terahertz signal from the device forms a high-contrast, real-time image, allowing automatic threat detection. Terahertz waves are absolutely harmless to humans, and are non-ionizing.

Flying Pests

The advent of cheap, fast drones has become a real headache for airport operators worldwide. Whether flown through dumb naivety, bravado or intentional espionage, the intrusion of any drone in the airspace over or around an airport is a serious safety breach with potentially catastrophic consequences. The anti-drone industry is new, dynamic, and has already come up with many approaches to detecting and removing these airborne pests by jamming, disorientating, and hacking among others. It is a cat-and-mouse game, however, with commercial drone manufacturers continuously hardening their products, too.

Dedrone provides a clever detection system consisting of multiple sensor types that will rapidly locate a drone and its operator, often before it encroaches toward the airport perimeter. The Adani product palette employs multiple technologies to detect and, where legal, disable intruding aerial threats. A wide choice of solutions can be combined with other systems, also to military specifications, if required. The Orion family of solutions from TRD integrates the detection and defeat of approaching airborne threats. The company not only supplies customers with off-the-shelf solutions, but also develops its own customized products to address specific needs. Whichever solution is chosen, it should also have a "friend-or-foe" ability because, just sometimes, airport operators want to fly a drone themselves over their own property.

Once you have decided which systems you are going to install and the location of your operational control room in the US, the UK/Europe, or the Middle East, you could contact Winsted who will be delighted to help you design the layout and build some stylish and ergonomic furniture to fit. And when it is finished, send us some pictures, please!

Suppliers

Adani | www.adanidefence.com

CIAS | www.cias.it

Dallmeier | www.dallmeier.com

Dedrone | www.dedrone.com

Haverkamp | www.haverkamp.de

L3Harris | l3harris.com

Nutech | nuctecheurope.com

RBtec | www.rbtec.com

Senstar | www.senstar.com

Sorhea | www.sorhea.com

Southwest Microwave | southwestmicrowave.com

TRD | www.trd.sg

Vivotek | www.vivotek.com

Winsted | www.winsted.com

SPECIAL
FOCUS

CRITICAL INFRASTRUCTURE

Greatest
Challenges
in Critical
InfrastructureWhat Providers Need to Know and
Do to Safeguard Premises

Our world is becoming increasingly complex and we are constantly facing new and unknown crises and disasters. To ensure that we are not caught unprepared, we must protect ourselves accordingly. The last crises have shown where our weak points are and thus also where we need to start in the future. Many countries were and still are unprepared for attacks against electrical utilities, for example.

The European Union has established Council Directive 2008/114. It is a key pillar of the European Programme for Critical Infrastructure Protection (EPCIP). It is there to direct identifying and designating European Critical Infrastructures and to protect them from all kinds of threats, intentional and accidental, as well as natural disasters. The latest addition to the directive came out as a proposal in 2020, together with an impact assessment. According to the European Parliament, "The proposal aims to enhance the resilience of European critical entities, by shifting from an assets-focused approach to a systems-focused approach, expanding the directive's scope, and aligning the new directive with a proposed revision of the EU Network and Information Security Directive ('NIS 2')."

Another aim for a more regulated protection of Critical Infrastructure was in Germany most recently. At the end of

2022, the Federal Cabinet of Germany has adopted key points of the so-called KRITIS (Critical Infrastructure) umbrella law. This law is awaited with great expectations and acclaim because it aims to close the gaps in the physical protection of critical infrastructure and to increase the resilience of our society.

What is Critical Infrastructure?

According to the BSI (Federal Office for Information Security in Germany), Critical Infrastructures are classified by "important significance" for a state community. It means that failure or impairment of these organizations and facilities would result in lasting supply bottlenecks and grave disruptions to public safety or other dramatic consequences.

Critical Infrastructure sectors are:

- Energy
- Health

- Information technology and telecommunications
- Transport and traffic
- Media and culture
- Water
- Finance and insurance
- Food
- Municipal waste disposal
- State and administration

All organizations from these sectors count as Critical Infrastructures, regardless of their size.

What Are the Challenges for Security Providers of Critical Infrastructure?

Heiko Viehweger, Sales Director DACH at Sorhea, knows about what it entails to secure Critical Infrastructures: "One of the greatest difficulties in installing security technologies in Critical Infrastructure is the need to balance security measures with operational requirements. Critical Infrastructure systems are often designed



to operate with high levels of availability, reliability, and efficiency, and security measures can potentially interfere with these goals. For example, security controls that restrict access or add additional layers of authentication can slow processes and lead to operational inefficiencies.

“In addition, Critical Infrastructure systems are often complex and interdependent, with many different components and stakeholders. This can make it difficult to identify and remediate vulnerabilities and coordinate security efforts across multiple systems and organizations.

“Another challenge is the cost of implementing and maintaining security technologies. Critical Infrastructure systems often require specialized and sophisticated security solutions, and the cost of implementing these solutions for large and complex systems can exceed planned budgets. In addition, security technology must be regularly updated and maintained

to remain effective, which can be difficult and resource intensive.”

Neil Foster, Project Development Manager at Optex Europe says: “Critical Infrastructure sites are usually large premises, often located in remote areas that are submitted to harsh and sometimes hazardous conditions. Effective perimeter protection requires sensing technologies that won’t be affected by other equipment onsite or by the natural elements, such as wind, rain, vegetation or wildlife. The choice of technologies will also be determined by the scale of the site. Fiber optic sensors and LiDAR technology, for example, can be used to create multiple detection zones within a perimeter and adjust the sensitivity within each zone. Point detection, too, is one of the latest sensing technology advances, enabling the exact location of an intrusion to be pinpointed, which enables a faster response and verification process.”

Which Aspects of the Perimeter Protection Are Not Negotiable?

According to Heiko Viehweger, these essential perimeter protection requirements should be non-negotiable:

- Physical barriers: Physical barriers, such as fences and gates, should be in place to prevent unauthorized access to Critical Infrastructure.
- Video surveillance: Video surveillance cameras should be installed at key locations on the site to monitor and record suspicious activity.
- Access control: Access to Critical Infrastructure should be restricted and controlled, with appropriate authentication and authorization mechanisms in place.
- Intrusion detection systems: Intrusion detection systems should be in place to detect unauthorized intrusion attempts and alert security personnel.
- Cybersecurity measures: Critical Infrastructure systems are increasingly connected to the internet and other networks, making them vulnerable to cyberattacks. To protect Critical Infrastructure systems from cyber threats, stringent cybersecurity measures, such as firewalls, encryption, and regular security audits, should be implemented.

Overall, perimeter protection is a critical aspect of Critical Infrastructure protection that must be prioritized.

Furthermore, GIT SECURITY asked Managing Director at Senstar, Michael Rumpf, to differentiate between logistics and Critical Infrastructure. Michael Rumpf’s reply was: “There are no real differences here. The need for protection in the logistics sector is similarly high. Logistics halls and transshipment warehouses sometimes contain enormous values of goods,

Security.




GEMOS 5.

- Next Generation PSIM
- Manufacturer-neutral hazard management system
- More than 50 different interfaces and fire alarm systems integrated
- CAD Import
- Monitoring of detector disconnections (revisionen)
- Print-out of fire brigade route maps in the event of a fire alarm

BKS GmbH |

D-42549 Velbert | www.g-u.com



In the independent test, the systems are tested with complex camouflage and movement types

dangerous goods, and vehicles that need to be protected against theft or manipulation. In the Critical Infrastructure sector, systems need to be protected for similar reasons and intruders need to be detected as early and reliably as possible. This is why redundant system concepts are often used. In most cases, a combination of fence and ground detection is used, and these systems are of course supported by video cameras.”

What Kind of Products Can Be Used to Secure Critical Infrastructure?

Our good friend from the kitchen, the onion, serves well to visualize the multilayer active security risk management concept that we need to protect anything other than the simplest building. At the perimeter of the site there should be a physical barrier – a fence – high enough and painful enough to deter scaling. Best of all, this can be equipped with motion and damage detection, for example the VibraTek system from Detection Technologies or the fiberoptic-based FiberPatrol product from EAS. Alternatively, you can go the whole hog and electrify the fence, but we do urge you to check that this is legal at your location before doing so! Advanced Perimeter Systems in Scotland can literally empower your site with a well thought out electric fencing solution.

Where visible physical barriers are either impractical or unwanted, invisible infrared, microwave, or radar barriers can

immediately detect intruders and trigger lights, sirens, or the dog-handler. The Micro-Ray linear mW barrier from Cias is one such product.



Solaris NG, the new generation autonomous, infrared barrier with a 100m range

A solar-powered alternative called Solaris is available from the French manufacturer Sorhea. The columns from Sicurit can incorporate dual detection technology to be sure of correct detection and a minimum of false alarms. To achieve the best possible infrared barrier performance, Sorhea boasts a high density of infrared beams that create a virtual wall that cannot be breached without sending an alarm. The denser the infrared wall, the finer and more reliable the detection is. With 10 cells on 3-meter columns, Solaris is – according

to the manufacturer – currently the only existing autonomous infrared barrier offering such a high infrared density over a range of 100 m. Its algorithm can tell the difference between a vehicle (train, tram, or even a plane) and an individual passing between two columns, so no unwanted alarm is created and the perimeter security system is not interrupted. This new generation is also available in an all-plastic version: made of polyacetal, the housing makes the column frangible. Solaris NG (latest version) can then be installed on very specific sites, such as airport runways and high voltage transformer sites.

Senstar, on the other hand, has developed a hybrid concept. According to John Rosenbusch, Sensor Fusion is the logical further development of such hybrid concepts. The metadata from the video and fence analysis is merged via an AI with the aim of reducing the false alarm rate to almost zero. The Sensor Fusion engine is more than a simple Boolean logic integration: It accesses low-level data to intelligently characterize potential risks. Data synthesis allows the system to achieve a level of performance above that of individual sensors.

Protection of Critical Infrastructures with Radar Technology?

Modern Radar systems offer outstanding performance, which makes them a perfect choice to even protect Critical Infrastructures with high requirements. Because of their reliability, they became an essential part for the security concept of hazardous environments and Critical Infrastructures. They also persuade with high functionality for perimeter protection. It's possible to keep an eye on multiple targets and to locate them within a large area. Their advanced features are specialized for the user and application to increase the efficiency of the detection.

It is possible to limit the detection area by distance or angle position. The user can adapt the monitoring to the local conditions. It is possible to define individual alarm and ignore zones if movement is allowed in distinct areas and in other areas it is forbidden. This feature offers great benefit for early intervention on Critical Infrastructures. Within the large detection area, the user can combine different security actions with one radar system.

Christian Bömmel, Head of Industrial and Automotive Sales at Innosent adds: “Radar was initially used by the military for navigation. The advantages, functions, and features of the technology meet perfectly

the needs of the security market, so it's no wonder that advanced radar systems are now so popular. Radar often outplays other technology when it comes to reliability and performance – which are important criteria for securing Critical Infrastructures.”

Where Do Perimeter Protection Technology Providers Need to Improve Their Performance?

Masaya Kida, Managing Director of Optex EMEA, says in an interview with GIT SECURITY: “The main challenge in outdoor security systems are nuisance alarms, which is why using sensing technology is paramount to designing a robust and stable security system. Sensing technologies have been designed specifically to ‘detect intrusions’ and will perform reliably, not affected by different light conditions or weather. I think you have tested a lot of video analytics systems in your GIT System Test Video Analytics and have identified some of the most common causes of nuisance alarms for those technologies. We will take part this summer in your testing when you extend the range of the tested systems beyond video analytics in GIT System Test Perimeter Protection, and test our LiDAR Redscan Pro technology. The biggest challenge that LiDAR and other sensing technologies help to achieve, besides creating reliable and accurate detection, is avoiding false alarms. Especially for Critical Infrastructure this is crucial. Too many false alarms interrupt operations, make security

teams lose confidence in the system, are time consuming and costly. This is a real problem for operators but also for installers and system integrators because of the end-users’ complaints to them.”

Is There an Independent Test for Perimeter Protection Technology?

In the September 2022 issue of GIT SECURITY, we published the results of the first “GIT System Test Video Analytics” (GSTVA) that was done in April 2022. Eleven powerful, currently available systems were subjected to intensive test scenarios we developed together with the expert office of Markus Piendl and the system house i-Alarmsysteme. In 2023, we will add another GSTVA and extend the range of tested systems beyond video analytics with the GIT System Test Perimeter Protection GSTPP.

For the first GSTVA the intrusion tests were divided into different scenarios and scenario groups. Variations were made between different types of movement, i. e. approaches were made at different speeds, angles, and rhythms. Different types of clothing and camouflage were used in further variations, which were evaluated separately, and both day and night tests were conducted. Some test scenarios involved destabilizing the video analysis systems through the use of pyrotechnics, for example. The results of the intensive testing are available via the QR code at the end of this article.



Preview 2023

Test Results 2022



Suppliers

Advanced Perimeter Systems | www.advancedperimetersystems.com
CIAS | www.cias.it
Detection Technologies | www.detection-technologies.com
Innosent | www.innosent.de/en
Optex | www.optex.co.jp
Senstar | www.senstar.com
Sorhea | www.sorhea.com

DOMERA®

BEYOND THE IMAGE.



INTELLIGENT



PICTURE-PERFECT



VERSATILE

Dallmeier

The camera for channel partners.

- Time-saving installation
- Maximum added value
- Easy to adjust using three-axis remote adjustment (RPoD)
- Suitable for over 90 % of applications



www.domera.ai

MADE IN GERMANY

Attack to the Core

Threats to and the Protection of Critical Infrastructure

The predicted lack of sufficient energy caused by the interruption of gas supplied from Russia, the drastic price increase of certain raw materials and, above all, the attacks on the Nordstream 1 and 2 pipelines, as well as the attacks on the German railway network, have raised public awareness and that of politics, commerce and the media of just how critical and threatened critical infrastructure is (KRITIS). Highlighting the complexity of KRITIS, the strategy, options and limits of its protection, as well as the necessity of emergency planning, is the aim of this article by Reinhard Rupprecht, Ministerial Director (retired).

The German abbreviation KRITIS (standing for CRITical InfraStructure) was not used until the turn of the century. Since then it has become established in the vocabulary of economists, technology and social science worldwide. The German Interior Ministry defines the term as “organizations and installations of great importance for the general public, where their failure or disturbance would lead to long-lasting supply problems, a significant reduction of public security or other dramatic consequences.”

The complexity of KRITIS being defined this way leaves room for limitations. The term is excellent for political evaluations and strategic direction, but as a legal term it needs to be made more precise and more accurate by defining thresholds.

The criticality arises from the effect of an industry, a structure, a logistics process, an organization or a company on the existential needs of the population, the state or commerce. The term KRITIS in all its complexity includes both a micro-economic and also a macroeconomic level of an industry, a national economy or an international business community. It covers the energy, information technology and telecommunication industries, transport and traffic, health, water management, finance and insurance bodies, the state and admin-

istration as well as media and culture. The German IT Security Law 2.0 also includes the communal waste disposal service and “...companies of particular public interest,” that is, companies in armament production, companies with an IT security function for confidential matters, the largest companies in Germany by domestic turnover together with their suppliers, as well as companies that process dangerous goods and fall under the special law for the reporting of incidents. In total, more than 20 industries can be considered as KRITIS.

The Spectrum of Threats and Danger

The breadth of the danger spectrum is made clear by recent developments and highly visible security events: The spread of the Covid-19 virus since 2020 is the pandemic with the most severe consequences worldwide in human history, has caused the death of millions of people, and overstretched the medical resources of many countries. The total lockdown policy in China led to worldwide delivery problems and manufacturing delays. Natural catastrophes, such as tsunamis, have caused many deaths while climate change is destroying the food resources of millions of people.

The Russian invasion of Ukraine in February 2022, together with the end of the Nordstream 2 project and reduced gas

supplies to Europe, has massively affected most European countries. On 26 September 2022, the Nordstream 1 und 2 pipelines were blasted apart and the attack showed how vulnerable the gas supply is.

On 8 October 2022, two data cables for the mobile radio service of the German railway were cut in an underground cable tray that was covered by a solid concrete cover. Later some distance away, the backup fiber-optic cable was also cut. This caused the entire railway radio communication network in the north of Germany to fail and all rail movements, even international ones, were stopped for hours. The culprits must have known the purpose of those cables.

Also in October 2022, three attacks on underwater internet cables became known. The operators of wind generator farms lost the connection to their installations due to a Russian hacking attack on the KI-SAT satellite network. Cyberattacks continually threaten KRITIS, and there has been a rising frequency of carefully prepared ATP (Advanced Persistent Threat) attacks over recent years that threaten KRITIS operators worldwide.

KRITIS Strategy

Countermeasures involve both governmental and commercial strategies, and there is a close cooperation between the two. A

strategy requires risks to be identified in advance, their effect to be kept as small as possible through emergency management and redundancy, and the use of constantly updated danger analyses to improve levels of protection.

New laws in Germany taking effect on 1 May 2023 oblige operators of critical infrastructure to take reasonable organizational and technical measures to prevent interruption of the availability, integrity, authenticity, and confidentiality of their IT systems, components and processes according to the state of the art in technology. It includes employing methods of recognizing attacks by continuously gathering and evaluating information from production processes and proposing action when faults occur. Continued compliance must be demonstrated every two years. A new obligation to report “critical components” has also been introduced that prevents their use before the manufacturer has been approved by the authorities for confidentiality.

European Regulations

In November 2022, the EU Parliament adopted the NIS2 Directive, which forms the European IT security framework for KRITIS operators. It sets minimum standards for the regulation of KRITIS. Companies in 18 sectors with more than 50 employees and 10 million euros turnover must implement their cybersecurity obligation at the latest by October 2024. Cybersecurity must also be upheld throughout the delivery chains, too, according to this directive. At the moment, one third of all KRITIS operators in the energy sector do not monitor a single item of critical operational technology (OT) through a security operation center.

Protection of Power and Communications Networks

Complete surveillance of all the power and communication cables on the seabed or buried in the ground is clearly impossible. But this does not mean that the operators of these networks are powerless against

possible extremist-motivated attacks: The laying of redundant cable networks is very important. The railway saboteurs mentioned above apparently knew how they could overcome the redundancy, which points to insider knowledge and poor levels of internal secrecy. It is also important to be able to localize cable breaks with the help of monitoring sensors and quickly repair them.

Protection of Energy Networks

The 100 % protection of energy supply networks also appears impossible. Even though many gas lines are often buried one or two meters deep, they are not unreachable. Protecting pipelines on the seabed is particularly difficult – the thousand sensors that the operators of Nordstream had installed only showed the danger once it was too late. Researchers at the Chinese Academy of Science have developed a method of creating a 3D image of a gas leak cloud, which gives its volume and concentration. The researchers use two systems to generate a 3D image to observe a gas cloud from two perspectives. This information is spatially combined with details of the location. This new approach could be used for early leak detection, risk evaluation and decision-taking about the best method to stop the leak.

Protection of Hubs and Systems

Hubs in cable and supply networks and individual KRITIS systems – such as solar parks, wind generators, transformer and switching installations, power stations and water pumping stations, computer centers, hospitals – are of course much easier to protect against attacks than long pipes and lines through appropriate construction,

mechanical and electronic security technology. On the other hand, such installations are easily recognized and are attractive targets for saboteurs, such as cybercriminals who attack the control systems to encrypt data with ransomware and then blackmail the operators.

Junctions of deep-sea cables at landing points are monitored around the clock. KRITIS systems like these need double perimeter protection consisting of a wall or fence, as well as video surveillance by infrared cameras and intelligent analysis, also as detection cables buried in the ground or attached to the fence. Glass-fiber monitoring systems in particular are able to provide reliable and fully automatic monitoring of a perimeter. Any damage to or breaks in the fence immediately raise the alarm. Particularly sensitive systems or spaces should also be protected by two-factor authentication.

Emergency Planning

A comprehensive emergency plan must be made for critical infrastructure in case an attack or other service interruption cannot be prevented. It is built on a comprehensive threat, danger, and weak-point analysis of the respective critical system. The plan must consider the consequences of any attack and the effect of other influences, and find and prepare possible alternative sources of supply.



Author
Reinhard Rupprecht
Min. Dir. (retd.)

An Emergency Plan Must Include at Least the Following

- Establish who is responsible within an organization for emergency planning and its implementation
- Look for possible alternative supplies and prepare their acquisition
- Purchase the required emergency power generators for all parts of the company
- Check the “critical hardware and software components” that could endanger a system if they fail, in accordance with legal requirements
- Check supply chains, their relevance and susceptibility, as well as the ability to find alternative sources of supply, and reduce storage capacity
- Prepare the business continuity management
- Prepare for the personnel consequences if operational limitations occur
- Accumulate reserves for the purchase of alternative supplies in an emergency
- Sensitize employees to emergencies and their consequences
- Check and strengthen the entire resilience of the company
- Plan how internal and external communications will take place in an emergency



PERIMETER PROTECTION

Sensors, KRITIS and AI

Sensor and Information Management Systems for the Protection of Infrastructure and Assets

The complete protection of critical infrastructure, in particular in the energy and supply sector, has been a mainstay of Senstar for many years, a provider of integrated security solutions that include video technology, access control and sensors for perimeter protection. GIT SECURITY spoke with the new CEO of Senstar GmbH Michael Rumpf and Head of Sales John Rosenbusch about the company's strategy for the near future – among other things also the continuation of the organic growth and expansion of their partner network.

GIT SECURITY: Mr. Rumpf, Mr. Rosenbusch, first of all, last year ended on a sad note with the death of Peter Göring shortly before his planned retirement. This was not only sad for Senstar but also for the security industry as a whole.

Michael Rumpf: The sad news of the death of Peter Göring hit us all in the company hard – from a personal and also a professional point of view. Mr. Göring was responsible at Senstar for sales in the EMEA region for more than 20 years, had made a significant contribution to the success and growth of the company and, as the technical manager for the region, was always available with good advice. Those are really big footsteps to follow.

Mr. Rumpf, you are taking over the company management after Mr. Göring.

Michael Rumpf: We have been preparing the structural changes for about a year already. I have been the registered Managing Director since the 1st January and Mr. Rosenbusch will now completely take over the

sales management of the DACH region. We are sure that these organizational changes will allow Senstar to meet its stated targets, and that they will enable more scalability.

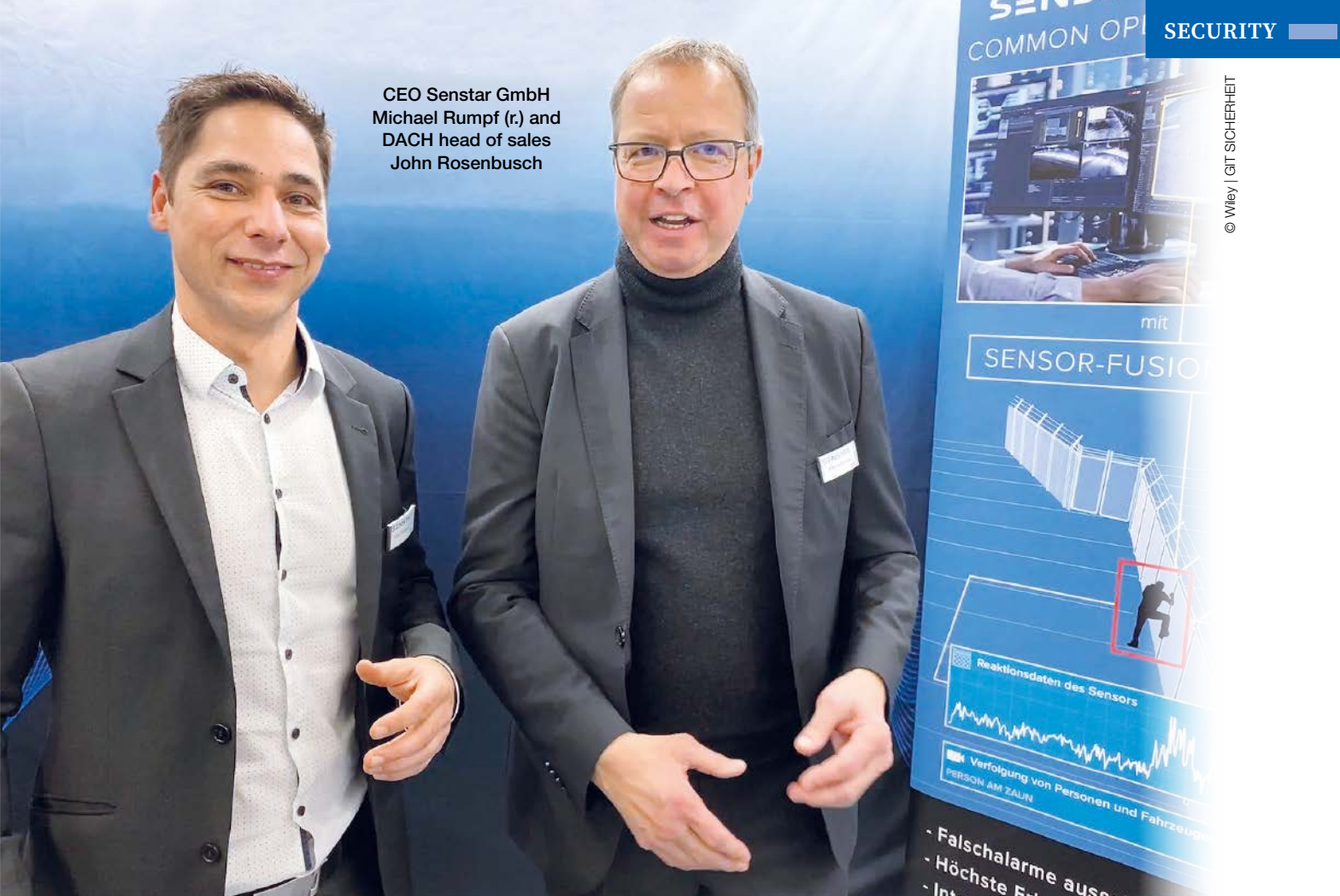
Which matters will be in the focus of your strategy now as the new CEO?

Michael Rumpf: We will definitely continue to concentrate on the organic growth of Senstar in Germany and Europe. There will be a few new positions to fill in the coming year in sales, business development and also in the engineering departments. In addition, we want to strategically align our products and the structure of Senstar more closely with our target markets. This includes implementing projects in the critical infrastructure, oil and gas, and penal justice sectors as well as the large logistics segment. It is particularly important for us to maintain and strategically grow our network of partners in these sectors. New products for these markets are constantly being developed together with our parent company in Canada.

Senstar and its products are concentrated on a number of vertical markets. You just mentioned that critical infrastructure, and in particular energy and water supply systems, are very important. Could you tell us more?

John Rosenbusch: The KRITIS sector [CRITICAL InfraStructure] has been a prime market for us for a number of years. We have a large choice of solutions to protect the perimeters of our critical infrastructure customers that alert proactively and with the minimum of false alarms. Designing our perimeter protection systems is unbeatably easy to do and highly efficient. The various types of technology can be scaled to any size depending on requirements.

We have provided a large number of fence detection systems over the past few years, particularly for solar energy generation plants throughout Europe, among them the Solarpark Tázlár, which is the largest in Hungary with a generation capacity of ca. 60MW. Our fence and ground detection systems are also used to



CEO Senstar GmbH
Michael Rumpf (r.) and
DACH head of sales
John Rosenbusch

secure electricity substations, gas pumping stations and underground gas storage facilities. We work closely together with the operators of such power and gas networks. But water and effluent treatment stations and even nuclear power sites are also protected by Senstar systems.

Before we talk about specific solutions, let us first consider your product portfolio: You say that you keep the largest portfolio of products in the security industry – what does that mean exactly?

John Rosenbusch: Senstar probably does have the largest choice of detection systems in the security market. It is all there, from the various fence detection systems, and the microwave barriers to secure open spaces, through to the buried detection systems. The systems have such a precise signal evaluation that an intruder can be pinpointed down to one meter accuracy. The highlight is the fiberoptic detection solution that can reliably protect up to 80 kilometers with one system. This technology is also used to detect leaks in pipelines or to protect telecommunications networks. And on top there is our Symphony Common Operating Platform that unifies video management, AI-supported video analysis, access control, business intelligence and of course our sensors, all in one user-friendly presentation. The development and manufacture of all our products takes

place exclusively in Canada and the USA. We support our customers locally with the planning of their systems and comprehensive solutions.

Senstar is particularly notable for its involvement in the subject of video analysis. You acquired the specialists Aimetis a few years ago for this...

Michael Rumpf: Mr. Rosenbusch and I both used to work for Aimetis and built a strong partner network for VMS and video analysis. The merging of the two Canadian companies Aimetis and Senstar, both with a similar philosophy, was a very good decision strategically. The portfolios of both companies complement each other perfectly and have allowed us to develop a very fruitful synergy over the past few years. Our long-term partners in particular have benefitted because the experienced resources of both companies have made it possible for us to develop hybrid system designs that seamlessly integrate the various detection systems and video management, including video analysis. Such systems are extremely efficient and economical as pure video solutions.

This has become a Senstar specialty that you call Sensor Fusion or a hybrid concept – it also means that you combine the positive characteristics of video analysis and fence detection systems

and suppress the negative ones. How does it look?

John Rosenbusch: Sensor Fusion is the logical development of such a hybrid concept. The metadata of the video and fence analysis are combined using AI to reduce the level of false alarms to almost zero. The Sensor Fusion engine is more than just a simple Boolean logic integration: It uses low-level data to intelligently identify potential risks. Through this data synthesis, the system can reach a high level of performance that lies above that of the individual sensors.

This has immediate, practical advantages for security applications, namely the ability to maximize the strengths of individual types of sensor and simultaneously to avoid their weaknesses. When the signal reaction data of the external sensors are synthesized with the video analysis data, false alarms caused by wind or shadows are practically eliminated, while the high probability of detection is maintained. We have managed to create a new type of product that has not been available on the security market to date.

Let us compare the perimeter protection requirements, say, of a logistics company with storage space and everything with that of a gas-driven power station or an electricity substation: An important aspect of any security



solution here is being able to guarantee continued operation. That probably means that you apply everything that your portfolio has to offer for such situations...?

Michael Rumpf: There are no major differences here. The level of protection required in the logistics industry is similarly high. There are goods of enormous value, dangerous goods and vehicles in logistics warehouses and distribution centers that must be protected against theft or manipulation. In the KRITIS industry, you also want to protect the systems for similar reasons and to reliably detect intruders as early as possible. That is why redundant systems are often set up. In most cases, a combination of fence and buried detection is installed and these systems are supported by video surveillance.

We work closely with the manufacturers of fencing systems, in particular on projects for critical infrastructure. For example, we recently provided a concept for a German energy supplier where a special wire mesh fence was designed that is extremely difficult to break through or to climb. The fence elements were constructed so that our sensor cable could be threaded through. This allows events on the fence to be reliably detected and the detection system is specially protected.

Interfaces to other security systems are of course often a consideration – and also the forwarding of alarms to external security patrol services because the systems being protected are often way off the beaten track.

Could you outline one or two typical projects?

John Rosenbusch: Let us stick with a classic one – the solar energy site. These

are typically surrounded by a wire mesh or palisade fence. Small systems have a circumference of 2 to 3 km, large systems often some 20 km, divided into separate fields. Our installers often use our FlexZone system to detect if an intruder is climbing over a fence, is cutting it or breaking through. It is a very reliable system that is easy to install, and cost efficient on top of that, and therefore perfect for the budgets of solar power parks. The system is attached to the fence, while gates are monitored with wireless, solar-powered sensors. FlexZone detects intruders in a fenced area and reports the event with closed contacts or via an interface to a superordinate video system. This automatically points a PTZ camera to the corresponding alarm zone and the security staff quickly have all the information they need to see what is happening. The alarm system on the fence only needs very little electricity and can be operated on emergency power without a problem for long periods.

Do you have another example?

John Rosenbusch: Another interesting example would be the protection of pipelines and communication networks. Pipelines or cableways for data communication are often buried over long distances. But these routes must also be protected against sabotage or damage by trenching work. Our FiberPatrol system can monitor up to 100 km of these routes. The system can distinguish machinery trench works at up to 30 meters distance, the movement of heavy vehicles, or the movement of people from the general background vibrations in the ground and reports an alarm including the respective GPS coordinates if the detection criteria are met. This allows potential damage to, or intervention in, the network

◀ **Electricity supply systems are constantly subjected to the risk of attacks, vandalism and theft**

to be quickly and reliably detected and prevented.

You maintain relations with a number of (technology) partners to achieve this. Who might this include?

Michael Rumpf: When various security systems have to work together, then the whole must be reliable, error-free and, above all, must function for the longest possible time. So we work closely together with various partners in the sector and create the interfaces between our systems. A good example of this is Advancis who offer interfaces to their Winguard solution not only for our detection systems but also to our video management systems. Naturally, there are many partner firms who provide network cameras, such as Axis or Hanwha. Competition aside, we have technology partnerships with companies like Bosch, Genetec and Milestone to make the messages from our PIDS system accessible in their management software. One of our most recent partnerships is with Wasabi Technologies, and this now allows our VMS customers to store their video data in the cloud in accordance with data protection regulations.

Mr. Rosenbusch, Mr. Rumpf, after what can only be called an eventful year in 2022, what will Senstar be prioritizing this year?

Michael Rumpf: As in previous years, we will have to keep the company and our products adapted to developments in the commercial environment and the security situation. Even though it now appears that the general availability of components has improved, it is still a concerning matter that costs us a lot of work and calls for good planning in order to be able to supply our customers without delays. Otherwise, we have a number of projects to complete and we have to find the right people for our organic growth. The year will be exciting because there will be many new developments, particularly in video analysis and AI, and we want to take our partners and end-users along with us on the journey.

CONTACT

Senstar GmbH

Maintal, Germany

Tel.: +49 6181 5704 100

senstar-gmbh@senstar.com

www.senstar.com

ADVERTORIAL

Full Color at Low Light

Hikvision Unveils Next Generation ColorVu Technology With Enhanced Low Light Imaging Using Super Confocal and Smart Hybrid Light Innovations

Hikvision enhances ColorVu, its high-quality, full-color technology, with Super Confocal and Smart Hybrid Light technologies. With these enhanced ColorVu offerings, even sharper imaging is made possible, with precise focusing in ultra-low light and flexible “hybrid” lighting modes to fit the scenario.

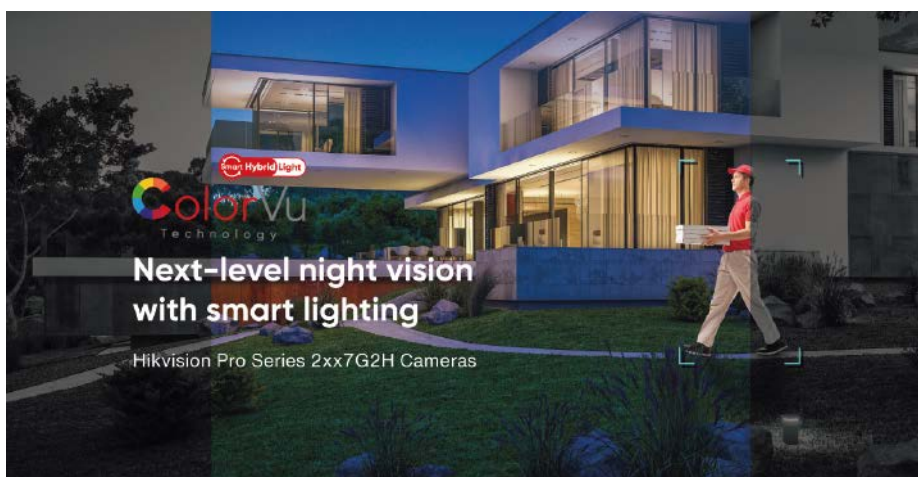
“By upgrading ColorVu technology, we aim to elevate our customers’ night vision experience in any setting with always sharply focused imaging and versatile lighting options,” says Rubio Hong, the Product Director at Hikvision. “We are very proud of our ultra-low light technology, which eliminates the headache of darkness and unclear footage.”

Improved Low Light Imaging Performance With the Super Confocal Technology

Hikvision’s industry-leading ColorVu technology provides full-color footage 24 hours a day, so users see the same sharply rendered images at night as they would see in broad daylight. Now boosted by Super Confocal Technology, ColorVu’s performance in low lighting gets even more stable and precise.

As infrared light focuses differently than visible light, it’s very difficult for dual-light cameras to create sharp images in low light. Given that cameras with ColorVu are equipped with large-aperture, high-resolution lenses, the focus depth is too small for the frame, which makes infrared imaging even more difficult.

But now, to solve this problem, Hikvision has infused Super Confocal Technology. This is a high-caliber lens design which reduces optical light dispersion to ensure that the point of focus on the sensor for the infrared light is virtually the same as that of the visible light (thus, “con” focal). Focusing both types of light at the same spot helps prevent blur and improves the user’s viewing experience by rendering clear, vivid images both in color and black and white. Achieving confocal



imaging with F1.0 super aperture is also an industry first.

Flexible Lighting Options With the Smart Hybrid Light Technology

Hikvision’s Smart Hybrid Light technology can automatically switch from IR light to visible white (supplemental) lighting at night. Equipped with this technology, cameras offer three supplemental lighting options to suit a user’s unique nighttime scenario, depending on the need. The white or visible light mode establishes color imaging; the IR mode (invisible to humans) enables continual black-and-white imaging at night with no light pollution; and the “smart” mode enables the light to automatically change between the two modes based on perimeter events.

With the smart mode turned on, the camera maintains infrared illumination at night until an event triggers color imaging to capture critical details. This means that once human or vehicle motion is detected by the camera, it switches to regular lights and turns to full color. This helps in two critical ways: Firstly, the camera’s color imaging captures better footage which can be used to identify the intruder; secondly, the triggered light acts as a deterrent to would-be trespassers who might potentially get startled and flee the scene.

Great Potential for Use in Both Indoor and Outdoor Applications

Recording “no action” footage at night or in poorly lit areas with infrared mode, the cameras’ location won’t be given away, and

the chance of a camera being seen and vandalized by intruders is vastly reduced. On the other hand, a bright light triggered by a security event and flooding the area helps deter intruders while recording with the same vibrant, colorful images as in daylight.

Therefore, cameras with ColorVu are ideal for both indoor and outdoor scenarios, such as warehouses, retail stores, public parks, and residential settings, where little or no movement is expected at night but discretion is desired for security cameras. Smart, automated lighting options combined with extremely accurate and sharply focused details creates a camera that truly goes above and beyond current security industry expectations and performance.

Find Out More

To discover more key features and capabilities of the ColorVu technology, please visit Hikvision’s website.



CONTACT

Hikvision Europe
Hoofddorp, The Netherlands
Tel.: +31 23 554 277 0
marketing.eu@hikvision.com
www.hikvision.com

VIDEO SURVEILLANCE

Every Meter Perimeter



Tailored Video Security Technology From Dallmeier Provides Perimeter Security and Workplace Safety

Vilsbiburg, close to Munich in Germany, is the location of the Flottweg SE headquarters and production plant. The separation technology specialist builds plant and machinery for solid-liquid separation here on a site covering about 110,000 square meters. In 2021, the company inaugurated its new Factory II, expanding its production area by approximately 18,000 square meters. A decisive element in protecting its business premises of just over six hectares and maintaining its status as an Authorized Economic Operator (AEO) is the video surveillance solution supplied by Regensburg-based manufacturer Dallmeier.

What do crude oil, water, liquid chemicals, and beverages such as beer have in common? Before they can undergo further industrial processing, they have to be purified, or certain constituents must be separated. The systems that perform this mechanical separation are made by Flottweg SE. Among other products, the company manufactures the largest decanter centrifuge in the world at its factory facilities in Vilsbiburg. Flottweg is very proud of its “Made in Germany” credentials and its record of preserving and creating jobs in the region. Responsibility and quality are inseparable elements of the company philosophy. This applies not only to process optimization and product quality assurance but also to protecting its employees and the company premises.

Security for Six Hectares

The company looked for a security solution for the new building in Vilsbiburg that met the latest technical standards, not least to

satisfy the criteria for AEO certification. Robert Waxenberger, Deputy IT Director for Flottweg SE, describes the requirements for the new solution as “innovative, sustainable, made in Germany, and GDPR compliant”. His experience from working on Factory 1, in which single-sensor cameras from Dallmeier have been working reliably for years, was decisive for this selection. In close cooperation, Flottweg and the security equipment installer Franz Sicherungstechnik developed a security concept for Factory 2 with components from the Dallmeier portfolio, consisting of the Panomera multifocal sensor cameras, megapixel dome cameras, the IPS 10.000 recording system, and the SeMSy Compact video management software.

“Unmanned” Test Run

The centrifuges and decanters undergo a stringent test procedure prior to shipping, and the test runs are conducted under camera surveillance in nine test bunkers

built specially for this purpose. “If anything untoward should happen during a test run, the parts would come at you with unimaginable force. The test must be carried out in the absence of humans for the safety of our employees. But since we also have to observe the progress of the testing, this is where we use cameras,” explains Robert Waxenberger. The dome cameras help the operator to monitor the process.

No AEO Certification Without Closed Perimeter Protection

With an export ratio of about 80 percent, certification as an Authorized Economic Operator (AEO) is immensely important to Flottweg as this simplifies shipping arrangements enormously. One part of the requirements to obtain the certification is a trio of physical security measures consisting of securing the perimeter, ensuring surveillance of the dispatch hall, and visual supervision of the loading area. The premises surrounding the factory hall are



Vilsbiburg – Flottweg SE company headquarters



Access management via number plate recognition with Dallmeier box cameras and ANPR solution



Factory hall and production facility for Flottweg centrifuges

monitored inside a closed perimeter. Each section of fence with a corridor of about 90 meters is subject to uninterrupted surveillance by Panomera S-series cameras.

The multifocal sensor systems are ideal for the long distances along the fence because their special sensor arrangement guarantees high image resolution even at long distances. So any sort of movement by people or vehicles can be tracked for long stretches with no loss of recording or changes of camera. Besides protection against unauthorized entry and assistance with incident investigation, the 1,700 square meters of shipping hall and dispatch area, as well as the loading area, are also monitored by cameras.

Apart from the image quality, the low costs of infrastructure were a powerful argument in favor of installing the Panomera systems: "If you only consider the hardware components, comparison offers are cheaper. But if you look at the overall situation, we only need a fraction of the infrastructure of cables, masts, network, and cameras. So, in regard to overall costs, the Panomera is the least expensive variant, and it also makes the operator's job much easier because he no longer has to keep track of the images from countless cameras on the monitor wall, as there are only a few to watch," explains Andreas Franz, Managing Director of Franz Sicherungstechnik.

Alarm Activation at the Gatehouse

Flottweg uses the SeMSy Compact Video Management Software (VMS) for alarm activation and analysis. It is an ideal VMS solution for smaller and mid-level requirements, and the innovative assistance system makes it easy for operators to rapidly find sequences of interest with the convenient search function. The site plan and a user-friendly dashboard enable incidents to be categorized quickly and efficiently investigated.

The prize-winning Mountera installation system (iF Design Award & Red Dot Award Winner) proved its efficiency for Flottweg too when installing the Panomera cameras.



Robert Waxenberger,
Deputy IT Director,
Flottweg SE



Andreas Franz,
Managing Director, Franz
Sicherungstechnik GmbH



Christian Linthaler,
Dallmeier Sales Director
international/national

Andreas Franz is impressed: "Mountera has made our lives much easier. A Panomera system weighs 17 kilograms, and the quick-lock design makes installation much, much simpler."

Number Plate Recognition

Behind the automated employee access management system is the new Dallmeier number plate recognition system. The ANPR cameras and associated software read the vehicle license plates and the barrier opens automatically for those that are registered. "This makes vehicle access easy for the employees, and Flottweg has the certainty that no unauthorized vehicles are present on the premises," says Andreas Franz. But suppliers and shippers who were approved by Flottweg as part of the AEO certification and were registered in advance also benefit from easier access to the loading bays.

Data Protection – "Privacy and Security by Design"

"As a manufacturer, we have the responsibility to supply our customers with safe products," says Christian Linthaler, Dallmeier Sales Director National/International. "With our guiding principle 'Privacy by Design', we offer a comprehensive range of settings for data protection and data

privacy on our products." The privacy of employees can be protected via privacy zones in the camera settings. Sensitive employee areas can, for example, be blacked out or completely excluded from the surveillance area.

"We were extremely satisfied with the customer-orientated solution and project management by Franz Sicherungstechnik. They did excellent work," concludes Waxenberger. "As global players with local roots, both Flottweg and Dallmeier combine tradition with leading edge methods. At the same time, we have the same quality requirements for planning, implementation, and products. We are very glad that we decided on a Dallmeier solution in cooperation with Franz Sicherungstechnik again."



**More Information
on Youtube**

CONTACT

Dallmeier electronic
Regensburg, Germany
Tel: +49 941 87000
www.dallmeier.com



Dallmeier Panomera cameras provide perimeter protection



Registered suppliers and shippers benefit from camera-controlled, simplified access to the loading bays



MACHINE AND SYSTEM SAFETY

Creation of Safety-Related Application Software

Practical Examples for Familiarization with Handling

Safety-related application software plays a crucial role when it comes to the reliability of the installed safety technology. The Softema software tool provides valuable assistance during the development of this software. Phoenix Contact offers corresponding services for familiarization with the handling of this tool.

The first safety-related controllers were introduced to the automation market over 25 years ago. What was a rarity at the time can now be found in countless machines and systems. At first glance, safety PLCs immediately differ from standard controllers due to their yellow color. But there is a much more important distinguishing feature: safety PLCs often have two beating “hearts” inside. This means that two processors control the program sequence and only enable the outputs in unison with each other. These

outputs can then safely start or stop motion sequences, for example.

The advantage of the safety-related controller is its flexibility when implementing safety-related links. This is why, when it comes to implementing health and safety requirements, the safety PLC is also part of the safety chain. As a result, the safety controller has been designed accordingly by the controller manufacturer and, for example, has been certified for safety level SIL 3 in accordance with international standard IEC 61508.

However, when it comes to the application software, it is the manufacturer of the application who is responsible for this task. The relevant software development requirements can be found in the standards for functional safety. Within the scope of the Machinery Directive, these standards are EN ISO 62061 and DIN EN ISO 13849-1. The latter is often favored in machine building. The standard distinguishes between different performance levels (PLr), which have been determined as the target for the safety function in the risk assessment. The

classification ranges from PLr a to PLr e for hazards with a high risk.

Separation of Safety-Related and Non-Safety-Related Software

The required performance level (PLr) is also crucial when creating the application software for the safety controller. Section 4.6 of DIN EN ISO 13849-1 lists general basic requirements that must be met for each performance level. They are supplemented by additional requirements that must be observed from performance level PLr c onwards.

In this context, it is assumed that the application software used is in a programming language with limited language scope (LVL – Limited Variable Language) – and preferably graphical programming. If, on the other hand, an unlimited language scope (FVL – Full Variability Language) is used, the much more extensive development and validation processes of basic safety standard IEC 61508 must be followed.

This is why most safety controllers only provide the user with a limited language scope. For example, this means that the controllers do not support program loops and program jumps, so that the software program remains clear and maintainable.

The separation of safety-related and non-safety-related application software is equally important, as the actual process control is usually modified more frequently. The programmer sometimes even makes changes just before startup. When using certified safety controllers, such as the safety PLCs from Phoenix Contact, this separation is ensured and safeguarded by a unique checksum.

Basic Requirements in Accordance with DIN EN ISO 13849-1

Starting with the specification, the simplified V-model can be applied for the generation of safety-related application software. The basic principles for fault avoidance and fault control also include modular and structured programming, as well as the validation planning of programmed safety functions in the possible operating states.

It is not unusual for adjustments to be made to the safe application software during the course of the project. The normative requirement for the definition of suitable development activities in view of software modifications is therefore very well documented. In addition to the aforementioned basic requirements, there are further additional requirements that are mandatory from performance level PLr c onwards.

Softema Tool for Implementing Normative General Conditions

The query as to whether the requirements have been implemented in accordance with DIN EN ISO 13849-1 is also integrated into the Sistema software utility of the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA). Specifically, it queries the following: "... safety-related software developed in accordance with Section 4.6 or no software available."

The implementation query is often quickly confirmed by users with a check mark. However, during the course of their work in Germany, the team at the Phoenix Contact Competence Center Services found that these requirements had only been implemented to some extent or had not been implemented at all. This was recognized by the IFA and, in addition to the Sistema software utility for the safety-related hardware, a free software tool for the normative software requirements – Softema – was made available on the German market in March 2022.

The Softema software tool is based on a matrix method that is used to specify the interconnection of the safety logic and all the required validation activities. Built-in user management enables role-based editing of the Softema project and therefore



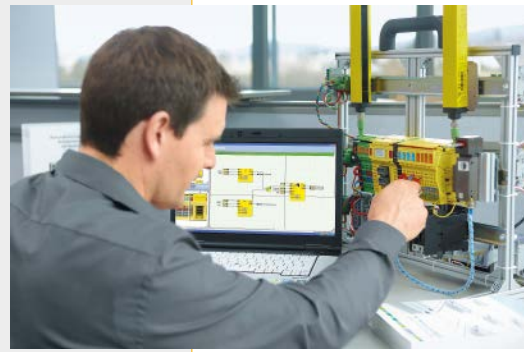
Programmable safety provides users with a high degree of flexibility when it comes to the design of safety functions. However, this advantage calls for a systematic and controlled approach with respect to the development and validation of the application software



Application software with limited language scope (LVL – Limited Variability Language)

Services for the Development and Testing of Safety-Related Application Software

The Machinery Directive demands compliance with health and safety requirements. This also includes the proper integration of safety functions as a risk-reducing measure. The use of safety-related application software plays a crucial role when it comes to the reliability of the safety function. However, users are often unsure of how the normative development and testing of safety-related application software should be implemented. In Germany, therefore, Phoenix Contact offers corresponding services that provide support in various ways. They cover a wide range of training options through to the creation of the complete verification documentation including the validation and effectiveness testing of the safety function. The normative requirements of DIN EN ISO 13849-1 provide the basis for this.



Simulation of the safety-related application software enables errors to be identified at an early stage

also provides protection against unauthorized changes.

Softema provides users with the methodology to implement the requirements in accordance with DIN EN ISO 13849-1. In addition to the project-specific Softema data, such as the Cause & Effect matrix, cross-project master data is available, which can be used for other Softema projects. This includes, for example, programming rules, personal data, and the description of function blocks.

Interested users can check out the handling of the software tool in the Softema guides which are currently only available in German language. Furthermore, Phoenix Contact and other companies already

offer Softema seminars in Germany where practical examples are used to familiarize participants with the handling.

Detection of Systematic Failures

When you reach a certain number of safety functions with a certain level of complexity, using a programmable safety controller rather than a classic safety relay is more advantageous. When the normative requirements are taken into consideration in the programming of the safety controller, this helps the user detect systematic failures early on in the creation of the safety-related application software. Hazardous situations in day-to-day work activities can thus be avoided. It is therefore necessary to inte-

grate the normative requirements into the development process.

Author

Andreas Otto

Safety & ICS Security
Consultant, Phoenix Contact
Deutschland GmbH



CONTACT

Phoenix Contact GmbH & Co. KG

Blomberg, Germany
info@phoenixcontact.de
www.phoenixcontact.com

Video Door Entry System

St Paul's Square, located in the iconic 201 St John Street, is a nine-block development of 85 modern one, two, and three bedroom apartments and maisonettes in the heart of London. Comelit-PAC was chosen by Greywood, who have a close working relationship with London Block Management, as the dedicated managing agents to the development. The specification included a digital panel alongside nine secondary bespoke video panels to accommodate the different blocks within the development. Access control was updated with a dedicated Simplekey advanced system. Greywood installed one digital panel with prox cutout to the main entrance of the building, complemented with nine secondary bespoke video panels to gain access to each development. Each apartment block has been fitted with the Simplekey access control solution coupled with mini hands-free monitors, allowing visual door entry operation through its specialist SimpleBus 2-Wire solution.

www.comelitgroup.com

Face Recognition OEM Module

Suprema AI, a company specialized in artificial intelligence-based integrated security solutions, officially launched a high-performance face recognition OEM module called Q-Face Pro at ISC West. It comes equipped with an excellent AI-based face recognition algorithm and a Neural Processing Unit (NPU) – the latest in AI processor technology – providing fast and accurate face recognition of up to 50,000 users. It also accurately detects fake faces and authenticates when users' faces change, such as when wearing different types and colors of masks, hairstyles, hats and glasses. Q-Face Pro meets European GDPR regulations and protects user information from external hacking attempts by incorporating a separate Secure Element (SE) chip and adopting the highest level of user face data encryption technology. Suprema AI provides SDKs for each major operating system, along with real-time technical support channels to optimize development solutions.

www.suprema.co.kr

SECURITY MANAGEMENT

Security Management



Funkwerk video systeme GmbH
Thomas-Mann-Str. 50 · D-90471 Nürnberg
Tel. +49(0)911/75884-518
info@funkwerk-vs.com
www.funkwerk.com/videosysteme
CCTV, system solution, system integration,
video monitoring security, building management

Security Management



Ksenia Security S.p.A.
Strada Provinciale Valtellino, 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



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
Heckenrosenstr. 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 1 · 58540 Meinerzhagen
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

Video Technology



Abetechs GmbH (Grundig Security)
Steinhof 39 · D-40699 Erkrath/Germany
Tel. +49 211 5380 6832
info@grundig-security.com · www.grundig-security.com
The impressive new GRUNDIG Security IP range covers everything required in modern, professional video surveillance applications.

Video Technology



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

Video Technology



EIZO Europe GmbH
Belgrader Straße 2 · 41069 Mönchengladbach
Tel.: +49 2161 8210 0
info@eizo.de · www.eizo.de
Professional monitors for video surveillance with visibility enhancement technology and 24/7 use, IP decoding solutions to connect IP cameras without any computer.

Video Technology



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

Video Technology

www.luna-hd.de

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
Umlandstr. 165 · 10719 Berlin
Tel. +49 30 12084892 · Fax: +49 30 120858695
hello@doorbird.com · www.doorbird.com
Access Control; Building Automation; Biometric Verification; IP Video Door Station; IP Intercom; RFID; Customized Intercom Systems; Made in Germany

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



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

Be Part of the Section



Just send a mail to
miryam.reubold@wiley.com
We will be glad to advise you!

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



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

FIRE PROTECTION

Time + Access



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



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).

Fire Protection



Labor Strauss Group
Headquarters: Wiegelestraße 36, 1230 Vienna, AUSTRIA
Tel.: +43 1 521 14-0
office@lst.at · www.laborstrauss.com
The specialists for fire detection systems and extinguishing control systems

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



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

PLANT SAFETY

Time + Access



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



Suprema Europe
Tel.: +33 1 84 73 29 43
Sales_eu@supremainc.com · www.supremainc.com
World-leading GDPR-designed biometric technologies, ID solutions, RFID physical access control and time management for your organization. Increase security and experience peace of mind with Suprema's trusted solutions.

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, optoelectronic and ultrasonic sensors, vision sensors, identification systems, interface modules

Company Index

Adani	40	Dormakaba	18	Ksenia	Inside Front Cover, 17	Salto	17, 21, 37
Advanced Perimeter Systems	42	Eagle Eye Networks	13, 35	L3Harris	40	Securiton	19
Advancis	18	ESG	6	Linde	11	Senstar	15, 40, 42, 48
AG Neovo	13	Euralarm	8	Magos	7	Sick	11
Ajax	20, 38	Evva	16	Meister Automation	10	Siemens	19, 20, 21
Altronix	32	Fiera Milano	6	Messe Düsseldorf	35	Smiths Detection	6
AMG	6	FirePro	8	Messe Frankfurt Middle East	8	Sorhea	40, 42
Amthal	7	G+H Isolierung	20	Mobotix	20, 27, 28	Southwest Microwave	40
Assa Abloy	15, 33, 34, 36, 39	Genetec	16	Motorola Solutions	14	STid	26, 36, Outside Back Cover
Astrum	15	Geutebruck	14	Moxa	10	Suprema	56
Axis	13	Gloria	20	Munk Group	12	TDSi	7
BKS	30, 43	Grasp Innovation	6	Navtech Radar	19	Telenot	17
Bosch	Front Cover, 13, 15, 22	Gretsch-Unitas	30, 43	Nutech	40	Til	17
Brivo	16	Halma	8	Onvif	8	TRD	40
Capra	18	Haverkamp	40	Optex	29, 42	TXOne	11
Cemo	11	HID	16, 37	Pacom	7	Uvex	12
Cias	7, 40, 42	Hikvision	14, 19, 51	Phoenix Contact	12, 54	Vivotek	35, 40
Comelit	56	Hoffmann Group	11	Pilz	10	Wanzl	19
Costar Technologies	6	Idis	6	Pizzato Elettrica	10	Winsted	40
Dallmeier Components	21	Innosent	42	Puretech	8	ZVEI	8
Dallmeier electronic	13, 40, 45, 52	i-PRO	14, 28	Qognify	7		
Dedrone	18, 40	Johnson Controls	16	Raytec	12, 15		
Detection Technologies	42	Konica Minolta	28	RBtec	40		

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

- Sabine Haag
- Dr. Guido F. Herrmann

Publishing Directors

- Dr. Heiko Baumgartner
Tel.: +49 (0) 6201/606-703
heiko.baumgartner@wiley.com
- 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
leising@leising-marketing.de

Wiley GIT Reader Service

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

Editorial

- Lisa Holland M.A.
Tel.: +49 (0) 6201/606-738
lisa.holland@wiley.com
- Matthias Erler
+49 (0) 6129 5025300
matthias.erler@wiley.com

- Eva Kukatzki
Tel.: +49 (0) 6201/606-761
eva.kukatzki@wiley.com

Editorial Assistant

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

Production

- Jörg Stenger
- Andi Kettenbach (Layout)
- Elli 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: DE55501108006161517443

GIT SECURITY is published
4 times per year.

Subscription 2023

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.

Print run: 20,000



Printed by

westermann DRUCK | pva

Printed in Germany | ISSN 2190-4367

WILEY

MAKE YOUR ACCESS CONTROL INTUITIVE



Instinctive Technologies for a World without Constraint



CARD MODE



SLIDE MODE



TAP TAP MODE



REMOTE MODE



HANDS-FREE MODE



VOICE COMMAND



SMARTER SECURITY ANSWERS

