EURO SECURITY

The international trade magazine for security & management in the EMEA region

● **Critical Infrastructure**
Real-time video images from surveillance devices attached to power lines

● **INTERSCHUTZ 2022**
Totally digital: From the "digital twin" to control center technology

● **Videosurveillance**
Maximize situational awareness in perimeter security applications

Content

—- www.euro-security.de —-

Polaris Market Research: Physical security market to rise to around €138 billion by 2028

According to a new study by Polaris Market Research, the global physical security market is expected to reach €137.99 billion by 2028.

Various factors - such as the growing number of smart city projects in the public sector, are pushing the sales of physical security systems. In addition, infrastructure improvements with access control solutions are contributing to increased market demand. The growing use of IP-based cameras for video surveillance is also stimulating market demand worldwide.

The changing security situation with rising threat of terrorism, increasing insecurity in work environments, and desire for better security in buildings and premises are driving the security industry revenue, according to Polaris.

The transportation sector will grow at the second-fastest compound annual growth rate over the forecast period as demand for traffic and crowd monitoring solutions increases. According to the US-based market research firm, terrorist attacks are the most important growth factor for the industry around the world. In recent decades, both crime rates and terrorist activities have increased.

Dr Claudia Mrozek

Maximize situational awareness in perimeter security applications

Bosch introduced MIC IP fusion 9000i 9mm camera to provide operators with 360-degree perimeter view in 30 seconds. MIC IP fusion 9000i 9mm with power plant background. For further information, please follow this link: **https://www.boschsecurity.com/xc/en/news/product-news/mic-ip-fusion-9000i-9mm/**

Transportation Fraport Twin Star Airport Management AD

How Video In The Cloud Lightens The Load For Bulgarian Airport Security

Double the pleasure – double the fun! The tourist attractions of 'twin' coastal airports in Varna and Burgas, Bulgaria, bring throngs through customs and ensure a busy scene for Fraport Bulgaria. They have partnered for over 10 years with Milestone Systems for ongoing development of their centralized, efficient and flexible video surveillance system, which meets their security demands as they grow.

Fraport Bulgaria moved from analog security technology to an IP-networked Milestone and Axis solution, which enabled them to later add Agent Vi AI analytics then progress into a cloud solution to ease the burden on storage. The video management platform centrally navigates all the physical security needs at both airports.

Trade fair for security
September 20 – 23, 2022
Essen/Germany

[SECURE YOUR BUSINESS]

Video//Access / Mechatronics / Mechanics / Systems/
Perimeter Protection//Digital Networking Security//
Services//Fire / Intrusion / Systems//

BE PART OF IT!

security
essen 22
the number one

MESSE ESSEN

www.security-essen.de

Transportation **Fraport Twin Star Airport Management AD**

Challenge: how analog troubles caused delays

Before the migration to Milestone's virtual solutions, the security and safety at both airports was based on different systems, each with a separate server, with physical storage on local hard drives. Archiving video on these recording servers often was damaged from harsh weather conditions.

Each system was accessed differently

- and so slowly
- that it wasted a lot of time, making it difficult for them to monitor the condition of all hardware, andeven impossible to recover data in cases of shutdown. This lack of reliability in the analog approach failed to facilitate the security team's work.

Fraport Bulgaria also wanted the alerts and analytical functions of a digital solution with alarms for violations, so they could operate both reactively and proactively.

Solution: smooth flying with unified security

Today, an in-house cloud solution for video management with Milestone's software platform provides centralized, optimized, easy operations, pro-

"We use artificial intelligence and defined perimeter zones. If an object is detected to stay longer than the customized rule we set in XProtect, an alarm is raised in the Milestone system, which the operators in the monitoring center see, and they can direct other cameras to focus on the area where the event is registered. Response is faster and better informed on which actions to take."

Vladimir Petrov, former Head of IT Fraport Bulgaria

cessing the entire flow of security information in a virtual infrastructure.

Milestone XProtect Corporate manages over 500 AXIS network cameras,

| Location Burgas and Varna, Bulgaria | Milestone software XProtect® Corporate | Milestone Add-ons XProtect® Smart Wall |
| Integrations AXIS Perimeter Defender, Agent Vi video analytics | Devices 500+ AXIS cameras | Partners RAD GROUP Communication Technologies |

and various analytical functions are integrated for metadata utilization: VMWare, Agent VI's InnoVi™ analytics, AXIS Perimeter Defender, and border crossing signalization alerting to unauthorized access and more.

The system alerts when a specific event occurs and directs the security team's attention right to the location. Everything is recorded and documented, from the event itself through the

to using much less staff resources, limiting the people factor helps to avoid human error.

The system was implemented with the system integrator RAD GROUP Communication Technologies – a Milestone Systems Gold Partner, who provides support and periodic updating of the Milestone XProtect Corporate software. RAD GROUP is a private Bulgarian company for system

reconfigured depending on the changing needs of the airports.

When Fraport Bulgaria wants another 500 cameras, adding and integrating is very fast – with just a few clicks. There is no need to buy additional storage hardware and install it on premises: it's all organized in a private cloud system. In it, each virtual machine is reserved and protected from unforeseen interruptions at the circuit

subsequent actions of the operator, and ends with closing the alarm on resolution.

Human intervention in decision making has been minimized by automating the analytics and response. The Agent Vi software detects and tracks objects, violations or other incidents, and based on pre- established rules, sends a signal to the system for certain actions. In addition

design and installation of complete information infrastructures, solutions for corporate networks and information security.

Result: an easy virtual journey

Milestone's open platform ensures that options are not fixed and limited. The Fraport Bulgaria solution is a living virtual system that can be upgraded quickly and easily, expanded and

level, and with access to a centralized disk. If they need to expand, resources can be added quickly. The advantage of this architecture is flexibility, security and quick response if necessary.

The high level of security, saving personnel resources and flexible upgrades are key advantages of implementing the Milestone video surveillance solution, according to Vladimir Petrov

at Fraport Bulgaria. He referred to the changing needs of the company and the ongoing updates over time. In 2018 a project for perimeter security was initiated adding AXIS thermal cameras to ensure detection of unauthorized, prolonged stays in any specified area.

Benefits keep climbing over time

Fraport also constructed an XProtect Smart Wall video display. This video wall has 12 big screens, each supported by two workstations with specialized graphics cards, and they have defined different priority zones and time zones. In case of an incident, the specific object or area where the event is registered is seen imme-

> "The value of Milestone software is that it's an open system that can be upgraded and connected to other systems at any time and without much effort, to ensure the highest level of security."
>
> **Vladimir Petrov, former Head of IT Fraport Bulgaria**

diately on the video wall. The biggest change was the airports' integration of Milestone with the corporate Microsoft Active Directory™, where user access to the system is set based on their security groups.

Other major shifts include a platform update with the integration of a mobile server giving users access via a standard web browser, also incorporating a mobile application for Android, which makes any smartphone or laptop

"If a camera captures a person's face, and we can compare information about the person's pass number and his image, we can very easily detect unauthorized access and raise an alarm in the security center where it's happening."

Vladimir Petrov, former Head of IT Fraport Bulgaria

The virtual environments for the servers of each airport provide reliability with flexible allocation of resources and guaranteed access to the disk resource for stored video recordings.

The way up is open to innovation

The continuous upgrade and integration options of the Milestone open platform allowed Fraport Bulgaria to add facial recognition access control in areas that were only admissible with a physical pass.

The company also plans to integrate AI to provide information on crowding and non-compliance with the recommended distance between people, as required by pandemic regulations.

function with the video surveillance like an additional camera, sending its images back to the central system. The latest functionality was designed for the security teams who monitor a fenced perimeter. Any detected violation can be registered and viewed in real time or reviewed and analyzed in recorded playback.

About Fraport Bulgaria

Fraport Bulgaria is a German-Bulgarian company that has the consignment to manage the Varna and Burgas Airports for 35 years. The two airports are gateways to the Bulgarian Black Sea coast, providing round-the- clock service. Fraport Bulgaria takes care of improving the quality of service and the overall experience of passengers, training and retraining employees, updating equipment, introducing new technologies, as well as expanding and modernizing the infrastructure.

• Varna lies 470 km northeast of Sofia
• Burgas is 125 km to the southwest

These areas are big tourist attractions for the miles of sandy beaches and thermal mineral water with low salinity. The mild climate has warm seasonal sunshine, yet is cooler than Mediterranean spots, being moderated by breezes and regular rainfall. Its wooded hills are lush all summer long. moderated by breezes and regular rainfall. Its wooded hills are lush all summer long.

Energy Sector

Transforming overhead power line surveillance
Reduced Cost – Real-time Monitoring – Digital Image Detection

Power grid operators are set to save time and money with new surveillance technology for overhead power lines. The monitoring system is developed by Laki Power and uses MOBOTIX cameras. For the first time, operators will have live, real-time video images of critical infrastructure from surveillance devices attached to power lines. Operators worldwide spend millions ensuring power lines are protected against fire and can operate in harsh and inaccessible environments. But installing and powering sensor equipment in remote areas is difficult and costly. The Laki Power technology dramatically improves access and cuts surveillance costs by over 90 percent. It has been developed in extreme Nordic weather conditions and uses MOBOTIX cameras to survey power lines and masts.

Risks & Challenges

As society switches from fossil fuels to more electricity, demand on power infrastructures increases significantly, so power grid operators need to maximise network capabilities. But protection against threats like fire, line icing and extreme environmental conditions in remote areas make monitoring network integrity challenging. Surveillance and security operations are based on regular visual inspections – sometimes requiring helicopter fly-bys - which are costly and time consuming. Spotting instant threats like fire are particularly difficult. Using CCTV equipment has, until now, been almost impossible because of power requirements in areas where there is no access to electricity. Installing diesel, solar or wind generators is costly and only for the most challen-

> „The MOBOTIX solution is critical to helping us develop an innovative way for power grid operators to transform the surveillance of overhead power lines. MOBOTIX enables our technology to deliver live video and high-resolution images in harsh, inhospitable conditions. It means that we can help grid operators to fast-track digital surveillance of network operations at a fraction of current costs. " Bjorgvin Sigurdsson, CEO, Laki Power

ging locations. Even then, such systems do not produce enough power to ensure optimum CCTV performance. Often existing monitoring and CCTV equipment used in harsh environments does not last very long.

Solutions & Benefits

MOBOTIX and its Icelandic business partner Hafnes ehf have helped Laki Power develop the new grid monitoring technology. For the first time, it gives power grid operators real-time surveillance images from equipment located directly on overhead power lines. The Laki Power LKX multi-purpose surveillance station is designed to withstand the high-voltage and electromagnetic fields that prevail on power lines. It uses MOBOTIX cameras and other sensors to monitor power cables, pylons and the immediate environment for damage and threats like fire, ice or fallen trees. According to estimates from grid operators, Laki Power saves over 90 percent of installation costs compared to current solutions. After several failed trials with other CCTV equipment, Laki

Power chose MOBOTIX technology. Besides image quality and clarity, MOBO-TIX cameras are very durable especially in harsh conditions. The cameras are fibreglass so do not corrode or interfere with conduction and, with other components, cut the number of moving parts making the LKX less likely to fail. The LKX has camera heaters which mitigate freezing and lens fogging due to moisture. Because of the MOBOTIX equipment and robustness of the product, Laki Power estimates the LKX can last for up to ten years before it may need replacing. The LKX replaces regular, visual inspection with remote, 24/7 video surveillance, making costly and difficult onsite visits redundant. If an onsite inspection is required, real-time video can check if conditions are safe. Video data is also used to review incidents for future prevention and proactive rather than reactive maintenance. Depending on application, the LKX uses several MOBOTIX cameras including high-resolution, 360-degree ones with night vision and fish-eye lenses. Laki Power is also testing MOBOTIX

thermal cameras for fire event detection. The LKX generates power from the electromagnetic field surrounding the power line using induction. This removes the need for a separate power source.

Summary

With MOBOTIX CCTV equipment, Laki Power is helping power grid operators cut costs and improve power network management and energy transmission rates. Alongside trial projects with the Icelandic and Norwegian grid operators, Landsnet and Statnett, Laki Power is working with multiple other operators around the world to test the product.

Laki Power has established an ongoing partnership with MOBOTIX to develop and enhance the LKX product platform with advanced capabilities. This includes technologies such as MOBOTIX thermal imaging cameras to detect wildfire risks and helping operators leverage big data and video images for intelligent, AI-based network management.

Cloud Solutions

Cisco Unveils Innovations Driving New Security Cloud Strategy

Cisco unveiled its new strategic vision of a unified platform for end-to-end security across hybrid multi-cloud environments • The company is designing the Cisco Security Cloud to be the most open security platform with no public cloud lock-in • Cisco is taking steps to realize its vision with innovations across the industry's most complete portfolio, driving security resilience for its customers

Cisco unveiled its plan for a global, cloud-delivered, integrated platform that secures and connects organizations of any shape and size. The company is designing the Cisco Security Cloud to be the industry's most open platform, protecting the integrity of the entire IT ecosystem - without public cloud lock-in.

"With the complexity of hybrid work, continued acceleration of cloud adoption, and the ever-advancing threat landscape, organizations are looking for a trusted partner to help them achieve security resilience. We believe Cisco is uniquely positioned due to its scale, breadth of solutions and cloud-neutral business model to meet their needs," said Jeetu Patel, Executive Vice President and General Manager of Security and Collaboration at Cisco. "Cisco is already delivering upon key tenets of our cloud platform vision. We're excited to increase our innovation velocity to truly deliver on the vision of the Cisco Security Cloud."

The Security Cloud will provide an integrated experience for securely connecting people and devices everywhere to applications and data anywhere. With unified management, the open platform will provide threat prevention, detection, response, and remediation capabilities at scale. Cisco has been on the journey toward the Security Cloud for some time and is sharing additional progress with new innovations across its security portfolio.

Secure Access

Ushering in the next generation of zero trust, Cisco is building solutions that enable true continuous trusted access by constantly verifying user and device identity, device posture, vulnerabilities, and indicators of compromise. These intelligent checks take place in the background, leaving the user to work without security getting in the way. Cisco is introducing less intrusive methods for risk-based authentication, including the patent-pending Wi-Fi fingerprint as an effective location proxy without compromising user privacy.

To evaluate risk after a user logs in, Cisco is building session trust analysis using the open Shared Signals and Events standards to share informa-tion between vendors. Cisco unveiled the first integration of this technology with a demo of Cisco Secure Access by Duo and Box.

"The threat landscape today is evolving faster than ever before," said Aaron Levie, CEO and Co-founder of Box. "We are excited to strengthen our relationship with Cisco and deliver customers with a powerful new tool that enables them to act on changes in risk dynamically and in near real-time. You can expect to see more innovation and execution from Box and Cisco that help businesses protect their content across any location, application, or device."

Secure Edge

To radically simplify how organizations connect and protect users, things, and applications, anywhere, Cisco is excited to introduce Cisco+ Secure Connect Now, a unified Secure Access Service Edge (SASE) solution. Cisco+ Secure Connect Now is a turnkey offer available in several countries that allows customers to quickly deploy SASE and ease day-to-day operations through a cloud-managed platform. The as-a-service subscription is optimized for value and mana-

ged through a unified dashboard. Cisco offers unmatched breadth and depth in its networking and security capabilities, which is why Telefonica Tech will add Cisco's SASE suite to its service portfolio.

"As businesses shift to support hybrid work and work from anywhere models, we are committed to helping them adapt to the increased demand for high performing and secure connectivity," said Rames Sarwat, Director of Cyber Security & Cloud Products and Services at Telefonica Tech. "Together with Cisco, we will offer customers an innovative, managed service that will combine SD-Branch with Cisco SASE to address a complete set of next-generation connectivity and security use cases for the branch and the hybrid worker."

Secure Operations

Cisco added a new Talos Intel On-Demand service offering custom research on the threat landscape unique to each organization. To help accelerate incident detection and response, Cisco announced enhancements to Cisco Secure Cloud Analytics with its ability to automatically promote alerts into SecureX and map those alerts to MITRE ATT&CK. This follows the general availability of SecureX device insights to aggregate, correlate, and normalize data about the devices in their environment, and the integrations of Kenna and Secure Endpoint to better prioritize vulnerabilities. Cisco also introduced the Secure Firewall 3100 Series, designed for hybrid work with a new encrypted

visibility engine that uses artificial intelligence and machine learning to detect hidden threats.

Simplification

Cisco is introducing simplification across the portfolio with the new unified Secure Client. Streamlining how administrators and users manage endpoints, half of Cisco Secure agents, including AnyConnect, Secure Endpoint, and Umbrella, will be unified by mid-year 2022 with additional agents to be added over time. This follows the new cloud-delivered Secure Firewall Management Center, which is enabled through the Cisco Defense Orchestrator and unifies cloud and on-premise firewall management.

[https://tinyurl.com/36x864my]

Cloud Controls released

Framework To The Public, Making Security Certification Ever More

Cisco released the Cisco Cloud Controls Framework (CCF) to the public. The Cisco CCF is a comprehensive set of international and national security compliance and certification requirements, aggregated in one framework. It empowers teams to make sure cloud products and services meet security and privacy requirements thanks to a simplified rationalized compliance and risk management strategy, saving significant resources.

Meeting the fast-evolving requirements for security certifications and standards across the globe is becoming increasingly important, but also extremely challenging, and resource- and time-intensive

for Cloud-based software providers. "The Cisco CCF is central to our company's security compliance strategy. By making it available for public use, we are helping ease compliance strain and enable smoother market access and scalability for the cloud community," explains Prasant Vadlamudi, Cisco's Senior Director for Global Cloud Compliance. "By sharing our CCF with customers and peers, we also continue to support our commitment to transparency and accountability that are foundational to Cisco's DNA."

The CCF is the foundational methodology for Cisco to accelerate certification achievements across our cloud offerings and establish a strong security baseline. It is the result of years of standards research to certify SaaS products for multiple standards for repeatable practices and efficiencies. The CCF offers a structured, "build-once-

use-many" approach for achieving the broadest range of international, national, and regional certifications.

With this framework, organizations can define, implement, and demonstrate controls that are foundational to security and privacy certifications consistently across SaaS portfolios, such as SOC 2, ISO 27001: 2013, ISO 27701, ISO 27017, ISO 22301, ISO 27018, Germany's BSI C5, FedRAMP Tailored for the US public sector, the Spanish ENS, Japan's ISMAP, PCI DSS v3.2.1, the EU Cloud Code of Conduct, and Australia's IRAP.

The CCF comes with guidance on how to implement these controls and the audit artifacts needed to demonstrate controls operating effectiveness. Cisco will regularly update the CCF as regulations evolve and new frameworks are integrated into our compliance processes.

Access Control

Security technology manufacturer Telenot fully enters the access control technology market

hilock 5000 ZK: powerful and efficient access control

In addition to burglar and fire alarm systems, access control systems play an essential role in protecting people, rooms and the material and non-material assets they contain. With hilock 5000 ZK, Telenot presents a powerful, flexible and scalable system that controls who can enter where and at the same time helps to efficiently control operational processes and visitor flows - in office buildings as well as in large industrial operations. Optionally, the system can also be combined with a VdS-compliant burglar alarm system.

"For companies of all kinds as well as for public buildings, it is of obvious importance to control secure access to the building as well as the flow of people and access authorisations inside in a structured and precise way.

Because security starts at the company door," says Hendrik Spering. The Telenot product manager is one of the developers of the innovative access control system hilock 5000 ZK, the latest addition to the company's portfolio. Now the specialists for electronic security technology have presented a comprehensive expansion stage for the system.

Optimum processes for every requirement

As usual from Telenot, hilock 5000 ZK impresses with the highest performance and efficiency for every type of building. "When we developed it, we had in mind a system that is flexible in every respect, enabling optimum business processes and visitor flows, regardless of whether it is a small shop, an administration building or a large industrial facility," Spering elaborates. Particularly practical: thanks to the VdS recognition of the hilock 5500 control unit as a switching device for a burglar alarm system, access control and burglar alarm technology can be linked together economically and in a VdS-compliant manner, as required by building insurance companies.

Basic licence enables comprehensive solutions

The basic principle of the access control system hilock 5000 ZK is simple: Every individual who wants to enter the building is checked before entry.

If someone is not authorised, they are not allowed to enter. The complexity is hidden in the details: For companies, for example, it is important that all employees can enter the company premises without delay. However, if there are areas that should only be accessible to certain groups of people, the same access control system must also regulate such authorisation solutions. And this, if necessary, with time restrictions or under other predefined conditions. The new access control system makes it possible to flexibly configure and control such authorisation solutions in buildings of any kind. This makes it easier for users to realise optimal business processes or visitor flows.

"In combination with the compasZ 5500 management software as well as the hilock 5500 evaluation control unit with integrated Ethernet interface, we offer an economical solution for every property size and type," says Spering. It is very easy to set up function time models, for example, to control the opening of shops. Special routines for public holidays are also no problem for the system. Both reduce the time spent on administration considerably and serve the security of the company. In addition, all access rights can be coordinated across locations - whether from one or several sites. The new hilock 5000 ZK system also offers countless other applications such as area change control, counting functions, lift control, toggle authorisations, admin management, creation of organisational units and groups. The highest encryption standards ensure maximum security - from the management software to the hilock 5500 evaluation and control device, the RFID reader and the transponder. Even with the basic licence, the access control system allows you to set up a solution that is sufficient for many applications.

Should an extension of functions or licences become necessary, for example due to the opening of a new location, this can easily be carried out by the specialist company via the Telenot online shop, which is accessible around the clock.

Access control with chip, code or smartphone access

For on-site use, users can access a

Powerful and efficient access control

wide range of peripheral products. In addition to the familiar cryplock RFID readers - optionally with or without an additional keypad - Telenot has a brand new selection of mechatronic locking elements in its range - lever handles, door fittings, locking cylinders, furniture locks or locker locks.

They connect centrally wired online access control systems with mechanical locking systems. This new type of access control has many advantages, as Spering explains: "The costs incurred in a company because of lost keys are considerable. Depending on the system and the key, they can easily reach a four-digit amount. With our mechatronic locking system, only the lost transponder has to be blokked." This is done easily and quickly in the software.

Flexible authorisation management

The innovative character of the access control system is also evident in the management of authorisations. With Credential Data Management (CDM), the user has a choice of two online variants (classically wired or as a radio system) and an offline system. With the latter, access authorisations are written directly to the transponders.

Since the component has no direct access to the evaluation and control unit (i.e. it is offline), the transponder is also used for data transfer between the online and offline systems. In addition, a smartphone Access CDM can also be integrated into the system. In this case, an app on the smartphone serves as a transponder.
[www.telenot.de]

Genetec

Next-generation Synergis Cloud Link: Provides more features, enhanced cybersecurity, and helps future-proof security installations

Genetec Inc announced the immediate availability of a new generation of its Synergis Cloud Link PoE-enabled IoT gateway for access control. Manufactured in North America to mitigate supply chain delays, Synergis Cloud Link addresses increasing demand for non-proprietary access control solutions and provides a safe and secure gateway to a cloud or hybrid deployment.

When modernizing an existing security system, Synergis Cloud Link's open architecture allows organizations to leverage their current access control infrastructure and easily upgrade to a secure IP-based solution. Synergis Cloud Link provides a more efficient approach to multi-site deployments and replaces the need for servers, reducing the cost of ownership. The Synergis Cloud Link IoT gateway has embedded functionalities that keep an organization's access control running even when connection to the server is down. The new generation of Synergis Cloud Link provides more features, enhanced cybersecurity, and helps future-proof security installations. Synergis Cloud Link features enhanced cybersecurity such as encrypted user data, Secure Boot, and an EAL6+ industry gold standard Secure Element that stores cryptographic elements.

"The need for non-proprietary access control solutions has never been greater," said Thibault Louvet, Access Control Product Group Director, Genetec Inc. "Our new generation Synergis Cloud Link enables us to provide organizations with a powerful, secure and intelligent gateway to the latest technology while allowing them to easily connect to hybrid or cloud access control environments and keep their existing security investment including hardware, wiring, and infrastructure."

The device is compatible with non-proprietary access control modules from the industry's most established manufacturers including HID Global, Axis Communications, ASSA ABLOY, Mercury Security, Allegion, SimonsVoss, STid, and others. A single Synergis Cloud Link device can support up to 256 readers and electronic locks, 600,000 cardholders, 150,000 offline events, as well as monitor hundreds of zones and alarms.

Synergis Cloud Link features a new firmware design, improving reliability and lifecycle management and updates management. It also opens the door to containerized approach for operating software on the device, expanding its future capabilities.

[https://tinyurl.com/4thmwrzx]

BioStar 2 with Automated Failover

Suprema

BioStar 2 Gains Enhanced Stability and Continuity With Automated Failover

Suprema announced the successful integration of its BioStar 2 security platform with Mantech Continuous Cluster Server, a high availability solution provided by Korean service provider Mantech.

BioStar 2 is a comprehensive access control management platform that manages mission-critical security data. Through integration with MCCS, BioStar 2 is able to enhance system stability and expand service continuity. This also ensures greater cost-efficiency, productivity, and availability for BioStar 2 customers by minimizing unnecessary waste of resources to manage failure, such as manpower, applications, and extra storage.

MCCS, the failover system of BioStar 2, uses automated failover and real-time replication to help prevent server downtime, data loss, and system failure. It can detect the failure of servers, storage, networks, application services, and operating systems. When failure occurs, it automatically switches to a backup system and replicates data in real-time so the company can protect mission-critical data 24/7 with no downtime.

"Integrating with MCCS has enabled BioStar 2 to provide an even safer and more secure platform service than ever for our enterprise customers," said Suprema CEO Hanchul Kim, "Suprema will continuously make efforts to enhance BioStar 2 capabilities, meeting the needs of all our customers, from small offices to the largest organizations."

The lead theme of INTERSCHUTZ 2022 is: "Teams, Tactics, Technology – Connecting Protection and Rescue". According to INTERSCHUTZ Project Manager Bernd Heinold, the world's leading trade fair for firefighting, rescue, civil protection and security is thus targeting two aspects that are crucial for the present and the future: the use of innovative digital solutions, but also cooperation between the various players and institutions. "The keyword is connectivity at all levels," Heinold said at an online press conference in Hannover, just one hundred days before the start of the fair. "Digitalization has fundamentally changed all areas of life and continues to do so. The same is true for emergency response – from firefighters to rescue services right through to disaster responders, all over the world."

INTERSCHUTZ showcases solutions facing the challenges of our times

From 20 to 25 June 2022, the topics at INTERSCHUTZ in Hannover, Germany, will revolve around those of firefighting, rescue, civil protection and safety/security. The economic, ecological and political challenges of our times make this flagship fair an important driver of change. The spread of global warming and the resulting natural disasters have already noticeably changed everyday life for many helpers and rescue forces. This has recently been compounded by the coronavirus pandemic and the humanitarian emergencies caused by political conflicts. These all require new approaches and solutions. Digital technologies for the support and connectivity of key players are becoming increasingly important. INTERSCHUTZ 2022 will specifically focus on digital transformation processes. Visitors can look forward to an extensive program – both live on-site and online.

INTERSCHUTZ showcases solutions facing the challenges of our times

For the first time, INTERSCHUTZ has dedicated a complete hall to the topic of digitalization. In Hall 16, companies and research institutions will be presenting solutions for the digital networking of systems and players. As a practical example of the digital application possibilities, Dirk Aschenbrenner, president of the Association for the Promotion of German Fire Protection (vfdb), demonstrated a rescue robot at the press conference, which will also be on display at INTERSCHUTZ.

Another new feature consists of the "Smart Public Safety Hub" at the center of Hall 16, where various companies will be networking under a single roof and demonstrating joint, interdisciplinary application scenarios – for example, the use of drones to assess the situation or support rescue forces, communication between an airfield firefighting vehicle positioned in the outdoor area with the control center in the hall, or the digital description and analysis of deployment sites on a 2/3/4-dimensional scale.

And likewise, the new special show "Future Trends in Public Safety" takes a look at the future technological, organizational and social megatrends in civil security.

The 5G network, permanently installed on the exhibition grounds since the beginning of the year, makes it possible to experience completely new opportunities, as offered by the new standard and direct successor to LTE or Advanced LTE (4G) and UMTS (3G) on the basis of concrete user examples.

At INTERSCHUTZ, it is not only the exhibitors' solutions that are digital, but also the event formats: For the first time, visitors and exhibitors will have the opportunity to literally experience different scenarios up close on the demonstration grounds in a combination of real and virtual displays. These may include everyday disasters as well as current or conceivable catastrophes and crises. With the help of modern media technology, the participants are integrated into the presentation. As a real laboratory at INTERSCHUTZ, the demonstration area becomes a unique experience space.

Equally new is the INTERSCHUTZ Digital Conference, which is scheduled to be broadcast over three days (Tuesday to Thursday) in the Media Factory. This means that even interested parties who cannot make it to Hannover this year will have the opportunity to learn about the various aspects. The conference language of the Digital Conference is English. Like the INTERSCHUTZ Central Forum in Hall 26, the program will cover all the major industry topics, including the electrification of emergency vehicles. Incidentally, there will also be numerous exhibits on this topic at the trade show.

Austrian industry leader Rosenbauer, for example, will demonstrate the world's first fully electric turntable ladder at INTERSCHUTZ. The Berlin Fire Department will be reporting live on its experiences with the eLHF electric firefighting and rescue vehicle, which also comes from Rosenbauer and has already been in use in the capital since September 2020.

"International cooperation is becoming increasingly important. Only recent disasters such as vegetation fires or other natural events have shown this," said the presidents of the vfdb and the German Fire Brigades Association (DFV), Dirk Aschenbrenner and Karl-Heinz Banse. Dr. Bernd Scherer, Managing Director of VDMA Feuerwehrtechnik, also pointed out the continuing willingness of fire departments to invest in vehicles and equipment. vfdb, DFV and VDMA are all non-commercial partners for the event, supporting Deutsche Messe.

Supporting program features numerous highlights.

Parallel to INTERSCHUTZ, the DFV is organizing the 29th German Firefighters' Day, which will attract many more firefighting fans to Hannover.

The event is being organized under the motto "Safety.Life" in cooperation with the state of Lower Saxony, the Lower Saxony Fire Brigade Association, the City of Hannover and the Hannover Fire Brigade. Immediately before INTERSCHUTZ, a "Blue Light Mile" has once again been planned for downtown Hannover. There, the people of Hannover will already get in the mood on the Sunday before the fair.

Action and excitement during the trade fair will be provided by various competitions and live training courses, including, for example, the "S-Gard Safety Tour," the "Holmatro Rescue Challenge," and the "Firefit Championships Europe," which will be held in Germany for the first time after the INTERSCHUTZ Community Days in the summer of 2021, will also be returning to the exhibition grounds.

All in all, visitors can therefore look forward an extensive program of congresses, workshops, training sessions, live demonstrations and competitions in addition to the products on show in the exhibition. Tickets for INTERSCHUTZ can already be purchased online at www.interschutz.de.

From Rosenbauer to Binz:
INTERSCHUTZ shows emergency vehicles of the future

Hannover will become the capital of the blue light scene in a few weeks, despite isolated cancellations by exhibitors from the vehicle technology industry in recent days.

"We regret the cancellations of companies such as Magirus, Ziegler or Schlingmann, of course. Nevertheless, more than 1000 companies from 50 countries will present themselves at INTERSCHUTZ - including many market-leading vehicle manufacturers such as Rosenbauer, Volkswagen Nutzfahrzeuge, BMW, Tatra Trucks,

Oshkosh, Scania or Volkan and 200 other companies from the firefighting technology sector.

So visitors can look forward to an exciting INTERSCHUTZ, because in view of the current challenges, the topics covered at the world's leading trade fair are more relevant than ever before," said Bernd Heinold, INTER-

SCHUTZ Project Manager at Deutsche Messe AG.

Representatives of exhibiting vehicle manufacturers and equipment suppliers expressed similar sentiments. "We can finally present our range of products and services to a large audience again," said a delighted Matthias Quickert, sales manager at Binz

Automotive, one of the leading companies in special vehicle construction, for example. The company had therefore even booked additional stand space for the demonstration area.

Innovations and new technologies for fire departments and rescue services According to INTERSCHUTZ project manager Bernd Heinold, one focus of the trade show will be electro mobility. As an example, he cites Rosenbauer's first electric firefighting and rescue vehicle (eLHF), which is already in test operation at the Berlin Fire Department and will be on show live at INTERSCHUTZ. The project, which is also causing a stir internationally, hints at the future of urban vehicles.

However electro mobility is also making headway in the field of rescue vehicles. One example: Volkswagen Nutzfahrzeuge (VWN). "We are delighted to have INTERSCHUTZ at the gates of our plant in Hanover, so to speak," says Klaus Stiegler, key account manager responsible for emergency vehicles. Among other things, VWN will be showing a product range from command vehicles and multipurpose vehicles to ELW 1 and ELW 1.5 command vehicles. Various command and command vehicles will also be part of the exhibition program at other companies. These include a new type of ELW 3 from BINZ, which can serve as a mobile control center in the event of major emergencies and disasters. In addition, various hybrid solutions will be presented, as well as current vehicles with combustion engines. A number of spectacular contributions also await visitors to the demonstration area. Among others, a visit of a large airfield fire fighting vehicle (GFLF) of the Hanover airport fire department is planned. But powerful vehicles of all sizes on four and more wheels are

not the only ones represented: BMW, for example, will be showing two sprinting motorcycles.

International networking more important than ever

"Rarely before has the need for innovation been so great, especially in the area of hazard prevention," says the president of the Association for the Promotion of German Fire Protection (vfdb), Dirk Aschenbrenner. "Numerous disasters in recent months and,

not least, the pandemic and the incipient movement of refugees from Ukraine have demonstrated in many areas the importance of modern crisis management. For example, the heavy rain disaster last summer highlighted the need for off-road and robust vehicle technology. The international exchange of know-how and experience is important." INTERSCHUTZ is the best platform for this, he said, as it brings together manufacturers from more than 50 countries, including, for example, Oshkosh from the USA and Scania from Sweden.

Innovation meets tradition

For the final day of INTERSCHUTZ on June 25, Thomas Russ of the Lower Saxony Fire Brigade Association has organized a vehicle parade from the INTERSCHUTZ grounds through Hanover's city center and back. In the convoy consisting of several dozen vehicles, for example, a 60-year-old fire truck as well as a nostalgic "Barkas" ELW from GDR times will be on display. "The grand finale will be a meeting with the Red Knights International Firefighters Motorcycle Club, the world's largest motorcycle club for firefighters and their families.

Fire brigades, disaster relief workers and rescue services are facing challenges that did not previously exist in this range. This is because the number of operations and the severity of events are increasing: severe weather disasters, vegetation fires, the corona pandemic and the refugee crisis. These are just a few examples. The main theme of INTERSCHUTZ 2022, "Teams, tactics, technology – protection and rescue networked", sums it up: The world's leading trade fair for fire brigades, rescue services, civil protection and safety (20 to 25 June 2022) will become a huge showcase for providers of innovative solutions for the present and future – for example in hall 16.

Totally digital: From the "digital twin" to control center technology

One hall full of innovations

A survey conducted some time ago as part of a study of 650 participants in fire brigades, aid organizations and the Federal Agency for Technical Relief showed that the emergency services are dissatisfied with the digital development in their organizations. From the point of view of the study participants, comprehensive interfaces for compatible IT systems and hardware were considered necessary. INTERSCHUTZ provides a comprehensive overview of the many possibilities. Stefan Truthän, one of the managing directors of the fire protection engineering office hhpberlin, cites a "digital twin" of hazard prevention as a spectacular example of digital innovations. "This is not about the state of the fire brigade, but

about the state of an entire city," says the expert. "This will turn us into a digital filling station, so to speak, where the fire brigade would receive information about the exact condition of a building, for example, during an operation." The company will be showing what this could look like in practice in hall 16 at booth F42. Experience 5G use cases live

One of the prerequisites for such and other plans to become reality and deliver data in real time is the new 5G mobile communications standard. The topic will occupy a wide space at INTERSCHUTZ. For example, various 5G applications will be demonstrated in hall 16 and on the outdoor area – such as the driving of a special signal vehicle in the city traffic of the future, in which automated vehicles will move in addition to human road users.

On the way to a networkedfire brigade

Digitalization and networking are also major challenges in the further development of leadership support tools and software. Eurocommand, for example, offers an innovative platform with its 5th generation leadership support software – CommandX CX5 – with which the functionalities known on the market are extended to include mobile applications with live data transfer, dashboards, guard display and the integration of drone data. But networking with each other with different systems is also part of the developments (hall 16/F16).

However, digitization also makes other solutions to problems possible. Eurocommand Managing Director Sascha Pomp comments: "If an operations manager can now monitor and control the room temperature in his own home with his smartphone,

why shouldn't he also get information about the water level in the fire engine or where the approaching vehicles are located via intelligent solutions?"

Geodata is playing an increasingly important role. This was demonstrated not least by the heavy rain disaster last summer in the Ahr Valley. Where they were available, leaders could make faster and more accurate decisions. But geodata can also be useful regardless of large-scale operations. For example, when deciding on the location of a new fire station, as the company Esri emphasizes. Esri will show how this can work in hall 16 at booth H15. By the way, Esri products are used worldwide to visualize the current corona situation, including by the Robert Koch Institute (RKI).

Drones as operational support

And another topic is increasingly coming to the fore: drones. The so-called unmanned aerial vehicles have already proven to be an important tool in hazard prevention in many large and small operations: Whether in the exploration of deployment sites, the search for missing persons or the detection of fire nests with the help of

thermal imaging cameras – the application possibilities are manifold and offer scope for innovative ideas.

Three examples at INTERSCHUTZ:

The German Rescue Robotics Center (DRZ) will be providing information on robot and drone deployment examples in hall 17 at booth D06.

Among other things, the German Aerospace Center (Deutsches Zentrum für Luft- und Raumfahrt; DLR) is presenting a project called "Live-Lage – Use of drones for the rapid reconnaissance of operational situations", which was developed together with the Fire Brigade of the German city Duisburg (hall 16, E/F/G16).

A start-up from Ludwigsfelde in Brandenburg, Germany has completely different ideas: The company NatureTec is engaged in the development of unmanned cargo drones for fighting forest fires (hall 16/F48).

Digital networking solutions for improved communication

Digital applications are literally limitless. A few more examples: Hexagon/

Swissphone will be showcasing the entire range of comprehensive alerting solutions for a wide variety of industries and a wide variety of tasks – whether for blue light organizations such as fire brigades, rescue services and the police or for authorities and administrations (hall 16/A06).

Digital networking solutions are offered by three other companies that are also closely networked with each other: Divera, for example, determines the availability of employees and

Intergraf shows digital reality solutions that combine sensor, software and autonomous technologies. For more than 30 years, the company has been equipping the police, fire brigade, rescue services, disaster and plant protection with technologies for operations management and resource allocation (hall 16/G42).

Sinus Nachrichtentechnik will be showcasing control center technology for BOS and industry, as well as digital alerting, VoIP telecommunications systems, command and con-

trol vehicle (ELW) solutions, radio network systems and much more (hall 16/E15).

emergency personnel. Among other things, this involves alerting with feedback function or the planning of personnel availability (hall 16/E08).
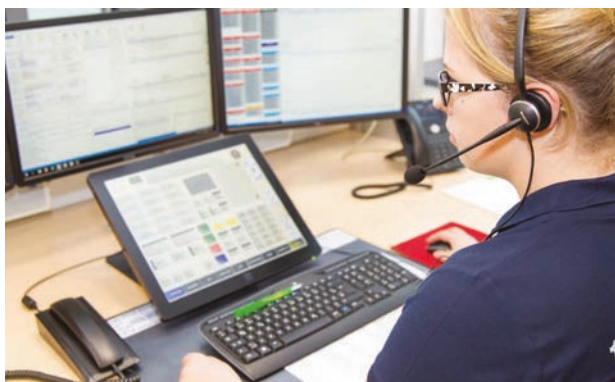
rescueTablet presents software right next door (hall 16/ E06) that provides up-to-date information on the situation and location of the operation, maps map material and hydrant plans, provides rescue cards and offers a central solution for required information.

And Status 3 IT (hall 16/E12) offers hardware and software solutions for controlling digital radios in vehicles and radio control panels.

[www.interschutz.de/en]

Pan-European

Vodafone, Cardinality.io and Google Cloud build a smarter pan-European network performance platform

Allows Vodafone to update its pan-European network faster, more dynamically, and more efficiently • Eight billion network data sources per day improves network-related decisions • Enhances use of smart planning for cheaper and more effective network rollouts.

Building a smarter pan-European network performance platform

In May 2022 Vodafone, Cardinality.io and Google Cloud announced that they have built a smarter, pan-European cloud-native network performance platform to give Vodafone's customers a consistently faster and highly reliable mobile experience across Europe.

The platform is now being implemented across eleven European countries in which Vodafone operates and will transform the way it plans, builds, and manages its network over the next five years.

Vodafone's European operating companies will be able to draw billions of vital network performance datapoints from a secure cloud data pool using the new platform. It will replace over 100 separate network performance applications in use today, providing a single source of clean data in the cloud that can be optimised and analysed using artificial intelligence (AI).

Vodafone will use the data to monitor, manage and enhance its entire pan-European mobile network, including Critical National Infrastructure (CNI). The platform will enable Vodafone to focus 5G investment with pinpoint precision in the areas where the demand is greatest such as in cities, travel corridors, ports, industrial hubs, and in specialist areas such as mobile private networks, as well as target those rural areas with patchy coverage.

Capable of processing and analysing up to eight billion mobile network performance events per day, Vodafone data scientists can have deep insights into network data such as traffic patterns to make informed and instant, network-changing decisions. This means Vodafone can add capacity and integrate new network connectivity in response to major incidents, public and political events,

manage energy efficiency and restore services after severe weather storms – within minutes and hours, not days – on either a highly localised level or internationally across borders.

Johan Wibergh, Chief Technology Officer of Vodafone, said: "As the needs of our 300 million plus mobile customers evolve so will our network using this new platform. It is a global data hub that gives us a real-time view of what is happening anywhere on our network, uses our global scale to manage traffic growth cheaper and more efficiently as customer data consumption grows by around 40% per year, and supports the full automation of our network by 2025."

Performance management tools are used for most network processes including capacity planning, optimisation, troubleshooting, enhancing the customer experience, and introducing new 5G and edge computing services. By simplifying data operations at scale and generating real-time insights, the new platform will make all these processes faster, smarter, and more personalised.

Vodafone has already seen major network and IT incidents fall by nearly 70% this year by simplifying and digitalising core operations, and within a few years, it expects to resolve 80% of all incidents end-to-end without human intervention. In turn, this is freeing up Vodafone's expanding technology workforce to develop new products and services 50% faster, cheaper and at scale.

Also, using these advanced ML (machine learning)/AI monitoring tools, Vodafone can detect and block fraudulent or suspicious activity on the network across Europe often before its customers are impacted. It will underpin Vodafone's pioneering work in smart planning across its entire European footprint – a method of using

key network metrics to prioritise upgrades whilst significantly reducing the cost of maintaining and extending its networks.

Called Vodafone Unified Performance Management (UPM), the platform combines Google Cloud's leading smart analytics portfolio and ML/AI tools with Cardinality.io's deep telecom industry expertise and award-winning cloud-native DataOps and analytics platform to deliver the solution on the best of breed hybrid cloud architecture. All data is stored within Vodafone's own on-premise data lake on servers in Europe. Data will be protected with appropriate state of the art security and privacy protections such as encryption, anonymisation, pseudonymisation and aggregation and will be accessible only by authorised users.

"Moving data to the cloud while providing governance across multiple on-premises sites is an immense challenge," said Vivek Gupta, Director, Network AI and Telecom Partnerships, Global Telecom Industry Solutions, Google Cloud. "Cardinality.io's close integration with Google Cloud unlocks immense value for Vodafone as it seeks to provide an unparalleled customer experience to its European subscriber base."

"With Vodafone UPM, Cardinality.io provides the bridge that makes it possible to efficiently move data from multiple far edge locations to a centralized Google Cloud data repository," said Prashant Kumar, Chief Technology Officer and Co-founder of Cardinality.io. "Thanks to the Cardinality.io platform's data virtualization capabilities, open API interfaces and microservices-based architecture, Vodafone can choose the third-party tools it prefers for creating dashboards, reports and advanced analytics."

Retail Security

What is Intelligent Video Surveillance and Why Should Retailers Care?

Modern-Day Brick & Mortar Retail

These days, ever-evolving technology is an essential part of our everyday lives. We use it to make hundreds of decisions each day, whether it be checking the weather to determine how to dress or searching for a recipe to prepare for dinner. We use technology to help us improve our lives, and likewise, business owners do the same, relying on data and solutions that extract, aggregate, and visualize the information to make-decisions and derive valuable insights.

Retailers, specifically, see significant benefits from leveraging technology, such as video analytics, to improve their brick-and-mortar stores. Video analytics technology is powered by Artificial Intelligence (AI) to process video to identify and classify objects in the video, such as people, vehicles, and other items.

This metadata is then indexed, enabling operators to quickly and easily search, filter and alert on real-time feeds as well as recorded video processed on demand. Intelligent video analytics solutions make video searchable and filterable, as well as actionable through increased situational awareness and real-time alerting.

By aggregating video data over time, video content analytics also makes video intelligence quantifiable, by visualizing the video metadata and providing business intelligence that critically helps management understand trends, make decisions, and develop strategies that increase conversion rates and improve the customer experience.

Video Analytics Applications in Retail Environment

Traditionally, video surveillance is used by retailers for investigating and, when possible, preventing shoplifting and shrinkage. Video analytics technology streamlines these applications and introduces additional use cases.

Many actionable insights and extensive business intelligence can be derived from video analysis, enabling data-drive safety, security and operational decision making. Video analytics solutions are being used by retailers as a proactive means to create strategies that enhance the shopping experience, improve retention, and increase sales.

Video analytics provides retailers with a wealth of customer trend data that can be leveraged to increase operational efficiency and ultimately enhance the customer experience. For example, by assessing and understanding visitor traffic trends, including where they tend to dwell, which products and displays they interact with, and how they navigate a store, a retailer can examine the effectiveness of a store's layout and product placement using video analytics technology. This can help retailers identify both popular items and areas, as well as potential problem hot spots.

Video analytics-generated heatmaps help achieve this by illustrating customer traffic patterns throughout the store, highlighting most common pathways and aisles that customers navigate, and the most (or least) popular product displays or information kiosks. Marketers and merchandising managers can leverage this actionable information when developing strategies, planning campaigns, and ordering inventory. Similarly, store planners use this information to optimize space utilization in a physical store.

Ultimately, data-driven heatmaps and trend reports help retailers make informed and intelligent decisions about placing products or displays, help marketing with product popularity insights and help store designers create an optimized shopping environment.

In addition to better elucidating in-store activity, in the aftermath of a crime, video analysis makes understanding incidents much easier. A common issue that retailers face is loss-prevention. Video analytics can help security operators advance loss-prevention investigations through accelerated video review and extensive search and filter functionality. In real-time, rule-based alerts can increase security's situational awareness by notifying operators of pre-defined suspicious behaviors that require further investigation – for instance, excessive loitering near high value items or stock rooms or detecting entrances to a staff-only area. By better understanding traffic trends in the store through video analytics, retailers can also uncover patterns, make plans, and configure alerts to behaviors that will help mitigate shrinkage in the short and long term.

Beyond loss-prevention and security, video surveillance platforms can be used by retailers to optimize staffing. Through the trend reporting and traffic insights visualized by video analytic technology, retailers make better decisions about their staffing needs based on the time of day, week, month or even year.

Whether for safety and security or the evolving operational efficiency and customer experience use cases, video analytics empower retail businesses with a new dimension of intelligence that they can't afford to overlook.

Learn more about video analytics for retail in The Retailer's Guide to Revolutionizing the In-Store Experience with Intelligent Video Surveillance.

[www.briefcam.com]

Maximize

situational awareness in perimeter security applications

Bosch introduced MIC IP fusion 9000i 9mm camera to provide operators with 360-degree perimeter view in 30 seconds. MIC IP fusion 9000i 9mm with power plant background

Bosch has introduced the MIC IP fusion 9000i 9mm camera, offering a wide thermal view to increase the level of security in perimeter detection applications. Equipped with a 9mm lens, the new camera expands the current MIC IP fusion 9000i line-up of AI-powered security solutions. Specifically designed for short range perimeter security at critical sites, the MIC IP fusion 9000i 9mm camera delivers full 360-degree coverage in 30 seconds. Obtaining a full circle view

quickly lowers security costs per square meter, resulting in customer savings. The camera is protected by full metal housing and offers the same level of longevity and reliability of existing 19mm and 50mm lens models.

360-degree coverage in 30 seconds
The new 9mm lens delivers an expanded thermal view (70° x 52°). As a result, a single camera only requires six prepositions to provide 360-de-

gree coverage in 30 seconds. Like other MIC IP fusion 9000i models, the 9mm camera combines a thermal imager with a 1080p starlight optical imager in a single housing. For security regardless of lighting conditions, the camera can blend object detection data from both thermal and optical video streams via metadata fusion technology. The combination of built-in Intelligent Video Analytics and metadata fusion technologies provides operators with enhanced overall

awareness of their environment regardless of which video stream they are viewing. Metadata fusion automatically triggers alerts to help operators focus on things that need attention, even if they are not necessarily visible in the video stream being watched due to poor lighting, smoke or complete darkness.

For example, while a person is walking in a tunnel, a serious incident takes place causing the tunnel to quickly fill with smoke. Due to poor visibility, the optical camera can no longer detect persons. However, the thermal imager will continue to distinguish them, and the metadata overlay is visible on the optical image. An alarm is triggered, and the operator receives notification of the event from both image streams and can immediately switch to the thermal image by clicking on the metadata. Once the operator sees the video data related to the event, he can determine the next right action to take.

Expanding the lens portfolio

Operators can now choose the optimal MIC IP fusion 9000i model for their applications. The longer-range lens (50mm) provides long-range detection and early warning for borders, shipping channels or airport runways, while the 19mm lens is built for medium range applications. The new 9mm version now supports short range applications in which a full circle overview needs to be provided within seconds.

Performance in extreme environments

The MIC IP fusion 9000i 9mm camera features a solid metal body with superior metallurgy and finish to provide exceptional protection against corrosion. Built for long-term performance in extreme environments, the camera can withstand high wind, rain, and snow, as well as 100-percent humidity and extreme temperatures from -40° to 65° C (-40° to 149° F). The use of all-metal intermeshing gears allows greater resistance to shock and vibration and longer operational life compared to cameras with plastic gears and rubber belts. In the event of shock or external force such as gale force winds, the camera relies on positional encoders to resume the exact pre-programmed position without the need for operator interference.

Overall, the MIC IP fusion 9000i 9mm camera completes the high-performance line of smart perimeter protection cameras with a short-range option. By choosing MIC cameras, operators can protect their assets day and night with exceedingly fast 360-degree imaging. Regardless of weather, temperature, vibration, or shock, the new MIC IP fusion 9000i 9mm camera delivers situational intelligence to help operators deal with incidents that require a quick and precise response.

[https://tinyurl.com/3et39brs]

Deep learning

Bosch expands Inteox camera portfolio that seamlessly integrates with Milestone to meet safety and security requirements of many applications

Bosch has expanded the Inteox open camera portfolio with the addition of two fixed cameras: The Flexidome and Dinion inteox 7100i IR cameras. The AI-powered cameras bring a new level of efficiency to a variety of indoor and outdoor applications for city surveillance, airports, government, and traffic. In partnership with video management solutions provider Milestone Systems, Bosch offers full integration into the Milestone XProtect suite of security solutions to meet the most advanced safety and security requirements of many applications.

The right levels of performance for a variety of applications

The new fixed Inteox cameras offer a menu of video analytics, 4K resolution, built-in infrared illumination, and durable housing to perform in rugged environments to meet varying customer requirements around the clock. With Camera Trainer, a machine learning software embedded in all Inteox cameras, system integrators can tailor Intelligent Video Analytics (IVA) to detect objects and situations that

matter most to their customers. For example, operators can teach the camera to recognize if a barrier on a parking lot or at a railway crossing is open or closed. Another example is teaching cameras to detect and subsequently blur ATM or card payment terminals to protect customers' privacy. To quickly respond to changing or varying customer requirements system integrators can add third-party software apps to Inteox cameras via the Azena Application Store. The cameras also offer advanced configuration and continuous health moni-

toring from anywhere via the Bosch Remote Portal, a cloud-based service offering for device management.

Deep learning for next-generation solutions

The Flexidome and Dinion inteox 7100i IR object classification (OC) models command the necessary computation power to enable deep neural network-based video analytics, like Traffic Detector.

The pre-trained AI detector, available out of the box helps system integrators to meet the strict requirements of traffic applications. It tackles more complex tasks like accurately classifying vehicles at crowded intersections, roadways, and tunnels.

Traffic Detector can detect and count cars, trucks, buses, motorcycles, bicycles, and people. Combined with IVA, Traffic Detector data is augmented with object speed, GPS location, and color.

Partnership with Milestone Systems

System integrators and users further benefit from Bosch's ongoing partnership with Milestone Systems, a leading provider of open platform video management software. Inteox cameras can leverage Milestone's powerful video management solutions and add user-defined functionality to meet the most advanced surveillance needs, including:

- Bosch Video Analytics natively integrated in Milestone XProtect allows user to detect the things that matter most. It includes automated alerts for line-crossing, object-in-field, or any of the other 16 alarm tasks captured by XProtect.
- Bosch deep neural network-based video analytics, like Traffic Detector are natively integrated in Milestone XProtect. These analytics use high-quality, real-life data

from the field, which enables users to tackle more complex tasks faster, easier, and with greater accuracy.
- Bosch machine learning technology Camera Trainer natively integrated in Milestone XProtect lets users define rules and alerts without the need for external plug-ins. Use cases include teaching the camera to recognize occupied and free parking spots and triggering alerts when all spots are occupied.
- Freely search Video Analytics metadata via Forensic Search plug-in via the XProtect Smart Client with new, user-specific criteria. Whereas other applications only allow setting up search criteria as initial alarm criteria, Forensic Search lets users add new criteria at any time, providing complete flexibility in the search for evidence after an event.

[https://tinyurl.com/2p864uv4]

New G+D survey proves that the future of banking is phygital

Opportunities in the phygital landscape

The new survey "Opportunities in the phygital landscape" conducted by Global Data on behalf of Giesecke+Devrient (G+D) identifies the most important trends in how banks, financial institutions and financial service providers will interact with their customers in the near future. The focus is clearly on the integration of physical and digital services.

The term "phygital" denotes the convergence of the physical and digital worlds: analogue and virtual business activities are combined into a new, customer-oriented mix. G+D has investigated how this could look in practice for the banking and financial services industry. The study "Opportunities in the phygital landscape", conducted in late 2021, interviewed a total of 45 mid and senior-level executives in 15 traditional banks and 11 neobanks (digital-only banks) across 15 countries. The report highlights contrasting attitudes towards physical

and digital service offerings among experts.

While the findings indicate that customers will no longer bank exclusively in physical branches, the idea that this spells the end for bank branches is mistaken. In fact, most bank managers want to expand their physical touchpoints. The banking landscape of tomorrow must therefore combine physical and digital to offer phygital services. The vast majority of banks, both traditional (92%) and neo (80%), believe in the relevance of the

physical payment card in the years ahead. Cards act as an unique brand element and are the symbol of the connection between the bank and the customer. In a phygital approach, the established ecosystem of banks, neobanks and financial institutions is combined with new touchpoints for online services. The increase in digital offerings is also leading to data growth, giving a paramount role to handling, analysis and integration of these data: 98% of all banks surveyed see this as an opportunity for new cross-selling and up-selling op-

tions, individual customer offerings as well as increasing the value generated by transactions.

Pathways to the phygital business model

The current banking landscape is characterised by the rise of neobanks, their focus on increasing their physical touchpoints and the growing importance of companies with large numbers of direct customer contacts, such as retailers, in generating bank-relevant data. Payment systems based on different technologies and the use of cloud services enable an end-to-end, channel-independent service experience for customers. Neobanks have so far benefited from the comparatively low costs of not having a branch infrastructure and legacy core banking systems. However, this potential competitive advantage often leads to a lack of visibility among customers and consequently to lower brand loyalty, and high churn rates. Twenty-seven per cent of neobank managers see a lack of trust among their customers as a major problem, compared to just 3% of retail banks with physical branches. Neobanks must therefore try to increase the number of physical touchpoints in order to align their online services more closely with the wishes and needs of their customers. That said, customer centricity is a challenge for 47% of neobanks, and even higher for traditional institutions at 57%. A phygital world that focuses on the customer experience is a top strategy for 47% of neobanks, compared to only 17% of traditional banks.

Automation creates space for a physical presence

These customer experiences need to be similar or interlinked across all contact channels. However, 43% of traditional banks, and even 60% of neobanks, see a corresponding multichannel strategy as a major challenge. This approach will not be possible without greater automation, the use of flexibly scalable cloud platforms and agile business processes. Only if virtual resources, such as chatbots and automated processes, help handling the majority of transactions, it will be possible for both traditional banks and neobanks to ensure customers have access to a personal touchpoint when required and without any distraction in customer experience. However, although 20% of traditional banks see this as the most important part of their phygital strategy, only 7% of neobanks see a need for action here. Despite that, both are in agreement that it is ultimately the quality of products and services, but also the ability to provide individualised offers for the customers that determine their success or failure. Consequently, the yardstick for this is customer satisfaction, which therefore forms the basis for profitable business models.

"Banks face a significant challenge in becoming more customer-centric and developing the right mix of physical and virtual services to do so," explains Gabrielle Bugat, Member of Group Management Team of G+D, heading the Card & Digital Payment business of G+D.

"Phygital strategies can enable the experience that the customer expects. As they look to strengthen this dual offering, both neobanks and traditional institutions need the right tools to allow them to create more space for physical touchpoints and direct interaction with their customers. The transformation in banking continues, bringing banks and customers much closer together."

Whitepaper: Opportunities in the phygital landscape https://phygital.gi-de.com/#section-7683

Article: https://www.payments-cardsandmobile.com/interview-the-future-of-banking-is-phygital

Are banks ready for the phygital future?

The proliferation of innovations in the payment industry is radically transforming the sector. There are increasing options for consumers, and as customer expectations rise, banks must be quick to react and adapt.

Traditional banks and neobanks from across 15 countries were surveyed as part of G+D's recent independent market survey, conducted by Global Data, which aimed to find out what financial institutions see as current challenges in the payment landscape, what banks can learn from one another, and how banks can take steps to improve interactions along the customer journey through phygitality.

Digital banking and physical branches: a winning combination

With responses from a range of digital and traditional banks across the world, the survey revealed some clear trends. All participants believe that a combination of physical and digital wins, with only 20% of neobanks dismissing the idea of not having a physical presence to be successful in the long run.

Another universal agreement was that 89% of banks (both traditional banks and neobanks) believe that the physical payment card will continue to be relevant in years ahead. A 2021 study by Juniper Research also concluded that while digital-wallet users
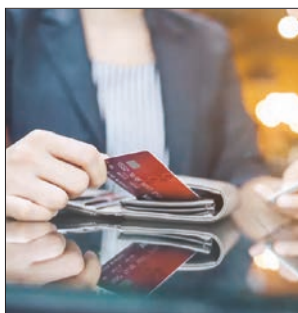
are set to exceed 4.4 billion by 2025, yet banks still expect digital wallets to coexist with physical cards for years to come.(1)

Physical payment cards remain a tangible emblem of trust. Just as e-book sales continue to rise, sales of print books are also growing.(2)

Physical touch is still very important for us, as humans, and the survey emphasizes this with expectations of payment card longevity. For banks, branded, tangible elements are a way of connecting with customers.

Overcoming banking challenges

Both traditional and neobanks agree

that a phygital approach to customer service is key, yet they both concur that implementing it is a challenge. Specifically, developing a cohesive, consistent customer journey via physical and digital channels is exigent yet complicated. Overall, traditional banks saw this as more of a challenge than neobanks did, with 37% of traditional banks defining it as a "huge challenge." Linked to the positive trend of dismantling aged legacy systems and taking advantage of new digital services such as open banking systems, these results underline the complexities of integrating sometimes historically grown financial services from a range of providers.

Connecting applications and data with APIs and web services increases flexibility and provides customers with up-to-date service experiences. Alas, solutions licensed in a variety of countries and by different companies can cause bureaucratic headaches for banks who must ensure data privacy and a seamless customer journey. Yet this challenge must be overcome – creating an ideal customer experience

and utilizing communication channels effectively is a driver of long-term success. Although neobanks have a competitive advantage by starting greenfield in most cases, they aren't necessarily leading the way in the communications space. Just under two-thirds of neobanks questioned say that a multi-channel approach of connecting interactions is difficult (compared with 43% of traditional banks). This underlines the necessity for all financial institutions to adapt and learn to thrive in the new phygital world.

Banking expectations for the future

The future of digital is human. That's the consensus of both traditional banks and neobanks. Both agree that

automation is set to play a major role in the future of banking, with 96% of respondents agreeing on this. Both agreed upon the importance of human elements sitting alongside automation (87% of traditional banks and 67% of neobanks). How do banks go about integrating automation as part of their banking strategy? Research has shown that the majority of customer dissatisfaction happens at just a few touchpoints: waiting in line at a bank branch, confusion when using a mobile app, or lack of clarity when completing a customer journey. Chatbots and automated voice responses (AVRs) can provide automated sup-

port, but one thing should never be forgotten: sometimes, customers simply want to speak to a human being. And in summary, it's that combination that will drive a bank's success. By combining physical touchpoints and best-in-class smart solutions, banks will be equipped with the tools for success, with both helping to create a competitive advantage – and excel at the customer experience.

(1) Digital wallet users to exceed 4.4 billion by 2025, as mobile drives digital payments' revolution, Juniper Research, 2021, (2) Sales Are Up Nearly 9% For Print Books – But Who's Reading Them?, Forbes, 2022

Case study

Keep traffic moving on Italy's Pedemontana Veneta Highway

A new highway relies on AI-powered video technology from Hanwha Techwin and Sprinx to keep traffic moving smoothly and safely and to provide operators with crucial information on traffic volume and speed.

The need for a motorway to link the cities of Vicenza and Treviso in Italy emerged in the 1970s as the Venetian countryside became increasingly urbanised, while the opening of the European Union to the east in the 1990s also brought more traffic across the region.

To address this, the first stone of what is now the Pedemontana Veneta or "SPV" toll highway was laid in November 2011 in Romano d'Ezzelino,

and in 2012 work began on the first stretch of the 2.6-billion-euro road. Once completed in May 2022, the SPV's 162 kilometres will link Vicenza and Treviso, interconnect with three national motorways and deliver greater mobility for the area's 4.9 million inhabitants and the 500,000 businesses that call the region home.

Overcoming challenges

Constructing the highway presented a number of engineering challenges

including bridging the Poscola, Astico, Laverda, Muson and Brenta rivers – the latter requiring a bridge of 430 metres in length alone. The highway also features two natural tunnels and 33 artificial tunnels, the longest of which runs to six kilometres.

Given the amount of traffic the road is expected to carry, it is vital that SPV's operators keep the highway moving smoothly and safely and that they have access to data on traffic vo-

lumes and average speeds. To do so, they are relying on an AI-powered video surveillance system from Hanwha Techwin and its technology partner, Sprinx.

Italian distributor SIRIUS – COMPASS and systems integrators SIS scpa and Pagano Spa worked together to install 600 cameras along the route of the SPV, calling on Hanwha Techwin's high-resolution Wisenet cameras with day & night ICR technology and a wide dynamic range to deliver high-quality images regardless of light levels. The installation also features Hanwha Techwin 32x zoom PTZ dome cameras, all managed through a Wisenet WAVE video management system.

Easing congestion and early incident detection

The cameras are integrated with analytics expert Sprinx's 'traffix.ai' solution, which uses deep learning and image processing to deliver a wide range of server-based analytic functions that increase safety for road users and provide greater insight into how the highway is being used.

These functions include automatically detecting traffic incidents in real-time

and immediately alerting the highway's operators to initiate an emergency response. Whether it is a stalled vehicle in one of the highway's lanes, or a car travelling the wrong way down the highway, the system can reliably detect events that could cause traffic congestion at best and serious accidents at worst. The solution can also spot and alert operators to smoke in any of the highway's many tunnels, which might indicate a traffic incident or a fire.

Using Hanwha Techwin's cameras as a traffic sensor, the Sprinx software solution is also able to detect queues of traffic and objects in the road, such as cargo spilt by vehicles en route and which present a hazard for oncoming traffic. Added safety is also ensured by the system's ability to alert operators to any pedestrians who have strayed onto the highway.

Delivering insights into road use

Deploying AI in the system delivers additional benefits for the SPV beyond safety alone. Using Sprinx's traffic analytics, the system installed along the length of the highway keeps track of vehicles moving in any of the Wi-

senet cameras' field of view, and is able to collect data on the highway's two lanes at the same time and in both directions of travel.

The traffic data that can be recorded and stored as a result provide a rich source of insight into how and when the highway is being used and by what types of vehicles. The system allows operators to undertake vehicle counting, measure traffic density and ascertain the average speed of vehicles along the route. Fully integrated with the Wisent Wave video management system, all this information is delivered via an intuitive web user interface.

" "Together, Hanwha Techwin and Sprinx make the Pedemontana Veneta highway safer for road users and help keep traffic flowing," says Gerando Capezzuto of SIS scpa. "Using the performing combination of Sprinx's AI video analytics and the Wisenet Wave VMS platform of Hanwha Techwin, we are able to instantly detect incidents along hundreds of kilometres of road to provide a faster response, while the insights it has provided into how the highway is being used are proving invaluable in maximising the efficient use of the road."

[www.hanwha-security.eu]

Case Study

Nomura invests in a global, state-of-the art access control system

Headquartered in Tokyo, Nomura is a top tier international bank providing investment and merchant banking services to corporate and institutional customers. With offices in all major financial centres across the globe, the mission of Nomura is to deliver superior services and solutions to meet all investment needs of their clients. To ensure they execute their mission in a safe and secure environment, Nomura has invested in a Honeywell access control solution that is expandable for the future.

The Situation

Having offices located around the world, it is imperative that Nomura has a secure and easy to use access control system with a global footprint. One that is flexible enough to manage the access control demands at any Nomura office location from a single point whilst maintaining local operational autonomy. With the ever-present threats of terrorism, choosing the right access control system for Nomura was crucial. In London, Nomura has prestigious offices in Angel

"The Honeywell Pro-Watch solution is fantastic! It's a robust, resilient and flexible security management system capable of integration. Integrating it with our own PeopleSoft human resource system and intranet saves us significant administrative time by eliminating repetitive data entry associated with managing and aligning cardholder information and access rights."

Andy Williams, Head of Security EMEA, Nomura

Lane. When it acquired the site, upgrading the access control solution quickly became a priority for the company's head of security in order to securely manage authorised visitors, account for people while on site and keep staff members secure at all times.

The Angel Lane building contains a large number of personnel, all requiring varying levels of access control authority, some to strictly controlled, authorised areas. The access control system must operate 24/7 to accommodate varying shift patterns and provide customised reports with multiple criteria. The system would need to store up to 4000 card holders, in-

The Pro-Watch solution would run on the bank's own network via a single database and enable Nomura to centrally control access to an unlimited amount of doors and areas across not just the Angel Lane site, but also every other Nomura office in the world including its remote data centres. It consists of one enterprise server that provides global management of a number of independent regional servers. The enterprise server acts as central storage area for system configurations and stores cardholder information and transaction history. The regional servers function independently as local databases while sharing information with the enterprise server.

The Benefits

Supporting an unlimited number of cardholders and readers, Pro-Watch Enterprise Edition is perfect to meet the challenges of Nomura's growing business. Pro-Watch combines the flexibility and scalability that Nomura requires without compromising simplicity. The system takes the term 'user-friendly' to a higher level and has made it simple to enforce

Nomura's access policy via built-in wizards and shortcuts. The Windows®-based graphical user interface minimises operator training and the built-in software wizards enhance system uniformity across sites. This contributes to a reduced installation time and a shorter overall learning curve for new users. Integrating with the Nomura intranet system also makes it simple for line managers to request changes to access rights for people in their department.

And in relation to complying with FSA regulations, access rights are managed such that separate groups are created for employees in the corporate-advisory area and the brokering

cluding staff, authorised contractors and visitors.

In addition, the solution needed to enable Nomura to separate and isolate people who make investment decisions from people who are privy to undisclosed material information which may influence those decisions. These 'chinese walls' are a Financial Services uthority (FSA) regulation to safeguard insider information and ensure no improper trading occurs.

The Solution

A Honeywell Pro-Watch security management system (Enterprise Edition) was specified by Nomura who then invited independent security consultant CornerStone GRG to carry out security design, production of specification and manage the tendering and installation process. As a result, security integrator Universal Security Systems was awarded the installation contract.

department to help enforce the 'chinese walls' within the bank.

With its built-in redundancy, Pro-Watch provides additional value in disaster recovery planning too. In the case of a power failure or a problem on part of the main server, access control rights can be managed at any one of the other Nomura sites on the global

Pro-Watch network.

"The Honeywell Pro-Watch solution is fantastic!" comments Andy Williams, Head of Security (Europe, Middle East and Africa) for Nomura. "It's a robust, resilient and flexible security management system capable of integration. Integrating it with our own PeopleSoft® human resource system and intranet saves us significant administrative time by eliminating repetitive data entry associated with managing and aligning cardholder information and access rights."
Using Pro-Watch, Andy Williams' security team now has complete command and control over all system and event information and can monitor door alarms in multiple locations simultaneously.
Reporting is straight-forward as well. In the event that historical data is required, access control logs can be quickly and simply accessed. Should a fire alarm occur, a report can be generated quickly to show the details of all personnel within the building at that point in time. 'Gate/time' reports are also beneficial as they can be given to the HMRC as supporting evidence that an individual was present on site on a particular time and date.

Partners of Choice Universal Security Systems

Universal Security Systems Ltd. specialises as a security systems integra-

tor in the design, installation and support of technology based security solutions. Clients are primarily medium and larger sized organisations of many kinds, who require protection for major, prestigious and/or multi-site property estates.
"Universal Security Systems was selected because of its excellent technological ability and cost-effective solutions," said Andy Williams, Head of Security EMEA, Nomura. "They have a positive attitude and made achieving the aggressive installation schedule look easy. They are commercially astute and we benefit from them being our central point of contact for our security requirements in the EMEA region."

CornerStone Consulting Group

CornerStone GRG Ltd. is an independent, international consultancy firm providing a range of security services. They help organisations protect their people, assets, intellectual property and profits by identifying the threats and minimising the risks that face today's global businesses. CornerStone is commit- ted to providing specialist guidance, unbiased advice and support to their clients.
"CornerStone interpreted our requi-

rements precisely, managed the project perfectly and made essential recommendations on how to value engineer the installation without leaving Nomura exposed in any way," said Andy Williams, Head of Security EMEA, Nomura.

Company News

Company name changed

GFR - Gesellschaft für Regelungstechnik und Energieeinsparung mbH, based in Verl in Germany's North Rhine-Westphalia region, has been part of Bosch Building Technologies since 2019 and is changing its name to Bosch Building Automation GmbH effective April 1, 2022. The company's portfolio comprises complete automation solutions for the operation of buildings on a sustainable basis and related services with a comprehensive range of hardware and software. "We are achieving strong growth with connected building automation and energy efficiency solutions that are planned and implemented on a highly customized basis in close cooperation with our customers. The Bosch brand will open more doors for us and give us the opportunity to position ourselves even more prominently on the market for building automation," explains Volker Westerheide, managing director of GFR. The building automation specialist will continue to market its products under the Digicontrol product brand.

EHI - European Trading Institute

Germany: Theft only slightly declining

The decline in inventory discrepancies is moderate, from 4.2 billion euros in 2020 to 4.1 billion euros last year. According to expert estimates, inventory discrepancies are made up of theft by customers (2.1 billion euros), theft by employees (810 million euros), theft by service staff and suppliers (320 million euros) and organisational deficiencies (870 million euros).

T-Systems

Number 1 IT service provider

T-Systems once again took first place in the Lünendonk list of leading IT service providers in Germany, just as it did last year

T-Systems has retained its top position in the Lünendonk list of leading IT service companies in Germany. As in the previous year, the Telekom subsidiary placed just ahead of Atos. In its ranking, market research company Lünendonk & Hossenfelder compares IT service providers that generate more than 50 per cent of their revenue from IT outsourcing, hosting, managed services, and other data center services.

High demand for digital experts

Colleagues having a discussion in a server room at the office
The ranking is part of a study titled "The Market for IT Services in Germany". Sales in the market as a whole also increased significantly in the second year of the coronavirus. 2021 saw average growth of just over 13 percent. Mario Zillmann, partner at Lünendonk, says the driver behind this is the pressure for digitalization and transformation in companies: "They require external expertise – often due to a lack of in-house experience – and the demand for IT experts is higher than ever before." Demand was particularly high for services related to the cloud, IT modernisation, and data analytics.
Ranked in the Top 5 for IT consulting and system integration
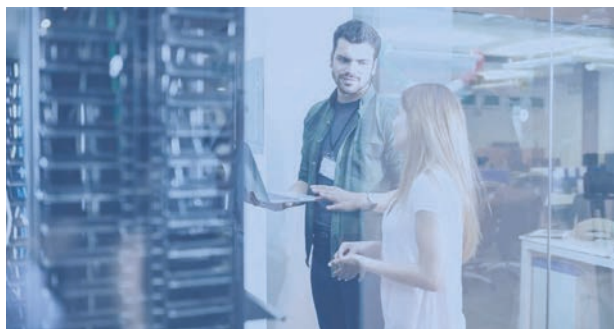
While the Telekom subsidiary is in the lead for IT services, it holds fourth place in the Lünendonk list of leading IT consultants and system integrators in Germany – again, just like last year. Accenture, Capgemini, and IBM came out on top. This market also saw strong overall growth: The 25 leading IT consultancies in Germany grew by an average of 14.5 percent in 2021, bringing their total revenue in Germany to EUR 15.8 billion.* By comparison: in 2020, growth was just under 5 percent.
* based on estimates by Lünendonk

2022 Building Occupant Survey Report

Our second annual study on workers' perceptions and feelings on the health and safety of their workplace

Return to Office? What Workers Say Is Their Top Concern with Buildings

Results from a new survey show that indoor air quality should be a focus for facilities leaders - Whether you work in a hospital, airport, school or office building – safety is likely one of your top concerns.

That's why Honeywell conducted a survey with Wakefield Research to get insights from people who work in buildings and how they feel about the air they breathe in their workspaces.

The survey included 3,000 office workers in buildings of 500 or more people in Germany, India, Middle East, United Kingdom, United States and Association of Southeast Asian Nations (ASEAN).

Here are the highlights:

- 72% of office workers surveyed are concerned about air quality in their buildings.
- Employees who were surveyed feel strongly that indoor air quality is critical to feeling confident in the buildings they work in. Indoor air quality (IAQ) can be impacted by several factors, including carbon dioxide, temperature, humidity, total volatile organic compounds (TVOCs) – a wide range of organic chemical compounds – and particulate matter in the air.
- Technologies like air quality monitors and other building management systems can help workers feel more confident.
- Nine out of 10 respondents said they want regular updates on their workplace's indoor air quality.
- Now more than ever, employees expect transparency about the air they're breathing in their workspaces.
- Of the building occupants surveyed, 29% of C-level executives said they receive frequent updates on air quality in their workplace while just 13% of non-C-level building occupants said they were actively informed.
- About two in five of those surveyed could accurately identify all the factors that contribute to indoor air quality.
- Educating building occupants on the components of indoor air quality is also important to how they feel about the safety of their workspaces.
- More than a third of respondents (36%) do not know that the carbon dioxide level factors into indoor air quality, and 41% of respondents said they are unaware that humidity contributes to building air quality.
- More than six in 10 respondents said they're ready to leave their job if their employer doesn't take steps to create a healthier indoor environment.

In an evolving and increasingly hybrid world, more employees are uncompromising when it comes to their ideal work environment.
Creating a safer indoor environment isn't just the right thing to do for the wellbeing of your building occupants – it can also be critical to navigating an evolving talent landscape.

The full report for download: [https://tinyurl.com/yckwd8at]

Educational Sector

SOPHOS SURVEY:

Ransomware Attacks on Education Institutions Increase

Education Sector Suffers Highest Data Encryption Rate and Longest Recovery Time

Sophos, a global leader in next-generation cybersecurity, has published a new sectoral survey report, The State of Ransomware in Education 2022. The findings reveal that education institutions – both higher and lower education – are increasingly being hit with ransomware, with 60% suffering attacks in 2021 compared to 44% in 2020. Education institutions faced the highest data encryption rate (73%) compared to other sectors (65%), and the longest recovery time, with 7% taking at least three months to recover – almost double the average time for other sectors (4%).

Additional findings include:

- Education institutions report the highest propensity to experience operational and commercial impacts from ransomware attacks compared to other sectors; 97% of higher education and 94% of lower education respondents say attacks impacted their ability to operate, while 96% of higher education and 92% of lower education respondents in the private sector further report business and revenue loss

- Only 2% of education institutions recovered all of their encrypted data after paying a ransom (down from 4% in 2020); schools, on average, were able to recover 62% of encrypted data after paying ransoms (down from 68% in 2020)

- Higher education institutions in particular report the longest ransomware recovery time; while 40% say it takes at least one month to recover (20% for other sectors), 9% report it takes three to six months

"Schools are among those being hit the hardest by ransomware. They're prime targets for attackers because of their overall lack of strong cybersecurity defenses and the goldmine of personal data they hold," said Chester Wisniewski, principal research scientist at Sophos.
"Education institutions are less likely than others to detect in-progress attacks, which naturally leads to higher attack success and encryption rates. Considering the encrypted data is most likely confidential student records, the impact is far greater than what most industries would experience.
Even if a portion of the data is restored, there is no guarantee what data the attackers will return, and, even then, the damage is already done, further burdening the victimized schools with high recovery costs and sometimes even bankruptcy. Unfortunately, these attacks are not going to stop, so the only way to get ahead is to prioritize building up anti-ransomware defenses to identify and mitigate attacks before encryption is possible."
Interestingly, education institutions report the highest rate of cyber insurance payout on ransomware claims (100% higher education, 99% lower education).
However, as a whole, the sector has one of the lowest rates of cyber insurance coverage against ransomware (78% compared to 83% for other sectors).
"Four out of 10 schools say fewer insurance providers are offering them coverage, while nearly half (49%) report that the level of cybersecurity they need to qualify for coverage has gone up," said Wisniewski.

"Cyber insurance providers are becoming more selective when it comes to accepting customers, and education organizations need help to meet these higher standards. With limited budgets, schools should work closely with trusted security professionals to ensure that resources are being allocated toward the right solutions that will deliver the best security outcomes and also help meet insurance standards."

In the light of the survey findings, Sophos experts recommend the following best practices for all organizations across all sectors:

- Install and maintain high-quality defenses across all points in the environment. Review security controls regularly and make sure they continue to meet the organization's needs

- Proactively hunt for threats to identify and stop adversaries before they can execute attacks – if the team lacks the time or skills to do this in-house, outsource to a Managed Detection and Response (MDR) team

- Harden the IT environment by searching for and closing key security gaps: unpatched devices, unprotected machines and open RDP ports, for example. Extended Detection and Response (XDR) solutions are ideal for this purpose

- Prepare for the worst, and have an updated plan in place of a worst-case incident scenario

- Make backups, and practice restoring from them to ensure minimize disruption and recovery time

The State of Ransomware in Education 2022 survey polled 5,600 IT professionals, including 320 lower education respondents and 410 high education respondents, in mid-sized organizations (100-5,000 employees) across 31 countries.

The 3 benefits

of bringing your Axis camera to the cloud

The popularity of cloud services is continuously growing across all aspects of the modern world. Cloud infrastructure is now well established as an enabling factor for connecting platforms and services that are cost-effective and safe, and the business benefits of doing so are clear. As such, it is inevitable that the cloud will eventually become the default storage method for video surveillance in the professional security industry [1]. Although, connecting security equipment to a cloud platform is not always the first thought of a buyer of a security device. Our device partner Axis uses a partnership model which allows customers to utilise the best edge devices, appliances, and cloud by selecting devices and applications that suit their needs [2]. This delivers

endless possibilities from one surveillance device. AXIS technology features such as the one-click connection system allow your camera to be linked to our cloud system seamlessly in a matter of seconds. When connected, it will unlock the possibility to analyse video data and deliver features such as motion detection, facial recognition, and behaviour analysis. Furthermore, device management from encryption keys to firmware upgrades, can all be conducted from the same administration interface.

Depreciating assets and budget

When budgeting for a traditional security system, you assume to pay a large upfront investment. Yet as soon as you install your camera on your system of servers, you will also have to

budget for recurring costs such as video footage backups, system updates, server maintenance and space alongside the energy costs involved in these servers. In terms of depreciating assets, the value of your technology such as your servers will go down every year until they become redundant with little value. The average lifespan of that server is only 5-8 years which means you'll have to invest in a whole new system when that time comes [3]. This server could also break before it becomes redundant creating a completely unpredicted cost that you cannot plan for. Therefore, the long-term cost of an onsite security system can be far higher than predicted. When moving your storage to the cloud, these recurring costs will be replaced with a

low-cost monthly subscription per device which eradicates any need for server investment. Allowing more accurate budgeting with no surprise costs.

Server Costs

Similarly, you won't have to factor in the costs of extra training or hiring budget for IT engineers that may be needed to keep up the maintenance of the system. The cloud will take care of any system updates minimising the need to pay for an engineer to manually update systems and features such as remote access and one-click connect which eliminates the need for costly site visits. Furthermore, if your business is growing faster than your onsite storage allows, you do not need to purchase extra servers just extra amounts of cloud storage which means you can use this additional saved budget on expanding other business functions.

Features that the cloud provides

When your security equipment is connected to the wider network, the data that it generates can be used for a much wider variety of purposes beyond the protection of people and assets which your traditional system provides. Access control as-a-service (ACaaS) provides automated control of your entrance and exit points by managing doors remotely and allowing or removing access from anywhere. When combined with video surveillance, you can create a powerful system that can incorporate two-factor authentication for improved security which can be used as a virtual concierge removing the need for someone manning a door.

Data analytics can also be drawn from your camera with features such as people counting which can be used to monitor how many people are on your premise at one time. Aggression detection and loitering can

protect potential threatening incidents before they escalate, and this footage can be quickly cut and sent from the smart dashboard and sent in an already encrypted file to make investigating any potential incidents easy and data compliant. In a retail environment, you can identify behaviours and shopping patterns with features such as queue mapping, hot zones and people counting to improve queue waiting times or identify areas that can be used to better tailor the environment. While the transaction checker can identify the exact point a purchase is made and bring up the footage of fraud during the checkout process.

Benefits of cloud backup of your data

Storing your data remotely removes a lot of hassle for yourself which means that you can focus your energy on the job itself and not have to worry about whether your data is safely secured. Your data is backed up automatically meaning if your own system crashes or footage is deleted by human error, no data will be lost as it can be re-accessed again through the cloud. Additionally, the footage can be accessed from anywhere through our online platform, so you never have to worry about not being able to access vital footage. Many firms who have experimented with IP-video cameras in the past have run into security problems when added to corporate networks as the device has been left vulnerable to cybersecurity issues due to default passwords and a lack of firmware up- grades. A cloud platform for video surveillance is designed from the ground up to ensure data is encrypted and will be sensitive to new vulnerabilities or malware, providing an additional layer of defence against both physical and cyber-attacks.

YouTube-Video: https://youtu.be/svdLstKYdMI

(1) https://tinyurl.com/dtz3d2jr

(2) https://tinyurl.com/2p9ffyx9

(3) https://tinyurl.com/mr3n3b98

Market research

Market for electronic safety technology
increases turnover to almost 5 billion euros
• Significant differences between the specialist sectors • Digitalisation and networking are trendsetters • Services gain in importance

With a 4.5 percent increase in turnover to around 4.9 billion euros, the market for electronic safety technology in Germany grew again in 2021.

"In the past year, security technology in Germany has recovered significantly overall and is approaching the five-billion mark in terms of sales," said Dirk Dingfelder, chairman of the ZVEI security trade association. "Many property owners and operators have modernised their technology during the Corona pandemic and have already implemented pending investments," Norbert Schaaf, Chairman of the Board of BHE Bundesverband Sicherheitstechnik e.V., explained the upward trend in the market.

Services in particular, such as maintenance and repair, have played a significant role in last year's growth spurt. "The month-long corona-induced lockdown made it possible in many cases to carry out maintenance and repair work on security and other systems," Dingfelder and Schaaf said. "The bottom line is that significantly more additional projects were implemented than were postponed."

Dingfelder sees digitalisation and networking in security technology, but also in building automation and in related trades, as an increasingly clear trend. "The market is moving more and more towards digital services, networked products and systems," he emphasised. "The new standard DIN EN 50710 'Requirements for the provision of secure remote services for fire safety systems and security installations', published in May 2022, has set another milestone on this path," Schaaf explained.

However, the imponderables have become greater elsewhere: "The shortage of skilled workers is increasing at all levels of the value chain," Dingfelder and Schaaf stated. "Among other things, bottlenecks in electronic components of all kinds are burdening the industry."

Large differences in growth between the individual trades

Sales of fire alarm technology - by far the largest trade in security technology, which is also heavily dependent on the construction industry - rose by 4.1 per cent to just under 2.3 billion euros in 2021. The front-runner in growth, however, is voice alarm systems with an increase of almost 14 percent to 130 million euros.

Video systems also showed an above-average development with an increase of 7.7 percent to 700 million euros. The wide range of possible applications and the flexibility of video security technologies, for example for people counting to comply with Corona requirements, resulted in a relative boom here.
Access control systems also held their own in the market with a plus of 8.8 percent to 420 million euros.

In 2021, hold-up and burglar alarm systems were able to turn their negative trend from the previous year into a slight plus with an increase of 0.6 percent to 875 million euros.

For the first time, smoke and heat ventilation systems (SHEVS) are shown separately in the statistics with a turnover of 160 million euros. Together with other technologies, such as call systems according to DIN VDE 0834, escape door systems, personal assistance call and other systems and components, this block recorded an overall growth of 3.2 percent in 2021 compared to the previous year.

[www.bhe.de, www.zvei.org]

light+building
autumn edition

2. – 6.10.2022
Frankfurt am Main

Breaking new ground

The world's leading trade fair for
lighting and building services technology

EuroCIS 2022 exceeds expectations

Propensity to invest in technology as high as ever in retail Positive mood in the exhibition halls – personal encounters are centrestage again V-connect

EuroCIS 2022, The Leading Trade Fair for Retail Technology, has drawn to a close on Thursday (2 June 2022) in Düsseldorf with very good results. With its ranges it impressively underlined how the past two pandemic years have triggered a huge surge in digitalisation in bricks-and-mortar retail. Many retailers have heavily accelerated their omni-channel strategies and are now investing in the digitalisation of their stores.

Summarising results Petra Cullmann, Executive Director at Messe Düsseldorf, delights: "The atmosphere in the exhibition halls was positive across the board and governed by optimism. From conversations with our customers we know that expectations have been far exceeded. At last, face-to-face contacts could be made and intensified again."

On the three days of EuroCIS 9.070 trade visitors from 88 countries were registered. 345 exhibitors from 33 countries participated, occupying 10,721 m² of net exhibition space.

"These figures are reason for optimism and anything but foreseeable after the compulsory, pandemic-induced break in 2021 and the postponement from January to June 2022. With its trade fair activities EuroCIS has provided a powerful impetus for the industry. The exhibitors are happy to have come to Düsseldorf and are avidly enquiring about participation options for next year when EuroCIS will be held as part of EuroShop again following its usual cycle," says Elke Moebius, Project Director EuroCIS. This year's EuroCIS focuses on innovations in the areas of Analytics, Payment, Check-out solutions, Connected Retail and Omni-channel, Artificial Intelligence, Self-Scanning Check-Out and Customer-Centric Marketing.

Solutions such as intuitively operated check-out kiosks and stations, digital signage solutions with touch-screen functionality or interactive shop windows thrilled the international expert audience as well. Lift & Learn systems that invite shoppers to interactively learn about products across all retail channels, were also presented. They offer retailers major added value: ranging from virtual shelf extension and higher customer loyalty to increased revenue. EuroCIS also showcased innovative back-office technologies which enable retail companies to analyse and optimise workflows at all the process stages in store, at the warehouse and along the entire supply chain, thereby making them fit for the future. Ulrich Spaan, Board Member at the EHI Retail Institute, sums up: "The success of EuroCIS 2022 reflects the high relevance of leveraging technology within retail organisations today. Technology penetrates all fields of retail and the pandemic has accelerated this trend yet again. 'Smart Retail' plays a pivotal role in the favour of shoppers who expect frictionless customer journeys and personalised services between on and offline channels."

The next EuroCIS will be held in Düsseldorf as part of EuroShop 2023 from 26 February to 2 March 2023. www.eurocis-tradefair.com

SENSORMATIC SOLUTIONS

Over 70% of consumers would change their shopping habits after learning a brand isn't operating sustainably

Johnson Controls brand Sensormatic Solutions surveyed 1,000 U.S. consumers and found 81% are concerned or very concerned about the environment's future • Nearly half of consumers believe businesses must lead the charge toward sustainability • Most consumers believe that reducing material waste and greenhouse gas emissions are the most critical outcomes retailers should pursue

Sensormatic Solutions released its survey results related to U.S. consumer sentiment towards sustainability. A plurality of respondents (49%) believes that the responsibility for implementing sustainable practices falls on corporations and retailers, as opposed to individuals or government regulators. The new data highlights that the era of retail responsibility for sustainable initiatives is in full swing. The survey also showed that consumers are highly invested in shopping sustainably. Over half of those surveyed – 53% – said they would use a brand or store less frequently if they discovered that a brand or store wasn't operating sustainably, and 18% said they would stop shopping with that retailer altogether. Furthermore, 70% of consumers say they are willing to pay at least 5% more for products that can demonstrate a fully sustainable supply chain – even though cost is the most cited barrier to sustainable shopping (55%) closely followed by consumers' perception that the stores they frequent do not offer many sustainable options (47%).

"This survey speaks to a belief we've long held: prioritizing sustainable solutions is simply good business," said Kim Melvin, global leader of marke-

ting, Sensormatic Solutions. "Facilitating sustainable retail operations has been at the heart of Sensormatic Solutions business for some time; but now, that same sentiment is mirrored among consumers. American shoppers of all ages want to see brands make investments that support responsible retail at all levels. In fact, they don't see businesses engaging in sustainable operations as an option – they see it as an obligation."

Consumers want to know that their dollars are going to companies they understand are doing the right thing when it comes to the environment. Nearly 90% of consumers think that retailers don't do enough to showcase3 their sustainability efforts.

Perhaps the most compelling takeaway around corporate responsibility is consumers' belief that retailers' sustainability work is far from complete. Over 90% of respondents said that it's important to them that retailers continue to improve environmental performance and energy management in their stores. Sixty-two percent would like to see this done through a switch to sustainable packaging alternatives, and 54% would like retailers to enhance inventory intelligence to avoid overstocks, wasted goods,

added deliveries while optimizing fulfillment methods, and more.

Consumers held varying definitions of "sustainable practices," ranging from installation of energy-efficient displays to utilization of alternative packaging, and participation in recycling programs, among others. As such, when exploring options to bolster sustainable retail initiatives, retailers can decide which options work best for their business model. Modern retail analytics platforms, like Sensormatic IQ, can help support that. Sensormatic IQ's integrated platform provides outcomes-based insights about enterprise operations which can highlight areas of opportunity for sustainable improvements.

Additional information regarding Sensormatic Solutions efforts to foster a more sustainable retail landscape can be found on the Sustainability page or in our 2022 white paper: "Our Retail Sustainability Story of Sensormatic Solutions by Johnson Controls".

Survey Methodology: Sensormatic Solutions collected responses from 1,000 U.S.-based consumers, 18-years and older, via a third-party provider to determine findings of its 2022 Sustainability Survey. The survey was conducted between January 28 – January 30, 2022.

Unique combination

of AI analytics, motor-driven triaxial adjustment and IR/white light outside the bubble

Dallmeier presents DOMERA, "probably the most versatile camera series in the world"

With the DOMERA 6000* camera series, Dallmeier presents a completely new generation of dome cameras. The multi-talent camera delivers top notch video analysis results even under the most demanding light conditions. This is supported by AI-based Edge analytics as well as image capture with the latest generation of sensors in four and eight megapixels.

With a theoretical total of well over 300 conceivable combinations, the modular DOMERA housing and mounting system is usable for most indoor and outdoor video applicati-

ons. Rapid installation and adjustment to changed surroundings is assured by the "Dallmeier RPoD", with remote-controlled, motor-driven lens adjustment in three axes, the PTRZ (Pan Tilt Roll Zoom) function. For lighting, the first ever ring of IR and white light LEDs located outside of the bubble is used. The system thus eliminates that lighting problems that beset traditional dome cameras. This makes DOMERA the only camera on the market which offers all these advantages in a single product.

Bold claim in the premium segment

Particularly when specifications in terms of image quality, security and analytics performance are high, end customers and installers often have difficulty finding the right solution for their requirement among the wide range of available cameras: How good are image quality and analytics? How easy or difficult is it to set the camera up, and how difficult is it to adjust viewing angles or image sections afterwards? Are there any lighting problems, e.g., from scratches in the bubble or reflecting walls? And finally, questions on all aspects of quality and durability, and of course cybersecurity and privacy, are becoming increasingly important. With the new DOMERA 6000 camera series, Dallmeier makes the bold claim that it has the right answers to these requirements.

Edge analytics with AI for a wide range of analysis applications

Fitted with a high-performance SoC, the DOMERA cameras can perform latest generation AI-based Edge analytics. The reliable detection and classification of objects such as people or vehicles thus enables a whole range of basic analyses such as People Counting, Loitering or Intrusion.

Users can then depict many possible analysis applications from these for their specific requirements using various parameters via the web-based user interface. By activating relays, and by supporting standard protocols such as MQTT, it is possible to automatically trigger various related actions, e.g., activating 3rd party lighting or alarm systems.

In addition, the loudspeaker available as an option allows manual or automatic audible communication. Regular updates serve to guarantee that the neural networks are always up-to-date and undergoing constant training. Upon request, the Dallmeier experts will also develop or train neural networks for customer-specific requirements.

Highest image quality, and rapid, web-based setup

The 6000 series offers high image quality with four or eight MP resolution, HDR functionality and extreme light sensitivity, and the cameras are consequently ideally suited for indoor and outdoor use under difficult light conditions. A further special highlight is the completely new adaptive IR and white light lighting system, for which a registered design application has already been filed. Here, the lighting is integrated in the housing ring, which means it is mounted outside the bubble. This exceptional design guarantees a long service life, as it eliminates the problems associated with conventional IR dome cameras, in which tiny scratches in the bubble cause interfering reflections. Being adaptive, it also minimizes effects such as reflection from walls.

The motor-driven, triaxial adjustment with the Dallmeier "Remote Positioning Dome" - RPoD for short - saves setup time. Its PTRZ (Pan Tilt Roll Zoom) function enables users to adjust the image section and the area to be captured, and even to change
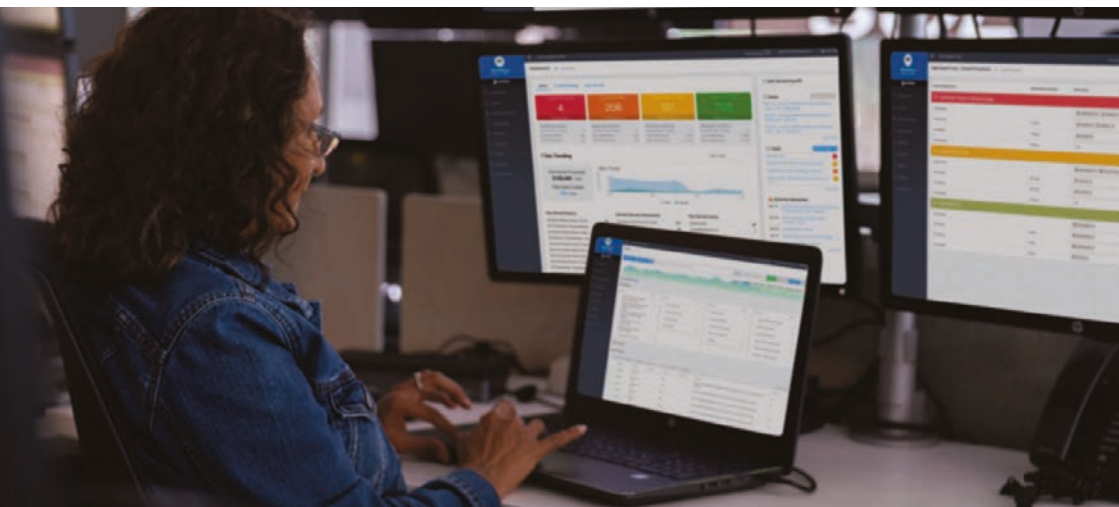
them later from anywhere via web interface. Thus, a 90-degree rotation for corridor mode can be set up in no time. The initial configuration and setup for the camera is browser-based and does not require any additional software.

Well over 300 variants with just 18 components

An especially useful feature for installers: Theoretically, the DOMERA® components can be combined to create well over 300 different products. This is made possible by an ingenious modular system of in total 18 components: four camera base models, various lighting rings and several housing and mounting variants. Moreover, support for ONVIF S and T profiles means that the cameras can be integrated in any VMS system. Consequently, 90 percent of all typical video applications can be implemented easily and with utmost quality and security – with minimal training and low warehousing requirement on the part of the installer. For this innovative system, the DOMERA® series has already received the Red Dot Design Award 2022.

"The customer's perspectives were central to the development of the DOMERA 6000 series from the very beginning. For end customers, we offer maximum image quality, and through the AI analytics a user advantage that far exceeds pure video functionality," says Dieter Dallmeier, Founder & CEO, Dallmeier electronic. "In turn, the installer is able to offer his end customer real added value – with minimal outlay for configuration, installation and setup. Combined with the quality for which we are known and the correspondingly low support burden, excellent commercial options for installers present themselves in this area too."

*DOMERA® 6000

Cyber Threat Information Sharing and Analysis Organization for Public Safety

Public Safety Threat Alliance created as the cybersecurity services hub for world-class information sharing and threat intelligence collaboration for the global public safety community

Motorola Solutions announced the establishment of Motorola Solutions' cyber threat information sharing and analysis organization (ISAO) for public safety. The Public Safety Threat Alliance, a Cybersecurity and Infrastructure Security Agency (CISA)-recognized ISAO, highlights Motorola Solutions' unwavering commitment to public safety organizations and the communities they serve. CISA, which falls under the U.S. Department of Homeland Security, serves as the National Coordinator for Critical Infrastructure Security and Resilience, on this important initiative.

In accordance with the 2015 Executive Order "Promoting Private Sector Cybersecurity Information Sharing", ISAOs are groups focused on sharing information related to cybersecurity risks and incidents with membership drawing from the public and private sectors. With the establishment of the Public Safety Threat Alliance, members will be able to share and analyze information from multiple sources to proactively contribute to a stronger cybersecurity posture for the public safety community, their constituents, and other stakeholders, including government agencies and businesses.

"The establishment of the Public Safety Threat Alliance fills a critical void, creating a single entity entirely focused on the collection, analysis, production and sharing of actionable public safety-focused cyber threat information and intelligence," said Billy Bob Brown, Jr., executive assistant director for Emergency Communications, CISA. "Now, the public safety community is better equipped to focus their cyber threat intelligence and defense efforts on specific adversaries and their malicious cyberattacks."

The Public Safety Threat Alliance will leverage information related to cybersecurity risks from across Motorola Solutions' Cybersecurity Services, coupled with information from members and trusted partners including CISA, other ISAOs, and nonprofits dedicated to sharing cyber threat intelligence, to generate actionable intelligence which will improve members' cybersecurity posture, defense and resilience against ever-evolving threats to their no-fail Public Safety missions.

"For example, it's been reported that there was a 1,885 percent increase in ransomware attacks against governments worldwide in 2021," said Scott Kaine, corporate vice president of Cybersecurity, Motorola Solutions. "With cyber threats increasing in scope, scale and complexity, the Public Safety Threat Alliance can help to dramatically increase the efficacy with which intelligence is used to monitor, detect and respond to potential threats before they result in downtime of public safety services."

Membership in the Public Safety Threat Alliance is open to all public safety agencies.

[www.motorolasolutions.com]

Upgrade of Entry-level IP Surveillance System for Easier Connection, Use and Maintenance

Dahua Technology, Chinese video-centric smart IoT solution and service provider, upgraded the Dahua Entry-level IP surveillance system for a series of entry-level IP products, such as IP camera, NVR, switch, etc. to help users install and maintain equipment more easily while using IP security systems.

The upgrades make the system easier for connection, use and maintenance. End-users can quickly learn how to install an IP security system that shows high expansibility, openness and compatibility in certain scenarios.

Multiple connection modes are available for easy connection. PoE (Power over Ethernet) and WiFi technologies are used to reduce wiring difficulties for end-users and vendors when installing IP security systems.
Meanwhile, Plug&Play (PnP) enables the IP monitoring system to adapt to hardware changes with minimal in-

Download COS Pro APP

tervention by the user. If the IP camera is plugged into the NVR's built-in switch, the camera will automatically initialize, while the pictures will appear directly on the NVR display. If IP camera is connected to an external PoE switch, the Plug&Play function needs to be manually enabled on the NVR interface. In this case, NVR will automatically search for IP camera in the LAN and add it automatically.

Easy use mainly relies on Dahua DMSS and Cos Pro (released in late April). By integrating the NVR chan-

nel management function in these two apps, end-users and installers can complete a series of operations, such as device search, initialization, channel addition, preview and drawing, on their phones, when configuring a small IP security system. There is no need for them to use additional monitors and laptops, which greatly simplifies the configuration of the IP system.

To make maintenance easier, the system supports binding device keychains through DMSS. When users forget the password, they can retrieve it on the DMSS app easily and quickly. Meanwhile, the device supports convenient cloud upgrades. When the device is hosted on the Cos platform, the installer can receive the fault information of the device on the Cos app, and do some basic fault handling remotely.
This upgraded entry-level IP surveillance system, as a simple step for users to enter the IP world, is mainly applicable in small shops, apartments, villas and other small security scenarios. Dahua continues to innovate for better user experience and create more values for customers around the world.

Cutting-edge security solutions to Passenger Terminal Expo 2022

Rohde & Schwarz is showcasing innovative solutions for airports, governmental authorities, and internal and external security organizations. Exhibits at the show include effective drone defense and revolutionary passenger security scanning solutions, advancing security and transforming the passenger experience at airports worldwide.

At this year's annual Passenger Terminal Expo, taking place in Paris, France, from June 15-17, 2022, Rohde & Schwarz (hall 7.3, booth Z1.3160) will showcase innovative solutions for drone detection and security scanning. Rohde & Schwarz is a key partner for airports, law enforcement and governmental authorities, as well as for internal and external security organizations.

To be seen at the show, the R&S QPS201 enhanced Advanced Imaging Technology (eAIT) security scanner delivers a market-leading high security performance and a fast and more comfortable passenger experience to complement the significant investments being made throughout airports worldwide to redefine the passenger experience. R&S QPS201 delivers high-performance security screening using safe millimeter wave radio frequency technology to rapidly and accurately screen passengers automatically for concealed objects. In use at some of the world's busiest airports since 2015, the security scanner has achieved European Civil Aviation Conference (ECAC) approval and has been certified by the Transportation Security Administration (TSA), as it meets its stringent detection requirements.

Drones are a real and present threat to airports worldwide. Off-the-shelf unmanned aerial systems (UAS) are constantly in the headlines these days, with drone incidents an almost weekly occurrence. To counter these UAS threats, accurate classification of the type of the detected drone is critical to the subsequent decision-making process. Modular and scalable, R&S ARDRONIS can be deployed on a variety of platforms and readily in-tegrated to accommodate specific threat profiles. The strength of this CUAS solution lies in the reliable localization of the drone pilot. Enhancing airport security, R&S ARDRONIS detects and locates drone pilots before a UAS takes off, preventing and minimizing costly downtimes at the airport. The drone's remote-control uplink is detected from the moment it is switched on, providing an early warning benefit.

Rohde & Schwarz supports customers by offering comprehensive services throughout the product's lifecycle. A global service network with local contacts ensures short response times. The service portfolio includes standardized products, such as calibration and repair services, and individual service concepts tailored to customer requirements.

Aquisition of Valid's payment and identity solutions business in the U.S

Giesecke+Devrient (G+D), a global security technology group, today announced the acquisition of the payment and identity solutions business of Valid USA. With this step, G+D aims to accelerate growth in the U.S., one of the world's largest payment and identity markets. G+D customers will benefit from the enlarged business size in the face of persistent industry-wide supply chain challenges.

G+D and Valid, headquartered in Brazil, signed an Asset Purchase Agreement (APA) for the acquisition of Valid's payment and identity solutions business in the U.S. by G+D. This includes the three manufacturing facilities in Downers Grove (Illinois), Bolingbrook (Illinois) and Fort Wayne (Indiana), which collectively employ more than 400 people as well as parts of the Valid USA headquarters in Lisle (Illinois). G+D has been firmly established in the U.S. since 1990,

with offices and production sites across the country, providing technologies and solutions for payment, connectivity, identities and digital infrastructures. Valid is a global technology provider that offers solutions in payment, mobile, data and identity solutions, as well as digital marketing and digital certification. Among the customers in the U.S., where Valid has been present since 2012, are key financial institutions and merchants, as well as various government customers. Both Valid solutions perfectly complement G+D's existing payment and identity business, enabling a gradual and seamless transition for all affected customers.

After the deal is closed, which is planned for later in the year, the G+D Group will integrate the acquired businesses into its existing organization: The parent company G+D will take over the local payment card production facilities, while its subsidiary Veridos, a provider of integrated identity solutions, will further expand the existing driver's license card business. The investment strengthens G+D's and Veridos' offering and position,

providing further impulse for its accelerated growth in the U.S., one of the world's largest payment and identity markets. Ralf Wintergerst, Group CEO and Chairman of the Management Board of G+D said: "Part of G+D's success strategy is that we continue to invest intensively in new technology fields as well as our core business. With the acquisition of Valid's payment and identity business in the U.S., we are not only reaffirming our long-term commitment to the U.S. market. The expanded solution portfolio will also allow us to continue growing strategically in both fields – payment and identities."

Eli Carmeli, President and CEO of Valid USA states: "Valid chose the G+D Group because of its experience, knowledge and leadership in its operating segments. Furthermore, the fact that G+D already has a presence in the American market further benefits its current and prospective customers. Valid and G+D, together, are looking for a transition that aims at continuity in the excellence of the services provided."

Videotechnology

Trespassing

Investigation & Analysis with Intelligent Video Surveillance
Protecting Property from Trespassers
Without the proper technology and protocols in place, trespassing can happen quite easily — whether it is intentional or not.

Trespassing happens for any number of reasons. Bad actors looking to gain access to secured information or intending to do physical harm can enter seemingly "off limits" areas and suddenly businesses are dealing with a security breach. Whether the trespassers' motivations are malicious or otherwise, it is important for businesses to be alerted when someone is in a place they shouldn't be.

From airports and hospitals to theme parks and entertainment venues, and any type of private property in between, businesses can leverage AI-based video content analytics to extend surveillance security applications and further protect their facilities against trespassers.

Detecting Trespassing in Real Time

Stopping a trespasser in real time gives businesses the ability to prevent theft, loss, damage or injury by proactively responding to situational changes as they unfold. And video analysis-driven real-time alerting gives operators the opportunity to do just that. Real-time alerting can be used for perimeter protection and responding when a person is detected on or past the defined perimeter. Alerts can be configured and triggered based on unique environmental factors, such as the time of day, and when people are or are not expected to be in the defined area.

A human operator defines the rules that reflect what is "normal" and configures alerts to be triggered when objects or activities outside the scope of "normal" are detected. Not only can operators be notified when any person enters a defined area, they can be alerted when a specific person enters that area through the use of face matching technology and watchlists.

Operators have the ability to upload watchlists of video or digital images to the video analysis program, which enables the software to automatically monitor all camera feeds for face matches.

When a possible face match has been detected, human operators receive an alert and can validate a correct match. Based on the human evaluation, the detected person can be more closely monitored and tracked, when necessary, confronted to prevent him/her from entering the premises.

Private businesses may have many reasons for securing their facilities, including protecting against former employees or known threats. By adding those who should not be on property to the watchlist, video content analytic software with facial recognition technology can help businesses be proactive about their security.

Investigating Trespassing after the Fact

While either preventing or stopping a trespasser in real-time is ideal, investigating a trespassing incident after the fact is crucial to helping a business (and law enforcement, if necessary), figure out what happened, and how to prevent it in the future.

After a trespassing incident, time is of the essence to understand what happened and what the associated risks may be, and the ability to accelerate video search and response to unfolding events is critical for helping security personnel track down suspects and provide key evidence. For example, when deployed in a hospital, video analytic software can help management understand how a trespasser gained access to a secure pharmacy.

Video content analytics technology processes video, identifies objects (such as people or vehicles) in the video footage, and classifies and indexes the video object metadata so that footage can be easily and quickly searched and analyzed. Hours or days of footage can be combed in a matter of minutes, with operators filtering video to focus the video search and show only people or objects that fit a certain description. This empowers security teams to extract crucial details, gather evidence and accelerate investigations.

Did the trespasser steal medication? Where did they go after they left the pharmacy, and how did they move about the hospital? Video content analytic software can help the hospital uncover those answers and therefore implement measures to ensure it does not happen in the future.

Deriving Insight from Trespasser Behavior

Of course, preventing and stopping trespassers is of utmost importance, but equally imperative is gaining insights from the incident to prevent future events and increase security measures if necessary.

Video analytic software can reveal patterns in visitor behaviors, such as when and where trespassing tends to happen, which paths around the property are taken and where individuals dwell or linger, through data visualizations.

For instance, places open to the public like a theme park or theater may experience frequent trespassing. For management, understanding why and how trespassers are accessing restricted areas is crucial to making necessary improvements, such as enhanced signage or increased security.

Author: Lizzi Goldmeier
[www.briefcam.com]

Videotechnology

4K pan-tilt-zoom camera with powerful zoom capability

As the latest addition to its line-up, the Sony's SRG-X40UH pan-tilt-zoom (PTZ) camera combine high image quality, versatile connectivity and flexibility in installation.

Sony expands its renowned PTZ camera line-up with the introduction of the new SRG-X40UH. The camera adopts 4K Exmor R™ CMOS image sensor and delivers high-quality images at 4K[i] alongside powerful zoom capability with wide viewing angle, UVC and HDMI connectivity and will be available in autumn 2022. The camera is an ideal choice for remote communication and monitoring in a wide range of markets which have seen strong growth in the last couple of years, such as corporate, education, healthcare, and more. With simple functionality and interface connection, it's easy to connect and use for live streaming video.

As an affordable 4K PTZ camera, the SRG-X40UH will deliver outstanding detail and high-quality imagery, natural color reproduction and high sensitivity that capture facial or other relevant details in remote communications situations, even in low light. In addition, oversampling from 4K will deliver excellent image quality even in FHD.

A powerful zoom up to 40x in FHD and 30x in 4K with the Clear Image Zoom technology[ii], combined with an approximately 70 degrees wide viewing angle will complement smooth and rapid PTZ movement with a ceiling mounting option means that this camera can capture important scenes in different locations, from small conference rooms to large auditoriums.

The SRG-X40UH, with its simple UVC and HDMI connections and PoE+ support, can be integrated into existing systems with minimum cabling, and remotely controlled through a VISCA/VISCA over IP command.

[i]   4K 30p image is supported via HDMI. Full HD 60p is supported via UVC

[ii] Optical zoom capability is 20x.

New report on worldwide usage of cloud surveillance

Eagle Eye Networks has released its second annual Cloud Video Surveillance Camera Worldwide Statistics report, delivering data and insight into security camera usage and trends globally and regionally.

The report, which can be downloaded, analyses aggregate data from a sample set of 200,000 cameras, and includes more than 150 camera manufacturers. The report covers a wide range of industries including corporate enterprises, retail, restaurant, warehouse, industrial, education, healthcare, hospitality, and multifamily dwellings.

"Organisations moving to cloud-based video surveillance make key deployment decisions across several factors," said Dean Drako, Founder and CEO of Eagle Eye Networks. "We are sharing the most common implementation configurations and trends with a goal to help everyone moving to cloud security camera systems make better decisions."

Key data included the compilation of data within the report includes such findings as:

- Increased adoption of higher resolution cameras, audio-enabled cameras, and regional differences in usage across the Americas, EMEA and APAC
- Relative level of use of the four most common video analytics
- Flexibility of true cloud systems to support hundreds of camera types and manufacturers around the world
- Growth in number of camera manufacturers
- Preferred video recording location and recording retention duration
- Regulated industries' usage of cloud video surveillanc3

www.een.com/2022-security-camera-statistics-report

What is Biometrics?
How is it used in security?

Biometrics are rising as an advanced layer to many personal and enterprise security systems. With the unique identifiers of your biology and behaviors, this may seem foolproof. However, biometric identity has made many cautious about its use as standalone authentication.

Modern cybersecurity is focused on reducing the risks for this powerful security solution: traditional passwords have long been a point of weakness for security systems. Biometrics aims to answer this issue by linking proof-of-identity to our bodies and behavior patterns.

In this article, we'll explore the basics of how cybersecurity uses biometrics.

To help break things down, we'll answer some common biometrics questions:

- What is the meaning of biometric?
- What is biometric data?
- What is a biometric scanner?
- What are the risks of biometric security?
- How can we make biometrics more secure?

To begin, let's start off with the basics.

What is Biometrics?

For a quick biometrics definition: Biometrics are biological measurements — or physical characteristics — that can be used to identify individuals. For example, fingerprint mapping, facial recognition, and retina scans are all forms of biometric technology, but these are just the most recognized options.

What is Biometrics? How is it used in security?

Researchers claim the shape of an ear, the way someone sits and walks, unique body odors, the veins in one's hands, and even facial contortions are other unique identifiers. These traits further define biometrics.
Three Types of Biometrics Security

While they can have other applications, biometrics have been often used in security, and you can mostly label biometrics into three groups:

• Biological biometrics
• Morphological biometrics
• Behavioral biometrics

Biological biometrics use traits at a genetic and molecular level. These may include features like DNA or your blood, which might be assessed through a sample of your body's fluids.

Morphological biometrics involve the structure of your body. More physical traits like your eye, fingerprint, or the shape of your face can be mapped for use with security scanners.

Behavioral biometrics are based on patterns unique to each person. How you walk, speak, or even type on a keyboard can be an indication of your identity if these patterns are tracked.
Biometric Security Works

Biometric identification has a growing role in our everyday security. Physical characteristics are relatively fixed and individualized — even in the case of twins. Each person's unique biometric identity can be used to replace or at least augment password systems for computers, phones, and restricted access rooms and buildings. Once biometric data is obtained and mapped, it is then saved to be matched with future attempts at access. Most of the time, this data is encrypted and stored within the device or in a remote server.

Biometrics scanners are hardware used to capture the biometric for verification of identity. These scans match against the saved database to approve or deny access to the system.

In other words, biometric security means your body becomes the "key" to unlock your access.

Biometrics are largely used because of two major benefits:

• Convenience of use: Biometrics are always with you and cannot be lost or forgotten.
• Difficult to steal or impersonate: Biometrics can't be stolen like a password or key can.

While these systems are not perfect, they offer tons of promise for the future of cybersecurity.

Examples of Biometric Security

Here are some common examples of biometric security:

• Voice Recognition
• Fingerprint Scanning
• Facial Recognition
• Iris Recognition
• Heart-Rate Sensors

In practice, biometric security has already seen effective use across many industries.

Advanced biometrics are used to protect sensitive documents and valuables. Citibank already uses voice recognition, and the British bank Halifax is testing devices that monitor heartbeat to verify customers' identities. Ford is even considering putting biometric sensors in cars.

Biometrics are incorporated in e-Passports throughout the world. In the United States, e-passports have a chip that contains a digital photo-

graph of one's face, fingerprint, or iris, as well as technology that prevents the chip from being read — and the data skimmed — by unauthorized data readers. As these security systems are rolled out, we are seeing the pros and cons play out in real-time.

Are Biometric Scanners Safe? - Improvements and Concerns

Biometrics scanners are becoming increasingly sophisticated. You can even find biometrics on phone security systems. For example, the facial recognition technology on Apple's iPhone X projects 30,000 infrared dots onto a user's face to authenticate the user by pattern matching. The chance of mistaken identity with the iPhone X biometrics is one in a million, according to Apple.

The LG V30 smartphone combines facial and voice recognition with fingerprint scanning and keeps the data on the phone for greater security. CrucialTec, a sensor manufacturer, links a heart-rate sensor to its fingerprint scanners for two-step authentication. This helps ensure that cloned fingerprints can't be used to access its systems.

The challenge is that biometric scanners, including facial recognition systems, can be tricked. Researchers at the University of North Carolina at Chapel Hill downloaded photos of 20 volunteers from social media and used them to construct 3-D models of their faces. The researchers successfully breached four of the five security systems they tested.

Examples of fingerprint cloning are everywhere. One example from the Black Hat cybersecurity conference demonstrated that a fingerprint can be cloned reliably in about 40 minutes with $10 worth of material, sim-

ply by making a fingerprint impression in molding plastic or candle wax.

Germany's Chaos Computer Club spoofed the iPhone's TouchID fingerprint reader within two days of its release.

The group simply photographed a fingerprint on a glass surface and used it to unlock the iPhone 5s.

Biometrics - Identity & Privacy Concerns

Biometric authentication is convenient, but privacy advocates fear that biometric security erodes personal privacy. The concern is that personal data could be collected easily and without consent.

Facial recognition is a part of everyday life in Chinese cities, where it's used for routine purchases, and London is famously dotted with CCTV cameras. Now, New York, Chicago, and Moscow are linking CCTV cameras in their cities to facial recognition databases to help local police fight crime. Ramping up the technology, Carnegie Mellon University is developing a camera that can scan the irises of people in crowds from a distance of 10 meters.

In 2018, facial recognition was introduced in Dubai airport, where travelers are photographed by 80 cameras as they pass through a tunnel in a virtual aquarium.

Facial recognition cameras are also at work in other airports throughout the world, including those in Helsinki, Amsterdam, Minneapolis-St. Paul, and Tampa. All that data must be stored somewhere, fueling fears of constant surveillance and misuse of data…

Biometric Data Security Concerns

A more immediate problem is that databases of personal information are targets for hackers.

For example, when the U.S. Office of Personnel Management was hacked in 2015, cybercriminals made off with the fingerprints of 5.6 million government employees, leaving them vulnerable to identity theft.

Storing biometric data on a device – like the iPhone's TouchID or Face ID – is considered safer than storing it with a service provider, even when the data is encrypted.

That risk is similar to that of a password database, in which hackers may breach the system and steal data that's not effectively secured.

The ramifications, however, are significantly different. If a password is compromised, it can be changed. Biometric data, in contract, remains the same forever.

Ways to Protect Biometric Identity

With the risks to privacy and safety, additional protections must be used in biometric systems.

Unauthorized access becomes more difficult when systems require multiple means of authentication, such as life detection (like blinking) and matching encoded samples to users within encrypted domains.

Some security systems also include additional features, such as age, gender, and height, in biometric data to thwart hackers.

India's Unique ID Authority of India Aadhaar program is a good example. Initiated in 2009, the multi-step authentication program incorporates iris scans, fingerprints from all 10 fingers, and facial recognition.

This information is linked to a unique identification card that is issued to

each of India's 1.2 billion residents. Soon, this card will be mandatory for anyone accessing social services in India.

Biometrics make a good replacement for usernames as part of a two-factor authentication strategy. That incorporates:

- Something you are (biometrics)
- Something you have (like a hardware token) or something you know (like a password)

Two-factor authentication makes a powerful combination, especially as IoT devices proliferate. By layering the protection, secured internet devices become less vulnerable to data breaches.

In addition, using a password manager to store any traditional passwords can give you an additional safeguard. Takeaways on Biometrics

In summary, biometrics remains a growing way to verify identity for cybersecurity systems.

The combined protection of your physical or behavioral signatures with other authentications gives some of the strongest known security. At the moment, it is at a minimum better than using a character-based password as a standalone verification.

Biometric technology offers very compelling solutions for security. Despite the risks, the systems are convenient and hard to duplicate. Plus, these systems will continue to develop for a very long time into the future.

Featured Article on www.kaspersky.com: https://tinyurl.com/3cvbbmrd

©Kaspersky

MOBOTIX

VdS-approved Thermal Imaging Systems For Early Fire Detection

The MOBOTIX M16 VdS Thermal TR solution consisting of a thermal imaging camera, special firmware, and additional components has been approved by VdS Schaden-verhütung GmbH, Europe's largest institute for corporate security, since March 2022. MOBOTIX customers can therefore be sure that they will be warned of fire damage as early and as effectively as possible and know that, despite the optimum protection, any damage that occurs will be settled quickly and comprehensively by the insurance company. In addition, a VdS-approved system can, if necessary, provide discounts on insurance premiums or even enable insurance in the first place.

The VdS-approved fire protection solution opens up new sales potential for MOBOTIX AG and its partners, especially around certified fire alarm systems. While MOBOTIX thermal technology already provided the best early fire detection before, the video systems with their recognition can now also be integrated into existing VdS-certified fire protection systems. Moreover, the renowned seal of quality confirms the high level of MOBOTIX Thermal expertise and pays directly into the positive brand perception on the market.

Detecting fires reliably and as early as possible is the goal of early fire detection that MOBOTIX has been pursuing for a long time with its camera technology - to intervene quickly, prevent damage and protect people. It works like this:
Thermal Radiometry (TR) cameras from MOBOTIX with calibrated thermal image sensor measure thermal radiation in the entire image area and trigger a so-called event when limit values are exceeded. This can be an alarm or a network message, or even the direct triggering of a fire extinguishing system.

The camera-based MOBOTIX solution is impressive because it is quick and inexpensive to install, which is usually much easier and less expensive than, for example, linear heat detectors in the ceiling of a room.
In addition, the thermal camera system, which can be installed at a distance of up to 60 meters from the heat source, can also react more quickly. Heat at the start of the fire is detected even before the heat has risen to the ceiling. Unlike aspirating smoke detectors, the MOBOTIX M16 TR is not dependent on smoke development.
The MOBOTIX solution, which has already proven itself in practice, has now been confirmed with VdS recognition as providing optimum protection for people, systems and goods against fire damage through early fire detection.

"On the one hand, the VdS recognition confirms our excellent and reliable solution for early fire detection, but above all, it means for MOBOTIX customers optimal investment security in a fire alarm system that guarantees the criteria of the most renowned German institution for corporate security," explains Thomas Lausten, CEO of MOBOTIX AG.

VdS Schadenverhütung GmbH is a wholly-owned subsidiary of the German Insurance Association (GDV). It is one of the world's most renowned institutions for corporate security with a focus on fire protection, security, natural hazard prevention, and cyber security.

Its services include risk assessments, testing of facilities, certification of products, companies and specialists, and a wide range of training courses. The VdS seal of approval enjoys an excellent reputation among experts and decision-makers, is awarded to products and service providers, and has been named an essential purchasing criterion in the security market by the WIK survey.

The VdS-approved MOBOTIX solution mandatorily prescribes the system architecture with the M16 Thermal TR camera and three interface boxes and is already factory-equipped with special, certified software. It is also possible to upgrade a MOBOTIX M16 Thermal TR camera to the VdS level with a corresponding software update and the integration of the interface boxes mentioned above.

MOBOTIX M16 VdS Thermal Camera: Applications Far Beyond Fire Protection

MOBOTIX offers high-grade and durable industrial quality "Made in Germany" insensitive to dust and dirt. MOBOTIX outdoor video systems are robust and weatherproof, withstanding ambient temperatures ranging from minus 30 to plus 60 degrees Celsius.
The maintenance-free housing protects against humidity and corrosion. Reduced power consumption, bandwidth-optimized applications and fail-safety are the hallmarks of these flexible systems.

MOBOTIX thus achieves measurable return on investment, for example, through reduced insurance premiums or system downtime and insurance benefits in the event of damage. "With the VdS recognition, we offer our customers another convincing argument for choosing a MOBOTIX solution that has already proven itself in practice when it comes to fire protection," emphasizes Christian Heller, Vice President Sales North and Central Europe at MOBOTIX AG.

In addition to the reliable monitoring of even large and complex outdoor areas and warehouses, as well as the comprehensive monitoring of the indoor regions or even current-sensitive areas, the MOBOTIX M16 VdS thermal solution offers additional applications beyond fire protection: For example, thermal cameras are also ideally suited for monitoring sensitive areas (perimeter protection) day and night, even while maintaining privacy (data protection), since intruders can be detected and an alarm can be triggered without the faces of the persons having to be recognizable.

[www.mobotix.com]

INTERSCHUTZ 2022
For Heroes. For Rescuers. For You.

20 – 25 June 2022
Hannover ▪ Germany

interschutz.com

Deutsche Messe

Ready for the future.

INTERSCHUTZ