34. JAHRGANG | September 2025 | AUSGABE 9

GIT SICHERHEIT

30 926

MAGAZIN FÜR SAFETY UND SECURITY

Ausgabe ONLINE lesen:

Titelthema Seite 32:

Die Zukunft ist dezentral

Zutrittskontrolle für kritische Infrastrukturen
Gespräch mit Christian Heller, CSO von Frogblue

HEFT IM HEFT

VIDEO
ab S. 14

WILEY

Ksenia®
security innovation

creo-S
das neue BUS-Touchscreen-Bedienteil für die Sicherheit

creo-S ist das neue BUS-Touchscreen-Bedienteil, die sich ganz dem Sicherheitsmanagement von Wohn- und Geschäftsräumen widmet.

Dank seines minimalistischen Designs fügt es sich perfekt in jede Umgebung, ob modern oder klassisch, ein.
Der Benutzer hat die volle Kontrolle über das lares 4.0-System – einfach, direkt und sofort.

Erfahren Sie mehr:

www.kseniasecurity.com

So viel Intelligenz gab's nie

Intelligenz ist bekanntlich ein ausgesprochen gerecht und reichlich verteiltes Gut. Schließlich hört man selten die Beschwerde, nicht genug davon abgekriegt zu haben. Die Künstliche Intelligenz kommt ja noch on top – und nimmt seit Jahren geradezu schwindelerregende Fahrt auf. Es ist nicht mehr zu übersehen: Die Welt wird unweigerlich Tag für Tag immer cleverer... Was das für die Welt der Sicherheit bedeutet, lesen Sie in jeder Ausgabe der GIT SICHERHEIT – natürlich auch in dieser Septemberausgabe.

Im Fokus steht diesmal unter anderem ein „Heft im Heft" zum Thema Video (ab Seite 14): Darin zeigen wir, wie moderne Videotechnologien und KI-gestützte Analysen die Sicherheitsarchitektur von Unternehmen und Kritischen Infrastrukturen verändern. Es ist völlig klar: Videosysteme leisten schon längst weit mehr als reine Aufzeichnung. Wie zeigen Ihnen, wie intelligente Auswertung, Cloud-Integration und Datenschutz neue Maßstäbe setzen.

Die Sicherheit der gerade erwähnten Kritischen Infrastrukturen zieht derzeit alle Aufmerksamkeit auf sich – hier ist praktisch alles im Wandel, siehe KRITIS-DACH-Gesetz, NIS2 und Co. Daran knüpft auch unser Titelthema an. Zusammen mit Christian Heller und den Pfälzer Technologie-Pionieren von Frogblue zeigen wir ab Seite 32, wie dezentrale Zutrittslösungen speziell für KRITIS-Betreiber entwickelt werden.

Um sichere Kommunikation und digitale Vernetzung geht es ab Seite 10: Die PMRExpo als europäische Leitmesse für sichere Kommunikation zeigt kommenden November erneut Innovationen rund um Digitalfunk BOS, 5G-Campusnetze, Leitstellen, Cybersecurity und Critical IoT.

Nachhaltige Unternehmensführung steht im Mittelpunkt unseres Safety-Innentitels ab Seite 58: „Von der Kuh zum Schuh – Nachhaltigkeit, Automation und Verantwortung". Der Beitrag zum 115-jährigen Firmenjubiläum der Firma Atlas gibt Einblicke in die Entwicklung des Unternehmens, die Bedeutung eigener Produktionsstandorte und die Rolle von Nachhaltigkeit in der Sicherheitsschuhfertigung.

Haben Sie schon mal darüber nachgedacht, einen Roboterführerschein zu machen? Die fortschreitende Digitalisierung und Automatisierung der Arbeitswelt bringt schließlich auch neue Herausforderungen für die Qualifizierung mit sich. Der Beitrag des Deutschen Robotik Verbands (DRV) (ab Seite 68) stellt Sinn und Zweck des neuen Robo-Lappens vor.

Abgerundet wird die Ausgabe durch das dritte Interview aus unserer Kooperationsreihe mit dem VDMA (ab Seite 70), das die Auswirkungen der neuen Maschinenverordnung (MVO) und die Integration von Cybersecurity in die funktionale Sicherheit thematisiert. Die Experten erläutern, wie Maschinenhersteller und Betreiber auf die neuen Anforderungen reagieren können und welche Rolle Risikobewertung, Security by Design und die Zusammenarbeit in der Lieferkette künftig spielen werden.

Ich wünsche Ihnen eine anregende Lektüre und viele neue Impulse für Ihre tägliche Arbeit. Entdecken Sie die Beiträge dieser Ausgabe, bleiben Sie sicher – und mit GIT gut informiert! GIT

Herzlichst,
Ihr

T. Gimbel

Dr. Timo Gimbel
für das Team von Wiley
und GIT SICHERHEIT

TITELTHEMA

Die Zukunft ist dezentral

Zutrittskontrolle für kritische Infrastrukturen. Gespräch mit Christian Heller, CSO von Frogblue

Seite 32

PRO-4-PRO für 2025/2026

GIT-SICHERHEIT.DE/DE/PRODUKTE
PRODUCTS FOR PROFESSIONALS
Produkt- und Lead-Plattform für Sicherheit

Karlheinz Biersack

Daichi Maekawa und Osaka Branch

Christian Heller

MANAGEMENT

SECURITY

TITELTHEMA

SCHLIESSTECHNIK

ZUTRITT

SENSORTECHNIK

HEFT IM HEFT
VIDEO

Hendrik Schabsky

Christoph Ryll

Maximilian Korff und Holger Laible

INDEX

QUICK-FINDER

ORGANISATIONEN, INSTITUTIONEN UND UNTERNEHMEN IM HEFT

NEWS

Interschutz 2026: „Zeitenwende“ bringt zusätzliche Impulse

Die Interschutz 2026 (1. bis 6. Juni in Hannover) wird eine Messe im Zeichen der „Zeitenwende“. Bereits jetzt zeichnet sich ein starkes Ausstellerinteresse an der Weltleitmesse für Feuerwehr, Rettungswesen und Bevölkerungsschutz ab.

„Nahezu drei Viertel der insgesamt neun Hallen sind bereits belegt, auf dem Freigelände sind nur noch wenige Flächen frei. Damit steht schon jetzt fest, dass die Interschutz ihre Bedeutung als international führender Branchentreff noch weiter ausbauen wird“, so Bernd Heinold, Projektleiter der Interschutz bei der Deutschen Messe AG. Angesichts weltweit zunehmender Herausforderungen durch Klimawandel, Naturkatastrophen und Krisen sowie aufgrund der veränderten geo- und sicherheitspolitischen Lage hätten die ausstellenden Unternehmen erkannt, dass die Interschutz als Schaufenster ihrer Produkte und Dienstleistungen und als Orientierungshilfe unverzichtbar sei, so Bernd Heinold weiter.

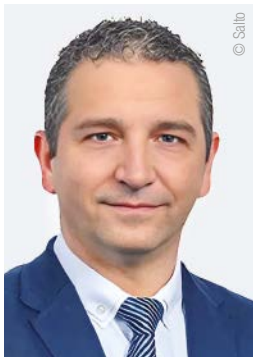
Stärker als bisher wird sich die Bundeswehr als neuer Player im Zusammenspiel aller Akteure im Krisenfall auf der Interschutz 2026 präsentieren. Grund ist die künftig intensivere Zivil-Militärische Zusammenarbeit (ZMZ) von staatlichen oder nichtstaatlichen zivilen Organisationen mit den Streitkräften im Bereich der Bündnis- und Landesverteidigung, in der Gefahrenabwehr oder bei Hilfeleistungen im Katastrophenfall.

Die „Zeitenwende“ habe zweifellos zu einem gestiegenen Problembewusstsein, aber auch spürbaren Finanzierungsimpulsen geführt, so Bernd Heinold. So würden in den kommenden Jahren erhebliche Investitionen aus Bundesmitteln in den Bevölkerungsschutz und somit auch in die Ausstattung der Feuerwehren und Rettungsdienste fließen. Dafür sei es unverzichtbar, Produkte und Dienstleistungen einem fachkundigen Publikum zu zeigen. Zugleich biete die Interschutz mit der Teilnahme kommerzieller wie ideeller Aussteller die beste Gelegenheit, Anwender und Hersteller ins Gespräch zu bringen, um künftige Herausforderungen zu bewältigen.

Dass der Klimawandel weltweit auf dem Vormarsch ist, ist unstrittig. Die Interschutz 2026 begegnet den Herausforderungen, die die globale Erderwärmung mit sich bringt, mit einem neuen Format, das sich auf die zunehmenden Wald- und Vegetationsbrände in aller Welt fokussiert. Auf dem Wildfire-Camp@Interschutz werden Experten aus dem In- und Ausland neue Möglichkeiten zur Bekämpfung und Vermeidung von Vegetationsbränden vorstellen und diskutieren.

www.messe.de

Stepan Kiese verstärkt Business Development bei Salto



Als Business Development Manager unterstützt Stephan Kiese Partner und Anwender von Salto in den Bereichen KRITIS sowie NIS2-Direktive

Salto Deutschland hat mit Stephan Kiese einen neuen Business Development Manager speziell für die Bereiche Kritische Infrastruktur (KRITIS) und NIS2-Anforderungen gewonnen. Stephan Kiese (49) verstärkt als Business Development Manager das Team von Salto Deutschland. Er befasst sich schwerpunktmäßig mit dem Sektor der Kritischen Infrastruktur (KRITIS) sowie den Anforderungen aus der NIS2-Direktive. Dabei nutzt er seine fundierten Kenntnisse im Bereich Cybersecurity und der physischen Sicherheit. Es gilt, Strategien zu entwickeln, um die Einhaltung der Vorschriften und die Erfüllung der hohen Sicherheitsstandards zu gewährleisten. Als Business Development Manager wird Stephan Kiese genau hier ansetzen und nicht nur die Ausarbeitung passender Konzepte, sondern auch die aktive Unterstützung von Partnern und Kunden durch gezielte Information und Beratung im Projektgeschäft übernehmen.

www.saltosystems.com

Athene würdigt Prof. Dr. Iryna Gurevych

Prof. Dr. Iryna Gurevych

Die renommierte Informatikerin Prof. Iryna Gurevych von der Technischen Universität Darmstadt (TU Darmstadt) erhält die erste Athene Distinguished Professorship. Mit dieser Auszeichnung würdigt Athene ihre herausragenden Beiträge in der Forschung zu künstlicher Intelligenz und Computerlinguistik und deren Anwendung in der Cybersicherheit. Die Informatik-Professorin Iryna Gurevych von der TU Darmstadt erhält die erste Distinguished Professorship des Nationalen Forschungszentrums für angewandte Cybersicherheit Athene. Mit diesem besonderen Programm fördert Athene herausragende Wissenschaftler an den beteiligten Hochschulen, deren Forschung in besonderer Weise wissenschaftliche Exzellenz mit großer Wirkmacht in der angewandten Cybersicherheit verbindet. Die Anerkennung als Athene Distinguished Professor ist verbunden mit der langfristig angelegten Förderung eines Forschungsvorhabens. **www.sit.fraunhofer.de**

BVSW: Markus Klaedtke zum Vorstandsvorsitzenden gewählt

Markus Klaedtke ist neuer Vorstands-vorsitzender des BVSW

Der Bayerische Verband für Sicherheit in der Wirtschaft (BVSW) hat einen neuen Vorstandsvorsitzenden: Auf der 47. Mitgliederversammlung wurde Markus Klaedtke einstimmig in das Amt gewählt. Er folgt auf Johannes Strümpfel, der seit Anfang Juni Vorstandsvorsitzender beim ASW-Bundesverband ist. Markus Klaedtke ist bereits seit 2015 für den BVSW aktiv und seit 2016 Vorstandsmitglied der Sparte A, die die Bereiche Industrie, Handel, Banken und Versicherungen vertritt. Hauptberuflich leitet er die Konzernsicherheit der Diehl Gruppe in Nürnberg. Darüber hinaus ist er Oberst der Reserve im Landeskommando Bayern und engagiert sich für die zivil-militärische Zusammenarbeit. Seine Erfahrungen in zivilberuflichen sowie militärischen Stationen möchte Markus Klaedtke in sein neues Amt einbringen, um die Kooperation zwischen Unternehmen und Behörden weiter auszubauen.

www.bvsw.de

Barox ernennt Adrian Briner zum Produktmanager

Adrian Briner

Die Barox Kommunikation AG verstärkt ihr Engagement in der Produktentwicklung und hat Adrian Briner zum Produktmanager berufen. Mit über 20 Jahren Berufserfahrung im Produktmanagement und in der Produktentwicklung – zuletzt als Head of Development Department bei der WEY Group AG – einem weltweit agierenden Unternehmen, bringt Adrian Briner umfangreiches Know-how in Software-, Hardware- und Produktentwicklung mit.

In seiner neuen Rolle bei Barox übernimmt er die Verantwortung für die Weiterentwicklung des Produktportfolios aus Ethernet-Switches, Medienkonvertern und IP-Extendern. „Mein Ziel ist es, das Barox-Angebot kontinuierlich an die dynamischen Anforderungen der Videosicherheitsbranche anzupassen“, so Adrian Briner. „Besonders im Fokus stehen neue Switch-Lösungen sowie API-, Plug-in- und Drittanbieter-Integrationen. Der Markt für Videosicherheit ist äußerst anspruchsvoll und unterliegt ständigen Veränderungen, wobei Kunden- und Installationsanforderungen je nach Anwendung stark variieren – und es liegt an uns als globalen Hersteller und Branchenführer, diesen Anforderungen proaktiv zu begegnen.“

Mit Adrian Briner investiere das Unternehmen gezielt in seine Zukunft“, betont Rudolf Rohr, Mitgründer und geschäftsführender Gesellschafter von Barox. Sein Know-how werde helfen, technologische Innovationen anzustoßen und die speziellen Anforderungen der weltweiten Kunden noch besser zu erfüllen. Adrian Briner wird vom Hauptsitz in Baden (Schweiz) aus agieren und das Unternehmen weltweit bei der Weiterentwicklung seiner Produkte vertreten.

www.barox.de

Gemeinschafts-aufgabe Sicherheit

Im Gespräch mit Markus Klaedtke, Vorstandsvorsitzender BVSW

Auf seiner 47. Mitgliederversammlung hat der Bayerische Verband für Sicherheit in der Wirtschaft (BVSW) Markus Klaedtke zum Vorstandsvorsitzenden ernannt (GIT SICHERHEIT berichtete). Schon seit 2015 ist er für den Verband aktiv und seit 2016 Vorstandsmitglied für die Bereiche Industrie, Handel, Banken und Versicherungen. Er ist Konzernsicherheitsleiter bei Diehl in Nürnberg und u. a. Oberst der Reserve im Landeskommando Bayern.

Herr Klaedtke, zunächst einmal herzlichen Glückwunsch zur Wahl zum Vorstandsvorsitzenden beim BVSW! Freuen Sie sich auf Ihre neue Aufgabe – und was reizt Sie an ihr?

Markus Klaedtke: Vielen Dank, ich freue mich sehr auf die neue Aufgabe. Ich übernehme ein gut aufgestelltes Haus - der BVSW hat sich in den letzten Jahren dynamisch weiterentwickelt und viel erreicht: Die Mitgliederzahl ist kontinuierlich gewachsen, wir haben unsere Kontakte zu den Sicherheitsbehörden ausgebaut und für jede unserer vier Sparten eine Kommunikationsplattform etabliert. Das Thema Kommunikation ist mir sehr wichtig, denn Sicherheit basiert auf dem raschen Teilen von Informationen. Deshalb habe ich mir für meine Position als Vorstandsvorsitzender des BVSW das Ziel gesetzt, den Austausch mit allen im Sicherheitsbereich Tätigen weiter zu intensivieren.

Geben Sie uns einen kleinen Steckbrief über sich und Ihre bisherige Verbandstätigkeit?

Markus Klaedtke: Ich bin seit 30 Jahren für die Unternehmenssicherheit der Diehl Gruppe tätig und dort Leiter der Konzernsicherheit. Davor war ich in unterschiedlichsten Funktionen bei der Bundeswehr und habe ein Studium der Wirtschafts- und Organisationswissenschaften an der Universität der Bundeswehr in Hamburg absolviert. Mittlerweile bin ich Oberst der Reserve sowie Kommandeur des Regionalstabs für territoriale Aufgaben der Bundeswehr Nord, wo ich insbesondere die zivil-militärische Zusammenarbeit verantworte. Darüber hinaus bin ich Berufshubschrauberpilot und privat ein leidenschaftlicher Motorradfahrer.

Seit meinem Start bei der Diehl Gruppe engagiere ich mich auch für den BVSW und habe lange den Arbeitskreis Nürnberg-Erlangen geleitet, eine Kommunikationsplattform für Behörden und Wirtschaft in der Region. Im Jahr 2016 wurde ich zum Vorstandsmitglied für die Sparte Industrie, Handel, Banken und Versicherungen gewählt.

Sie sind, wie gerade erwähnt, Leiter der Konzernsicherheit bei der Diehl Gruppe in Nürnberg, und damit täglich mit all den Herausforderungen für die Unternehmenssicherheit konfrontiert, die unsere Gegenwart prägen. Was sind aus Ihrer Sicht die drängendsten Anforderungen der Mitglieder diesbezüglich?

Markus Klaedtke: Das Wichtigste im Bereich der Sicherheit ist es, vor die Lage zu kommen, also nicht nur auf Ereignisse zu reagieren, sondern sie frühzeitig zu erkennen und die Situation aktiv zu gestalten. Diese Zielsetzung war schon immer herausfordernd und sie wird zunehmend anspruchsvoller, weil wir mit einer Vielzahl

parallel stattfindender Krisen konfrontiert sind, die sich in unserer global vernetzten Welt gegenseitig verstärken oder gar bedingen. Um Entwicklungen frühzeitig einordnen und Risiken bewerten zu können, wird eine effektive Kommunikation aller Akteure immer wichtiger.

Welche Schwerpunkte möchten Sie in Ihrem neuen Amt setzen?

Markus Klaedtke: Ein Schwerpunkt meiner Arbeit wird es sein, die Zusammenarbeit innerhalb der Sicherheitsgemeinschaft weiter auszubauen und auch kleine und mittlere Unternehmen verstärkt miteinzubeziehen. Wir sehen immer wieder, dass Großunternehmen im Bereich Sicherheit professionell aufgestellt sind: Sie verfügen über gut ausgebildetes Personal, klar definierte Prozesse und investieren kontinuierlich in Weiterbildung und Technik. Security hat sich hier oft schon als fester Bestandteil der Unternehmensstrategie etabliert.

Die Situation bei KMUs sieht bisweilen ganz anders aus. Das Thema Sicherheit wird hier „mitgedacht" und liegt oft bei den Personen, die den klassischen Arbeitsschutz verantworten. Dabei ist das Aufgabenfeld der Security deutlich breiter. Gleichzeitig kann auch ein Sicherheitsvorfall bei einem kleinen Zulieferbetrieb Auswirkungen entlang der gesamten Wertschöpfungskette haben. Sicherheit ist also kein isoliertes Thema einzelner Akteure, sondern eine Gemeinschaftsaufgabe und dafür ist der Austausch untereinander ganz entscheidend.

Ihr Vorgänger Johannes Strümpfel ist ja zum Bundesverband VSW (ehemals ASW) gewechselt, wo er den Vorstandsvorsitz übernommen hat. Im Interview mit GIT SICHERHEIT hat er betont, dass er in der föderalen Organisation mit Bundes-, Landes- und Regionalverbänden einen klaren Wettbewerbsvorteil sieht. Wie kommt dieser Vorteil in der Zusammenarbeit mit dem Bundesverband aus Ihrer Sicht zum Tragen?

Markus Klaedtke: Ich teile diese Einschätzung, der föderale Aufbau bietet einen echten Mehrwert: Die Landes- und Regionalverbände haben über Jahre gewachsene Netzwerke in den jeweiligen Bundesländern, sind nah an den Unternehmen und verfügen über ein tiefgreifendes Verständnis für die Gegebenheiten vor Ort. Gleichzeitig übernimmt der Bundesverband eine wichtige Rolle bei der Bündelung übergeordneter Interessen und bei der politischen Arbeit in Berlin. Er schafft Sichtbarkeit auf nationaler Ebene und kann Themen in die Bundespolitik tragen, die in den Landesverbänden entwickelt wurden.

Genau in dieser Kombination liegt die Stärke der föderalen Struktur, die Verbände ergänzen sich gegenseitig hervorragend. Ich freue mich sehr, dass Johannes Strümpfel jetzt auf Bundesebene Verantwortung übernimmt. Unsere Zusammenarbeit beim BVSW war immer von gegenseitigem Vertrauen und Offenheit geprägt und das wird auch weiterhin so sein.

Gibt es eigentlich spezifisch bayerische Themen die für Ihre Verbandsarbeit besonders wichtig sind?

Markus Klaedtke: Bayern als Flächenstaat mit vielen Unternehmen und einer wachsenden Bevölkerung hat schon immer eine eigene Stellung im Bund gehabt. Einerseits ist Bayern ein bedeutender Wirtschaftsstandort mit vielen global tätigen Unternehmen, die einen wichtigen Anteil an der Wirtschaftsleistung von Deutschland haben, aber auch potenzielle Ziele für Ausspähung, Sabotage oder Cyberangriffe darstellen. Das Thema Wirtschaftsschutz ist hier deshalb besonders wichtig.

Auch die geografische Struktur und die Verteilung der Unternehmen ist eine Besonderheit. Es gibt auf der einen Seite die Ballungszentren München, Nürnberg und Augsburg und auf der anderen Seite sehr ländlich geprägte Regionen. Wir als Sicherheitsverband sind deshalb gefordert, für diese beiden Realitäten Angebote zu entwickeln. Ein Beispiel dafür sind die regionalen Sicherheitskreise hier in Bayern.

Herr Klaedtke, Ihr Verband ist ausgesprochen aktiv bei der Verwirklichung seiner Ziele – die BVSW-Wintertagung, die BVSW SecTec oder der Bayerische Sicherheitstag sind hier zu nennen, aber auch die Präsenz auf Messen und wichtigen Branchenveranstaltungen. Können Sie uns zum Abschluss einen Einblick in die zukünftigen Planungen geben?

Markus Klaedtke: Die zukünftige Planung obliegt dem gesamten Vorstand, deshalb möchte ich dem nicht vorgreifen. Wie ich gesagt habe, liegt mir der Austausch aller Beteiligten am Herzen und da gibt es eine ganze Reihe von Maßnahmen, die infrage kämen. Auf jeden Fall kann ich Ihnen versichern, dass der BVSW weiterhin zu den aktivsten Landesverbänden gehören wird. GIT

BVSW
www.bvsw.de

Vom 25. bis zum 27. November eröffnet die PMRExpo 2025, Europäische Leitmesse für Sichere Kommunikation, in Köln ihre Tore

PMRExpo 2025

Treffpunkt für sichere Kommunikation in Köln

Vom 25. bis zum 27. November eröffnet die PMRExpo 2025, Europäische Leitmesse für Sichere Kommunikation, in Köln ihre Tore. Mit der Fachausstellung, dem PMRExpo Summit und der Connecting Area bietet sie ein einzigartiges Forum und Networking rund um die sichere einsatz- und geschäftskritische mobile Kommunikation für Behörden und Organisationen mit Sicherheitsaufgaben (BOS), Betreiber Kritischer Infrastrukturen (KRITIS) und Unternehmen aus sämtlichen Wirtschaftssektoren.

Zu den Themenfeldern der PMRExpo zählen u. a. Digitalfunk BOS, 5G und 5G-Campusnetze, Leitstellen, Cybersecurity und Critical IoT. Von besonderer Aktualität sind dabei unter anderem die Interkonnektivität von Schmalband- und Breitbandnetzen sowie der Aufbau privater Breitbandnetze, die meist von den Anwendern selbst betrieben werden. Diese haben mit den Standards LTE und insbesondere 5G erheblich an Bedeutung gewonnen.

Drei Tage Innovation und Branchendialog

An drei Messetagen präsentieren Aussteller aus aller Welt Innovationen, Produkte, Lösungen und Anwendungen. Unter anderem aus den Bereichen Applikationslösungen, Leitstellen- und Sicherheitstechnik, Infrastrukturelemente und Gerätezubehör. Begleitet wird die Messe vom PMRExpo Summit, auf dem hochkarätige Branchenexpertinnen und -experten die neuesten Technologien, Sicherheitsaspekte und Geschäftschancen vorstellen. Am ersten Summit-Tag, dem 25.11., stehen Kommunikation und Lösungen für Kritischen Infrastrukturen im Fokus; am 26.11. wendet sich der Summit speziell an die BOS; am Schlusstag, dem 27.11., widmet sich das Programm den Leitstellen.

Connecting Area: Vorträge zu 5G und 5G-Campusnetzen

Auch 2025 lädt die Connecting Area wieder zu kompakten Vorträgen, Präsentationen und Networking ein – der Fokus der Bühne liegt bei privaten 5G-Breitbandnetzen (5G-Campusnetzen). Experten und Nutzer geben hier Einblicke in Anwendungsbeispiele, Herausforderungen und Lösungsansätze.

Sonderfläche 5G-Hub for Private Networks

Nach dem erfolgreichen Auftakt im Vorjahr gibt es auch 2025 wieder eine Sonderfläche, die sich speziell dem Thema 5G widmet. Im „5G-Hub for Private Networks“ zeigen Aussteller live, wie private 5G-Netze und Non Public Mobile Networks (NPN) neue Maßstäbe für vernetzte Anwendungen in Industrie, Logistik, Sicherheit und kritischen Infrastrukturen setzen. Besucher erleben praxisnahe Szenarien und technologische Innovationen, die Effizienz, Flexibilität

und die Sicherheit eines Unternehmens steigern und dabei die Datensouveränität sicherstellen.

Zu den Themenschwerpunkten des 5G-Hub zählen:

- Smart Manufacturing mit 5G: Die Zukunft der vernetzten Produktion
- Effiziente Intralogistik & smarte Lagerhaltung
- Virtual & Augmented Reality ohne Verzögerung
- Drohnensteuerung in Echtzeit steuern
- Private 5G-Campusnetze: Vernetzung auf einem neuen Level
- Maximale Sicherheit in Kritischen Infrastrukturen

Auch dieses Jahr wird es auf der PMRExpo einen Hackathon geben

© Koelnmesse / PMRExpo/ Hanne Engwald

Hackathon: Technologie trifft Krise

Auch der Hackathon@PMRExpo powered by Corevas hat sich als Erfolgsformat auf der PMRExpo etabliert und geht dieses Jahr in die nächste Runde. Unter dem Motto „Technologie trifft Krise – gestalte die Kommunikation von morgen" treffen sich kreative Köpfe, um gemeinsam die Kommunikation in Krisensituationen neu zu denken. In einem 48-Stunden-Design- und Coding-Marathon entwickeln interdisziplinäre Teams KI-gestützte, praxistaugliche und gesellschaftlich relevante Lösungen. 2024 nahmen über 40 Hackerinnen und Hacker am Hackathon, 120 Community-Mitglieder und 12 Aussteller teil. Das Gewinnerteam startet aktuell mit seinem Projekt VisionPilot im Rahmen eines Exist-Gründerstipendiums durch. GIT

PMREXpo 2025
www.pmrexpo.com

Energiesektor in der Zeitenwende

BSI fordert robuste Cybersicherheit für die Energieversorgung

Eine sichere Stromversorgung ist Grundlage unseres gesellschaftlichen Lebens – das zeigt nicht erst der knapp eintägige Blackout in Spanien. Energiesicherheit ist eine zentrale Säule in der deutschen Sicherheitsarchitektur. Gleichzeitig stuft das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Bedrohung für Kritische Infrastrukturen aus dem Cyberraum als hoch ein. Das BSI sieht dringenden und konsequenten Handlungsbedarf.

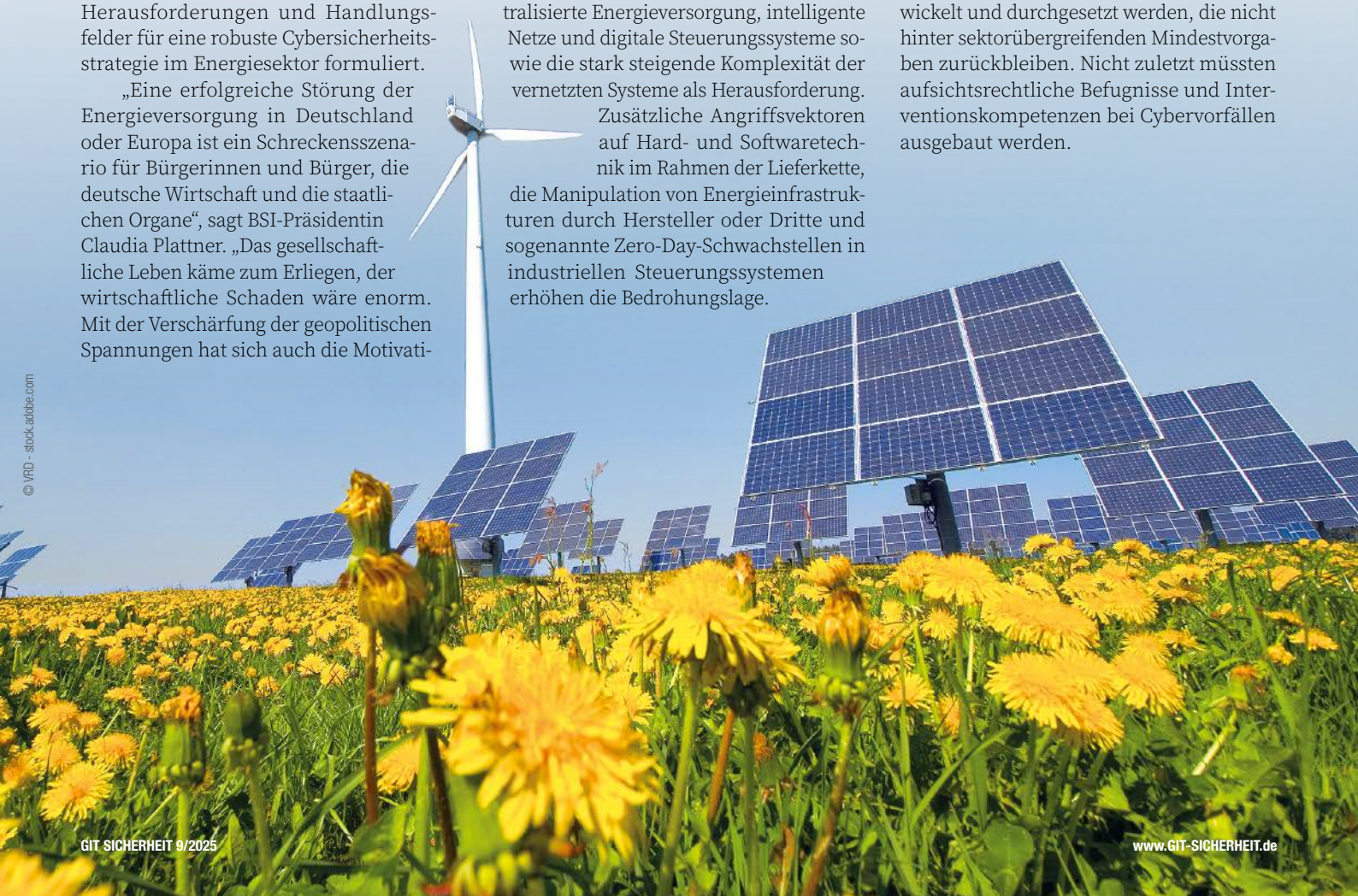
Der Energiesektor steht dabei besonders im Fokus von staatlich unterstützten Operationen, die auf Destabilisierung und Spionage abzielen, von Cyberkriminellen, die Energieunternehmen erpressen oder von Hacktivisten, die ideologische Ziele verfolgen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein Positionspapier veröffentlicht, das zentrale Herausforderungen und Handlungsfelder für eine robuste Cybersicherheitsstrategie im Energiesektor formuliert.

„Eine erfolgreiche Störung der Energieversorgung in Deutschland oder Europa ist ein Schreckensszenario für Bürgerinnen und Bürger, die deutsche Wirtschaft und die staatlichen Organe“, sagt BSI-Präsidentin Claudia Plattner. „Das gesellschaftliche Leben käme zum Erliegen, der wirtschaftliche Schaden wäre enorm. Mit der Verschärfung der geopolitischen Spannungen hat sich auch die Motivationslage möglicher Angreifender geändert. Wir müssen daher dringend in Sicherheitsstrukturen, technische Schutzmaßnahmen und resiliente Architekturen investieren, um unsere Energieversorgung langfristig abzusichern und die Risiken systemischer Ausfälle zu minimieren.“

Neben der geopolitischen Lage nennt das Positionspapier die zunehmend dezentralisierte Energieversorgung, intelligente Netze und digitale Steuerungssysteme sowie die stark steigende Komplexität der vernetzten Systeme als Herausforderung. Zusätzliche Angriffsvektoren auf Hard- und Softwaretechnik im Rahmen der Lieferkette, die Manipulation von Energieinfrastrukturen durch Hersteller oder Dritte und sogenannte Zero-Day-Schwachstellen in industriellen Steuerungssystemen erhöhen die Bedrohungslage.

Maßnahmen zur Stärkung der Cybersicherheit

Aus Sicht des BSI sind daher u. a. einheitliche Anforderungen in allen KRITIS-Sektoren und darauf aufbauend für alle Akteure im Energiesystem notwendig. Auch für kleinere Energieversorger, Netzbetreiber und dezentrale Anlagen sollten einheitliche, sektorspezifische Sicherheitsstandards entwickelt und durchgesetzt werden, die nicht hinter sektorübergreifenden Mindestvorgaben zurückbleiben. Nicht zuletzt müssten aufsichtsrechtliche Befugnisse und Interventionskompetenzen bei Cybervorfällen ausgebaut werden.



Cybersicherheit im Energiesektor Deutschlands

Auszüge aus dem Positionspapier des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stuft die Bedrohungslage im Bereich Kritischer Infrastrukturen (KRITIS) seit Jahren als „hoch“ ein. Der Energiesektor steht dabei besonders im Fokus von:

- Staatlich unterstützten Cyberoperationen (z. B. Russland, China, Iran, Nordkorea), die auf Destabilisierung und Spionage abzielen.
- Cyberkriminellen Gruppen, die Ransomware einsetzen und gezielt Energieunternehmen erpressen. Hacktivisten, die ideologische Ziele verfolgen, etwa im Kontext von Klima-/Energiepolitik.

Die Energiewende bringt notwendige strukturelle Veränderungen mit sich, durch die sich jedoch eine geänderte IT-Sicherheitsbedrohungslage ergibt:

- Dezentralisierung: Tausende kleinere Akteure wie private Haushalte mit Photovoltaikanlagen werden Teil des Energiesystems, oftmals ohne professionelle IT-Sicherheit und entsprechende Regulierung
- Intelligente Netze und digitale Steuerungssysteme: Smart Grids, digitale Zähler (Smart Meter) und ferngesteuerte Anlagen eröffnen neue Angriffsmöglichkeiten
- Sektorkopplung: Die zunehmende Integration von Strom, Industrie und Verkehrssystemen erhöht die systemische Komplexität und Verwundbarkeit

Mit der Digitalisierung entstehen neue Einfallstore für Angreifer:

- Supply-Chain-Angriffe auf Software und Hardware von Energieanlagen (z. B. Solarwechselrichter, Netzleittechnik)
- Manipulation von Energieinfrastruktur durch Hersteller oder Dritte (z. B. Wechselrichter oder Smart Meter und deren Kommunikationsschnittstellen)
- Zero-Day-Exploits in industriellen Steuerungssystemen (ICS) und SCADA-Umgebungen

Der Energiesektor, so das BSI, stehe im Zentrum einer sicherheitsstrategischen Zeitenwende. Die zunehmende Digitalisierung, die Diversifizierung durch erneuerbare Energien und die angespannte geopolitische Lage erforderten ein Umdenken bei der Cybersicherheit. Deutschland müsse proaktiv in Sicherheitsstrukturen, technische Schutzmaßnahmen und resiliente Architekturen investieren, um seine Energieversorgung langfristig zu sichern und die Risiken systemischer Ausfälle zu minimieren. Das BSI stehe mit seiner Expertise für eine zentrale Steuerungsrolle für die Cybersicherheit im Energiesektor zur Verfügung. GIT

Hier können Sie das Positionspapier des BSI herunterladen:

Bundesamt für Sicherheit in der Informationstechnik
www.bsi.bund.de

Eine Spinne hat ihr Netz vor einer Kamera gesponnen. Nachts wird es von den Infrarot-LEDs der Kamera beleuchtet – das Bildmaterial wird unbrauchbar, die Videoanalyse ist gestört

Bilder beim Gesundheits-Check

„Image Health Analytics“: Bildqualität ist entscheidende Voraussetzung für KI-basierte Videoanalyse

Moderne KI-gestützte Videoanalysen bieten heute beeindruckende Möglichkeiten: von intelligenter Objekterkennung bis hin zur Echtzeit-Alarmierung. Doch all diese Funktionen stehen und fallen mit einer oft unterschätzten Komponente: der „Bildgesundheit“. Ohne eine verlässliche visuelle Grundlage bleibt die künstliche Intelligenz blind. Ein Beitrag von Timo Sachse, Solutions Engineer EMEA bei Axis Communications.

Stellen Sie sich folgendes Szenario vor: Eine Videosicherheitslösung wird fachgerecht installiert und in Betrieb genommen. Aufzeichnung und Videoanalyse sind einwandfrei konfiguriert, das System läuft reibungslos. Wochen, Monate vergehen – die Technik funktioniert. Bis sie es plötzlich nicht mehr tut. Ohne Fehlermeldung, ohne Vorwarnung.

Was ist geschehen? Eine Spinne hat in der Zwischenzeit ihr Netz vor einer Kamera gesponnen. Nachts wird es von den Infrarot-LEDs der Kamera beleuchtet. Die künstliche Intelligenz (KI) interpretiert die Reflexionen falsch, sodass Objekte nicht mehr erkannt und Bewegungen nicht mehr richtig verfolgt werden. Das Bildmaterial wird unbrauchbar, die Videoanalyse ist gestört.

Ein anderes Beispiel: Eine PTZ-Kamera ohne integrierte Infrarot-Beleuchtung soll nachts eine Szene auf einem Hinterhof be-

obachten. Doch die externe Beleuchtung fällt aus – und die Kamera erkennt nichts mehr. Der Schwenkmechanismus arbeitet, das System funktioniert, aber die Szene selbst bleibt im Dunkeln. Die Kamera liefert keine verwertbaren Daten.

Störungen dieser Art treten meist nur temporär auf: nachts, bei niedrigem Sonnenstand, saisonbedingt oder durch Umgebungsveränderungen anderer Natur – wenn beispielsweise ein LKW das Sichtfeld einer Kamera blockiert. Es ist stets eine Herausforderung, solche Bildqualitätsmängel frühzeitig zu erkennen, bevor sie zu Sicherheitslücken werden.

Vom passiven Speichern zur aktiven KI-Analyse

Vor dem Boom der KI-gestützten Videoanalyse hatten die meisten Videosysteme einen eher passiven Charakter: Die Kameras zeichneten auf, die Rekorder speicherten. Kam es zu einem Vorfall, griff man auf die gespeicherten Videodaten zurück – oft Tage oder Wochen später. Heute sieht die Situation anders aus.

Durch den Einsatz KI-gestützter Videoanalyse sind Videosicherheitssysteme nicht mehr nur Beobachter, sondern aktive Sicherheitsinstanzen. Dank intelligenter Objektklassifizierung können Systeme zum Beispiel zwischen Mensch und Fahrzeug unterscheiden. Zudem werden Fehlalarme durch Kleintiere, Lichtwechsel oder Schatten weitgehend reduziert. Die Alarmierung zu einem Vorfall erfolgt gezielt und kontextabhängig, etwa bei einer zu langen Verweildauer oder beim Betreten geschützter Bereiche. Auf diese Weise ermöglichen moderne Videosysteme gezielte Reaktionen in Echtzeit – und beeinflussen Sicherheitssysteme direkt.

Entscheidend ist, dass die Alarmierung, die vollständig auf der visuellen, KI-gestützten Analyse der Kamerabilder basiert, korrekt funktioniert. Ist dem nicht so und die Alarme bleiben aus, können die Folgen schwerwiegend sein und ein echtes Sicherheitsrisiko darstellen.

Ein LKW parkt direkt vor einer Kamera und blockiert damit fast das komplette Sichtfeld. Die Hardware sendet ein Bild – es entspricht jedoch nicht der Szene, die eigentlich beobachtet werden soll

Die Grenzen der Objektklassifizierung

Bei der automatischen Alarmierung über Videosysteme, in Kombination mit KI-gestützter Objektklassifizierung, gibt es vier mögliche Szenarien, wenn man das Ergebnis der Videoanalyse mit dem tatsächlichen Geschehen in der Realität vergleicht.

Die erfolgreichen Zustände einer KI-gestützten Videoanalyse – fachtechnisch als True Positive und True Negative bezeichnet – bilden die Extrempole einer idealen Alarmbewertung. Von einem True Positive spricht man, wenn ein tatsächlich vorhandenes, relevantes Objekt korrekt erkannt und daraufhin eine Alarmierung ausgelöst wird. Ein True Negative wiederum liegt vor, wenn die Szene kein relevantes Objekt enthält und entsprechend auch kein Alarm ausgelöst wird.

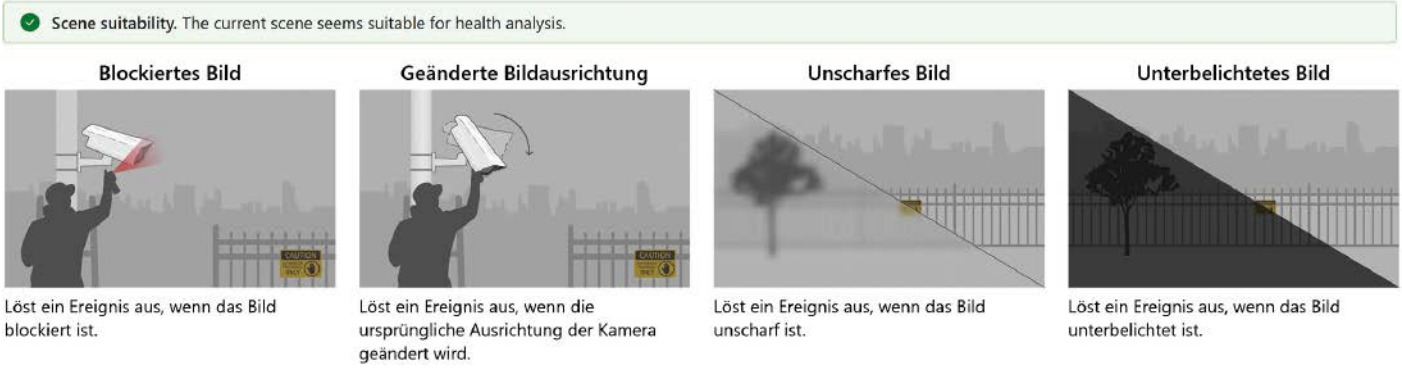
Ein False Positive liegt vor, wenn ein Alarm ausgelöst wird, obwohl kein relevantes Objekt vorhanden ist – etwa durch die KI-Analyse hervorgerufene Fehlklassifizierungen wie Bewegungen im Laub oder Lichtreflexionen. Ein False Negative entsteht, wenn ein tatsächlich vorhandenes Objekt nicht erkannt wird und somit auch keine Alarmierung erfolgt, obwohl sie erforderlich gewesen wäre.

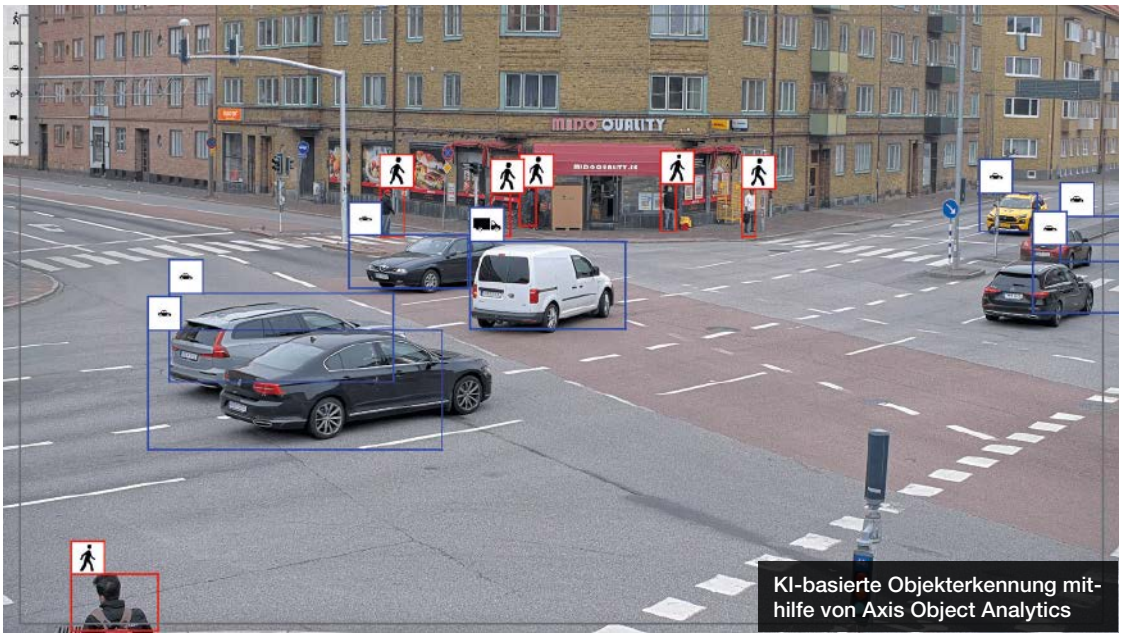
Kommt es zu einem False Negative, obwohl das Bildmaterial von hoher Qualität ist und alle relevanten Analyseparameter erfüllt sind, deutet der Fehler in der Regel auf ein Problem innerhalb der Analysesoftware hin. Zumeist liegt die Ursache allerdings in der sogenannten „Bildgesundheit", also in der Qualität und Nutzbarkeit des Bildes an sich. Verdeckte Sichtfelder, verschmutzte Kameraoptiken oder ungünstige Lichtverhältnisse können dazu führen, dass ein physisch vorhandenes Objekt von der KI nicht erkannt wird – nicht etwa, weil die KI-Analyse als solche nicht funktioniert, sondern weil das Eingangsbild nicht brauchbar war.

Um die Potenziale von KI-gestützter Videoanalyse also zuverlässig nutzen zu können, muss eines deutlich gemacht werden: Ein unbrauchbares Bild kann kein verwertbares Analyseergebnis erzeugen. Selbst die intelligenteste, KI-gestützte Videoanalyse kommt hier an ihre Grenzen. Während ein Mensch beispielsweise ein Spinnennetz im Bild als störend wahrnehmen würde, sich aber trotzdem auf den Rest der Szene kon-

Bitte umblättern ▶

Die KI-gestützte Analysefunktion Image Health Analytics von Axis: Statt einer pauschalen Prüfung, ob das Bild gestört ist, verfolgt diese Software eine differenzierte, mehrdimensionale Analyse





KI-basierte Objekterkennung mithilfe von Axis Object Analytics

zentrieren könnte, bewertet eine KI rein datenbasiert: Unscharfe Optiken oder blockierte Perspektiven führen dazu, dass sie keinen Alarm auslöst.

Bildqualität als wichtige Voraussetzung

Bevor eine KI die Inhalte einer Szene analysieren kann, muss daher die Qualität des Eingangsbildes sichergestellt werden. Dafür ist eine – der KI-Analyse vorgeschaltete –Analysesoftware nötig, die prüft, ob das Bild überhaupt analysierbar ist. Diese sogenannte Image Health Analytics ist ein wichtiger Schritt im gesamten Videoanalyseprozess. Erst wenn er erfolgreich war, kann der Anwender davon ausgehen, dass die KI-basierte Videoanalyse zur Objekterkennung korrekt erfolgen kann.

Auch eine regelmäßige Wartung ist in diesem Kontext entscheidend. Viele Videomanagementsysteme bieten in diesem Bereich nur rudimentäre Funktionen, sodass die Wartung in der Praxis oft vernachlässigt oder schlichtweg ignoriert wird.

Ein Beispiel: Eine Kamera wird in unmittelbarer Nähe einer Lüftungsanlage installiert. Durch die hohe Luftfeuchtigkeit am Montageort verschmutzt die Kamerakuppel schnell. Tagsüber bleibt der Qualitätsverlust meist unbemerkt – besonders dann, wenn das Bild dem Anwender als kleiner Ausschnitt eines Videostreams in einer Multi-View-Ansicht dargestellt wird. Nachts, bei Streulicht oder unter schwierigen Kontrastbedingungen, wird das ausgegebene Videobild jedoch zunehmend unbrauchbar.

Funktionen zur Bildüberprüfung

Früher war die Funktionsvielfalt in Videosicherheitskameras stark eingeschränkt. Die einzige Sicherheitsfunktion gegen Manipulation von außen war eine Manipulationserkennung, auch „Tampering-Alarm“ genannt. Diese reagierte ausschließlich dann, wenn das gesamte Bild massiv beeinträchtigt oder vollständig verdunkelt wurde – etwa durch bewusstes Verdecken der Kamera. Der Schwerpunkt lag damals also mehr auf absichtlicher Manipulation als auf operativer Bildqualität.

Heute sind es überwiegend unabsichtliche, äußere Einflüsse, die zu unbrauchbaren Bildern führen – von Staub, Regen und Lichtreflexionen bis hin zu Fremdkörpern vor der Linse. Nur in Ausnahmefällen, etwa bei vandalismusgefährdeten Installationen in Bahnhöfen oder Unterführungen, spielt gezielte Manipulation noch eine nennenswerte Rolle.

Die KI-gestützte Analysefunktion Image Health Analytics von Axis Communications setzt genau hier an: Statt einer pauschalen Prüfung, ob das Bild gestört ist, verfolgt diese Software eine differenzierte, mehrdimensionale Analyse. In der aktuellen Version sind insgesamt fünf Bildqualitätskriterien verfügbar, die gezielt auf optische und physische Problemquellen eingehen, um die Gesundheit eines Videobilds zu testen.

Intelligente Überprüfung der Bildgesundheit

Die Funktion Image Health Analytics fokussiert sich auf Veränderungen im Kamerabild, die innerhalb kurzer Zeit erfolgen und einen Großteil der Szene betreffen – etwa durch Verschmutzung, Reflexionen oder verdeckte Sicht. Die Software läuft dabei direkt auf der Kamera und belastet die übrigen Systemressourcen nicht zusätzlich.

Im ersten Schritt prüft die Software, ob das Bild bzw. die Szene grundsätzlich für diese Art der Analyse geeignet ist. Voraussetzung ist das Vorhandensein gleichmäßig verteilter, konstanter Strukturen im Bild. Grenzen für die Analyse ergeben sich beispielsweise bei leeren Flächen wie Wasseroberflächen oder einfarbigen Wänden, bei denen es keine erkennbaren Muster gibt.

Ist eine Szene grundsätzlich geeignet, folgen vier weitere Analyseprozesse. Die Prüfungskriterien sind dabei individuell konfigurierbar. So lassen sich die Empfindlichkeit der Detektion sowie die Auslöseverzögerung jeweils separat einstellen. Zudem können die einzelnen Bildqualitätskriterien je nach Einsatzszenario ein- oder ausgeschaltet werden. Dadurch lässt sich die Funktion flexibel an die Anforderungen verschiedenster Installationen anpassen.

Welche Reaktion schließlich auf ein Analyseereignis sinnvoll oder notwendig ist, hängt stets vom konkreten Einzelfall ab. Die Bildqualitätsanalyse liefert in erster Linie einen Hinweis darauf, dass etwas unter Umständen nicht in Ordnung ist.

Fazit

Image Health Analytics ist ein essenzieller Schutzmechanismus für die KI-basierte Videoanalyse. Sie erkennt automatisch, ebenfalls KI-gestützt, wenn das technische Bild zwar vorhanden, aber in seinem Nutzen für die KI-Analyse nicht verwertbar ist. Damit schützt sie die Investition in KI-Systeme und die Verlässlichkeit der Analyseergebnisse. GIT

Axis Communications
www.axis.com

Als stünde man direkt neben dem Flugzeug

Effiziente Sicherheitslösungen für Flughäfen: Cybersecurity, Perimeterschutz, Remote Tower und intelligente Videoanalyse mit Dallmeier-Technologie

Cybersecurity, Perimeter-Schutz, Remote Tower Lösungen und intelligente Videoanalysen: Modernste Technologien können Sicherheit auf Flughäfen auf effiziente und wirtschaftliche Weise gewährleisten. Vor welchen Herausforderungen sie stehen und welche Lösungen es gibt, erläutert Karlheinz Biersack, Director Business Development Airport bei Dallmeier electronic.

GIT SICHERHEIT: Herr Biersack, wo sehen Sie die Anwendungen der Dallmeier Videotechnik an Flughäfen?

Karlheinz Biersack: Unsere Kameratechnik ist mittlerweile sehr vielseitig im Einsatz. Von der Überwachung großer Parkplatzflächen über Terminalbereiche, Apron- und Runway-Überwachung, Airfield-Perimeterschutz vor Eindringlingen bis hin zu Remote-Tower-Lösungen haben sich unsere Lösungen erfolgreich etabliert.

Wie überall, steht dabei ja auch die Cybersecurity für Flughafenbetreiber im Zentrum der Aufmerksamkeit?

Karlheinz Biersack: Die politische Weltlage hat dafür gesorgt, dass Cybersecurity ein sehr wichtiger Aspekt für Kunden geworden ist. Wir als deutscher Entwickler und Hersteller erfüllen nicht nur die europäischen Anforderungen an die DSGVO und NIS-2, sondern auch die strengen Anforderungen der amerikanischen NDAA, die selbst Supply Chain Kontrolle und ethische Aspekte wie Verbot von Kinderarbeit und Ausbeutung vorsieht.

Damit wir unseren Kunden die höchstmögliche Sicherheit bieten können, lassen wir unsere Produkte auch von sogenannten White Hackern testen und berücksichtigen deren Anmerkungen und Empfehlungen in unserer Softwareentwicklung.

Welche Herausforderungen gibt es beim Schutz des Flugplatzes einschließlich des Perimeters?

Karlheinz Biersack: Klimaaktivisten haben aufgezeigt, wie anfällig bestehende Sicherheitssysteme und Lösungen sind, die das gesamte Airfield eines Flughafens schützen sollen. Ein Zaun und Patrouillen allein reichen nicht mehr aus, um immense Schäden durch Vandalismus und Flugausfälle abzuwenden. Dallmeier hat mit der Panomera-Perimeter und mit spezialisierter KI eine Lösung für den optimalen Perimeterschutz entwickelt.

Außerdem bieten wir zusammen mit dem Radar-Hersteller Navtech eine integrierte Lösung an, die ein gesamtes Airfield effizient überwachen kann und den Sicherheitskräften sofort Videoinformationen zur Verifizierung und zur Einsatzsteuerung zur Verfügung stellt. Im Februar dieses Jahres haben wir zusammen mit Navtech das „Airside Security Event“ in Bangkok organisiert.

Wie kann Videotechnik zur Optimierung von Ground Services beitragen?

Die Remote Tower Lösung von Dallmeier und Triac

Bitte umblättern ▶

KI-basierte Kameratechnik kann Objekte am Perimeter automatisch klassifizieren und dient Flughafen-Verantwortlichen zur visuellen Verifizierung

Karlheinz Biersack: Das Apron Management organisiert unter anderem den Ground Service. Nicht immer funktioniert dieser reibungslos. Bei den Expansionsplänen der Airports werden häufig Satelliten-Terminals gebaut. Damit nicht auch noch ein separater Apron Tower am Satelliten-Terminal gebaut und mit Personal besetzt werden muss, setzen Airports verstärkt auf Virtual Airport Lösungen. Dallmeier überzeugt dabei mit seiner speziellen Panomera Multifocal-Sensortechnologie, die riesige Bereiche in hoher Bildqualität abbilden kann.

GIT-Lesern ist Ihre Multifocal-Sensortechnologie schon lange vertraut – können Sie trotzdem noch mal kurz skizzieren, wie sie arbeitet?

Karlheinz Biersack: Wir können mit ihr riesige Bereiche mit wenigen Kameras abbilden. Durch die geringe Anzahl an Kamerasystemen vermeidet man schon bei der Planung und Genehmigung von Installationspositionen viel Ärger. Meine Erfahrung zeigt, dass es manchmal schwierig sein kann, von verschiedenen Abteilungen Genehmigungen für Installationspunkte, für die Installation und die notwendige Infrastruktur wie Stromversorgung, Netzwerkanschlüsse, Switchports, etc. zu erlangen. Je weniger man davon braucht, desto weniger Probleme hat man…

Auch der Kostenaspekt spielt eine Rolle, denn weniger Infrastruktur, weniger Installationsaufwand, weniger Wartungskosten und eine wesentlich effizientere Bedienung zeigen klar die Kostenvorteile der Panomera-Technologie auf.

Geben Sie uns einmal ein aktuelles Anwendungsbeispiel?

Karlheinz Biersack: Der Flughafen Kopenhagen beispielsweise hat sich nach einem PoC für die Dallmeier Panomera-Technologie entschieden. Mit nur 18 Kameras decken wir den kompletten Apron-Bereich ab. Bei einem Besuch des Airside Coordination Centers in Kopenhagen haben mir die Apron-Manager mitgeteilt, die Bildqualität sei so brillant, dass sie manchmal den Eindruck hätten, sie stünden direkt neben dem Flugzeug.

Diese Videoinformationen werden auch anderen Abteilungen und den Ground Service Providern zur Verfügung gestellt, um einen möglichst reibungslosen Service sicherzustellen. Außerdem kann unsere Kameratechnologie auch von Turnaround Managementsoftware-Anbietern wie Assaia genutzt werden, denn die Videobilder zeigen auch den Heckbereich des Flugzeuges und tragen somit dazu bei, dass die Turnaround-Analytik einen zusätzlichen Blickwinkel erhält und nicht durch große Tank- oder Catering-Fahrzeuge beeinträchtigt wird. Das sorgt für noch präzisere Turnaround-Analytikergebnisse.

Welchen Zusatznutzen bietet Ihre Videotechnologie für andere Flughafenabteilungen?

Karlheinz Biersack: Für Apron-Manger, De-Icing Manager, Air Traffic Controller und Operations Manager bietet Dallmeier die Integration von Flugdaten (Tail Number, Call Sign, Flugnummer und weitere Informationen) direkt in den Videostream an. Das bietet jedem Nutzer eine bessere Situational Awareness und mehr Information von einer Quelle, nämlich dem Videostream.

Der Nutzer muss nicht zusätzlich auf einen separaten Radar- oder Airport Management System-Monitor schauen. Selbst bei schlechten Sichtverhältnissen ist die Position des Flugzeuges mit den dazugehörigen Flugdaten im Video verfügbar. Immer mehr Airports nutzen die Flugdatenintegration im Video, um ein effizienteres Management zu erreichen.

Auch beim Security Check unterstützt die Panomera-Technologie. Wie funktioniert das?

Karlheinz Biersack: Manchmal sollen Passagiere, die den Security Check bereits abgeschlossen haben, nochmals überprüft werden, weil beim Scanvorgang doch noch ein Zweifel aufgetreten ist. Unsere Kameras stellen neben dem reinen Videobild auch Metadaten und Attribute zur Verfügung, nach denen in Sekundenschnelle – auch kameraübergreifend – gesucht werden kann. Somit kann man eine Person, die den Security-Check-Bereich bereits verlassen hat, in wenigen Sekunden ausfindig machen und einem weiteren Check unterziehen.

Welche Rolle spielt Videotechnologie bei der Optimierung der Passenger Experience?

Karlheinz Biersack: Es wird für das Airport Management immer wichtiger, das Passagiererlebnis zu verbessern. Zeiten für Check-In, Security-Check und Passportkontrollen sollen so gering wie möglich gehalten werden – nicht zuletzt deshalb, damit Passagiere mehr Zeit zum Konsumieren und Entspannen haben.

Unsere Kameratechnologie liefert neben den hochwertigen Videosequenzen auch Informationen wie Personenzähldaten, Wartezeitermittlungsdaten, Infos zu Personenansammlungen, etc. Damit kann das Airport Management bei Bedarf Prozesse anpassen und optimieren. So bieten unsere Kameras dem Airport einen doppelten Nutzen: Ohne ein separates Personenzählsystem mit separaten Sensoren installieren zu müssen, stellen unsere Kameras zusätzlich zu den Videobildern auch diese Daten zur Verfügung. Der Airport spart sich die Anschaffung separater Personenzählsensoren, die üblicherweise keine verwendbaren Videoinformationen für Security liefern können. Diese Informationen bzw. Daten können wir aufgrund optimierter AI-Analytik jetzt auch über die Kameras zur Verfügung stellen.

Inwiefern unterstützt Ihre Technologie die Überwachung von Runway, Taxiway und Apron-Bereichen?

Karlheinz Biersack: Um einen effizienten und sicheren Betrieb zu erreichen, greifen immer mehr Airport-Abteilungen auf die Videoinformationen zu. Air Traffic Controller, Apron-Manager bis hin zu Ground Service Providern nutzen die Videoinformationen, um einen reibungslosen Betrieb zu gewährleisten.

In Zeiten von Kostendruck und limitierten Personalressourcen haben Sie eine spezielle Remote Tower Lösung entwickelt. Was hat es damit auf sich?

Karlheinz Biersack: Zusammen mit unserem Technologiepartner Triac haben wir eine attraktive, flexible, erschwingliche und zugelassene Remote Tower Lösung entwickelt, die in Deutschland seit November 2023 erfolgreich im Einsatz ist.

Insbesondere Regionalflughäfen mit weniger Flugverkehr stehen unter enormem Kostendruck und haben Probleme, Fluglotsen einzustellen und diese langfristig an sich zu binden. Fluktuation von Fluglotsen führt zu wiederkehrenden Ausbildungskosten, die pro Person schnell mal bei 200.000 Euro liegen können. Die Remote Tower Lösung von Triac bietet die Möglichkeit, dass Fluglotsen einen Flugbetrieb aus der Ferne betreuen können – so schafft man Personalsynergien und Effizienz, denn ein Fluglotse kann die Flüge mehrerer Regionalflughäfen handeln.

Triac bietet ein Free-Seating-Concept für Fluglotsen an. Das bedeutet, der Fluglotse kann praktisch an jedem angeschlossenen Flughafen oder in einem der zwei Kontrollcenter arbeiten. Was dem Fluglotsen und seiner Familie entgegenkommt, denn er muss nicht mit seiner Familie an einem abgelegenen Ort wohnen und arbeiten, er kann den Arbeitsplatz frei wählen.

Der Schichtbetrieb von Fluglotsen kann umso effizienter organisiert und geplant werden, je mehr Flughäfen an das Remote Tower Konzept angeschlossen sind. Die technischen Features von Dallmeier wie Flugdatenintegration, automatisiertes Flugzeugtracking und Runway Incursion Mitigation Analytics unterstützen den Fluglotsen zusätzlich bei seiner Arbeit.

Ihre Airport-Lösungen finden sich ja weltweit?

Karlheinz Biersack: Das stimmt. Wir bieten vielfältige Lösungen an und können mit unseren Erfahrungen und zusammen mit unseren Technologiepartnern auch individuelle Wünsche von Airport-Kunden bedienen. Zu unseren zufriedenen Kunden gehören beispielsweise die Flughäfen Bristol (UK), St. Louis-Lambert (USA), Mailand-Linate (Italien), Kopenhagen (Dänemark), Istanbul (Türkei), Bangkok (Thailand) oder Neapel (Italien). GIT

Hier können Sie die Präsentationen des Airside Security Events 2025 einsehen:

Dallmeier electronic GmbH & Co. KG
www.dallmeier.com

250 Stunden Zeitersparnis pro Jahr…

… durch optimierte Bildverbesserung

Die Betsukawa Corporation hat sich auf Stromverteilungsanlagen und -dienstleistungen spezialisiert, darunter die Entwicklung, Herstellung, Installation und Wartung von Systemen wie Verteilertafeln, Schalttafeln und Unterverteilertafeln. Dazu kommen Lösungen für die städtische Infrastruktur, darunter Facility-Management-Lösungen, Produktionsautomatisierungslösungen für den Fertigungssektor, Energiemanagementlösungen für die effiziente Steuerung von Beleuchtung und HLK sowie Planungs- und Wartungsdienstleistungen für elektrische Bahnsysteme. Um die betriebliche Effizienz zu steigern, wurde die Bildverbesserungssoftware Vision Core FCS von Eizo implementiert. Die Projektleiter Daichi Maekawa und Mitsuru Shimazu erläutern, wie die Software eingesetzt wird und welche konkreten Vorteile sie gebracht hat.

Daichi Maekawa, Corporate Planning Office, DX Promotion Team

Mitsuru Shimazu, Osaka Branch, Sales Group, Betsukawa Corporation

GIT SICHERHEIT: Herr Maekawa, Herr Shimazu, was waren die größten Herausforderungen bei der Konzeption der Stromverteilungssysteme und was hat Sie dazu bewogen, VisionCore FCS zu implementieren?

Daichi Maekawa und Mitsuru Shimazu: Wir sind seit vielen Jahren im Bereich Stromverteilungsanlagen tätig und führen häufig Austausch- oder Umbauprojekte für Anlagen durch, die vor 20 bis 30 Jahren installiert wurden. Da unsere Entwürfe auf bestehenden Anlagen basieren, führen unsere Vertriebs- und Technikmitarbeiter Vor-Ort-Untersuchungen durch und machen Referenzfotos. Anhand dieser Bilder überprüfen unsere Konstrukteure dann die Kabelführung, die Farben der Kappen und die Kabelkennzeichnungen.

Aufgrund der Hochspannungsumgebung sind Nahaufnahmen jedoch oft nicht möglich. Außenbedingungen wie Gegenlicht und Schatten führen ebenfalls zu unklaren Bildern. Früher haben wir uns auf Standard-Windows-Tools zur Bildkorrektur verlassen – oder sogar die Standorte erneut besucht, um Fotos neu zu machen. Bei rund 3.000 Vor-Ort-Begehungen pro Jahr brauchten wir eine effizientere Lösung. Deshalb haben wir uns für die Bildoptimierungssoftware VisionCore FCS von Eizo entschieden.

Wie setzen Sie die Software ein?

Daichi Maekawa und Mitsuru Shimazu: Um die neue Software ohne Unterbrechung unseres bestehenden Workflows zu integrieren, haben wir ein internes Lade-Tool entwickelt. Dieses Tool kopiert Fotodateien automatisch in den Überwachungsordner von VisionCore FCS, verarbeitet sie und legt die verbesserten Bilder wieder im ursprünglichen Ordner ab, sodass unsere Mitarbeiter die Dateien wie gewohnt auf dem internen Dateiserver des Unternehmens speichern können. So wird sichergestellt, dass alle Bilder automatisch verbessert werden, ohne dass die Mitarbeiter ihre Arbeitsweise ändern müssen. Die Originalbilder und die verbesserten Bilder werden zusammen gespeichert, sodass sie leicht verglichen und verwendet werden können.

Welche Auswirkungen hatte die Implementierung und wie wurde sie innerhalb des Unternehmens aufgenommen?

Daichi Maekawa und Mitsuru Shimazu: Das Feedback unseres Designteams ist sehr positiv. Die Fotos sind demnach viel besser zu erkennen, und die automatische Verarbeitung ist eine enorme Hilfe. Obwohl VisionCore FCS erst vor kurzem eingeführt wurde, haben wir die potenzielle Zeiter-

VisionCore FCS von Eizo nutzt die proprietäre Bildoptimierungstechnologie des Unternehmens, um schwer erkennbare Bereiche in aufgenommenen Videos oder Standbildern zu identifizieren und zu verbessern

Bildoptimierungssoftware VisionCore FCS

Die Software nutzt die proprietäre Bildoptimierungstechnologie von Eizo, um schwer erkennbare Bereiche in aufgenommenen Videos oder Standbildern zu identifizieren und zu verbessern, sodass sie klarer und leichter zu interpretieren sind. Sie verfügt über eine Überwachungsfunktion, die benutzerdefinierte Ordner kontinuierlich überwacht. Wenn eine Datei hinzugefügt wird, führt die Software automatisch eine Codierung und Bildverbesserung durch und speichert die verarbeitete Datei in einem bestimmten Ordner oder auf einem FTP-Server.

sparnis anhand der Anzahl der Projekte, der Häufigkeit unklarer Bilder und der durchschnittlichen Korrekturzeit geschätzt. Das Ergebnis: eine jährliche Zeitersparnis von etwa 250 Stunden.

Was war der ausschlaggebende Faktor für die Entscheidung für VisionCore FCS?

Daichi Maekawa und Mitsuru Shimazu: Das ist zum einen die schnelle, automatische Verbesserung von Fotostapeln. Die Überwachungsordnerfunktion ist ein großer Vorteil – sie überwacht kontinuierlich den Server und verbessert automatisch ganze Stapel von Fotos. Dank der Flexibilität der Software ließ sich die Integration in unsere internen Systeme nahtlos realisieren. Wir haben während der kostenlosen Testphase alles ausprobiert und konnten uns so von der Lösung überzeugen. Dazu kommt die Kosteneffizienz durch einmalige Anschaffung. In einer Zeit, in der die meisten Dienste auf laufenden Abonnements basieren, stach VisionCore FCS von Eizo durch sein Einmal-Kaufmodell hervor. Das machte es für uns zu einer äußerst kostengünstigen Lösung.

Wie sehen Sie die Zukunft und was erwarten Sie von Eizo?

Daichi Maekawa und Mitsuru Shimazu: Wir prüfen Möglichkeiten, den Einsatz von VisionCore FCS auf andere Bereiche unseres Unternehmens auszuweiten, beispielsweise auf Überwachungssysteme und den Nachtbetrieb im Schienenverkehr, um unseren Kunden einen noch größeren Mehrwert zu bieten. Als Teil unseres DX-Förderteams (Digital Transformation) arbeiten wir auch an der Digitalisierung von Konstruktionszeichnungen. Derzeit erwägen wir die Einführung von Touchpanel-Monitoren, mit denen Benutzer digitale Zeichnungen während Besprechungen so einfach wie auf Papier mit Anmerkungen versehen können. Wir freuen uns darauf, dass Eizo auch in Zukunft innovative und vielseitige visuelle Lösungen anbieten wird, die unseren sich wandelnden Anforderungen gerecht werden. GIT

Eizo
www.Eizoglobal.com

Das ursprüngliche im Vergleich mit dem von der Eizo-Software bearbeiteten Bild

Durch den Donut geguckt

Video-Cloud-Lösung für Dunkin'-Filialen

Die Valeo IT Neteye ist seit über 20 Jahren Mobotix-Partner und hat in dieser Zeit für mehr als 300 Kunden fast 8000 Kameras in einer für den Kunden individuellen maßgeschneiderten Videolösung integriert. Durch die jahrelange Erfahrung der Mitarbeiter profitieren Valeo IT Neteye-Kunden von der Kompetenz des Unternehmens. Es schafft für seine Kunden IP-Videolösungen, die ein Höchstmaß an Sicherheit und Komfort ermöglichen und gleichzeitig einfach zu bedienen sind.

Seit zehn Jahren zählt DFNBG Gastro zu den Kunden des Mobotix-Partners Valeo IT Neteye. Das Unternehmen betreibt unter anderem 48 Dunkin'-Läden und beschäftigt rund 600 Mitarbeiter, von denen rund 25 Zugriff auf die Sicherheitssysteme des Unternehmens haben.

„Die Sicherheit der Mitarbeiterinnen und Mitarbeiter sowie der Schutz unserer Gastrobetriebe vor Vandalismus, vor allem aber auch die Vermeidung bzw. Aufklärung von Diebstählen waren am Beginn unserer Zusammenarbeit die Herausforderungen, vor denen wir standen", so Harry Taubert, Construction & Development Manager bei DFNBG Gastro. Mit Mobotix wurde die passende Lösung implementiert.

Dezent angebrachte Mobotix-Kameras sorgen für die notwendige Sicherheit in den Dunkin'-Filialen und schützen Mitarbeiter und Kunden vor möglichen Bedrohungen und Gefahren. Die Daten der Videolösung wurden vor Ort in einem Mobotix-Videomanagementsystem (VMS) gesichert – und das führte vor rund vier Jahren zum nächsten Auftrag der DFNBG an die Valeo IT Neteye.

Cloud und Bridge

Das permanente Wachstum der DFNBG Gastro brachten Herausforderungen mit sich. So wurde es beim Sicherheitssystem zum Beispiel immer aufwendiger, die Zugriffsrechte der wachsenden Mitarbeiterzahl zu managen. Überdies wuchsen die Anforderungen hinsichtlich der Datenschutzbestimmungen an das VMS vor Ort, das unter anderem einen separaten Raum und ständig weitere Sicherheitsstandards benötigte. Gerade bei Filiallagen in Einkaufspassagen waren die Anforderungen nur noch schwer zu stemmen.

Die Mobotix Cloud bot hierfür die passende Lösung. Seit vier Jahren erfolgt die sukzessive Migration von lokalem NAS (Network Attached Storage) in den Dunkin'-Filialen auf das cloudbasierte, datenschutzkonforme Video-Management System von Mobotix. Das Cloud-Angebot des Herstellers im Bereich Videoüberwachung-as-a-Service (VSaaS) ermöglicht es Nutzern, ihre Kameras bequem über eine App zu steuern. Die aufgezeichneten Videos werden in hochverfügbaren und cybersicheren Rechenzentren gespeichert, die in der Nähe der Nutzer angesiedelt sind.

DFNBG Gastro ist ein Nürnberger Unternehmen, das zahlreiche Gastrobetriebe im Franchisesystem betreibt – unter anderem 48 Dunkin'-Läden

Das Cloud-Angebot von Mobotix ermöglicht es Nutzern, ihre Kameras bequem über eine App zu steuern. Die aufgezeichneten Videos werden in hochverfügbaren und cybersicheren Rechenzentren gespeichert, die in der Nähe der Nutzer angesiedelt sind

Diese Lösung ist – wie auch die Kameras des Herstellers – Made in Germany und erfüllen sämtliche Anforderungen der DSGVO. Die Kombination aus intelligenter Kamera und zentraler Cloud-Plattform minimiert den Bandbreitenbedarf, da die Kameras Ereignisse vor Ort analysieren und nur relevante Daten in die Cloud übertragen. Entsprechend den DSGVO-Vorgaben sind die Videoaufnahmen in einem gesicherten Rechenzentrum gespeichert, das sowohl physischen Schutz durch Wachpersonal und Zugangskontrollen als auch digitalen Schutz durch Verschlüsselung bietet. Die Kommunikation zwischen den Kameras und der Cloud erfolgt über die Mobotix Bridge, eine hochsichere Verbindungseinheit zur Cloud.

Zentrales Zugriffsmanagement

Die Auslagerung der Datenspeicherung in die Cloud vermeidet den DSGVO-konformen Schutzbedarf vor Ort, der bei einer lokalen NAS-Lösung erforderlich wäre. Die Verwaltung der Cloud-Daten erfolgt direkt durch den Nutzer selbst. „Dass das von der Valeo IT Neteye vorgeschlagene und implementierte System sicher – auch cybersicher – ist und unsere Ansprüche mehr als erfüllt, war uns klar. Dass wir aber mit der Mobotix Cloud jetzt alle Zugriffsrechte zentral managen können, ist ein gewaltiger Vorteil, der uns richtig Zeit und Geld spart“, urteilt Harry Taubert. Rund die Hälfte der Dunkin'-Filialen wurden schon auf die Cloud migriert – und in den nächsten Jahren soll die Migration der restlichen Dunkin'-Filialen von DFNBG Gastro in die Cloud erfolgen. GIT

Mobotix
www.mobotix.com

Vom Reagieren zum Handeln

Der Blick zurück reicht nicht mehr aus: Proaktive Videosicherheit mit KI und Cloud

Die Anforderungen an moderne Sicherheitssysteme haben sich grundlegend verändert. Während Kameras früher hauptsächlich zur nachträglichen Aufklärung von Vorfällen genutzt wurden, müssen sie heute in der Lage sein, potenzielle Bedrohungen zu erkennen, bevor diese eskalieren – idealerweise in Echtzeit. Proaktive Sicherheit ist längst kein Trend mehr, sondern eine Notwendigkeit. Der Schlüssel liegt in der Kombination aus Künstlicher Intelligenz (KI) und cloudbasierter Architektur. Ein Beitrag von Erik Mosler, Regional Sales Manager DACH, Eagle Eye Networks.

Eagle Eye Networks setzt auf ein klares Drei-Stufen-Modell: Erkennen, Überprüfen, Handeln

Zahlreiche Unternehmen investieren erheblich in Überwachungstechnik. Doch die tatsächliche Wirkung bleibt häufig hinter den Erwartungen zurück. Dies liegt zunächst einmal daran, dass große Mengen an Videomaterial gespeichert, aber nie ausgewertet werden. Mitarbeiter müssen zudem monotone Live-Bilder überwachen – eine ermüdende Aufgabe, die fehleranfällig ist. Kritische Ereignisse werden oft erst erkannt, wenn der Schaden bereits eingetreten ist – wichtige Informationen bleiben unentdeckt oder werden zu spät identifiziert. Diese Systeme arbeiten rückblickend. Es fehlt die Fähigkeit, Bedrohungen frühzeitig zu erkennen, zu analysieren und gezielt zu reagieren – bevor etwas passiert.

Von der Kamera zur verwertbaren Information

Proaktive Videosicherheit bedeutet, Systeme nicht nur aufzeichnen zu lassen, sondern sie so einzurichten, dass sie interpretieren, unterscheiden und gezielt alarmieren können. Das geht weit über einfache Bewegungsmelder hinaus. Moderne, KI-gestützte Kameras verstehen Muster, erkennen Anomalien, identifizieren Objekte und bewerten Situationen im Kontext.

Beispiel: Statt Fehlalarme auszulösen, wenn sich Äste bewegen, Schatten auftauchen oder andere unkritische Aktivitäten stattfinden, erkennt das System präzise Personen und Fahrzeuge. Es analysiert, ob ein Alarm tatsächlich gerechtfertigt ist. Handelt es sich etwa um ein Fahrzeug, das außerhalb der Betriebszeiten auf dem Parkplatz erscheint? Oder ist es ein Mitarbeiter, der regulär zur Arbeit kommt?

Da das System mithilfe von KI zwischen relevanten und irrelevanten Ereignissen unterscheiden kann, werden Fehlalarme stark reduziert – und die tatsächlichen Benachrichtigungen sind gezielt und sinnvoll.

Echtzeit statt später Sichtung

Künstliche Intelligenz verwandelt den Datenstrom der Kameras in direkt nutzbare Informationen. Entscheidende Details – wie das Erkennen eines Eindringlings auf einem großen Gelände oder auffällige Bewegungen in sensiblen Bereichen – werden markiert, analysiert und in Sekundenschnelle an das zuständige Personal übermittelt.

Ein mühsames Durchsuchen von Stunden an Aufzeichnungen entfällt. Die Reaktion erfolgt gezielt und zum richtigen Zeitpunkt. Die Cloud ermöglicht dabei nicht nur Skalierbarkeit und standortübergreifenden Zugriff, sondern auch kontinuierliches Lernen und Aktualisieren der KI – ohne zusätzlichen Aufwand für die lokale IT.

Drei Ebenen für eine integrierte Sicherheitslösung

Eagle Eye Networks setzt auf ein klares Drei-Stufen-Modell: Erkennen – Überprüfen – Handeln

- Perimeterschutz: Unbefugte Zugänge im Außenbereich erkennen – selbst unter schwierigen Bedingungen wie Dunkelheit, Regen oder Kälte. Das System analysiert die Richtung, Geschwindigkeit und Entfernung von Bewegungen.
- Flächenüberwachung: PTZ-Kameras identifizieren und verfolgen Personen oder Fahrzeuge über weite Areale. Verdächtige Aktivitäten werden automatisch erkannt und in Echtzeit weiterverfolgt.
- Gebäudesicherheit und Zugangskontrolle: Eingänge, Flure und Fluchtwege

Proaktive Sicherheit ist längst kein Trend mehr, sondern eine Notwendigkeit

werden überwacht, um sicherzustellen, dass nur autorisierte Personen Zugang erhalten. Dabei geht das System über klassische Zugangskontrollen hinaus, indem es Mustererkennung und verhaltensbasierte Bewertung nutzt.

Alle drei Ebenen sind cloudbasiert miteinander vernetzt – für einen ganzheitlichen Überblick statt isolierter Einzelinformationen.

Besser entscheiden

Eine gut aufgebaute Sicherheitsarchitektur hilft dabei, schneller und besser zu entscheiden. Welche Information ist wirklich relevant? Wann muss reagiert werden? Wer muss benachrichtigt werden? KI-gestütztes Ereignismanagement reduziert die Informationsflut auf das Wesentliche. Entscheidungen basieren auf konkreter Analyse – nicht auf Bauchgefühl.

- Relevante Objekte werden automatisch erkannt
- Ungewöhnliches Verhalten wird hervorgehoben
- Alarme werden direkt an mobile Endgeräte übermittelt – dorthin, wo sie gebraucht werden
- Reaktionen werden dokumentiert und können später analysiert oder rechtlich nachvollzogen werden

Flexibilität durch die Cloud

Ein großer Vorteil cloudbasierter Videosysteme ist ihre Flexibilität. Neue Kameras lassen sich schnell einbinden, Standorte unkompliziert vernetzen. Die hohen Anfangsinvestitionen – typisch für On-Premise-Systeme – entfallen, da keine lokalen Server, komplexe Verkabelungen oder zusätzliche IT-Ressourcen erforderlich sind.

Wartung und Software-Updates erfolgen zentral. Die Lösung bleibt aktuell, widerstandsfähig und skalierbar. Und dank der Cloud kann sich die Architektur dynamisch an neue Sicherheitsanforderungen anpassen – ohne Kompromisse bei Datenschutz oder IT-Sicherheit.

Fazit

Die Zukunft der Videosicherheit hängt nicht von der Anzahl installierter Kameras ab – sondern davon, was mit den Bilddaten passiert. Echte Sicherheit bedeutet, dass Systeme verstehen, was sie sehen – und daraus sofortiges, sinnvolles Handeln ermöglichen.

Eagle Eye Networks verfolgt ein klares Ziel: den Wandel vom passiven Beobachten hin zum aktiven Eingreifen. KI und cloudbasiertes Video-Management machen genau das möglich – und verwandeln Kameras in vorausschauende Werkzeuge.

Das schafft neue Perspektiven für Unternehmen, öffentliche Einrichtungen und Betreiber kritischer Infrastrukturen, um Risiken gezielt zu managen – und die Kontrolle zu behalten, bevor eine Situation eskaliert. GIT

Eagle Eye Networks
www.een.com


© Dallmeier electronic

MK4-Revision des DMS 2400 von Dallmeier

Mit der MK4-Revision des DMS 2400 stellt Dallmeier eine leistungsstärkere Version seiner Recording Appliance vor. Die MK4-Variante ermöglicht die Speicherung von bis zu 40 hochauflösenden Video-Streams und bietet dadurch eine deutlich gesteigerte Aufzeichnungskapazität.

Die Appliance DMS 2400 (MK4) kombiniert die SeMSy Recording Server Software mit einer kompakten Server-Hardware. Sie eignet sich für Videosicherheitsanlagen in Einzelhandelsgeschäften, Tankstellen oder privaten Anwesen, die bei geringem Platzbedarf höchste Aufzeichnungsqualität erfordern.

Dank optimal abgestimmter Komponenten erreicht das System eine hohe Speichergeschwindigkeit und erlaubt die Aufzeichnung von bis zu 40 hochauflösenden Video-Streams bei einer Bildrate von 30 fps. Zwei abschließbare 3,5“-Festplatteneinschübe an der Rückseite ermöglichen eine Speicherkapazität von bis zu 48 TB. Das abgeschottete Linux-Betriebssystem und die Applikation SeMSy Recording Server sind auf einem separaten Flash-Modul installiert.

Die vorinstallierte SeMSy Recording Server Software ist als offene Plattform konzipiert. In Verbindung mit den entsprechenden Lizenzen können 3rd Party Kameras mit Motion Detection aufgezeichnet und über das ONVIF-Protokoll konfiguriert werden. Die Appliance ist zudem mit einer Datenbank für die Analyseergebnisse von Dallmeier Kameras und Panomera Systemen mit EdgeAnalytics-Technologie ausgestattet. Die empfangenen Ereignisse, Objekte und Klassen werden nahezu in Echtzeit mit den relevanten Metadaten gespeichert und können mit der SmartFinder-Funktion von SeMSy Compact gezielt ausgewertet werden.

Ein besonderer Kostenvorteil zeigt sich bei der Aufzeichnung von Panomera Kameras: „Für die Aufzeichnung eines Panomera Multifocal-Sensorsystems ist nur ein einziger lizenzierter Aufzeichnungskanal für den ersten Sensor erforderlich. Alle weiteren Sensoren benötigen lediglich freie Kanäle, die aber nicht lizenziert werden müssen. Das reduziert die Lizenzkosten und ermöglicht eine besonders wirtschaftliche Systemplanung“, erläutert Christian Linthaler, Chief Sales Officer bei Dallmeier.

Wie alle Dallmeier Recorder unterstützt auch der DMS 2400 (MK4) den mobilen Zugriff über den SeMSy Mobile Client. Diese Lösung ermöglicht Sicherheitsverantwortlichen den Zugriff auf Live-Bilder und Aufzeichnungen von verschiedenen Standorten. Durch KI-gestützte Objektklassifizierung werden relevante Ereignisse vorsortiert und übersichtlich dargestellt. Die intuitive Bedienung wird über Slider oder das „Trackwheel“ mit haptischer Bestätigung realisiert. Der SeMSy Mobile Client ist sowohl als Smartphone- als auch als Tablet-Version erhältlich. **www.dallmeier.com**

DoorBird erhält UL-Zertifizierung

© Bird Home Automation

Die Produktlinie D21x von DoorBird hat die UL-Zertifizierung erhalten, ein anspruchsvoller Sicherheitsstandard für Audio-/Video-, Informations- und Kommunikationstechnologie. Die UL-Zertifizierung bestätigt, dass DoorBird-Produkte die hohen nordamerikanischen Sicherheitsanforderungen erfüllen und damit eine zuverlässige und sichere Leistung unter anderem in den USA und Kanada gewährleisten. Die Produkte bieten umfassenden Schutz vor elektrischem Schlag, Brandgefahr und mechanischen Risiken – ein entscheidender Faktor für die Sicherheit von Nutzern, Mietern und Eigentum in gewerblichen, institutionellen und mehrfamiliengenutzten Gebäuden. Durch die Ausrichtung an international harmonisierten Standards wird die nahtlose Integration in globale Projekte erleichtert und das Vertrauen aller Projektbeteiligten gestärkt. **www.doorbird.com**

Genetec und Hanwha Vision: eine starke Partnerschaft


© Hanwha Vision

Ben Durrant, Account Executive bei Genetec Inc.

Mit einer langjährigen und erfolgreichen Technologiepartnerschaft haben Hanwha Vision und Genetec führende Videoanalyse- und Überwachungsinstallationen im öffentlichen Sektor und darüber hinaus geliefert. Ein aktuelles Projekt ist die Videoüberwachung für die Thames Valley Polizei, den größten nicht-metropolitanen Polizeidienst in England und Wales. Mehrere der lokalen Behörden hatten Systeme, die ein Upgrade benötigten. Man wollte Ressourcen bündeln und ein einziges System installieren, das sich über die gesamte Thames Valley-Region erstreckt, um die Sicherheit öffentlicher Räume zu verbessern, Kosten zu senken und die Effizienz zu steigern, so Ben Durrant, Account Executive bei Genetec Inc. Die Lösung, entworfen von CDS Integrated Security Systems, basiert auf dem Genetec Security Center und beinhaltet eine Reihe von multidirektionalen, KI-fähigen Kameras von Hanwha Vision. **www.hanwhavision.eu/**

Online-Fachseminar zu smarter Gebäudetechnik

Nach dem erfolgreichen Start der neu aufgelegten Online-Fachseminarreihe „Next Level Bau: digitale Innovationen für nachhaltige smarte und sichere Gebäude“ bietet Assa Abloy gemeinsam mit seinen Schwesterunternehmen Bird Home Automation GmbH und HID weitere Termine zur Teilnahme an. Am Mittwoch, den 1. Oktober 2025, findet von 10.00 bis 12.15 Uhr die nächste kostenfreie Veranstaltung statt. Dabei erfährt der Teilnehmer, wie sich dank moderner Technologien die Zukunft des Bauens nachhaltiger, sicherer – und damit smarter – gestalten lässt. **www.assaabloy.com**

Paxton erweitert Schulungsprogramm in Deutschland

Der weltweit tätige Hersteller von Sicherheitstechnologie Paxton hat sein erfolgreiches Schulungsprogramm für Installateure in Deutschland ausgebaut und bietet nun spezielle Präsenzschulungen für das Türsprechsystem Entry an. Dieses neue Angebot ergänzt die bereits etablierten Trainings für Net2 und Paxton10 und ermöglicht Installateuren ein umfassendes Fachwissen, um im wachsenden deutschen Markt für Zutrittstechnologie erfolgreich zu sein. „Wir freuen uns, unser Schulungsprogramm in Deutschland um Entry zu erweitern – zusätzlich zu Net2 und Paxton10. Diese Erweiterung unterstreicht unser Engagement, Installateure mit dem gesamten Spektrum der Paxton-Lösungen zu unterstützen. So ermöglichen wir ihnen, unterschiedlichste Kundenanforderungen zu erfüllen und ihr Geschäft im wachsenden deutschen Markt weiter auszubauen“, so Sylvain Pailler, Vertriebsleiter Zentraleuropa bei Paxton. **www.paxton-access.com**

Feststellung der Tür in jeder beliebigen Position

Mit dem Türfeststeller Dictator ZE können Türen in jeder beliebigen Position festgestellt werden. Die Türfeststeller ZE zeichnen sich durch eine sehr solide und robuste Konstruktion aus. Das Gehäuse ist aus einem Guss und daher sehr widerstandsfähig, auch gegen Vandalismus. Die Feststeller ZE sind einschließlich der Innenteile komplett aus nicht rostenden Materialien. Sie werden zudem in zwei verschiedenen Baureihen hergestellt: die Serie Standard und die Serie Design Line. Bei dieser Ausführung ist die Kolbenstange nur noch dann sichtbar, wenn die Tür festgestellt ist. Die Neukonstruktion ermöglicht es, dass selbst bei einem Hub von 160 mm der Türfeststeller nicht größer ist als der mit 90 mm Hub der Standard-Ausführung. Mit der Design Line können selbst extrem große Abstände – maximal 200 mm – zwischen Türunterkante und Boden ausgeglichen werden. **www.dictator.de**

Mobotix-Leitfaden für Sicherheit

Der Leitfaden „Neue Maßstäbe für Sicherheit“ von Mobotix zeigt, wie führende Unternehmen ihre Sicherheitsarchitekturen modernisieren und so wirtschaftlicher und zukunftssicherer aufgestellt sind. Mit dem Leitfaden erfährt der Interessierte, wie Cybersecurity, Compliance und physischer Schutz heute zusammenspielen, welche globalen Regularien (NIS2, CRA, IEC 62676-4) die Sicherheitsstrategie beeinflussen, Praxisbeispiele aus Logistik, Energie, Gesundheitswesen und öffentlicher Verwaltung, wie Mobotix-Lösungen Fehlalarme reduzieren, Betriebskosten senken und Ausfallsicherheit erhöhen, wie „Secure by Design“ konkret umgesetzt wird – inklusive Edge Computing, DSGVO-Konformität und vollständiger Verschlüsselung. Egal, ob bestehende Systeme modernisiert oder ein neues Sicherheitskonzept umgesetzt werden soll – dieser Leitfaden gibt Orientierung und Sicherheit für die nächsten Schritte. **www.mobotix.com**

Intelligente und ethische Sicherheit …

. . . mit KI, Edge-Technologie und ISO-Zertifizierung

Die Videoüberwachung steht vor einem grundlegenden Wandel: Statt bloßer Bilderfassung geht es zunehmend um Echtzeit-Analyse, Effizienz und Datenschutz. Die treibende Kraft dahinter ist der Einsatz künstlicher Intelligenz direkt in den Kameras selbst, auch als Edge-AI bekannt. i-Pro, ein Unternehmen mit über 60 Jahren Erfahrung und japanischen Wurzeln, hat diese Entwicklung frühzeitig erkannt und seine Strategie neu ausgerichtet: weg vom reinen Hardwarehersteller hin zum Anbieter intelligenter, datengestützter Sicherheitsanwendungen. Ein Beitrag von Gerard Figols, Chief Operating Officer bei i-Pro.

Seit seiner Unabhängigkeit von Panasonic hat i-Pro seine Strukturen radikal verschlankt und die Entwicklungszyklen drastisch beschleunigt. Innerhalb von nur vier Jahren wurde das Kameraportfolio von 50 auf fast 300 Modelle erweitert – mit einer neuen Geschwindigkeit und Flexibilität, die auf die Bedürfnisse eines dynamischen Marktes reagieren. Kunden profitieren von schnellen Innovationen und einer Modularität, die den Einsatz maßgeschneiderter Lösungen ermöglicht.

Mehr als Überwachung

Kameras von i-Pro dienen heute nicht nur der klassischen Überwachung, sondern agieren als IoT-Sensoren mit intelligenten Analysefunktionen. Im Unterschied zu herkömmlichen Systemen ist es möglich, dabei nicht alle Videodaten zur Auswertung an zentrale Server zu übertragen. Stattdessen erfolgt die Analyse direkt in der Kamera, und nur die relevanten Ergebnisse – sogenannte Metadaten – können weitergeleitet werden. Dies spart Ressourcen und erhöht die Geschwindigkeit und Effizienz erheblich.

Die Edge-Technologie von i-Pro erlaubt damit eine Vielzahl von Anwendungen: vom Zählen von Personen und Fahrzeugen bis zur Erkennung verdächtiger Muster und Objekte. So hilft die Technologie beispielsweise, Messebetreibern, Besucherströme zu analysieren, oder unterstützt polizeiüberwachte Bereiche durch schnelle Such- und Erkennungsfunktionen – datenschutzgerecht, effizient und flexibel.

Intelligente Metadaten-Suche

Ein zentraler Bestandteil des i-Pro-Ökosystems ist i-Pro Active Guard. Diese Anwendung ermöglicht es Anwendern, nicht nur Live-bilder zu betrachten oder einfache Aufzeichnungen zu durchsuchen, sondern gezielt auf Basis der durch die Kameras generierten Metadaten zu recherchieren. i-Pro Active Guard unterstützt dabei komplexe Suchabfragen, etwa nach bestimmten Objekten, Fahrzeugen oder Personenattributen, und liefert in Sekundenschnelle Ergebnisse. So wird das große Potenzial von KI-gestützten Kameras effizient nutzbar gemacht – insbesondere für Anwender, die schnell und gezielt auf Ereignisse reagieren müssen, wie Sicherheitsdienste, Polizei oder Betreiber kritischer Infrastrukturen.

Durch die enge Verzahnung von Kamera und Software schafft i-Pro mit Active Guard ein Werkzeug, das nicht nur zur forensischen Analyse geeignet ist, sondern auch Echtzeit-Überwachung mit klar strukturierten Metadaten kombiniert.

Upgrades für Bestandsanlagen

Auch der Umgang mit vorhandener Technik ist durchdacht: i-Pro ermöglicht es, bestehende Systeme mit moderner KI-Funktionalität nachzurüsten. Besonders hervorzuheben sind dabei die Modelle der X-Serie des Unternehmens, die nicht nur lernfähig sind und sich durch wenige Bildbeispiele auf neue Objekte trainieren lassen, sondern auch Videoströme von älteren Nicht-KI-Kameras – einschließlich anderer Hersteller – analysieren können. Damit können Unternehmen ihre Investitionen schützen und gleichzeitig ihre Systeme fit für die Zukunft machen.

Cybersicherheit von Anfang an mitgedacht

Mit zunehmender Vernetzung steigen auch die Anforderungen an die IT-Sicherheit. i-Pro setzt deshalb auf einen Security-by-Design-Ansatz: Alle Geräte sind standardmäßig mit verschlüsselter Kommunikation, sicherem Bootprozess und digital signierter

Das Fukoka Forschungs- und Entwicklungscenter

© i-Pro

Intelligenz inklusive: Eine i-Pro AI High Zoom Bullet-Kamera

Firmware ausgestattet. Zudem verfügen alle Kameramodelle über eine FIPS 140-2 oder bereits 140-3 Level 3-Zertifizierung – zwei der weltweit strengsten Standards für kryptografische Sicherheit. Ergänzt wird das durch regelmäßige Firmware-Updates und praxisnahe Empfehlungen zur Systemhärtung. So bietet das Unternehmen zuverlässigen Schutz für Daten und Infrastruktur – auch in sensiblen Einsatzbereichen.

Ethische Verantwortung und Zertifizierung

Der Fortschritt bringt Verantwortung mit sich: Datenschutz, Fairness und Transparenz stehen bei i-Pro im Zentrum. Als das erste Unternehmen in der phyischen Sicherheitsbranche hat i-Pro im Mai 2025 die ISO/IEC 42001-Zertifizierung für sein Managementsystem rund um den Einsatz künstlicher Intelligenz erhalten. Diese neue Norm definiert internationale Standards für den ethischen und verantwortungsvollen Umgang mit KI.

Auch konkrete Maßnahmen unterstreichen diese Haltung: So setzt der Hersteller auf Privacy-by-Design-Prinzipien, minimiert die Erfassung personenbezogener Daten und bietet Funktionen wie automatische Verpixelung von Gesichtern durch die Privacy Guard-Anwendung.

Offene Plattformen für vielfältige Anwendungen

Neben der Hardware ist auch das Software-Ökosystem von i-Pro offen gestaltet. Partner können eigene Anwendungen integrieren – von automatischer Nummernschilderkennung über Verhaltensanalysen bis hin zu speziellen Ansätzen für Städte, Einzelhandel oder Logistik. Diese Offenheit macht die Kameras zu Plattformen für vielseitige Anwendungen, bei denen nicht nur Sicherheitsziele im Vordergrund stehen, sondern auch betriebswirtschaftlicher Nutzen durch intelligente Datennutzung entsteht.

Ausblick: KI als Basis für neue Möglichkeiten

In einer zunehmend datengetriebenen Welt steht i-Pro für einen ganzheitlichen Ansatz: zuverlässige, qualitativ hochwertige Hardware, ergänzt um intelligente Software wie i-Pro Active Guard und verbunden mit einem klaren ethischen Rahmen. Die Strategie zahlt sich aus – ob für Behörden, Unternehmen oder Betreiber komplexer Infrastrukturen. Überwachung wird nicht länger als reines Sicherheitsinstrument verstanden, sondern liefert wertvolle Erkenntnisse für Betrieb, Logistik und Planung.

Während generative KI derzeit noch aktuell keine Anwendung in Überwachungskameras findet, entwickelt das Unternehmen seine Technologien konsequent weiter, um zukünftige Anforderungen zu erfüllen. Klar ist: Der Trend zu KI-basierten Sicherheitsanwendungen wird weiter an Bedeutung gewinnen – und i-Pro positioniert sich mit seiner Kombination aus Innovation, Qualität und Verantwortungsbewusstsein als ein wichtiger Akteur in diesem dynamischen Markt. GIT

i-Pro
www.i-pro.com

60 Jahre intelligente Videoanalyse

Im Gespräch mit Peter Treutler, Prokurist und Leiter der Business Unit IPS von Securiton Deutschland

Seit sechs Jahrzehnten befasst sich IPS Intelligent Video Software mit der Entwicklung moderner Videosicherheit. Was 1970 mit dem IPS Deltaguard begann, hat sich zu einer hochspezialisierten Technologie für den Schutz kritischer Infrastrukturen entwickelt. GIT SICHERHEIT sprach mit Peter Treutler, Prokurist und Leiter der Business Unit IPS bei Securiton Deutschland, über Meilensteine, Zukunftsvisionen und die besonderen Anforderungen an Hochsicherheitslösungen.

GIT SICHERHEIT: Herr Treutler, IPS Intelligent Video Software feiert beeindruckende 60 Jahre. Was waren die größten technologischen Meilensteine in dieser Zeit?

Peter Treutler: Vor 60 Jahren existierte der Begriff Videoanalyse noch gar nicht, und dennoch hat IPS bereits 1970 mit dem IPS Deltaguard einen technologischen Meilenstein geschafft: Erstmals wurden aus einem Videobild gezielt Informationen extrahiert und Bildinhalte automatisiert ausgewertet, um den Menschen bei sicherheitsrelevanten Aufgaben zu unterstützen. Mit dem IPS Teleguard konnten dann 1980 bereits Videobilder in unterschiedliche Zonen segmentiert werden, um einzelne Bildbereiche gezielt zu analysieren.

In den 1990er Jahren kam das IPS-3-Zonen-Konzept, welches sogar ein europäisches Patent erhielt. Bis zu diesem Zeitpunkt erfolgte die Videoanalyse in der Regel auf Basis einfacher Linienerkennung. Ein Alarm wurde ausgelöst, sobald ein Objekt eine definierte virtuelle Linie im Bild überschritt. Im Unterschied dazu ermöglichte das IPS-3-Zonen-Konzept eine fein abgestufte Zonenlogik, eine präzise Unterscheidung zwischen harmlosen und sicherheitskritischen Bereichen innerhalb eines Bildes und einer damit verbundenen logischen Verknüpfung der unterschiedlichen Zonen sowie automatisierte Aktionen. Ein weiteres Highlight war die IPS-3D-Videotechnologie, mit der erstmals sogar kameraübergreifende Analysen möglich wurden.

Welche Rolle spielt IPS grundsätzlich in der Entwicklung intelligenter Videosoftware?

Peter Treutler: IPS war Wegbereiter – nicht weniger. Dank den frühen IPS-Entwicklungen gibt es Videosicherheit wie wir sie heute kennen. Wir waren die Ersten, die ein intelligentes Zonenkonzept entwickelten und dafür auch ein Patent erhielten. Oder die 3D-Objektverfolgung auf den Markt brachten, welche heute in vielen sicherheitskritischen Anwendungen Standard ist und im Ursprung aus unserem Haus stammt. IPS hat von Anfang an auf intelligente Software gesetzt. Wir haben es zum Softwarepionier geschafft: IPS hat das Videobild nicht nur übertragen oder aufgezeichnet, sondern mit Intelligenz angereichert. Immer mit dem Ziel, den Menschen in sicherheitsrelevanten Situationen aktiv zu unterstützen.

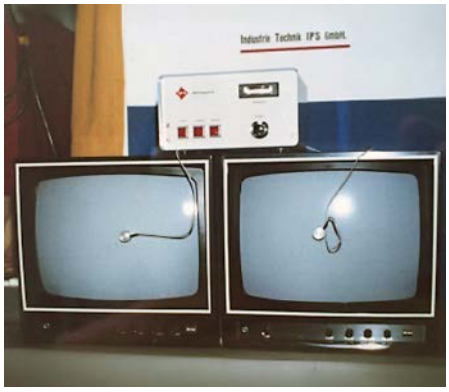
Was unterscheidet heute die Video Technologiemarke IPS Intelligent Videosoftware von anderen Anbietern?

Peter Treutler: Ein wesentlicher Unterschied liegt in unserem ganzheitlichen Ansatz: Bei der IPS-Technologie kommen Videoanalyse und Videomanagement aus einem Guss – und zwar von Anfang an als integrative, perfekt aufeinander abgestimmte Lösung. Unsere Spezialisierung hebt uns deutlich ab: IPS entwickelt Videosicherheitssoftware ausschließlich für den Einsatz in Hochsicherheitsbereichen und kritischen Infrastrukturen (KRITIS). Unsere Stärke ist, dass wir genau das in den Fokus unserer Entwicklungen stellen, was Hochsicherheitsanwender brauchen. Wir kennen die Herausforderungen dieser Kunden sehr genau, weil wir mit ihnen zusammenarbeiten. Diese Nähe zur Anwendungspraxis macht unsere Lösungen so präzise und zuverlässig – und unterscheidet uns deutlich von großen internationalen Anbieterplattformen.

Künstliche Intelligenz und Deep Learning sind in der Branche große Themen. Wie setzt IPS diese Technologien ein?

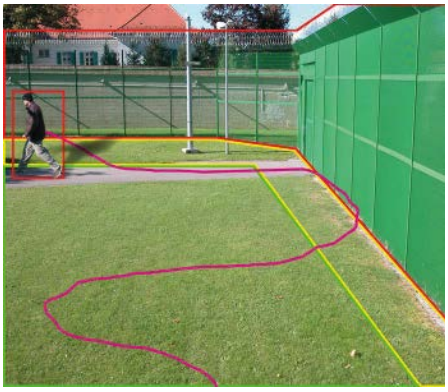
Peter Treutler: Wir setzen Künstliche Intelligenz – insbesondere Machine Learning und neuronale Netze – gezielt dort ein, wo sie echten Mehrwert bietet. Schon früh verhalfen Machine Learning basierte Klassifikatoren vor allem zur Unterdrückung unerwünschter Alarme. Bewegungen im Bild, wie z. B. vorbeiziehende Wolken, können gezielt identifiziert und aus der Alarmierung herausgefiltert werden.

Später haben wir begonnen, neuronale Netze zur Objekterkennung und Objektklassifikation einzusetzen, beispielsweise für Personen oder Fahrzeuge. In der aktuellen Generation unserer Videoanalyse nutzen wir



Der Deltaguard im Jahr 1970: Das System arbeitete mit einer auf den Bildschirm aufgeklebten Fotodiode, die Helligkeitsveränderungen im Videobild erkennen konnte.

IPS präsentierte sich 1974 auf der Security in Essen



Das IPS-3-Zonen-Konzept war in den 1990ern revolutionär und wird auch heute eingesetzt

KI dabei vor allem zur Alarmverifikation: Das bedeutet, dass unsere klassische, regelbasierte Analyse ein Ereignis erkennt, und die KI parallel prüft, ob es sich um ein relevantes Objekt – etwa eine Person – handelt.

Wir nutzen KI also als zusätzliche Schicht zur Absicherung – nicht als alleinige Entscheidungsinstanz. Denn gerade im sicherheitskritischen Umfeld, in dem wir mit unseren Produkten unterwegs sind, reichen rein KI-basierte Verfahren oft nicht aus. Zu viele Faktoren wie Tarnung, ungünstige Lichtverhältnisse oder komplexe Hintergründe können die Zuverlässigkeit beeinträchtigen. Deshalb vertrauen wir weiterhin auf unsere robuste klassische Videoanalyse, die durch KI intelligent ergänzt wird – nicht ersetzt.

Wo sehen Sie die Zukunft der intelligenten Videoanalyse in den nächsten fünf bis zehn Jahren?

Peter Treutler: In sicherheitskritischen Anwendungen bleibt Videotechnologie auch künftig unverzichtbar – besonders bei der lückenlosen Überwachung großer Perimeter. Drohnen und andere Roboter können die dauerhafte, flächendeckende Präsenz fest installierter Videosicherheitssysteme weder praktisch noch wirtschaftlich ersetzen.

Die Weiterentwicklung intelligenter Videoanalyse wird durch KI vorangetrieben – vor allem bei der Objektverifikation. Ziel ist es, echte Bedrohungen noch zuverlässiger von harmlosen Störfaktoren zu unterscheiden, unerwünschte Alarme zu reduzieren und die Systemzuverlässigkeit zu steigern.

Ein weiterer Trend ist die Anomalie-Erkennung: Systeme lernen, was „normal" ist, und melden Abweichungen – etwa bei Geisterfahrern oder Panikbewegungen. Im Perimeterschutz sehen wir diesen Ansatz jedoch kritisch, denn die Herausforderung bleibt: Sobald eine Anomalie erkannt wird, muss das System weiterhin genau klassifizieren und interpretieren können – ist das Objekt tatsächlich ein Mensch, der sich zudem verdächtig verhält, oder nur ein harmloses Tier? Die reine Anomalie-Erkennung ersetzt also nicht die präzise Objektanalyse.

Was können wir in den nächsten Jahren von IPS erwarten?

IPS NextGen-Produktfamilie des Jahres 2025 – nach wie vor made in Germany

Peter Treutler: In den nächsten Jahren dürfen unsere Kunden spürbare technologische Fortschritte erwarten – bei Leistung, Bedienbarkeit und Effizienz unserer Systeme. Ein zentrales Thema ist die IPS NextGen-Produktfamilie, die schrittweise unsere bisherige Systemgeneration ablösen wird. Der neue IPS NextGen Client bietet schon jetzt eine deutlich modernisierte, intuitivere und effizientere Benutzeroberfläche für Anwender und Techniker.

Parallel dazu entsteht mit der IPS NextGen VideoAnalytics eine modularisierte, ergänzend KI-gestützte Analyseplattform, die künftig alle bisherigen Module ersetzt. Ziel ist eine erheblich verbesserte Detektionsgenauigkeit, vor allem durch eine signifikante Reduktion unerwünschter Alarme – was unmittelbar zu einer Entlastung des Sicherheitspersonals führt.

Ein zukünftiger Meilenstein ist der in Entwicklung befindliche IPS NextGen VideoManager mit neuer Architektur und modernem Messaging-Konzept. Das System wird deutlich effizienter mit Ressourcen umgehen, sodass mehr Kameras und Analysen pro Server möglich werden – bei gleichzeitig geringerem Hardwareeinsatz. Cloudfunktionen wie Remote-Wartung und automatisiertes Patch-Management sind integrale Bestandteile.

Ein weiterer Fokus liegt auf der Optimierung unserer neuronalen Netze. Standard-KI stößt im sicherheitskritischen Umfeld schnell an Grenzen. Deshalb entwickeln wir spezialisierte Modelle, die auch unter extremen Bedingungen und in Hochsicherheitsbereichen zuverlässig detektieren. Auch die Vor-Ort-Unterstützung wird verbessert: Neue Tools und Assistenzfunktionen erleichtern Installation und Wartung – für effizienteres Arbeiten und minimale Ausfallzeiten. GIT

Securiton Deutschland
www.securiton.de

© Frogblue

Das Frogblue-Terminal S3 Plus B1 in Anthrazit

TITELTHEMA

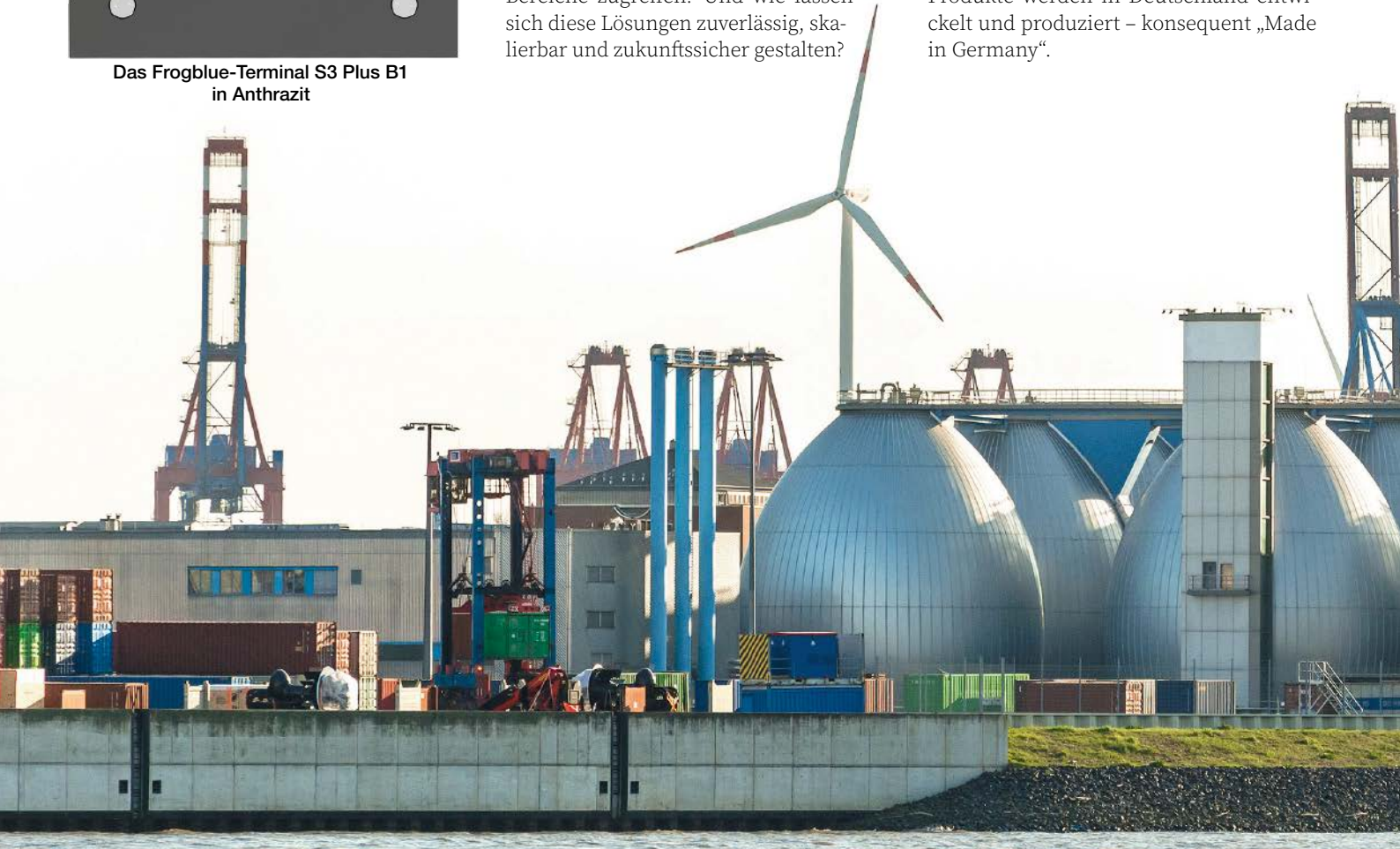
Die Zukunft ist dezentral

Zutrittskontrolle für kritische Infrastrukturen

Kritische Infrastrukturen stehen im Zentrum des gesellschaftlichen Lebens – sie sichern Energie, Wasser, Gesundheit, Finanzen, Verwaltung und vieles mehr. Sie alle eint: Schon ein einzelner unbefugter Zutritt kann weitreichende Folgen haben – von Betriebsunterbrechungen über Gefährdung von Menschen bis hin zu massiven wirtschaftlichen Schäden. KRITIS brauchen daher smarte Zutrittslösungen – wie die von Frogblue.

Die Spannbreite reicht von Strom- und Wasserversorgern über Justizvollzugsanstalten, Banken bis hin zu sensiblen Produktionsbereichen in Pharma, Chemie oder Hightech. Bei aller Verschiedenheit dieser Kritischen Infrastrukturen: die Anforderungen an die Zutrittskontrolle sind hoch: Wer darf wann und wie auf sicherheitsrelevante Bereiche zugreifen? Und wie lassen sich diese Lösungen zuverlässig, skalierbar und zukunftssicher gestalten?

Frogblue setzt mit seinem Frog-Terminal auf einen dezentralen Ansatz, das Zutritt und Türkommunikation realisiert und sich gemeinsam mit den „frogs“ genannten Frogblue-Modulen zu einer ganzheitlichen Gebäudesteuerung verbinden kann. Das Ganze ist nahtlos in bestehende Telekommunikationsstrukturen integrierbar. Alle Produkte werden in Deutschland entwickelt und produziert – konsequent „Made in Germany“.



KRITIS brauchen smarte Zutrittslösungen

Die Anforderungen an Zutrittssysteme steigen:

- Höchste Sicherheit bei gleichzeitiger Nutzerfreundlichkeit,
- Datensouveränität im europäischen Kontext,
- Flexibilität für Bestand und Neubau,
- Nachhaltigkeit durch den Wegfall von Steuerkabeln, Schaltschränken und die Reduzierung des Energiebedarfs.

Zentrale Steuerungen stoßen in diesem Umfeld oft an Grenzen – sie sind kostenintensiv, schwer skalierbar und im Ernstfall ein Single Point of Failure. Dezentrale Systeme hingegen bieten Redundanz, Robustheit und eine deutlich vereinfachte Nachrüstung.

Genau hier setzt das Frog-Terminal an. Es ist Teil einer dezentralen Architektur und kommuniziert per SIP/IP. Damit realisiert es Zutritt und Türkommunikation ohne zentrale Steuerung. Für die umfassende Gebäudesteuerung kommen zusätzlich die Frogs zum Einsatz – kleine, intelligente Steuerungseinheiten, die in Unterputzdosen installiert werden und via eigens entwickeltem, hochsicherem Bluetooth-Mesh Licht, Heizung, Jalousien oder Alarme verknüpfen. So können auch Bestandsgebäude – ob im Hochsicherheitsbereich einer Bank, in Haftanstalten oder in Produktionsstätten – nachgerüstet werden, mit minimalem Installationsaufwand und maximaler Sicherheit.

Anwendungsfelder in der Praxis

Die Praxis zeigt, wie unterschiedlich die Anforderungen sind:

- In Justizvollzugsanstalten muss Zutritt jederzeit nachvollziehbar und manipulationssicher sein – auch bei Strom- oder Netzwerkausfällen.

Das multifunktionale Frogblue-Modul frogDim1-3

- In Banken sind besonders Tresorräume und Wertbereiche zu schützen, wo Komfort keine Rolle, maximale Sicherheit aber Pflicht ist.
- In Pharma- und Chemieproduktion wiederum geht es darum, sensible Bereiche nur autorisiert zugänglich zu machen und die Nachvollziehbarkeit lückenlos zu dokumentieren – sei es aus Gründen regulatorischer Vorgaben, Qualitätskontrolle oder zum Schutz kritischer Prozesse.

Das Frog-Terminal eignet sich für alle diese Szenarien, weil es modular aufgebaut ist, verschiedene Authentifizierungsverfahren (PIN, RFID, Anruf, auch als Drei-Faktor-Authentifizierung) erlaubt und durch die dezentrale Architektur auch im Störungsfall zuverlässig weiterarbeitet.

Integration in bestehende Infrastrukturen

Ein entscheidender Vorteil für Betreiber kritischer Infrastrukturen: Frogblue-Lösungen lassen sich direkt in vorhandene Telekommunikations- und IT-Strukturen einbinden. Über den SIP-Standard kann das Frog-Terminal mit gängigen Cloud- und IP-Telefoniesystemen kommunizieren – von der Fritzbox über TK-Anlagen bis hin zu Cloud-basierten Lösungen. Dadurch wird Zutrittskontrolle nicht zu einer isolierten Insellösung, sondern fügt sich in die bereits bestehende Kommunikationsumgebung des Betreibers ein. Das spart Ressourcen, senkt Kosten und erleichtert den Betrieb.

Bitte umblättern ▶

KI, Nachhaltigkeit und europäische Souveränität

Neben klassischen Sicherheitsanforderungen rücken neue Themen in den Vordergrund:

- Künstliche Intelligenz kann helfen, Anomalien zu erkennen oder Videodaten effizient auszuwerten – ohne menschliche Überwachung rund um die Uhr. Entscheidend ist dabei, dass KI kein Selbstzweck ist, sondern messbaren Mehrwert bringt.
- Nachhaltigkeit bedeutet für Frogblue: keine Steuerkabel, kein Schaltschrank, weniger Materialeinsatz und ein minimaler Energiebedarf. Gerade in Bestandsgebäuden ist die Nachrüstung ohne aufwändige Verkabelung ein echter ökologischer und ökonomischer Vorteil.
- Europäische Datensouveränität: Frogblue setzt auf lokale Verarbeitung und verschlüsselte Kommunikation. Eine Cloud ist nicht notwendig – wenn die Frog Cloud genutzt wird, erfolgt das Hosting ausschließlich in einem Rechenzentrum in Deutschland. Für KRITIS-Betreiber ist das ein klares Sicherheits-Plus.

Sicher, zuverlässig, flexibel

Kritische Infrastrukturen verlangen nach Zutrittslösungen, die sicher, zuverlässig und flexibel sind. Das Frog-Terminal kann Zutritt und Türkommunikation in einem dezentralen Konzept verbinden – und sich nahtlos in vorhandene Telekommunikations- und IT-Strukturen integrieren.

Gemeinsam mit den Frogs kann zudem eine vollumfängliche Gebäudesteuerung ermöglicht werden. Dabei profitieren Betreiber von einem System, das vollständig in Deutschland entwickelt und produziert wird – ein klares Qualitätsversprechen „Made in Germany“. GIT

Frogblue
www.frogblue.com

Das Rückgrat unserer Gesellschaft

Gespräch mit Christian Heller, CSO von Frogblue

GIT SICHERHEIT: Herr Heller, warum ist Zutrittskontrolle gerade für kritische Infrastrukturen ein so zentrales Thema?

Christian Heller: KRITIS sind das Rückgrat unserer Gesellschaft. Angriffe – ob physisch oder digital – können enorme Auswirkungen haben. Daher muss Zutritt nicht nur sicher sein, sondern auch nachvollziehbar, transparent und flexibel erweiterbar. Gerade in Bereichen wie Energieversorgung, Banken, Justizvollzug oder Produktion ist es entscheidend, dass Systeme im Ernstfall nicht ausfallen. Dezentrale Lösungen sind dafür die beste Antwort.

Was unterscheidet Frogblue von klassischen, zentral gesteuerten Systemen?

Christian Heller: Wir setzen auf ein dezentrales Konzept. Es gibt keinen zentralen Server – Teilausfälle einzelner Komponenten beeinträchtigen die Kommunikation des Gesamtsystems nicht. Gleichzeitig ist die Installation einfach: keine Steuerleitungen, schnelle Inbetriebnahme, modular erweiterbar und mit der Möglichkeit, Alt- oder Fremdgeräte unkompliziert auszutauschen.

Welche Rolle spielt die Integration in bestehende Telekommunikationsstrukturen?

Christian Heller: Viele Betreiber haben längst IP-Telefonie im Einsatz – sei es mit einer Fritzbox, einer Zentrale- oder Cloud-TK-Lösung. Unser Frog-Terminal kann direkt dort eingebunden werden. Das macht die Integration nicht nur einfacher, sondern auch zukunftssicher. SIP ist der Standard, der uns die volle Flexibilität gibt.

Wohin entwickelt sich die Zutrittskontrolle in den kommenden Jahren?

Christian Heller: Die Zukunft wird bestimmt von drei Trends: Drahtlose Systeme, Datensouveränität und Nachhaltigkeit. KI und Datenanalyse werden hinzukommen, aber der Kern bleibt: Zutrittslösungen müssen sicher, komfortabel und upgradefähig sein. Wir müssen Systeme schaffen, die sich an neue Anforderungen anpassen – ohne dass gleich die gesamte Infrastruktur getauscht werden muss.

Unsere Vision ist klar: Wir wollen Zutrittskontrolle, Gebäudesteuerung und Kommunikation zusammenführen – in einem dezentralen, offenen System. Für KRITIS-Betreiber bedeutet das: maximale Sicherheit, nahtlose Integration und langfristige Investitionssicherheit.

BKS auf der SicherheitsExpo Berlin 2025

Zur SicherheitsExpo Berlin 2025 zeigt die BKS GmbH ihr umfassendes Portfolio an mechanischen und elektronischen Zutrittskontrolllösungen sowie das offene Gebäudemanagementsystem Gemos. Neue Apps, flexible Schließsysteme und modulare Lösungen ebnen den Weg für modernstes Zutrittsmanagement.

BKS positioniert sich auf der erstmals stattfindenden SicherheitsExpo in Berlin als ganzheitlicher Lösungsanbieter für moderne Zutrittskontrolle und intelligentes Gebäudemanagement. Der Fokus bei den präsentierten Zutrittskontrollsystemen liegt auf dem elektronischen Schließsystem Ixalo, das sich flexibel auf verschiedene Sicherheitsniveaus und Anwendungsszenarien zuschneiden lässt. Die digitalen Schließzylinder und Beschläge ermöglichen eine zentrale Verwaltung aller Zugangsrechte und eignen sich ideal für Unternehmen, öffentliche Einrichtungen, Industrieanlagen, Hotels und Privathäuser.

Mit der Ixalo | key App wird das Smartphone zum digitalen Schlüssel. Zutrittsrechte lassen sich bequem über den BKS KeyManager verwalten – ganz ohne Übergabe physischer Identmedien.

Speziell für kleinere Objekte wie Praxen, Kanzleien oder Einfamilienhäuser bietet die BKS | smart App eine intuitive, cloudbasierte Lösung zur Verwaltung von bis zu 25 Türen und 100 Nutzern. Die Kommunikation wird verschlüsselt realisiert, die Bedienung ist auch ohne technische Vorkenntnisse problemlos möglich.

Mit BKS | hotel stellt BKS zudem ein Zutrittskonzept für Hotels vor, das nicht nur Gästen mehr Komfort bietet, sondern auch die Arbeit an der Rezeption vereinfacht: Durch die Anbindung an eine möglicherweise bereits bestehenden Hotelreservierungssoftware lassen sich Zutrittsrechte mit wenigen Klicks vergeben und Gästekarten automatisch erstellen. Auch separate Bereiche wie Parkplätze oder Fitnessbereiche lassen sich mit BKS | hotel flexibel verwalten.

Neben digitalen Lösungen zeigt BKS auf der SicherheitsExpo Berlin zudem sein umfangreiches Portfolio in den Bereichen Schloss- und Beschlagtechnik sowie mechanischen und mechatronischen Schließsystemen: Von hochfesten Einsteckschlössern für Holz-, Stahl- und Rohrrahmentüren über klassische mechanische Zylinder bis hin zu innovativen mechatronischen Schlössern.

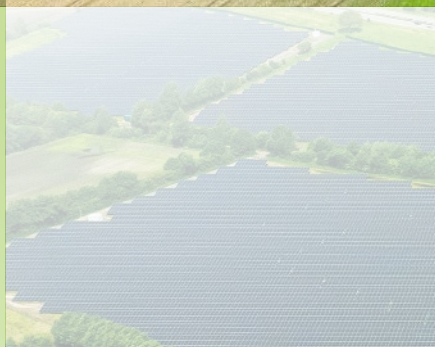
SicherheitsExpo Berlin: Halle 7, Stand B08 | www.g-u.com/de

SCHLIESSTECHNIK

Geschlossen in die Energiewende

Intelligente Schließtechnik für Photovoltaik-Parks von Nord bis Süd

Ein immer größerer Anteil des deutschen Strom-Mixes stammt aus erneuerbaren Energien und der Ausbau der Photovoltaik hat hieran entscheidenden Anteil. Mit der Solarleistung steigt auch die Bedeutung dieser Anlagen für eine versorgungssichere Energieinfrastruktur. Das Hamburger Photovoltaik-Unternehmen Greentech setzt bei der Sicherung von sechs Anlagen in Nord- und Süddeutschland auf das elektronische Schließsystem eCliq der Marke Ikon von Assa Abloy.



Erneuerbare Energien erzeugten im Mai 2025 rund zwei Drittel des in Deutschland produzierten Stroms – ein bisheriger Höchstwert. Laut Angaben der Denkfabrik Agora Energiewende trug dabei allein die Photovoltaik (PV) 29 Prozent bei und lieferte damit mehr Strom als alle fossilen Kraftwerke zusammen. Mit einer installierten Leistung von rund 100 Gigawatt (GW) stellen PV-Anlagen somit schon heute einen unverzichtbaren Baustein der Energieversorgung dar. Das Ziel für den PV-Ausbau in Deutschland liegt jedoch noch höher. Bis zum Jahr 2030 sollen 215 GW erreicht werden.

Großdimensionierte Projekte von Nord bis Süd

Diesen ambitionierten Ausbauzielen leisten auch Solar- und Speicher-Spezialisten wie Greentech durch zahlreiche Projekte Vorschub. Das im Jahr 2008 gegründete Hamburger Unternehmen zählt heute zu den namhaften Anbietern für den Betrieb von PV-Kraftwerken in Europa und verantwortet von der Projektentwicklung, der Planung und dem Anlagenbau sowie technischem und kaufmännischem Asset-Management weitere Leistungen in den Bereichen Engineering, technische Beratung, Finanzierung und Stromvermarktung.

Zuletzt gingen im Juni 2024 im Landkreis Steinburg drei Solarparks von Greentech ans Netz. Zusammen erreichen die Anlagen eine Gesamtkapazität von über 100 MWp (Megawatt Peak) und repräsentieren damit das bislang größte Portfolio des Solar- und Speicher-Spezialisten. Mit der kleinsten Installation in Nienbüttel nahe dem durch sein Open-Air-Festival bekannten Wacken erreicht Greentech mit 32.580 bifazialen Solarmodulen, verteilt auf einer Fläche von rund 17 Hektar, eine maximale Leistungskapazität von 21,45 MWp. Auch im Süden Deutschlands treibt das Unternehmen den Ausbau der Kapazitäten mit insgesamt drei Anlagen in Großheirath und Untersiemau voran.

Kritische Infrastruktur erfordert umfassenden Schutz

Mit der zunehmenden Bedeutung von Photovoltaik-Anlagen wächst jedoch auch das Risiko, dass diese zu potenziellen Zielen für Sabotage, Vandalismus oder Diebstahl werden. Der jüngste Verfassungsschutzbericht und Warnungen des BSI vor hybriden Bedrohungsszenarien machen deutlich: Digitale Sicherheit allein reicht nicht mehr aus.

Solarparks wie die von Greentech in Nienbüttel betriebene Anlage werden meist auf der „grünen Wiese“ errichtet. Die exponierte Lage und differenzierte Zugangsberechtigungen erfordern ein leistungsfähiges Schließsystem wie eCLIQ, das auch die dezentrale Verwaltung mehrerer Standorte erlaubt

Für Betreiber von Photovoltaik-Anlagen bedeutet dies die Notwendigkeit, neben der Cybersicherheit auch für umfassenden physischen Schutz vor unerlaubtem Zutritt und Manipulation zu sorgen. Die großflächigen und oft abgelegenen Solarparks stellen dabei besondere Anforderungen. Nicht zuletzt erfordern die Betriebsabläufe mit unterschiedlichen Serviceteams und Wartungsfirmen differenzierte Zugangsberechtigungen zu unterschiedlichen Anlagenbereichen.

Dezentrale Anlagen, zentrale Verwaltung

Auf der Suche nach einer geeigneten Schließlösung für diese Anforderungen, fiel die Wahl auf die Cliq-Technologie von Assa Abloy. Das System lässt sich flexibel erweitern, kombinieren oder nachrüsten und ist damit wie gemacht für den Anwendungsfall. Ein entscheidender Vorteil liegt in der wartungsarmen Konzeption. Anders als herkömmliche elektronische Schließzylinder benötigt eCliq keine regelmäßigen Batteriewechsel vor Ort. Energieversorgung und Datenübertragung erfolgen direkt über den Schlüssel beziehungsweise Programmierschlüssel. Dies bedeutet Kosteneinsparungen bei der Wartung.

Ebenso effizient gestaltet sich die Programmierung und Verwaltung des elektronischen Schließsystems. Zugangsrechte lassen sich individuell steuern und bei Bedarf zentral anpassen. Im Fall eines Schlüsselverlusts kann die betreffende Schließberechtigung gezielt aus dem System entfernt werden, ohne dass andere Zugänge betroffen sind. Diese Flexibilität ist entscheidend, wenn verschiedene Personen differenzierten Zugang zu unterschiedlichen Anlagenbereichen benötigen.

© Assa Abloy

Das elektronische Schließsystem eCLIQ bietet hohen Schutz gegen Manipulation und intelligente Angriffe. Es eignet sich daher besonders als Teil eines ganzheitlichen Sicherheitskonzepts, das sowohl die physische Resilienz als auch die Cybersicherheit berücksichtigt

Verlässlicher Partner für Beratung und Einbau

Bei der Umsetzung des Sicherheitskonzepts setzte Greentech auf die Expertise von Wilhelm Albers Hamburg. Das traditionsreiche Unternehmen übernahm nicht nur die umfassende Beratung zur Systemauswahl, sondern auch die fachgerechte Installation der Komponenten. Mit jahrzehntelanger Erfahrung im Bereich professioneller Sicherheitslösungen und einem breiten Portfolio rund um elektronische Zutrittssysteme zählt Wilhelm Albers Hamburg zu den führenden Fachhändlern und Servicepartnern im norddeutschen Raum.

Die Vorzüge des eCliq-Systems erweisen sich als entscheidende Vorteile für eine langfristige Betriebsstrategie. Die bislang gesammelten positiven Erfahrungen lassen die Verantwortlichen bei Greentech daher bereits über eine mögliche Ausweitung des Einsatzes nachdenken: „Die große Flexibilität, die hohe Sicherheit sowie die langfristig gut planbaren und vergleichsweise geringen Kosten des Systems haben uns überzeugt. Wir planen daher eCliq auch in weiteren Anlagen einzusetzen“, erklärt Max Langkabel, Team Lead Power Plant IT & ICS von Greentech. GIT

Assa Abloy Sicherheitstechnik
www.assaabloy.com/de

Francis Cepero, CEO Primion

ZUTRITT

Brückenschlag am Wendepunkt

Strategische Neuausrichtung bei Primion: CEO Francis Cepero über KI, OT/IT-Konvergenz und regulatorische Anforderungen

Unter dem strategischen Leitbild „Prevent, Protect, Preserve“ will Primion die Technologieführerschaft ausbauen – u. a. durch Stärkung der Kundenbeziehungen und den Ausbau der internationalen Präsenz. Die F&E-Investitionen wurden hochgefahren, im Fokus stehen u. a. KI und OT/IT-Konvergenz sowie Zero Trust Security. Primion-CEO Francis Cepero spricht mit GIT SICHERHEIT über die Hintergründe.

GIT SICHERHEIT: Herr Cepero, Sie sind seit Juli vergangenen Jahres CEO bei Primion Technology und leiten auch die Tochtergesellschaft Opertis. Sie sind mit dem Anspruch angetreten, Primion im globalen Sicherheitsmarkt erfolgreich zu platzieren und neue Anteile zu gewinnen. Können Sie schon mal eine persönliche Zwischenbilanz ziehen?

Francis Cepero: Ja, sehr gern. Nach rund neun Monaten kann ich sagen: Es war ein sehr intensiver und spannender Start. Wir haben begonnen, zentrale strategische Weichenstellungen vorzunehmen. Besonders wichtig war mir, alle Stakeholder – Mitarbeitende, Kunden, Partner – in diesen Prozess aktiv einzubinden. Gemeinsam haben wir eine klare Vision entwickelt und erste operative Maßnahmen auf den Weg gebracht, etwa im Bereich Innovation, Internationalisierung und Kundenorientierung. Unsere Position im Markt ist stark, aber wir haben auch noch viele Potenziale, die wir vorantreiben wollen. Die Resonanz auf unseren Kurs – intern wie extern – ist sehr positiv. Das stimmt mich optimistisch für die nächsten Schritte.

Ihre Vision für die Weiterentwicklung von Primion überschreiben Sie mit den Begriffen „Prevent, Protect, Preserve“. Sie möchten weltweit bevorzugter Lösungspartner für integrierte Sicherheits- und Zeitwirtschaftslösungen werden und dabei Maßstäbe setzen und sogar die Richtung der Branche vorgeben. Könnten Sie das bitte etwas näher ausführen? Welche konkreten Ziele haben Sie sich insoweit auf mittlere und lange Sicht gesetzt?

Francis Cepero: „Prevent, Protect, Preserve“ ist mehr als ein Slogan – es ist unser strategisches Leitbild. „Prevent“ steht für vorausschauende Risikoanalyse und präventive Schutzmaßnahmen. „Protect“ meint den aktiven Schutz von Menschen, Daten und Infrastruktur. Und „Preserve“ umfasst die dauerhafte Sicherung von Prozessen und Ressourcen.

Wir möchten als Innovationsführer agieren, nicht nur reagieren. Mittelfristig heißt das: Der Ausbau unserer Technologieführerschaft, insbesondere durch den intelligenten Einsatz von KI, den Ausbau unserer internationalen Präsenz sowie die kontinuierliche Stärkung der Kundenbeziehungen. Langfristig streben wir an, neue Standards für vernetzte Sicherheitstechnologien zu setzen – in Europa und darüber hinaus.

Lassen Sie uns etwas genauer auf Ihre Lösungen schauen. Wenn Sie über Lösungen sprechen, dann meinen Sie vor allem maßgeschneiderte Lösungen in komplexen Umfeldern. Dabei pflegen Sie auf Langfristigkeit angelegte Kundenbeziehungen. Wie sieht das in der Praxis aus – vielleicht geben Sie uns das eine oder andere Beispiel?

Francis Cepero: Ein gutes Beispiel ist unsere langjährige Zusammenarbeit mit einem großen internationalen Forschungszentrum. Dort haben wir ein ganzheitliches Sicherheitskonzept implementiert, das Zutrittskontrolle, Besuchermanagement, Fluchtwegesteuerung und Zeiterfassung umfasst – abgestimmt auf hochsensible Arbeitsbereiche. Wir arbeiten mit unseren Kunden oft über viele Jahre zusammen, begleiten sie durch mehrere Entwicklungsstufen und passen die Systeme kontinuierlich an neue Anforderungen an. Unsere Lösungen sind also nie von der Stange, sondern immer das Ergebnis intensiver Analyse, Beratung und Integration.

Können Sie uns das auch noch mal am Beispiel des Workforce-Managements anschaulich machen?

Francis Cepero: Workforce Management ist heute viel mehr als nur Zeiterfassung. Es geht um die intelligente Planung und Steuerung von Personalressourcen – unter Berücksichtigung von Arbeitszeitgesetzen, Tarifverträgen und betrieblichen Anforderungen. Bei einem internationalen Industriekunden haben wir beispielsweise eine Lösung realisiert, die nicht nur die An- und Abwesenheitszeiten erfasst, sondern auch die Urlaubsplanung, das Schichtmanagement und die Integration in ERP, Payroll, und HR-Systeme Dritter ermöglicht. Das verbessert die Effizienz und schafft Transparenz für Mitarbeitende und Management gleichermaßen.

Wenn wir auf die Entwicklung des Marktes für Sicherheitslösungen schauen, dann sehen wir eine zunehmende Integration vormals eher getrennter Welten – also IT und OT sowie die klassische physische Sicherheit. Das liegt wegen der dadurch erreichbaren erhöhten Effektivität und Effizienz von Sicherheitsstrategien auch nahe.

Wo stehen wir heute, was diese Entwicklung betrifft?

Francis Cepero: Wir stehen an einem Wendepunkt. Die Grenzen zwischen IT-Sicherheit, physischer Sicherheit und Operational Technology verschwimmen. Viele Organisationen haben erkannt, dass eine ganzheitliche Sicherheitsstrategie nur funktionieren kann, wenn alle Bereiche zusammen gedacht und gesteuert werden. Allerdings stehen wir alle noch am Anfang, was die operative Integration betrifft, sowohl technisch als auch organisatorisch. Hier setzen wir als Primion mit unseren modularen und integrativen Plattformlösungen an, die genau diese Brücke schlagen.

Wenn dies also ein starker Treiber der Entwicklung ist, könnten Sie einmal näher erläutern, wie dies für die Lösungen aus Ihrem Hause wirksam wird? Die traditionellen Schwerpunkte bei Primion liegen bei Zutrittskontrolle und Zeiterfassung. Dazu kommen die integrierten Sicherheitslösungen, sodass Sie beispielsweise auch Rettungswegetechnik und Videoüberwachung integrieren können?

Francis Cepero: Genau. Unsere Lösungen basieren auf offenen, modularen Architekturen. Das ermöglicht nicht nur die Einbindung klassischer Zutritts- und Zeitwirtschaftskomponenten, sondern auch von Brandmeldeanlagen, Videoüberwachung, Fluchtwegsicherung oder Aufzugsteuerung – alles über eine zentrale Plattform steuerbar. Wichtig ist dabei die Interoperabilität mit IT- und OT-Systemen. So können etwa sicherheitsrelevante Informationen direkt an zentrale Leitsysteme übermittelt und dort mit weiteren Daten verknüpft werden. Das erhöht die Reaktionsgeschwindigkeit und die Sicherheit signifikant.

Wie weit kommt bei Ihren Projekten die Operational Technology ins Spiel, also die Integration von prozessualen Steuerungssystemen?

Francis Cepero: Operational Technology spielt eine zunehmend wichtige Rolle. Bei kritischen Infrastrukturen etwa müssen Zutritt und Anlagensteuerung eng verzahnt sein; etwa, um sicherzustellen, dass nur autorisiertes Personal in bestimmte Steuerungsbereiche gelangt oder dass sicherheitskritische Prozesse automatisch ausgelöst werden. Ein Beispiel: In einem Industrieunternehmen wurde unsere Zutrittslösung mit dem Produktionsleitsystem gekoppelt – so wird der Zugang zu Maschinen auch durch Schulungsnachweise oder Sicherheitsunterweisungen gesteuert. Das ist gelebte IT/OT-Konvergenz.

Geben Sie uns ein paar praktische Beispiele anhand von aktuellen Projekten?

Francis Cepero:. Aktuell realisieren wir für einen Energieversorger eine umfassende Zutritts- und Sicherheitslösung, bei der auch die Anbindung an OT-Systeme erfolgt, etwa zur Steuerung von Umspannwerken. Parallel arbeiten wir mit einem globalen Logistikunternehmen an einem Projekt, bei dem unsere Workforce-Management-Lösung mit Zutritts- und Videodaten kombiniert wird, um sicherheitskritische Abläufe zu analysieren und zu optimieren. Solche Projekte zeigen, wie integrierte Sicherheitslösungen einen echten Mehrwert schaffen.

Ein weiterer, freilich überragender, Trend, der Wirtschaft und Gesellschaft ja insgesamt derzeit beschäftigt, ist die Künstliche Intelligenz. Was bedeutet das aus Ihrer Sicht für Sicherheitslösungen an sich und was verändert sie in Ihrem Unternehmen?

Francis Cepero: Künstliche Intelligenz wird die Sicherheitsbranche tiefgreifend verändern. Wir sehen bereits heute KI-basierte Systeme, die Muster in Zutrittsverhalten erkennen oder Videoüberwachungsdaten intelligent auswerten. Zum Beispiel zur Erkennung verdächtiger Bewegungsmuster.

Bei Primion investieren wir gezielt in KI-Forschung, etwa im Bereich Anomalie-Erkennung und vorausschauender Wartung. Gleichzeitig arbeiten wir an ethischen und regulatorischen Leitlinien, denn der verantwortungsvolle Einsatz von KI ist für uns ebenso wichtig wie die technische Exzellenz.

Herr Cepero, eine regelrechte Technologieoffensive ist Teil eines strategischen Maßnahmenpakets, das Sie beschlossen haben. Das bedeutet wohl, dass Sie personell und finanziell in Forschung und Entwicklung investieren? Geben Sie uns einen näheren Eindruck?

Francis Cepero: Wir haben die Investitionen in F&E deutlich erhöht, sowohl personell als auch technologisch. Dabei setzen wir bewusst auf agile Teams, die interdisziplinär arbeiten. Wir haben neue Innovationsprojekte aufgebaut und die Zusammenarbeit mit Experten intensiviert. Zudem legen wir großen Wert auf ein Innovationsklima, das Kreativität und Experimentierfreude fördert. Unsere Roadmap umfasst neben KI und OT/IT-Konvergenz auch weitere spannende Themen wie zum Beipsiel die Zero Trust Security und Green Security.

Dabei arbeiten Sie auch mit Universitäten und anderen Technologiepartnern zusammen. Können Sie das eine oder andere Beispiel dafür nennen, woran Sie hier arbeiten?

Francis Cepero: Ein aktuelles Beispiel sind unsere Projekte im Bereich KI und Machine Learning. Gemeinsam entwickeln wir Modelle zur intelligenten Zutrittsanalyse – also Systeme, die nicht nur erfassen, wer wann wo war, sondern auch erkennen, ob das Verhalten regelkonform war oder ob es Hinweise auf Sicherheitsrisiken gibt. Auch das Thema sichere Integration von Gebäudetechnik in hybride Sicherheitsarchitekturen steht auf unserer Agenda. Sie sehen – es tut sich viel!

Sie möchten in Ihrem Kernmarkt Europa weiter expandieren. Was ist hier der Stand und was planen Sie diesbezüglich in nächster Zeit?

Francis Cepero: Unsere internationale Präsenz ist solide, aber wir sehen weitere Wachstumsmöglichkeiten. In Europa wollen wir unsere Position weiter stärken, unter anderem durch gezielte Partnerschaften. Auch in weiteren Ländern prüfen wir Markteintritte gemeinsam mit lokalen Partnern, um kulturelle und regulatorische Unterschiede bestmöglich zu adressieren. Unser Ziel ist es, in allen Regionen mit Lösungen zu überzeugen, die an die jeweiligen Marktanforderungen angepasst sind.

In der EU stehen – verstärkt durch Verschiebungen der geopolitischen Lage – das KRITIS-Dachgesetz und NIS 2, respektive die zugrundeliegenden Richtlinien im Zentrum der Aufmerksamkeit. Wird dies für Ihr Segment beflügelnde Wirkungen haben?

Francis Cepero: Definitiv. Die neue Gesetzgebung schärft das Bewusstsein für Sicherheitsrisiken und erhöht die Anforderungen an Unternehmen, insbesondere im Bereich kritischer Infrastrukturen. Für uns bedeutet das: mehr Verantwortung, aber auch mehr Nachfrage nach integrierten und anpassbaren Sicherheitslösungen. Unsere Systeme sind bereits heute so konzipiert, dass sie regulatorische Anforderungen flexibel abbilden können. Wir beraten unsere Kunden aktiv, wie sie NIS 2 und das KRITIS-Dachgesetz umsetzen können – technologisch und organisatorisch. GIT

Primion Technology GmbH
www.primion.io

SENSORTECHNIK

Auf dem Weg zu einem neuen Goldstandard

Sicherung von Umspannwerken mit moderner LiDAR-basierter 3D-Überwachung

Als Teil des Eon-Konzerns liefert EG.D Strom an 2,7 Millionen Menschen in den südlichen Regionen der Tschechischen Republik, an der Grenze zu Österreich und Deutschland. Das Unternehmen betreibt und unterhält Infrastrukturen wie Stromleitungen und Umspannwerke. Es wollte herausfinden, wie volumetrische Detektion in Verbindung mit LiDAR-Technologie eingesetzt werden kann, um die physische Sicherheit seiner Umspannwerke zu verbessern. Dafür entschied sich das Unternehmen für HxGN dC3 LidarVision von Hexagon.

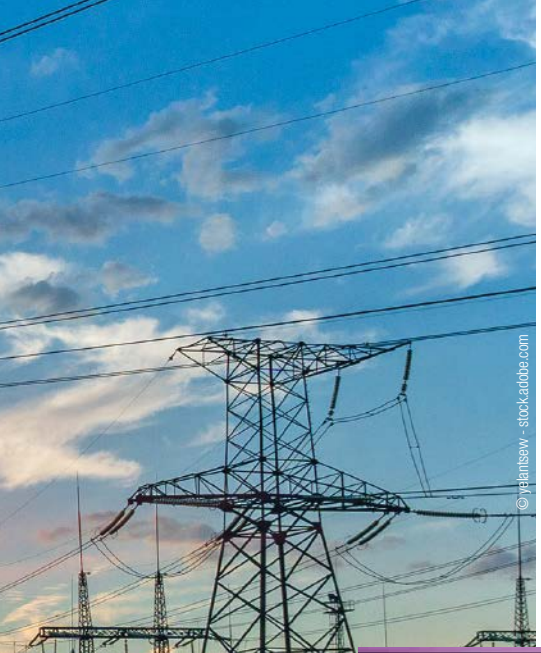
Nach Angaben der Internationalen Energieagentur (IEA) wird der weltweite Stromverbrauch im Jahr 2024 fast doppelt so stark ansteigen wie im Jahresdurchschnitt der vergangenen zehn Jahre. Gleichzeitig werden neue Vorschriften wie die Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen (CER), die im Juli 2026 in allen Mitgliedstaaten der Europäischen Union in Kraft treten wird, und das deutsche KRITIS-Dachgesetz eingeführt. Ihr Ziel ist es, Organisationen, die für nationale kritische Infrastruktur verantwortlich sind, dabei zu unterstützen, ihre Resilienz gegenüber bestehenden und zukünftigen Bedrohungen nachhaltig zu gewährleisten.

EG.D, ein langjähriger Kunde von Hexagon, wollte herausfinden, wie volumetrische Detektion in Verbindung mit LiDAR-Technologie eingesetzt werden kann, um die physische Sicherheit seiner Umspannwerke zu verbessern. Zu diesem Zweck entschied sich das Unternehmen für HxGN dC3 LidarVision von Hexagon.

Widerstandsfähigkeit gewährleisten

Für Energieversorger sind Umspannwerke ein wesentlicher Bestandteil des Energienetzes, da sie den Strom sicher und zuverlässig mit der richtigen Spannung an Abnehmer wie Haushalte, Unternehmen, Schulen oder Krankenhäuser übertragen. Größere Zwischenfälle in Umspannwerken sind aufgrund der strengen Überwachungs-, Wartungs-, Sicherheits- und Schutzmaßnahmen selten. Wenn es jedoch zu einer solchen Situation kommt, kann sie erhebliche Probleme verursachen. Dies wurde zum Beispiel Anfang 2025 deutlich, als ein Brand in einem Umspannwerk im Vereinigten Königreich die Stromversorgung von 5.000 Haushalten unterbrach und den Betrieb an einem großen internationalen Flughafen beeinträchtigte.

Bis vor kurzem beruhte die Sicherung unbemannter Umspannwerke vorwiegend auf traditionellen Ansätzen des Perimeterschutzes. Dazu gehören Zäune (in der Regel aus Stahl und ausgestattet mit passiven Infrarotsensoren), Einbruchmeldesysteme, Videoüberwachung sowie Zugangskontrollsysteme, die durch Karten oder biometrische Verfahren den autorisierten Zugang regeln. EG.D beschloss jedoch, ein Pilot-



LiDAR-Technologie im Einsatz zur Sicherung eines Umspannwerks

projekt in Angriff zu nehmen, um die Möglichkeiten der neuesten LiDAR-basierten 3D-Überwachungstechnologie zu testen.

Pilotprojekt für mehr Sicherheit

Tomáš Sofka, zuständig für Sicherheitstechnik bei EG.D, erklärt: „Wir arbeiten seit vielen Jahren mit Hexagon im Bereich GIS zusammen und waren besonders von den innovativen Lösungen im Bereich der volumetrischen Erkennung und der LiDAR-Technologie beeindruckt. Wir wollten prüfen, wie die Technologie eingesetzt werden kann, um die Sicherheit zu erhöhen, um Unbefugte vom Betreten von Umspannwerken abzuhalten, Eindringlinge zu lokalisieren und den Schutz des Wartungspersonals zu verbessern, während es vor Ort in der Nähe von Hochspannungsanlagen arbeitet."

Auf Basis dieser Anforderungen hat sich EG.D für HxGN dC3 LidarVision entschieden. Die fortschrittliche 3D-Überwachungssoftware basiert auf volumetrischer Detektionstechnologie und wurde entwickelt, um ganze Standorte zu sichern – im Gegensatz zu herkömmlichen Perimeterschutzsystemen, die sich meist nur auf die Zaunlinie konzentrieren.

Im Projekt kommen fünf strategisch platzierte LiDAR-Sensoren zum Einsatz, welche die Einrichtung von sicheren und sterilen virtuellen Zonen ermöglichen und auch den Zaun abdecken. Entscheidend ist, dass diese Zonen per Mausklick ein- und ausgeschaltet oder bearbeitet werden können. Wenn zum Beispiel Wartungsarbeiten durchgeführt werden, kann der Bereich, in dem die Arbeiten stattfinden, deaktiviert werden. In der Zwischenzeit bleiben andere Bereiche aktiv, um zu verhindern, dass sich Arbeiter in einen nicht freigegebenen oder potenziell gefährlichen Bereich begeben.

Autorisiertes Personal und Unbefugte können zudem in Echtzeit im EG.D-Sicherheitsleitstand überwacht und verfolgt werden. Das System erkennt die Anzahl der Personen und ihre genauen Positionen, zusammen mit ihren Geschwindigkeiten und Bewegungsrichtungen (wenn sie gehen oder laufen) und sogar ihre voraussichtlichen Laufwege. Zusätzliche Informationen können durch PTZ-Kameras oder Alarmsysteme ergänzt werden und Lautsprechersysteme auf dem Gelände ermöglichen die Kommunikation mit den betreffenden Personen.

Ein weiterer wesentlicher Vorteil eines solchen Systems ist die Möglichkeit, für jedes Umspannwerk einen digitalen Zwilling zu erstellen. Auf diese Weise können mögliche Bedrohungsszenarien virtuell durchgespielt werden, um die Wirksamkeit und Zuverlässigkeit von Sicherheitsmaßnahmen zu testen. Im Wesentlichen wird eine 3D-Darstellung der gesamten Anlage erstellt, mit der Benutzer interagieren können. Auf diese Weise kann die Positionierung von LiDAR-Sensoren und Kameras optimiert werden, um potenzielle tote Winkel oder schlechte Sichtwinkel zu eliminieren, bevor jemand die Anlage betritt.

Das System kann durch Wärmesensoren und Kameras erweitert werden, die die Temperatur in bestimmten Bereichen überwachen und einen Alarm auslösen, wenn sie von der Norm abweicht. Dies hilft bei der Detektion von Eindringlingen (Menschen oder Tiere) sowie bei der frühzeitigen Erkennung von Feuer, noch bevor ein Brandherd zu sehen ist.

Ein neuer Standard, der weltweit Beachtung findet

„Die Zusammenarbeit war in allen Phasen des Projekts beispielhaft und professionell," so Sofka. „Die Reaktion des Managementteams auf den Pilotbetrieb war überwältigend positiv, und wir können Hexagon anderen Organisationen nur empfehlen."

Angesichts des Erfolgs des Pilotprojekts entwickeln EG.D und Hexagon gemeinsam einen Plan zur Einführung von HxGN dC3 LidarVision in weiteren Energieanlagen des Netzes. Das Unternehmen gibt sein Wissen auch aktiv an andere Energieversorger z. B. in den USA und im asiatisch-pazifischen Raum weiter, die diesen neuen Ansatz als möglichen Goldstandard für die Sicherheit von Umspannwerken in Erwägung ziehen. GIT

Hexagon
www.hexagon.com

Digitale Sicherheitslösungen unterstützen Unternehmen bei der Einhaltung von Normen, Richtlinien und Gesetzen, auch im Bereich Kritischer Infrastruktur

ZUTRITT

Digitales Plus

Elektronische Sicherheitslösungen für Unternehmen

Mit elektronischer Sicherheitstechnik heben Unternehmen ihr Sicherheitskonzept auf das nächste Level. Funktionen wie digitale Überwachung, automatische Alarmierung oder zentrale Verwaltung sind eine optimale Ergänzung zu mechanischen oder mechatronischen Vorrichtungen. Das sehen auch Polizei und Versicherungen so. Das Portfolio von Telenot deckt all diese Themen ab – einschließlich Planung, Installation und Wartung.

Stehen Unternehmen vor der Aufgabe, ihre Sicherheitsarchitektur zu verbessern, ist die Erweiterung ihrer mechanischen oder mechatronischen Schutzvorrichtungen um elektronische Lösungen ein zentraler Baustein. Nicht nur, weil digitale Sicherheitstechnik inzwischen „State of the Art“ ist, sondern vor allem, weil viele Versicherungen erst dann einen vollen Schutz im Schadensfall gewährleisten. Auch bei der Polizei gilt die Kombination aus mechanischen und elektronischen Sicherheitssystemen als Optimum, um Schäden durch Einbruch, Überfall, Brand oder andere Gefahren vorzubeugen.

Plus an Sicherheit durch digitale Technik

Elektronische Einbruchmeldeanlagen, Zutrittskontrollsysteme oder Brandmeldeanlagen erweitern und verbessern die Sicherheit in Unternehmen und Behörden. Gleichzeitig sind sie aufgrund ihrer technologiebedingten Anpassungsfähigkeit eine langfristig gut angelegte Investition. Das heißt, mit digitaler Technologie stellen sich große wie kleine Unternehmen sicherheitstechnisch zukunftsorientiert auf – beispielsweise mit dem Hersteller Telenot. Dann können sie die folgenden Vorteile moderner Zutritts-, Alarm- und Brandmeldesysteme voll ausschöpfen.

Überwachung und Kontrolle in Echtzeit

Eine moderne elektronische Gefahrenmeldezentrale erlaubt die Überwachung von Gebäuden in Echtzeit, beispielsweise mit Bewegungsmeldern, Magnetkontakten und Glasbruchmeldern. Das beschleunigt die Reaktionszeiten bei einem Sicherheitsvorfall. Insbesondere dann, wenn der Alarm über eine lückenlos vernetzte Meldekette bis in die zuständige Sicherheitszentrale übertragen wird und das Personal dort sofortige Gegenmaßnahmen ergreift. Auch individuelle Zugangsberechtigungen lassen sich heute flexibel in Echtzeit erteilen oder entziehen, einfach per elektronischer Zutrittskontrollanlage. Werden Einbruchmeldesystem und Zutrittskontrollsystem dazu noch digital miteinander vernetzt, bekommen Verantwortliche eine Sicherheitskontrolle, die analoge Technik weit übertrifft.

Zeit- und Ressourcenersparnis in der Verwaltung

Viele Standorte, häufig wechselndes Personal oder viele externe Lieferanten sind mit digitalen Sicherheitslösungen kein Problem mehr. Die zentrale, standortübergreifende Verwaltung elektronischer Zutritts- und Einbruchmeldesysteme reduziert den zeitlichen und personellen Aufwand für einen kontrollierten Zugang beträchtlich. Noch komfortabler wird es mit dem Fernzugriff per Smartphone oder Tablet. Die permanente Protokollierung und automatisch generierte Dokumentationen erleichtern den Arbeitsalltag und schaffen eine zusätzliche Sicherheitsebene, falls Nachweise erforderlich sind.

Eine moderne digitale Gefahrenmelderzentrale wie die Hiplex 8400H von Telenot erlaubt die Überwachung von Gebäuden in Echtzeit

Cyber-Security, Normen- und Rechtssicherheit

Digitale Sicherheitslösungen unterstützen Unternehmen außerdem bei der Einhaltung von Normen, Richtlinien und Gesetzen. Beispielsweise durch Systeme mit VdS-Zertifizierung sowie eine Datenverschlüsselung und Datenspeicherung gemäß Datenschutzgrundverordnung DSGVO. Regelmäßige Software-Updates beheben potenzielle Schwachstellen und halten die Sicherheitstechnologien auf dem neuesten Stand, was den Schutz vor Cyber-Bedrohungen verbessert.

Zukunftssicher durch flexible Systeme

Ein besonderer Vorteil digitaler Sicherheitstechnik ist ihre große Flexibilität und Skalierbarkeit. Hybride Anlagen aus verkabelten, funkbasierten und mechatronischen Komponenten sowie eine digitale Steuerung und Verwaltung lassen sich standortübergreifend an nahezu jede Situation anpassen. Die Vernetzung verschiedener Sicherheitssysteme spannt zusätzlich einen effektiven Schutzschirm mit schlanken Prozessen und umfassender Kontrolle auf. Aufgrund der digitalen Systemarchitektur sind nachträgliche Änderungen, Umbauten oder Erweiterungen in der Regel schnell und kosteneffizient umzusetzen, wodurch sich Unternehmen in diesem Bereich auch längerfristig sicher aufstellen können.

Zuverlässiger Partner für anspruchsvolle Sicherheitsanforderungen

Telenot bietet sowohl Einbruchmeldetechnik und Zutrittskontrollsysteme als auch Brandmeldeanlagen und Übertragungstechnik an. Die aktuelle Produktpalette des Herstellers erfüllt alle Voraussetzungen, dass auch Unternehmen mit anspruchsvollen Sicherheitsanforderungen wie in der Industrie oder im KRITIS-Bereich von den Mehrwerten elektronischer Sicherheitslösungen profitieren können.

Zu den digitalen Lösungen des Herstellers gehören unter anderem das Zutrittskontrollsystem Hilock 5000 ZK und die Gefahrenmeldezentrale Hiplex 8400H. Beide sind miteinander vernetzbar, was eine wirtschaftliche Integration der Sicherheitsfunktionen Alarm und Zugang ermöglicht. Der modulare, einfach skalierbare Aufbau beider Systeme schafft optimale Bedingungen für eine flexible Anpassung an veränderte Unternehmensprozesse und für effiziente Erweiterungen auf neue Räume, Gebäude oder Standorte. Beide Sicherheitssysteme sind hybrid, lassen also parallel die Einbindung von kabelgebundenen und funkbasierten Komponenten zu. Zusätzlich können Offline-Komponenten an das Zutrittskontrollsystem angebunden werden. So sind auch anspruchsvolle Gebäudeensembles und standortübergreifende Sicherheitslösungen kein Hindernis. Die Zertifizierung der Einbruchmeldeanlage nach neuesten Normen und die VdS-gemäße Integration des Zutrittskontrollsystems stellen darüber hinaus eine normkonforme Gesamtlösung sicher.

Die gleiche Philosophie weist das Brandmeldesystem Hifire 4000 BMT von Telenot auf. Auch hier sorgen VdS-anerkannte Komponenten und Systeme, eine für alle Gebäudegrößen und -arten skalierbare Struktur und offene Schnittstellen zur Integration in Gebäudemanagementsysteme für die entsprechende Systemflexibilität. Zusammen mit Übertragungstechnik des Herstellers können Unternehmen aus allen Branchen ein Komplettpaket aus digitalen Sicherheitssystemen umsetzen, das höchsten Sicherheitsansprüchen genügt. Das flächendeckende Netz der autorisierten Telenot-Stützpunkte in Deutschland und Europa sorgt für die notwendige fachkundige Projektplanung, Installation und Wartung vor Ort und einen schnellen Service im Bedarfsfall. GIT

Telenot
www.telenot.com

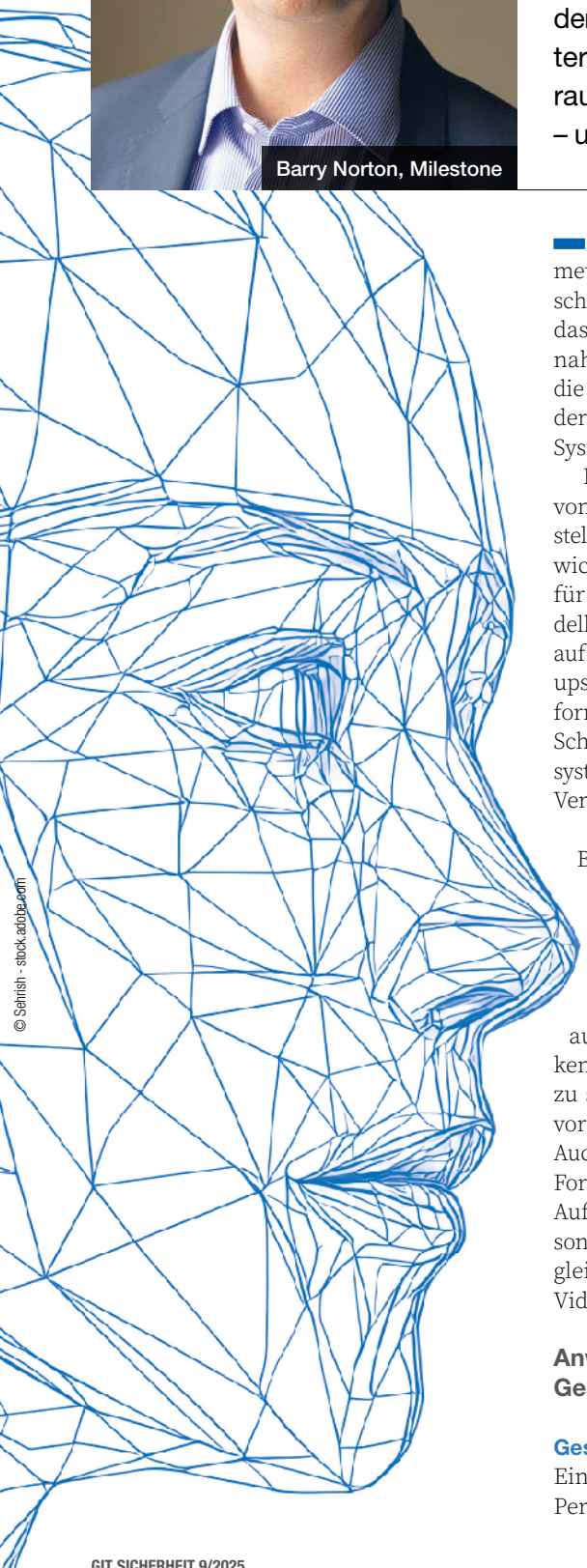
Barry Norton, Milestone

BIOMETRIE

Gesichtswahrend

Gesichtserkennung ohne Speicherung personenbezogener Daten

Videoüberwachung ist längst mehr als reine Aufzeichnung – sie wird zum intelligenten Werkzeug für Sicherheit und Organisation. Besonders mittelständische Unternehmen profitieren heute von KI-gestützter Gesichtserkennung. Unbefugte im Lager? Zutritt zum Serverraum? Moderne Gesichtserkennung ist ein hilfreiches Werkzeug – und lässt sich mit den Ansprüchen des Datenschutzes vereinbaren.



Durch die automatisierte Analyse biometrischer Merkmale lassen sich Personen schnell und zuverlässig identifizieren, ohne dass das Sicherheitspersonal jede Aufnahme überwachen muss. Dies entlastet die Unternehmen und steigert die Effizienz der gesamten Sicherheitsinfrastruktur. Die Systeme werden immer leistungsfähiger.

Dies steht auch hinter einer Kooperation von Milestone Systems mit dem Chiphersteller Nvidia. Mit ihrem Projekt Hafnia entwickeln sie eine KI-optimierte Datenbank für das Training von visuellen Sprachmodellen. Gleichzeitig setzt Milestone Systems auf Datenschutzlösungen des Berliner Startups Brighter AI, die personenbezogene Informationen automatisch anonymisieren. Schließlich sammeln Videoüberwachungssysteme sensible Daten und sind durch ihre Vernetzung besonders angreifbar.

Die Sicherheitsbranche, so fasst es Barry Norton, Experte für Produktinnovation bei Milestone Systems, zusammen, entwickelt Wege, um effektive Überwachung mit Datenschutz zu vereinen. „Moderne Gesichtserkennungslösungen konzentrieren sich auf statistische Analysen und Mustererkennung, ohne personenbezogene Daten zu speichern, und bieten so Sicherheitsvorteile, die trotzdem leistungsstark sind". Auch in der Frage des Datenschutzes sei der Fortschritt rasant. Mithilfe von KI könnten Aufnahmen so verändert werden, dass Personen unkenntlich seien – wobei die Daten gleichzeitig für maschinelles Lernen oder Videoanalysen weiterhin nutzbar seien.

Anwendungsbereiche und Arten der Gesichtserkennung

Gesichtsverifizierung (Eins zu eins)

Ein Eins-zu-eins-Vergleich, bei dem eine Person eine Identität beansprucht (z. B. durch Vorzeigen eines Ausweises), und das System überprüft, ob das Gesicht mit der angegebenen Identität übereinstimmt.

Beispiel: Im Flughafen in Frankfurt am Main können Passagiere beim Check-in eine biometrische Identitätsprüfung nutzen und danach alle mit Gesichtserkennungstechnik ausgestatteten Kontrollpunkte kontaktlos passieren.

Gesichtsidentifikation (Eins zu viele)

Ein Eins-zu-Viele-Vergleich, bei dem ein von einem System erfasstes Gesicht mit einer Datenbank mehrerer Gesichter und Gesichtsmerkmale verglichen wird, um die Person zu identifizieren. Dieser Prozess wird häufig in Sicherheits- oder Überwachungskontexten verwendet.

Beispiel: Im Falle eines vermissten Kindes an einem Flughafen könnte ein System die Gesichter aller Passagiere, die die Kontrollpunkte passieren, scannen und mit einem Foto des Kindes in einer Datenbank vergleichen. Wenn eine Übereinstimmung gefunden wird, wird ein Alarm ausgelöst.

Gesichtswiedererkennung (Viele zu viele)

Viele-zu-Viele-Vergleiche, bei denen mehrere Gesichter mit mehreren anderen Gesichtern verglichen werden. Dies wird in der Regel verwendet, um die Bewegung einer Person über verschiedene Bereiche hinweg anonym zu verfolgen, indem ihre Gesichtsbilder an verschiedenen Kontrollpunkten abgeglichen werden, ohne ihre Identität zu kennen.

Beispiel: Im Einzelhandel könnte die Gesichtswiedererkennung verwendet werden, um zu verfolgen, wie lange eine anonyme Person von einem Bereich eines Ladens zu einem anderen unterwegs ist, indem ihr Gesicht wiedererkannt wird, wenn sie verschiedene Kamerablickwinkel betritt und verlässt.

Echtzeit-Gesichtserkennung

Echtzeit-Gesichtserkennung bezieht sich auf die sofortige Verarbeitung eines Live-Videofeeds, bei dem Gesichter mit einer Datenbank verglichen werden, um sofortige Warnungen zu erzeugen, wenn eine Übereinstimmung gefunden wird.

Beispiel: Bei großen öffentlichen Veranstaltungen wie Sportstadien könnte Echtzeit-Gesichtserkennung verwendet werden, um gesperrte Personen zu erkennen. Der Fußballklub Bröndby Kopenhagen war 2019 der erste Fußball-Verein, der diese Technologie einsetzt, um Fans mit einem Stadionverbot zu identifizieren.

Aufgezeichnete Gesichtserkennung („Post-Event")

Dies bezieht sich auf die Analyse von Videoaufzeichnungen nach dem Ereignis anstatt in Echtzeit. Die Gesichtserkennung wird auf aufgezeichnete Daten angewendet, um Personen zu identifizieren oder zu verfolgen.

Beispiel: Nach einem Verbrechen könnten Ermittler Gesichtserkennungssoftware auf aufgezeichneten Videos von Überwachungskameras verwenden, um Verdächtige zu identifizieren, indem sie deren Gesicht mit bekannten Datenbanken abgleichen.

Identifikation durch äußere Merkmale

Harte Biometrie

Harte Biometrie bezieht sich auf physische Merkmale, die eindeutig genug sind, um zur Identifizierung einer bestimmten Person verwendet zu werden, wie Gesicht, Fingerabdruck oder Iris.

Beispiel: Der Fingerabdruck- oder das Gesichtsscanning zum Entsperren eines Telefons oder die Verwendung von Iriserkennung für den sicheren Zugang zu Hochsicherheitsgebäuden wie Rechenzentren.

Weiche Biometrie

Weiche Biometrie (persönliche Merkmale) umfasst allgemeine Attribute wie Größe oder Körperform, die nicht eindeutig genug sind, um eine Person zu identifizieren, aber bei der Wiedererkennung helfen können, wenn sie mit anderen Informationen kombiniert werden.

Beispiel: Verwendung von Größe und Körperform, um einen Verdächtigen in einer Kameraszene zu identifizieren, wenn Gesichtsmerkmale allein nicht zuverlässig sind.

Ähnlichkeit des Aussehens

Hierbei werden Personen nicht anhand biometrischer Merkmale, sondern anhand ihres Erscheinungsbildes, d.h. ihrer Kleidung oder Accessoires, unterschieden. Sie wird häufig für schnelle Ermittlungen und statistische Analysen eingesetzt, ohne die Identität der Personen festzustellen.

Beispiel: Ein Einzelhandelsgeschäft kann Kunden anhand ihrer Kleidung verfolgen, um zu überwachen, wie lange sie im Laden bleiben, ohne dabei Gesichter oder persönliche Daten zu erfassen.

Lebendigkeitserkennung

Das ist eine wichtige Methode, um festzustellen, ob das Subjekt vor einem Gesichtserkennungssystem ein lebender Mensch ist und kein Foto oder eine Videoaufzeichnung.

Beispiel: In einigen mobilen Zahlungssystemen erfordert die Gesichtserkennung, dass Benutzer blinzeln oder ihren Kopf leicht bewegen, um sicherzustellen, dass sie eine lebende Person sind und nicht jemand, der versucht, ein Foto zur Authentifizierung zu verwenden.

Mathematische Darstellung biometrischer Daten

Nicht umkehrbare mathematische Darstellungen sind zum Beispiel Listen von Zahlen basierend auf dem Gesichtsbild oder dem Aussehen einer Person. Diese Zahlen repräsentieren Merkmale, können aber nicht verwendet werden, um das Gesicht zu rekonstruieren.

Beispiel: Wenn eine Organisation nur die mathematischen Darstellungen eines Gesichts anstelle eines tatsächlichen Bildes speichert, ist es selbst bei Diebstahl der Daten nahezu unmöglich, das Gesicht der Person zu rekonstruieren oder die Daten mit einem anderen System zu verwenden.

Datenschutz- und Sicherheitsüberlegungen

Moderne Gesichtserkennungssysteme integrieren mehrere Sicherheitsebenen, die durch verantwortungsvolle Datenhandhabung persönliche Daten schützen und gleichzeitig die Wirksamkeit des Systems gewährleisten. Die wichtigen Schutzmaßnahmen umfassen:

- Isolierung von biometrischen Vorlagen, die Gesichtserkennungsvorlagen von anderen persönlichen Daten trennen, mit dedizierten sicheren Speicherumgebungen.
- Verschlüsselungssysteme für biometrische Daten, die Gesichtsmerkmale erkennen und automatisch ein biometrisches Template einsetzen – das ist eine abstrakte, numerische Repräsentation der Merkmale (z. B. Augenabstand, Kontur, Verhältnis verschiedener Gesichtsbereiche). Anonymisierung biometrischer Daten, die Gesichtsmerkmale in nicht umkehrbare mathematische Darstellungen umwandelt – in Zahlen – und so die Rekonstruktion der ursprünglichen Gesichtsbilder verhindert.
- Kaskadierende Löschprotokolle, die sowohl rohe Gesichtsdaten als auch abgeleitete biometrische Vorlagen automatisch nach ihrer autorisierten Nutzungsdauer entfernen
- Segmentierte Zugriffskontrollen, die administrative Funktionen der Gesichtserkennung (wie Anmeldung und Vorlagenverwaltung) vom regulären Systembetrieb trennen GIT

PERSONENSCHUTZ

Open-Source-Intelligence

OSINT als Grundpfeiler des digitalen Vorstandsschutzes

Unternehmen werden heute nicht nur zur Zielscheibe hochentwickelter Cyberangriffe, sondern auch extremistischer und aktivistischer Attacken. Im Fokus der Angreifer stehen dabei insbesondere Vorstände und Top-Manager, welche aufgrund ihres privilegierten Zugangs zu sensiblen Daten und ihrer symbolischen Bedeutung für das Unternehmen eine besonders lukrative Zielgruppe darstellen. Digitaler Vorstandsschutz auf Basis von Open-Source-Intelligence (OSINT) entwickelt sich zum unverzichtbaren Bestandteil moderner Unternehmenssicherheit. Ein Beitrag von Philipp Schotzko, Senior Security Intelligence Analyst bei epp GmbH.

Eine Befragung von IT- und Cybersicherheitsexperten aus dem Jahr 2024 liefert eindeutige Zahlen: 64 Prozent der deutschen Führungskräfte wurden in den vergangenen zwei Jahren Opfer von einer Cyberattacke. 72 Prozent der IT-Experten bestätigen, dass Führungskräfte häufiger Opfer von Cyberangriffen werden als andere Angestellte. Diese alarmierenden Zahlen sind Ausdruck einer sich rasant verändernden Bedrohungslandschaft. Weil zunehmend mehr Daten und Online-Profile von Führungskräften öffentlich verfügbar sind, werden Identitätsangriffe für Kriminelle immer einfacher.

Das Spektrum der Bedrohungen reicht von raffinierten Phishing-Attacken über Social Engineering bis hin zu systematischen Doxing-Kampagnen, bei denen persönliche Informationen von Führungskräften gezielt öffentlich gemacht werden. Viele der für solche Angriffe benötigten Informationen können online gefunden werden – aus Unternehmensquellen, Medieninhalten oder den Social-Media-Aktivitäten der Zielpersonen selbst.

Diese Entwicklung wird durch den oft unbedachten Umgang vieler Führungskräfte mit dem Internet noch verstärkt. Angaben zur Person, zum Geburtsdatum und zum beruflichen Hintergrund stellen viele Top-Manager öffentlich auf Business-Netzwerken zur Verfügung, ohne die Tragweite dieser Preisgabe zu durchdenken.

Digitale Spuren

Führungskräfte verwenden häufig für private Accounts auf sozialen Netzwerken ihren Klarnamen sowie identische oder ähnliche Profilbilder wie in beruflichen Kontexten. Durch systematische Analyse historischer Benutzernamen, Verlinkungen zu anderen Accounts, KI-gestützte Bilderkennung und Abgleiche mit bekannten Kontaktdaten können Angreifer präzise Bewegungs- und Verhaltensprofile über Zielpersonen erstellen.

Diese scheinbar harmlosen digitalen Spuren werden zu gefährlichen Angriffsvektoren, wenn sie in den Händen profes-

sioneller Cyberkrimineller oder extremistischer Gruppierungen landen.

Extremismus trifft Wirtschaftsführung

Parallel dazu geraten in Deutschland Führungskräfte und politische Entscheidungsträger aber auch zunehmend zur Zielscheibe physischer Angriffe. Gesellschaftspolitische Konflikte werden heutzutage sehr schnell von extremistischen und aktivistischen Gruppierungen instrumentalisiert. Themen wie Migration, Antikapitalismus oder Antimilitarismus dienen diesen Gruppierungen als Vorwand, gezielt Aktionen gegen Vorstände und politische Entscheidungsträger zu initiieren.

Dabei ist die Vorgehensweise der Täter hochgradig systematisch: Sie recherchieren gezielt persönliche und berufliche Informationen, etwa aus LinkedIn-Profilen, Unternehmens-webseiten, Medienberichten oder anderen öffentlich zugänglichen Quellen. Mit diesen Daten planen die Täter nicht nur digitale, sondern zunehmend auch gezielt physische Angriffe. Einschüchterungskampagnen, direkte Bedrohungen und sogar Anschlagsplanungen sind mittlerweile keine Seltenheit mehr.

Seit 2023 ruft beispielsweise die Kampagne „Switch off - the system of destruction“ unter einer ideologischen Mischung aus militantem Antikapitalismus, Klimawandel und sozialer Ungerechtigkeit zu Angriffen auf Unternehmen und öffentliche Einrichtungen auf. Sie legitimiert dabei Gewaltaktionen gegen kapitalistische Infrastrukturen, insbesondere gegen Unternehmen aus den Bereichen Künstliche Intelligenz, Chipfertigung und Rüstungsindustrie. Laut deutschen Sicherheitsbehörden handelt es sich um die derzeit bedeutendste militante linksextremistische Kampagne mit über 100 zugeordneten Straftaten.

Diese Entwicklung gefährdet nicht nur die Stabilität der deutschen Wirtschaftsordnung, sondern vor allem auch die persönliche Sicherheit betroffener Führungskräfte.

OSINT-basierte Risikoanalyse als Schlüssel

Open Source Intelligence, kurz OSINT, dient als leistungsstarkes Instrument zur Sammlung, Analyse und Interpretation offener und frei zugänglicher Informationen aus dem Internet. Dieses Instrument ermöglicht es, vielfältige Einblicke zu gewinnen, die von der Identifizierung von Sicherheitsbedrohungen über Wettbewerbsanalysen bis hin zum Schutz der Reputation reichen.

Eine professionelle OSINT-Analyse entwickelt sich zum unverzichtbaren Fundament der modernen Executive Protection. Die systematische Ermittlung personenbezogener Daten im digitalen Raum, bestehend aus Open-, Deep- und Dark Web, ermöglicht es, potenzielle Angriffsvektoren zu identifizieren, bevor sie von Kriminellen ausgenutzt werden.

Führungskräfte können ihre digitale Sicherheit bereits mit einfachen Maßnahmen deutlich erhöhen. Dazu gehören die regelmäßige Überprüfung und Anpassung der Privatsphäre-Einstellungen in allen genutzten sozialen Netzwerken sowie die Reduzierung öffentlich sichtbarer persönlicher Informationen in Business-Profilen. Ergänzend sollten Führungskräfte ihre Online-Präsenz durch professionelle OSINT-Analysen kontrollieren und ein systematisches Monitoring-System zur Früherkennung von Bedrohungen implementieren.

Wohnanschriften-Anonymisierung gehört ebenfalls zu den grundlegenden Schutzmaßnahmen. Die Prüfung und bei Bedarf Anonymisierung privater Wohnanschriften in Online-Diensten wie Google Maps und Apple Maps – sowohl national als auch international – reduziert das Risiko gezielter physischer Bedrohungen erheblich.

Ebenso wichtig ist die systematische Veranlassung von Auskunftssperren sowie Datenlöschung. Die proaktive Löschung sensibler Daten auf Drittseiten und in Suchmaschinen, kombiniert mit der Erstellung von Gefährdungsschreiben zur Beantragung behördlicher Auskunftssperren, schafft wichtige Schutzbarrieren.

Investition in die Zukunft der Unternehmenssicherheit

Die Bedrohungslandschaft für deutsche Führungskräfte wird sich in den kommenden Jahren weiter verschärfen. Unternehmen, die heute nicht in umfassende OSINT-basierte „Digital Executive Protection“ investieren, setzen nicht nur ihre Führungskräfte, sondern ihre gesamte Geschäftskontinuität aufs Spiel.

Die Zeit reaktiver Sicherheitsmaßnahmen ist vorbei. Modern aufgestellte Unternehmen setzen auf proaktive, datengesteuerte Bedrohungsanalyse als Grundpfeiler ihres Executive Protection Programms. Mithilfe systematischer Analyse öffentlich verfügbarer Informationen lassen sich die komplexen Risiken der digitalen Ära erfolgreich bewältigen und Führungskräfte effektiv schützen. GIT

epp GmbH
www.ep-partners.net

NIS-2-RICHTLINIE

Im Endspurt

Zur deutschen Umsetzung der Cybersicherheitsrichtlinie NIS 2

Die Umsetzung der Cybersicherheitsrichtlinie NIS 2 ist überfällig. Deutschland schafft es erst Ende 2025, über ein Jahr nach der gesetzten Frist. Frühere Anläufe scheiterten an der Auflösung des Bundestags. Ende Juli wurde der aktuelle Entwurf immerhin im Kabinett beschlossen, nach der Sommerpause kann das Parlament ihn verabschieden. Nur weil 18 weitere EU-Länder die Umsetzungsfrist ebenfalls verpasst haben, könnte das bereits eingeleitete Vertragsverletzungsverfahren der EU-Kommission noch einigermaßen glimpflich ausgehen. Ein Beitrag von Ulrich Plate, Senior Information Security Consultant bei Ngenn.

Für die rund 30.000 in Deutschland künftig regulierten Unternehmen spielt der Zeitpunkt des Inkrafttretens kaum eine Rolle, denn es wird keine Übergangsfristen oder gar Aufschub geben. Wer sich nicht unverzüglich auf die Einhaltung der gesetzlichen Anforderungen vorbereitet, geht ein hohes Risiko ein. Die in der NIS 2 festgelegten technischen und organisatorischen Maßnahmen für die Informationssicherheit sollten umgesetzt und dokumentiert sein, bevor die nächste Ransomware-Attacke oder andere Krisen eintreten. Denn wenn im Ernstfall die Aufsichtsbehörden feststellen, dass Vorgaben fahrlässig verletzt oder gar vorsätzlich missachtet wurden, wird es richtig teuer: Ordnungsstrafen wie im Datenschutz, persönliche Haftung der Leitungsorgane, sogar eine behördliche Untersagung der Geschäftsausübung sind möglich. Schon die Registrierungs- und Meldepflichten sollte man nicht versäumen, auch dafür können bereits kostspielige Bußgelder verhängt werden.

Zehntausende Unternehmen erfasst

Dabei wissen viele Unternehmen noch gar nicht, dass sie von der Regulierung erfasst werden. Im direkten Anwendungsbereich der NIS 2 sind Branchen, die bislang nicht als Betreiber kritischer Infrastrukturen galten: Zu den knapp 1200 KRITIS-Betreibern, die schon unter dem bisherigen Gesetz reguliert waren, kommen bald zehntausende Einrichtungen neu dazu. Aber auch viele derjenigen, die nicht direkt verpflichtet werden, werden mittelbar denselben Sicherheitsanforderungen unterworfen.

Die NIS 2 verlangt vom Risikomanagement aller Einrichtungen in ihrem Geltungsbereich, dass sie auch ihre Lieferkette absichern. Das heißt: Jeder Lieferant, jeder Drittdienstleister, dessen Tätigkeit zu „betriebsrelevanten Geschäftsprozessen“ einer NIS-2-Einrichtung beiträgt, muss

sich gegenüber seinen Auftraggebern zur Einhaltung der Regeln verpflichten.

Hier hat die Sogwirkung der Richtlinie längst begonnen, lange vor Inkrafttreten des Gesetzes. Das liegt daran, dass Dienstleisterverträge meist befristet sind. Wenn ihre Erneuerung turnusmäßig ansteht, muss künftig berücksichtigt werden, wie die Vorschriften für die Informationssicherheit auch beim Partner oder Dienstleister eingehalten werden.

Wer für Banken beispielsweise Videoüberwachung oder andere Sicherheitstechnik anbietet und betreibt, kennt das Spiel. Für den Finanzsektor gilt statt NIS 2 die Schwesterverordnung DORA, mit weitgehend identischem Maßnahmenkatalog, aber europaweit unmittelbar gültig, nicht wie die Richtlinie erst nach nationaler Umsetzung. Unter DORA haben die Banken deshalb schon Ende letzten Jahres begonnen, systematisch ihre Zulieferer zu erfassen, auf Einhaltung der Sicherheitsanforderungen zu verpflichten und inzwischen eine vollständige Liste der Partner an die Bankenaufsicht gemeldet.

Chancen und Pflichten für Dienstleister

Statt zu warten, bis das Gesetz zur Einhaltung der Regeln zwingt, wäre das genaue Gegenteil vernünftig. IT-Service-Provider fallen meist selbst schon in den Anwendungsbereich der NIS 2, aber auch alle Sicherheitsfachleute, Integratoren, Errichter, kurz: die klassischen Zulieferbetriebe, die für zukünftig NIS-2-regulierte Unternehmen tätig sind, sollten wissen, dass sie in Bezug auf Cybersicherheit absolut makellos auftreten müssen. Mit klaren Konzepten und wirksamen Maßnahmen überzeugt man aktuelle und potentielle Kunden, dass sie in guten Händen sind. Sie müssen sich schließlich darauf verlassen können, dass ihre Dienstleister nach allen Regeln der Kunst und dem Stand der Technik vorgehen. Nur unter diesen Voraussetzungen können sie weiterhin rechtskonform mit dem Partner zusammenarbeiten.

Für Dienstleister und Lieferanten eröffnen sich deshalb im Zuge von NIS 2 echte Chancen. Bei den gesetzlichen Mindestsicherheitsanforderungen ist nichts radikal Neues dabei. Viele Vorgaben sind aus ISO-Standards oder Best-Practice-Regelwerken wie ITIL längst bekannt. Ein funktionierendes Informationssicherheitsmanagement ist aber nicht selbstverständlich. Wer seinen Kunden regelmäßige Sicherheitsupdates, Multifaktor-Authentisierung bei Wartungsarbeiten, gehärtete Systeme, Netzwerksegmentierung, und im Ernstfall ein erprobtes Notfall- und Krisenmanagement anbieten kann, ist dem Wettbewerb womöglich den entscheidenden Schritt voraus. Um als Lieferant im Geschäft zu bleiben, sollte das eigene Cybersicherheitsniveau der Bedeutung der Kunden mindestens angemessen sein. GIT

Ngenn
www.ngenn.net

Schutzbeschläge in vier Widerstandsklassen

Die neuen Schutzbeschläge der Glutz AG ermöglichen eine durchgängige Formsprache von ES0 bis ES3, sowohl in runder als auch in eckiger Ausführung. Dies ermöglicht es, Türen innerhalb eines Gebäudes im einheitlichen Design zu gestalten und gleichzeitig unterschiedlichen Sicherheitsanforderungen von RC 1 bis RC 4 gerecht zu werden. Mit einer schlanken Aufbauhöhe des Außenschildes von lediglich 12 mm und der zylindrischen Formensprache eröffnen sich elegante Gestaltungsmöglichkeiten. Die neue Generation der Schutzbeschläge zeichnet sich durch eine vereinfachte und schnelle Montage aus. Dank weniger loser Teile bei Schutzeinsatz und Zylinderabdeckung wird die Installation noch einfacher. Diese wird zusätzlich durch die verbesserte Easyfix-Technologie unterstützt. Die direkt in der Grundplatte integrierten Gewindenocken verhindern ein Losdrehen bei der Demontage. **www.glutz.com**

CYBERSICHERHEIT

Cyber-Security-Trends 2025

Steigende Cybersecurity-Anforderungen trotz Fachkräftemangel bewältigen

Im Jahr 2025 müssen Unternehmen unter Beweis stellen, dass sie ihren Aufgaben im Bereich Cybersicherheit gerecht werden. Die verschärften Regularien und Vorschriften wie beispielsweise NIS2 und der Cyber Resilience Act erhöhen den Druck erheblich. Es gilt, die eigene Infrastruktur kritisch zu durchleuchten und sie gegen die neuesten Entwicklungen in der Bedrohungslandschaft zu rüsten – und das alles trotz des ausgeprägten Fachkräftemangels. Alain de Pauw, Divisionsleiter IT Security Services bei Axians Deutschland und Schweiz erklärt die wichtigsten Trends im Cyber-Security-Bereich und wie Unternehmen darauf am besten reagieren.

Die gute Nachricht zuerst: Der BSI-Lagebericht 2024 sieht mittlerweile Fortschritte im Aufbau einer tragfähigen Cybersicherheitsarchitektur, betont dabei aber die Bedeutung einer hohen Cyberresilienz. Immerhin rüsten auch Hacker zunehmend auf und professionalisieren sich im hohen Tempo. Insbesondere fünf folgende Trends werden deutsche Unternehmen im neuen Jahr bezüglich der Cyber-Security-Landschaft beschäftigen:

1. Verschärfung von Regularien und Verordnungen

NIS2, DORA und der Cyber Resilience Act (CRA) sind die wichtigsten Regelwerke, die 2025 für Unternehmen relevant sein werden. Der Grad an Compliance schwankt jedoch noch stark. Während viele Unternehmen bereits ihre Hausaufgaben gemacht haben, kämpfen andere noch darum, die vorgeschriebenen Maßnahmen in die Praxis umzusetzen. Viele Kunden stehen dabei vor der Herausforderung, ihre Prozesse anzupassen, insbesondere Kunden ohne bestehende ISO-Zertifizierungen. Speziell für den Finanzsektor kommt der Digital Operational Resilience Act (DORA) hinzu. Dieser zielt darauf ab, die Widerstandsfähigkeit dieser Branche gegen Cyberattacken zu stärken, weshalb die Nachfrage nach Beratung und Lösungen zur Umsetzung dieser Vorschriften steigt. Insgesamt verschärfen die neuen Regulierungen und Verordnungen die Anforderungen an die Cyber Security zunehmend. Auf der einen Seite ist dies zu begrüßen, auf der anderen Seite müssen Unternehmen darauf achten, im Dschungel der Vorschriften nicht den Überblick zu verlieren.

2. Quantenkryptografie nimmt Fahrt auf

Bis die ersten Quantencomputer auf den Markt kommen, wird es noch eine Weile dauern. Das hält Angreifer jedoch nicht davon ab, sich schon jetzt darauf vorzubereiten. So weist das BSI darauf hin, dass sich verschlüsselte Daten von Online-Banking, Smart-Home-Systemen oder Messaging Apps wie auch Teams speichern lassen, um sie in ein paar Jahren mithilfe von Quantencomputern in Sekundenschnelle zu entschlüsseln. Unternehmen und insbesondere Betreiber kritischer Infrastrukturen müssen daher beginnen, ihre Daten zu schützen und sich mit dem Thema Post-Quantenkryptografie auseinanderzusetzen. Dasselbe gilt auch für Cyber-Security-Dienstleister, die sich vorbereiten sollten. Ziel sollte es sein, Schutzmaßnahmen gegen mögliche Bedrohungen durch Quantencomputer zu entwickeln, um Kunden vor künftigen Bedrohungen zu schützen.

3. Kritische Infrastrukturen stärker schützen

Oft ist vielen Anwender im medizinischen Bereich nicht bewusst, dass ältere Geräte wie Röntgengeräte, MRTs und Co inzwischen auch über WLAN miteinander kommunizieren und an das Internet angebunden sind. Das macht sie auch für Angreifer immer öfter zum lohnenden Ziel. Denn Schnittstellen sind regelmäßig nicht

ausreichend gesichert. Sind die Hacker im Netzwerk, können sie nicht nur auf sensible Daten zugreifen, sondern auch Arbeitsabläufe stören. Im Krankenhausalltag kann dies verheerende und lebensbedrohliche Folgen haben. Das haben Einrichtungen im Medical-Bereich erkannt und sind bestrebt, ihre Operational Technology (OT)-Umgebungen stärker mithilfe von Vulnerability Scanning und Security Operations Center (SOC) Services für IoT- und OT-Systeme abzusichern.

4. SOC-Standorte in Europa immer gefragter

In diesem Jahr haben vor allem auch mittelständische Unternehmen festgestellt, dass reine Netzwerksicherheit häufig nicht mehr ausreicht und ein SOC in Zeiten des Fachkräftemangels eine effiziente Lösung gegen Angreifer darstellt. 2025 ist davon auszugehen, dass sich dieser Trend weiter fortsetzt und zudem stärker auf SOC-Standorte in Europa gesetzt wird. Dies hat zum einen Datenschutz- und Compliance Gründe, zum anderen ist die Koordination einfacher und das Vertrauen höher. Die Akzeptanz von SOC-Lösungen, die über die Cloud bereitgestellt werden, steigt zudem.

5. Beliebtheit von Managed Services

Managed Services und „as a Service"-Modelle sind gerade wegen des Fachkräftemangels im Trend. Unternehmen setzen verstärkt auf externe Anbieter, um die wachsende Komplexität der Cyber Security trotz ausgelasteter IT-Abteilungen zu bewältigen. Der Bedarf an transparenten Geschäftsmodellen und leistungsfähigen Lösungen wächst und rückt Managed Services und Cloud Services in den Mittelpunkt. Um Daten wirksam zu schützen, gilt es Fachleute hinzuzuziehen, die die Herausforderungen komplexer Infrastrukturen kennen und die interne IT-Abteilung entlasten. Derzeit ist davon auszugehen, dass die hybride Zusammenarbeit zwischen internen Teams und externen Dienstleistern immer weiter verstärkt wird.

6. KI-gesteuerte Cyberangriffe und Abwehrmechanismen

Künstliche Intelligenz (KI) wird von Cyberkriminellen zunehmend für hochentwickelte Phishing- und Ransomware-Angriffe eingesetzt. Laut BSI werden derzeit zwar keine neuen Methoden verwendet, doch die bereits bestehenden lassen sich durch KI vereinfachen und beschleunigen. Dadurch verschwimmen die Grenzen zwischen gezielten und ungezielten Phishing-Angriffen immer mehr. Insbesondere Informationen und Zugangsdaten sind für Hacker durch KI leichter zu erlangen. Deepfakes und automatisierte Angriffe sind hierbei besonders besorgniserregend. Gleichzeitig nutzen Unternehmen KI, um Bedrohungen effizienter zu erkennen und abzuwehren. Lösungen wie Endpoint Security, Betrugserkennung und SIEM sind hier nur einige von vielen Beispielen, die zur Unterstützung der Cyber Security Anwendung finden. GIT

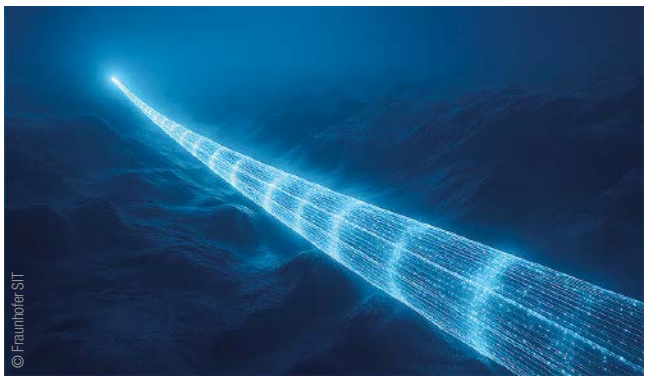
Autor:
Alain de Pauw
Divisionsleiter IT Security Services bei Axians Deutschland und Schweiz

© Axians, Vinci Energies

Axians
www.axians.de
www.vinci-energies.com

Studie: Unterseekabel systematisch schützen

Internet-Unterseekabel werden international zunehmend als kritische Infrastruktur eingeordnet. Bisher fehlte jedoch eine systematische Untersuchung zur Wirksamkeit der unterschiedlichen Schutzmaßnahmen. Athene-Wissenschaftler Jonas Franken von der TU Darmstadt war an einer Studie des UNIDIR (United Nations Institute for Disarmament Research) beteiligt, die diese Lücke schließen soll. Sie ordnet staatliche Schutzmaßnahmen für Unterseekabel einem Resilienzmodell zu, an dem Staaten und Betreiber ableiten können, wie gut sie auf Störungen ihrer Unterseekabel vorbereitet sind. Das Modell hilft, Schwachstellen systematisch zu erkennen und gezielt weitere Schutzmaßnahmen zu ergreifen.



© Fraunhofer SIT

Die Studie des UNIDIR „Achieving Depth – Subsea Telecommunications Cables as Critical Infrastructure" zeigt, wie Staaten Seekabel als KRITIS einstufen können und was diese Einstufung in der Praxis bedeutet. Sie wurde unter anderem von Athene-Wissenschaftler Jonas Franken von der TU Darmstadt verfasst.

www.sit.fraunhofer.de

WARNMELDER

Der Alarm der Leben rettet

Warum CO- und Gaswarnmelder Leben retten können – und worauf es bei Auswahl und Installation ankommt

Rauchgase, Kohlenmonoxid und Gas können für den Menschen in geschlossenen Räumen zu einer tödlichen Gefahr werden. Rauchwarnmelder, die insbesondere schlafende Personen schützen, sind in Wohngebäuden bundesweit vorgeschrieben. Für Kohlenmonoxid und Gas gibt es keine entsprechenden Vorschriften. Brandschutzexperte Lars Inderthal von Dekra erläutert, für wen auch CO- und Gas-Melder sinnvoll sind.

Rauchmelder sind unverzichtbar und müssen seit 2024 in allen Wohnungen in Deutschland installiert sein. Damit sie effektiv schützen, gilt es, monatlich die Prüftaste zu drücken, um die Funktion der Lebensretter sicherzustellen. Die wichtigste Aufgabe von Rauchmeldern: Sie verhindern, dass man im Schlaf von Brandrauch überrascht wird und Rauch und Flammen ausgeliefert ist. Dazu geben Rauchmelder im Brandfall einen schrillen Warnton ab. Sie werden in allen Schlaf- und Wohnräumen sowie in Fluren an der Decke angebracht. Je nach Bauart müssen sie alle 5, 8 oder 10 Jahre ausgetauscht oder mit neuer Batterie ausgestattet werden.

Viele Todesfälle durch Kohlenmonoxid

Im Unterschied zu Rauchmeldern reagieren CO-Warnmelder auf Kohlenmonoxid (CO) in der Umgebungsluft. Laut Bundesärztekammer (2022) sterben in Deutschland im Schnitt jährlich rund 500 Menschen an einer Kohlenmonoxid-Vergiftung, Tausende müssen in Krankenhäusern behandelt werden. Ein großer Teil der Kohlenmonoxid-Unfälle ist auf menschliches Fehlverhalten zurückzuführen. Besonders gefährlich ist es, in geschlossenen Räumen mit Kohle oder Gas zu grillen oder Verbrennungsmotoren zu betreiben. Auch der Betrieb von Heizpilzen oder ähnlichen Geräten in geschlossenen oder schlecht gelüfteten Räumen ist gefährlich.

Kohlenmonoxid entsteht bei „unvollkommener Verbrennung“, das heißt, wenn nicht ausreichend Sauerstoff vorhanden ist. Weitere mögliche Quellen sind defekte Gasthermen oder unzureichende Abgasabführung von Brennstellen. Auch aus Holzpellets kann Kohlenmonoxid austreten. Pelletlager dürfen aus diesem Grund nicht in direkter Verbindung zu Aufenthaltsräumen stehen und müssen vor dem Betreten gelüftet werden.

Was CO so gefährlich macht: Es bleibt als farb-, geruch- und geschmackloses Gas oft unbemerkt und kann schon in geringen Konzentrationen in der Atemluft beim Menschen zu tödlichen Vergiftungen führen. Neben der erforderlichen Achtsamkeit im Umgang mit Feuerstellen und der regelmäßigen Wartung von Geräten wie Gasthermen oder Kaminöfen kann ein CO-Melder zusätzlichen Schutz bieten.

Gaswarmelder: Ein Plus an Sicherheit

Ein Gaswarnmelder, eine dritte Variante der Warngeräte, eignet sich für alle Orte, an denen mit Erd-, Stadt- oder Flüssiggas geheizt oder gekocht wird. Strömt aus einer Gasanlage unbemerkt Gas aus, kann sich zusammen mit Raumluft ein Gemisch bilden, das durch einen Funken oder eine brennende Zigarette explodieren kann. Gase, die schwerer sind als Luft, können sich bei einem Leck im Bodenbereich ansammeln und unter ungünstigen Umständen bei schlafenden Personen zur Erstickung führen.

Ein Gaswarnmelder bietet für Gas-Applikationen ein zusätzliches Plus an Sicherheit. Das gilt auch für Wohnungen, in denen Gasherde, Gasöfen, Gasthermen oder Durchlauferhitzer eingesetzt werden oder allgemein, wenn es im Haus einen Erdgasanschluss gibt. Gaswarnmelder sind wie CO-Warnmelder bisher nicht vorgeschrieben. Sie messen den Gehalt von Gas in der Luft und geben ein akustisches, teilweise auch ein optisches Warnsignal ab, wenn ein Grenzwert überschritten wird. Manche Geräte zeigen die aktuelle Gaskonzentration kontinuierlich an. Auch eine Kopplung mit dem Smartphone ist bei bestimmten Modellen möglich.

Auf den Einzelfall kommt es an

Welche Art von Warngerät in einer Wohnung sinnvoll ist und wie es installiert werden muss, hängt von den Gegebenheiten des Einzelfalls ab. Erdgas zum Beispiel ist leichter als Luft und bildet im Raum eine gefährliche explosionsfähige Atmosphäre. Butan oder Propan, das zum Beispiel in Gasflaschen für Gasgrills oder Heizpilze verwendet wird, ist hingegen schwerer als Luft und sammelt sich an Tiefpunkten am Boden. Entsprechend müssen die Sensoren des Warngerätes in der richtigen Höhe positioniert werden. Wichtig auch: Nur richtig installierte Warngeräte bieten den möglichen Schutz. Um Fehlalarme zu vermeiden, ist ein Mindestabstand zur Gasquelle einzuhalten. Zugleich darf der Abstand aber nicht zu groß sein. GIT

DEKRA e. V.
www.dekra.de

BRANDBEGRENZUNGSDECKEN

Brandbegrenzungsdecken für Elektrofahrzeuge

Etablierung neuer Standards für Sicherheit und Prävention

Elektromobilität bringt nicht nur innovative Antriebstechnologien mit sich, sondern stellt Einsatzkräfte und Betreiber von Verkehrsflächen im Brandfall vor neue Herausforderungen. Wie lassen sich periphere Schäden nach Unfällen oder technischen Defekten bei Elektrofahrzeugen wirkungsvoll begrenzen? Welche Lösungen bieten echten Mehrwert und welche Rolle spielen Normen wie die DIN SPEC 91489 bei der Etablierung einheitlicher Standards? Im Gespräch mit Jens Erbstößer, Geschäftsführer der Erbstößer GmbH und einem der maßgeblichen Köpfe hinter der Entwicklung der neuen DIN SPEC, beleuchten wir die Rolle von Brandbegrenzungsdecken für Elektrofahrzeuge.

GIT SICHERHEIT: Herr Erbstößer, Sie waren maßgeblich an der Entwicklung der DIN SPEC 91489 beteiligt. Was war der Auslöser für die Initiative zur Normierung von Brandbegrenzungsdecken für Elektrofahrzeuge?

Jens Erbstößer: Es gab, im wahrsten Sinne des Wortes, viele Auslöser. Bei Betriebsstörungen und Havarien von Elektrofahrzeugen, häufiger ohne Brandschadensereignis als mit, standen den sekundär beteiligten Firmen, z. B. Abschleppunternehmen, Kfz-Händler, Parkraumbetreiber, usw. kaum technische Lösungen zur Verfügung, den peripheren Schaden zu begrenzen, bis im Brandfall gerufene Feuerwehreinsatzkräfte vor Ort eintreffen. Wenn es doch zu einer Entzündung kommt, greift man schnell auf die „gute, alte Löschdecke“ zurück. Leider war bei Ernstfällen festzustellen, dass diese nur sehr bedingt geeignet war. Viele, auch internationale, Hersteller hatten zwar schnelle Lösungen an der Hand, jedoch ohne dass die Anwender den tatsächlichen Nutzen zuverlässig verifizieren konnten. Daher der Druck der Marktbeteiligten zumindest Lösungsansätze für einen Produkt-/Prüfstandard zu definieren. Aus zeitlichen Gründen wählte man den Weg über eine DIN SPEC.

Bitte umblättern ▶

Welche konkreten Herausforderungen haben sich bei der Arbeit im Normungsgremium ergeben – insbesondere im Hinblick auf die Vielzahl an beteiligten Akteuren aus Industrie, Feuerwehr und Versicherungswirtschaft?

Jens Erbstößer: Wir betreten hier Neuland – besonders deutlich wird das bei der Frage der Versicherungswirtschaft: Wie ordnet man Brandbegrenzungsdecken ein? Zum vorbeugenden Brandschutz (z. B. F30/F90) zählen sie nicht, obwohl sie vor dem

Brandbegrenzungsdecken sind eine wirkungsvolle proaktive Maßnahme, um Schäden durch Brände von Elektrofahrzeugen zu verhindern

Brandausbruch eingesetzt werden. Zum abwehrenden Brandschutz ebenfalls nicht, da kein aktives Löschen erfolgt. Daher der Begriff „proaktives Hilfsmittel“. Ziel ist es, eine Feuerwiderstandsdauer bis mindestens zum Ende der üblichen Hilfsfrist zu erreichen, damit sich Einsatzkräfte schnell und sicher nähern und Löschmaßnahmen ergreifen können. Gleichzeitig soll der Einfluss des Brandes auf die Umgebung – etwa durch Hitze, Rauch oder Flammen – begrenzt werden.

Die Decke muss mobil, durch höchstens zwei Personen einsetzbar und dennoch aus robustem, dämmendem Material gefertigt sein. Dieser Spagat aus Schutzwirkung und Handhabbarkeit bestimmt Art und Umfang der erforderlichen Prüfungen.

In welchen realen Anwendungsszenarien sehen Sie den größten Nutzen von Brandbegrenzungsdecken – etwa bei Quarantäneplätzen, Tiefgaragen oder Transporten?

Jens Erbstößer: Dies ist meine persönliche Meinung und als Diskussionsgrundlage gedacht – eine Norm existiert noch nicht, es handelt sich um einen Vorschlag zum Sammeln von Erfahrungen. Den größten Nutzen sehe ich in der präventiven Vorhaltung: Wie Feuerlöscher sollten Brandbegrenzungsdecken in „umhausten“ Bereichen mit stehendem Verkehr (Tiefgaragen, Parkhäuser, Fähren etc.) Standard sein. Passende Halterungen gibt es bereits im Handel; besonders sinnvoll ist der Einsatz in älteren Bestandsbauten mit ergänzendem Serviceangebot. Bleibt ein Fahrzeug liegen, können Decken die Fluchtzeit verlängern, da sie in Tests die Gasausbreitung zuverlässig verringerten. Betreiber sollten klare Anweisungen geben, z. B. auffällige Fahrzeuge einpacken – etwa fahrtüchtige E-Autos mit Karosserieschäden auf Fähren. Daher sehe ich die Decken nicht als Teil der Feuerwehrausrüstung, sondern als stationäre Ausstattung. Im Freien sind sie vor allem für Abschleppunternehmen bei verunfallten Fahrzeugen sinnvoll. Werkstätten oder Entsorgungsbetriebe können zusätzlich ihre Quarantäneplätze damit ausrüsten.

Die DIN SPEC 91489 legt umfangreiche Prüfanforderungen fest, z. B. zur thermischen Beständigkeit und Schnittfestigkeit. Welche dieser Anforderungen halten Sie für besonders praxisrelevant – und warum?

Jens Erbstößer: Das Augenmerk lag drauf, auf zerstörende Testungen mittels brennender Elektro-Fahrzeuge oder Lithium-Batterien, pro Deckentyp zu verzichten. Deshalb einigte man sich auf eine Kombination von unterschiedlichen, äquivalenten Prüfungen. Die Grundvoraussetzung für eine Eignungsfeststellung ist das Bestehen des Tests zur thermischen Beständigkeit in Korrelation mit dem aufgebrachten Löschwasser. Danach folgen die anderen Checks, z. B. Schnitt und Reißfestigkeit. Einzelne, herausgepickte und bestandene Prüfungen sind jedoch nicht gleichbedeutend mit einer Konformität zur DIN SPEC 91849. Beispielsweise nützt die beste thermische Beständigkeit nichts, wenn das Material so steif und schwer ist, dass es sich nicht an das Fahrzeug anschmiegt und dessen Umschließung manuell nicht zulässt. Wirksam ist eine Brandbegrenzungsdecke nur mit dem nachgewiesenen Gesamtpaket aller Einzelprüfungen.

Wie schätzen Sie die Akzeptanz und Marktdurchdringung von Brandbegrenzungsdecken in Deutschland im Vergleich zum Ausland ein? Gibt es Unterschiede im Umgang mit dem Thema?

Jens Erbstößer: Verbunden mit Aufklärung über die Besonderheiten von Elektro-Fahrzeugen mit Lithium-Batterien, sind im Verkehrsbereich textile Lösungen in Deutschland durchaus gesucht und werden eingesetzt. Dies war ein Hauptgrund sich mit dem Thema auseinander zu setzen. Bekannt waren vor allem Hersteller aus Großbritannien, Norwegen und den Niederlanden, die auch an das Konsortium herangetreten sind. Überrascht waren wir jedoch, als wir feststellten, dass bereits Lettland normativ aktiv war. Dieser Standard beruhte hauptsächlich auf einer Prüfung zur Eignungsfeststellung eines Herstellers bei Fahrzeugbrand. Die inzwischen stattgefundenen Messen und Vortragsveranstaltungen spiegelten Zufriedenheit über unseren Lösungsansatz wider, sodass man über eine Akzeptanz im europäischen Rahmen sprechen kann.

Welche Rolle spielt die Brandbegrenzungsdecke im Zusammenspiel mit anderen Brandschutzmaßnahmen – und wo liegen aus Ihrer Sicht die Grenzen ihrer Wirksamkeit?

© Erbstößer

Brandbegrenzungsdecken sollten sowohl mobil einsatzbereit, in handlichen Taschen oder fest installiert, beispielsweise in Parkhäuern oder auf Fähren in geeigneten Schränken verfügbar sein

Jens Erbstößer: Brandbegrenzungsdecken sind eine mobile und proaktive Maßnahme des abwehrenden Brandschutzes. Grenzen sehe ich bei der dauerhaften, stationären Lagerung – Brandbegrenzungsdecken können Brandschutzwände oder -abschlüsse nicht ersetzen. Auch (Lade-)Einrichtungen, bei denen die Sicherung der Fluchtzeit der im Arbeitsraum Beschäftigten an erster Stelle steht, sollten besser durch bauliche Brandschutzmaßnahmen oder semi-mobile Lösungen, wie geprüfte Sicherheitsschränke (EN DIN 14470-1/VDMA 24994:2024-08.) und Brandschutzboxen mit Eignungsfeststellung realisiert werden.

Wie sehen Sie die Zukunft der Normung in diesem Bereich? Wird aus der DIN SPEC 91489 eine europäische oder gar internationale Norm entstehen – und was wäre dafür notwendig?

Jens Erbstößer: Der Vorschlag für einen Standard ist jetzt ca. ein Jahr im Markt den Nutzern bekannt. Erste Hersteller haben nun auch Prüferfahrungen gesammelt. Die Reaktionen auf unsere Zielvorgaben waren positiv, daher denke ich, dass das Projekt im DIN intern auf offene Ohren stößt und vorangetrieben werden kann. In welchem Umfang hängt von den Reaktionen der Mitgliedsstaaten und natürlich auch von der Finanzierung ab. GIT

Erst, wenn eine Decke alle Tests, wie Reiß- und Schnittfestigkeit, Handling sowie die thermische Beständigkeit in Korrelation mit dem aufgewendeten Löschwasser, bestanden hat, erreicht sie die Konformität zur DIN SPEC 91849

Erbstößer GmbH
https://erbs.de

Elock2 auf der FeuerTrutz 2025

Mit einem klaren Fokus auf den baulichen Brandschutz präsentierte sich Elock2 auf der FeuerTrutz 2025 in Nürnberg. Auf der Brandschutzmesse stellte der Hersteller Zutrittslösungen vor, die insbesondere bei der Absicherung von Flucht- und Rettungswegen zum Einsatz kommen können. Im Mittelpunkt des Messeauftritts stand dabei der digitale Türwächter TW4.

Der TW4 ist für Türen in Flucht- und Rettungswegen konzipiert und lässt sich an Holz-, Stahl- und Rohrrahmentüren nachrüsten. Das System vereint akustische und optische Alarmfunktionen mit elektronischer Zutrittssteuerung. Bei unbefugtem Betätigen des Türdrückers kann zunächst ein Voralarm ausgelöst werden. Wird die Tür geöffnet, wird ein Daueralarm ausgelöst. Berechtigte Personen können die Tür je nach Konfiguration alarmfrei passieren – etwa mithilfe eines Transponders oder über eine zeitgesteuerte Freigabe.

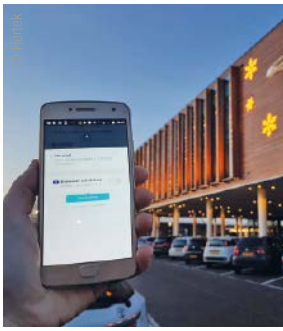
Darüber hinaus zeigte das Unternehmen weitere Komponenten zur Sicherung von Fluchttüren, darunter Steuerungseinheiten mit Panikfunktion. Diese Funktion erlaubt im Notfall das schnelle und sichere Verlassen eines Raums, etwa bei einer Rauchentwicklung oder in Gewaltszenarien.

Elke Wagner, Sales Manager bei Elock2 GmbH und Leiterin für Kommunikationsschulungen äußerte sich hochzufrieden über den Messeverlauf: „Der digitale Türwächter TW4 stand ganz klar im Zentrum des Messeauftritts von Elock2 auf der FeuerTrutz. Großes Interesse bekamen aber auch viele weitere unserer Systemlösungen. Ein intensives Gespräch führten wir beispielsweise mit Betreibern einer Kindertagesstätte über die Elock2 Panikfunktion, die ein schnelles und sicheres Verlassen von Räumen im Notfall ermöglicht."

Die vorgestellten Systeme sind modular aufgebaut und eignen sich laut Hersteller besonders für die Nachrüstung im Bestand.

www.elock2.de

Digitale Sicherheitsplattform Hertek Connect



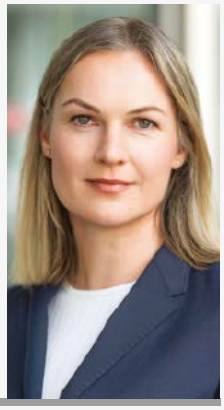
Mit Hertek Connect stellt das Unternehmen den Facherrichtern einen zusätzlichen Service zur gezielten Voll- und Teilüberwachung komplexer Brandmeldeeinrichtungen bereit. Die digitale Sicherheitsplattform erleichtert die Verwaltung der angeschlossenen Penta-Brandmelderzentralen und macht jeden Wartungseinsatz effizienter. Besonders in störungsanfälligen oder umfangreichen Objekten sowie an abgelegenen oder schwer zugänglichen Standorten hilft die zusätzliche Anlagenkontrolle mit Hertek Connect. Hertek Connect besteht aus der „Kommandozentrale" Connect Support und der App Connect Control für die gezielte, standortabhängige Überwachung.

www.hertek.de

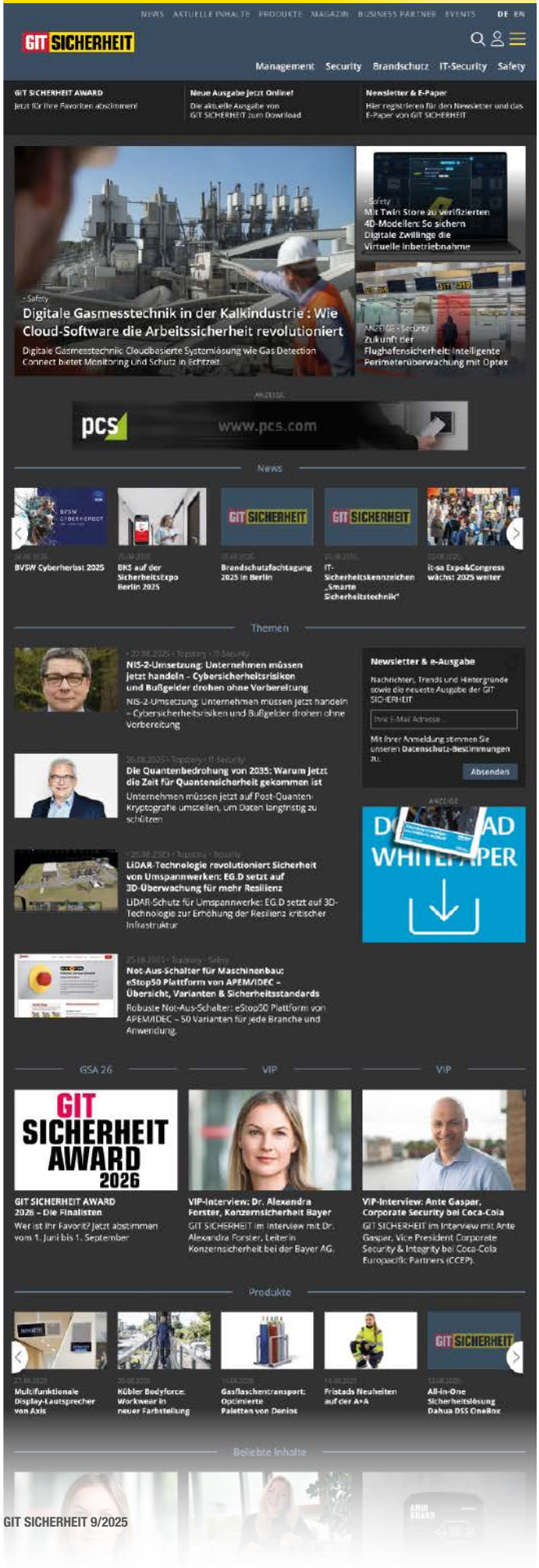
GIT SICHERHEIT

Die GIT SICHERHEIT ist für mich wichtig, weil sie sich meinem Eindruck nach durch eine große Nähe zu den verschiedenen Akteuren der Sicherheitsbranche auszeichnet. Es ist wahrscheinlich diesem Vertrauen zu verdanken, dass man immer wieder Informationen aus erster Hand und für die Branche selten offene Einblicke erhält.

Dr. Alexandra Forster,
Leiterin Konzernsicherheit
bei der Bayer AG



Diesen Monat auf GIT-SICHERHEIT.de



IMPRESSUM

Herausgeber
Wiley-VCH GmbH

Geschäftsführer
Dr. Guido F. Herrmann

Senior Director, Publishing and Content Services
Dr. Katja Habermüller

Publishing Director
Dipl.-Betriebswirt Steffen Ebert

Product Manager Safety & Security
Dr. Timo Gimbel
+49 6201 606 049

Wissenschaftliche Schriftleitung
Dipl.-Verw. Heiner Jerofsky
(1991–2019) †

Anzeigenleitung
Miryam Reubold
+49 6201 606 127

Sales Director
Jörg Wüllner
+49 6201 606 748

Redaktion
Dipl.-Betrw. Steffen Ebert
+49 6201 606 709

Matthias Erler ass. iur.
+49 160 72 101 21

Cinzia Adorno
+49 6201 606 114

Tina Renner
+49 6201 606 021

Textchef
Matthias Erler ass. iur.
+49 160 72 101 21

Herstellung
Jörg Stenger
+49 6201 606 742

Claudia Vogel (Anzeigen)
+49 6201 606 758

Satz + Layout
Andreas Kettenbach

Lithografie
Elke Palzer

Sonderdrucke
Miryam Reubold
+49 6201 606 172

Wiley GIT Leserservice (Abo und Versand)
65341 Eltville
Tel.: +49 6123 9238 246
Fax: +49 6123 9238 244
E-Mail: WileyGIT@vuservice.de
Unser Service ist für Sie da von Montag - Freitag zwischen 8:00 und 17:00 Uhr

Verlag
Wiley-VCH GmbH
Boschstr. 12, 69469 Weinheim
Telefon +49 6201 606 0

Verlagsvertretung
Dr. Michael Leising
+49 36 03 89 42 800

Bankkonten
J.P. Morgan AG, Frankfurt
Konto-Nr. 6161517443
BLZ: 501 108 00
BIC: CHAS DE FX
IBAN: DE55501108006161517443

GIT SICHERHEIT
Auflage: s. ivw.de
inkl. GIT Sonderausgabe PRO-4-PRO

Abonnement 2025
10 Ausgaben (inkl. Sonderausgaben)
122,30 €, zzgl. MwSt.
Einzelheft 17 € zzgl. Porto + MwSt.

Schüler und Studenten erhalten unter Vorlage einer gültigen Bescheinigung einen Rabatt von 50 %. Abonnement-Bestellungen gelten bis auf Widerruf; Kündigungen 6 Wochen vor Jahresende. Abonnementbestellungen können innerhalb einer Woche schriftlich widerrufen werden, Versandreklamationen sind nur innerhalb von 4 Wochen nach Erscheinen möglich.
Alle Mitglieder der Verbände ASW, BHE, BID, BDSW, BDGW, BDLS, PMeV, Safety Network International, vfdb und VfS sind im Rahmen ihrer Mitgliedschaft Abonnenten der GIT SICHERHEIT sowie der GIT Sonderausgabe PRO-4-PRO. Der Bezug der Zeitschriften ist für die Mitglieder durch Zahlung des Mitgliedsbeitrags abgegolten.

Druck
westermann DRUCK | pva

Printed in Germany, ISSN 0948-9487

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

WILEY

GIT SICHERHEIT

INNENTITEL – SAFETY

Hendrik Schabsky,
CEO der Atlas GmbH & Co.KG

INNENTITEL

Von der Kuh zum Schuh

Nachhaltigkeit, Automation und Verantwortung: Atlas im Wandel der Zeit

Anlässlich des 115-jährigen Firmenjubiläums spricht Hendrik Schabsky, CEO des Sicherheitsschuhspezialisten Atlas, über die Entwicklung des Unternehmens, die Bedeutung eigener Produktionsstandorte, Nachhaltigkeit in der Sicherheitsschuhfertigung sowie die Rolle von Automation und Fußgesundheit. Das Gespräch gibt Einblicke in die strategische Ausrichtung und die Herausforderungen eines traditionsreichen Familienunternehmens im Wandel der Zeit.

GIT SICHERHEIT: Herr Schabsky, Sie führen Atlas in der fünften Generation. In diesem Jahr feiert ihr Unternehmen sein 115-jähriges Jubiläum. Was sind aus Ihrer Sicht die prägendsten Meilensteine in der Unternehmensgeschichte?

Hendrik Schabsky: Oh, da gibt es eine ganze Menge. Wenn wir heute 2025 auf 115 Jahre Atlas zurückblicken, dann stehen die ersten 50 Jahre, also die Unternehmensgeschichte in erster und zweiter Generation, ganz im Zeichen des Kohleabbaus und des Stahlbaus hier in Dortmund und im Ruhrgebiet.

Rund 300 Mitarbeitende beschäftigt das Unternehmen Atlas an seinem Headquarter in Dortmund

1971 fand dann der Umzug von Unna nach Dortmund statt. Mein Großvater, legte dann in den 70er-Jahren die Grundlagen für das weitere Wachstum. Das Thema Stahl war irgendwann vorbei im Ruhrgebiet. Wir mussten unsere Produkte weiterentwickeln, mussten schauen, wie wir den Struktur- und Kulturwandel in der Region gestalten. 2006 gründeten wir Atlas Brasil und damit unsere eigene Fertigungsstätte. Das war für uns ebenfalls einer der ganz prägenden Meilensteine. Mit diesem Schritt haben wir unsere eigene Fertigung wieder komplett ins Haus geholt.

Atlas Brasil ist eine hundertprozentige Tochter Ihres Unternehmens. Wie ich im Vorfeld erfahren habe, hat dort mittlerweile der dritte Standort eröffnet?

Hendrik Schabsky: Die Eröffnung steht kurz bevor. Wir sind gerade noch in den Endarbeiten. Wie erwähnt, haben wir 2006 die ersten Standorte ganz im Süden Brasiliens, in Lajeado und Bom Retiro eröffnet. Wir sind dort ganz nah an den Rohstoff gegangen. Denn für unsere Produkte brauchen wir nach wie vor sehr viel Leder.

Leder ist heutzutage ein Abfallprodukt der Fleischproduktion, obwohl es natürlich zugleich ein hervorragender Rohstoff ist, den wir für unsere Produkte verwenden. Sportlich sagen wir immer: „Dort, wo es gute Steaks gibt, dort gibt es auch gutes Leder." Und der dritte Standort in Teutô-

nia wird jetzt in diesem Jahr in Betrieb genommen.

Schauen wir einmal auf die letzten Jahre zurück: Sie haben die Geschäftsführung des Unternehmens in der Corona-Pandemie übernommen – ein denkbar schwieriger Zeitpunkt. Hinzukommt, dass man Teil einer langen Familien-Tradition ist, man sich aber zugleich in seinem Job beweisen muss…

Hendrik Schabsky: Absolut! Man bekommt eigentlich nichts geschenkt. Ein Familienunternehmen in fünfter Generation führen zu können, ist einerseits ein Privileg, andererseits aber auch vor allem Verantwortung, die man übernimmt. Unsere rund 1.500 Mitarbeiterinnen und Mitarbeiter, ebenso wie unsere Kundinnen und Kunden erwarten von uns tagtäglich Höchstleistungen. Und die müssen wir gemeinsam im Team, aber auch ich in eigener Person erbringen. Und ja, es macht Spaß und Freude und ich bin stolz darauf, dieses Unternehmen in fünfter Generation zu führen.

Es hat natürlich seine Vorteile, wenn man über seine eigene Produktion verfügt. Atlas hat so die volle Kontrolle, auch über die Arbeitsbedingungen.

Hendrik Schabsky: Ja, der Trend in den letzten Jahren ging auch in der Sicherheitsschuh-Branche verstärkt dahin, Aufträge an Ateliers zu vergeben. Dort werden die Produkte dann in Lohnfertigung zusammengefügt. Genau das ist bei uns eben nicht so. Das hat Vorteile in der Tat, wenn es z. B. um das Thema Lieferkettentransparenz geht, wie es das Lieferkettengesetz fordert. Und wir können dadurch natürlich auch unheimlich schnell Produktentwicklungen direkt in die Produktion mit einfließen lassen und auf saisonale Veränderungen reagieren.

Und genau dafür steht Atlas eigentlich auch. Das Thema „Lieferverfügbarkeit" ist etwas, was uns immer ausgezeichnet hat, was uns heutzutage auch immer noch der Fachhandel, der technische Fachhandel und auch die Industrie sehr hoch anrechnen. Unsere Produkte sind lieferfähig.

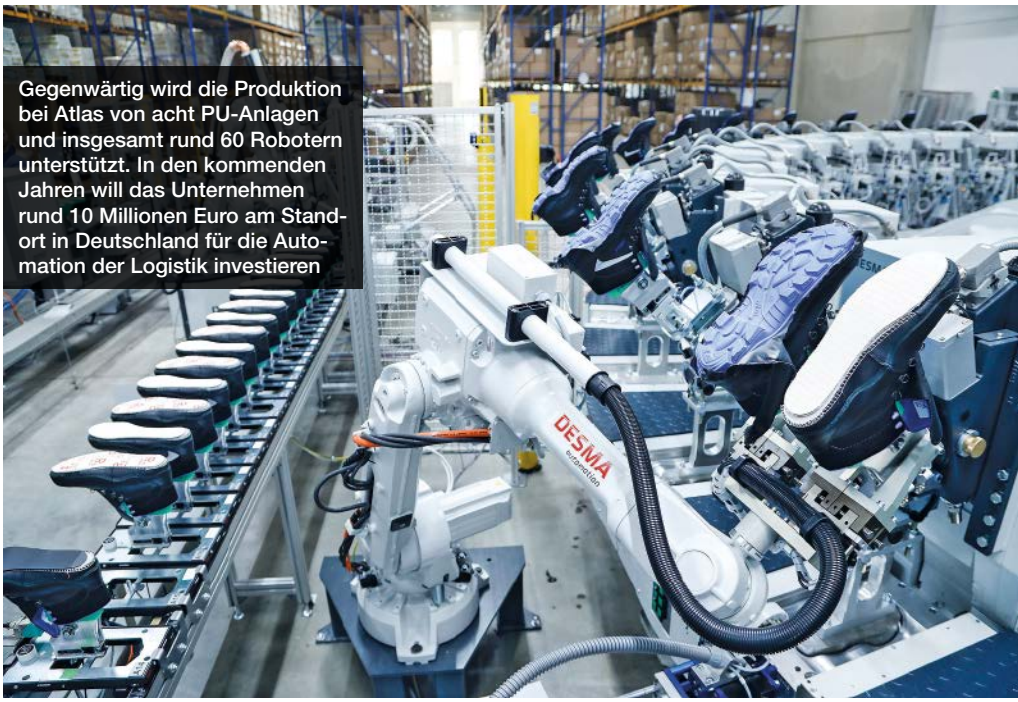
Was sind die wesentlichen Märkte für Atlas?

Hendrik Schabsky: Kernmarkt ist nach wie vor Deutschland. Wir vertreiben unsere Produkte aber heutzutage aktiv in 21 verschiedenen Ländern und haben in allen angrenzenden europäischen Ländern eigene Vertriebsteams. Wir sehen insgesamt auf dem europäischen Markt, dass die Nachfrage nach hochwertigen Produkten permanent steigt. Die Arbeitgeber geben mehr für PSA für ihre Mitarbeitenden aus. Und das ist etwas, was uns natürlich auch verpflichtet, in diesen Märkten aktiv zu sein.

Wie begegnet Atlas denn dem demografischen Wandel und dem Fachkräftemangel?

Hendrik Schabsky: Unsere Mitarbeitenden sind tatsächlich relativ jung. Einige sind aber auch schon viele Jahre dabei. Wir müssen permanent wachsen. Das Team erweitert sich praktisch ständig. Wir müssen schauen, dass wir als Arbeitgeber attraktiv sind. Da gehören verschiedenste Themen dazu.

Aber ich glaube, was uns ausmacht, ist diese Kommunikation auf Augenhöhe. Obwohl wir ein mittelständisches Unternehmen mit allein 300 Kolleginnen und Kollegen hier am Standort in Dortmund sind, schaffen wir es noch, bei zwölf Familienpizzen zu Mittag zusammenkommen und uns austauschen. Ich glaube, das ist es, was den Unterschied macht.



Gegenwärtig wird die Produktion bei Atlas von acht PU-Anlagen und insgesamt rund 60 Robotern unterstützt. In den kommenden Jahren will das Unternehmen rund 10 Millionen Euro am Standort in Deutschland für die Automation der Logistik investieren

In Deutschland zu produzieren ist teuer. Wie weit reicht bei Atlas gegenwärtig der Grad an Automation?

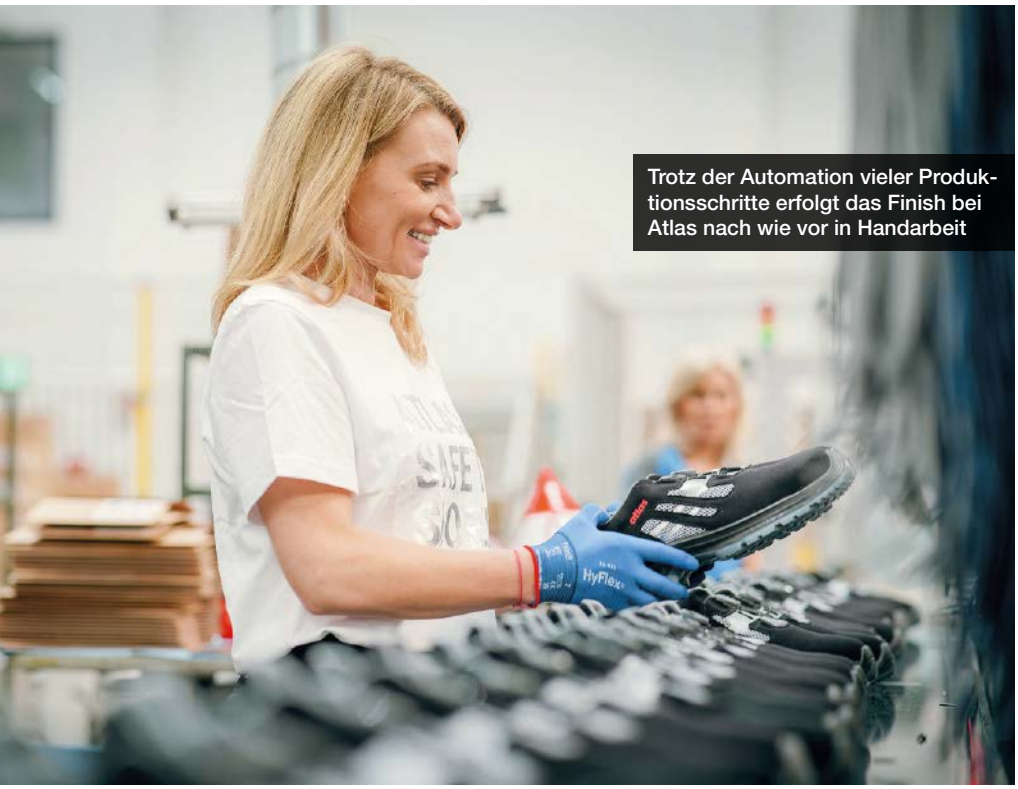
Hendrik Schabsky: Wir haben hier in der Produktion und auch in der Entwicklung rund 200 Beschäftigte am Standort. Das teilt sich einmal auf in die Logistik, aber auch in die Besohlung und das Finishing der Produkte. Die Automation haben wir in den letzten Jahren kontinuierlich erweitert. Gegenwärtig unterstützen acht PU-Anlagen und insgesamt 60 Roboter die Produktionsprozesse. Für uns ist das ein ganz wichtiger Schritt, um auch weiterhin wettbewerbsfähig zu sein. Das geht nicht ohne Automation. Und in diese investieren wir. Dennoch gibt es nach wie vor viele Arbeitsschritte, die Handarbeit erfordern, wie das Ziehen der Schnürsenkel oder das Einlegen von Einlegesohlen

Was sind für Atlas die wichtigsten Entwicklungen in den letzten Jahren gewesen. Welche Trends gibt es und wie setzt sich Atlas vom Wettbewerb ab?

Hendrik Schabsky: Fangen wir mal mit der Sohle an. Das ist nämlich sozusagen die wichtigste Komponente, auf der wir tagtäglich laufen. Ein Viertel aller Knochen stecken in den Füßen. Deshalb müssen wir ein absolutes Top-Produkt liefern. Die Sohlen fertigen wir komplett am Standort in Dortmund. Dazu nutzen wir multifunktionales Polyurethan oder kurz MPU. Jede Laufsohle, die aus Laufsohle im unteren Teil und der Mittelsohle, also der Zwischensohle besteht, wird hier im Hause selbst geschäumt. Wir verwenden dazu also keine thermoplastischen Granulate, wie zum Beispiel TPU, was nur aufgeschmolzen wird. Sondern es wird wirklich jede Sohle hier im Hause gefertigt und dann auch individuell für die verschiedensten Arbeitsbereiche geschäumt. Wir nutzen verschiedene Rezepturen. Das ist nach wie vor ein absoluter USP aus dem Hause Atlas.

Zudem waren Strickmaterialien ein wichtiges Thema und wie man diese additiv fertigen kann. Ferner waren nahtlose Obermaterialien von großer Bedeutung, wie sie

Bitte umblättern ▶



Trotz der Automation vieler Produktionsschritte erfolgt das Finish bei Atlas nach wie vor in Handarbeit

in unserer Runner-Serie zum Einsatz kommen. Wir schauen heutzutage aber auch in der Industrie auf das Thema Gore-Tex. Wie können wir z. B. im Outdoor-Bereich noch besser werden? Wie können wir das Thema Atmungsaktivität, Wasserdichtigkeit und alle anderen Performance-Ansprüche in einem Produkt noch besser zusammenbringen?

Beim Begriff Gore-Tex denkt man natürlich schnell an das Obermaterial „Extraguard". Auf der A+A 2023 war Atlas das erste Unternehmen, das eine ganze Serie vorgestellt hat, bei der Extraguard zur Anwendung kam.

Hendrik Schabsky: Wir waren eine der Ersten, die wirklich vom Halbschuh bis hin zum Stiefel eine entsprechende Kollektion vorgestellt haben. Es geht natürlich zum einen um das Innenfutter Gore-Tex mit der Membran, nun aber in Kombination mit einem optimalen Obermaterial.

In der Vergangenheit kam hierbei fast ausschließlich Leder zum Einsatz. Der Einsatz von Extraguard ermöglicht allerdings eine noch bessere Atmungsaktivität. Der entscheidende Faktor aber ist, dass Wasser nicht so stark aufgenommen wird. Leder saugt Wasser an, der Schuh wird also schwerer. Saugt sich das Material voll, entsteht dadurch auch eine Kältebrücke. All diese Nachteile von Leder hat Extraguard eben nicht.

Wie wichtig ist denn das Thema Nachhaltigkeit bei Atlas?

Hendrik Schabsky: Wir waren schon die letzten 20 Jahre Pioniere beim Thema Nachhaltigkeit. Hier am Standort in Dortmund haben wir im Bereich der Gebäudeinfrastruktur wie zum Beispiel dem Ausbau der Photovoltaik viel gemacht, um nachhaltig zu sein. In Brasilien haben wir seit geraumer Zeit unsere eigene Kindertagesstätte, was auch etwas Nachhaltiges ist, wenn es um die sozial-ökonomischen Faktoren geht.

In den letzten zwei, drei Jahren haben wir für uns aber speziell den Fokus gesetzt, dass wir Nachhaltigkeit ins Produkt bringen. Das haben wir u. a. mit unserer Runner-Serie ermöglicht, bei der sowohl in der Laufsohle und auch in der Zwischensohle Rezyklate eingesetzt werden. PU-Reste, die wir z. B. als Austrieb haben, werden hier am Standort direkt granuliert und der Produktion wieder zugeführt. Auf diese Art können wir Rezyklate wieder in das Produkt bringen. Nachhaltiger geht es eigentlich nicht, wir sparen Abfall und bringen gleichzeitig Top-Material wieder in den Schuh.

Recyceltes Polyester als Obermaterial wird mittlerweile auch standardmäßig eingesetzt, sodass wir insgesamt immer mehr Rezyklate in die Produkte bekommen. Auch alle unsere Einlegesohlen sind heutzutage mit Rezyklaten ausgestattet.

Das Thema Fußgesundheit ist bei Atlas ebenfalls ein zentraler Schwerpunkt?

Hendrik Schabsky: In der Tat! Wir sind heutzutage eben nicht nur ein Schuhfabrikant, sondern wir sind auch Dienstleister. Das Thema Fußgesundheit in den Fokus zu stellen, ist eines meiner persönlichen Anliegen. Wir wollen darüber aufklären, wie wichtig das Thema Fußgesundheit ist.

Ich sagte es vorhin schon, ein Viertel aller Knochen steckt in den Füßen, das wissen viele gar nicht. Sie sind sozusagen das Fundament, auf dem wir tagtäglich laufen und letztlich auch die Performance der Mitarbeitenden ganz maßgeblich beeinflussen können. Dafür haben wir ein Konzept entwickelt, das nennt sich Fit-Day. Wir fahren mit unseren Produktexperten, Orthopädieschuhmachern, Meister- und Meisterinnen raus an die Werkbänke der Industrie und machen dort Fußvermessungen, 3D-Fußvermessungen bis hin zur Individualisierung über die Einlegesohle.

Das Spektrum bei den Einlegesohlen reicht von unseren sogenannten Ergo-Med Sohlen, über die Fit InSole, eine semi-orthopädische Einlegesohle die individuell angepasst wird, bis hin zur orthopädischen Einlegesohle, die wir gemeinsam mit GetSteps versenden. Das ist absolut ein Servicethema und auch ein definitives Alleinstellungsmerkmal, dass wir diesen Service flächendeckend in Europa anbieten können.

Zum Schluss wollen wir noch einen Blick in die Zukunft werfen. Im November steht die A+A an und Atlas wird dort voraussichtlich mit zwei neuen Serien aufwarten …

Hendrik Schabsky: Ja, mehr verrate ich jetzt auch nicht. Zur Messe werden wir natürlich das Thema Fit-Day und die Dienstleistung nochmal in den Fokus stellen. Wir werden, wie schon gesagt, zwei neue Serien präsentieren: Eine Serie, die speziell im S1-Bereich wichtig ist. Da können sich Atlas-Fans auf etwas ganz Neues freuen. Strickmaterialien werden dabei eine Rolle spielen ebenso wie eine neue Sohle. Und im S3-Bereich werden wir auch nochmal eine Lederalternative vorstellen. GIT

Atlas GmbH & Co.KG
www.atlasschuhe.de

ADVERTORIAL

Auffangwannen für verschiedenste Einsatzzwecke

Fässer, IBCs, Behälter, Kanister, Gebinde etc. mit brennbaren und nicht brennbaren, aber wassergefährdenden Flüssigkeiten, wie z.B. Öle, Farben, Lacke, Emulsionen, Verdünnungen, Reinigungsmittel dürfen nur so gelagert werden, dass bei einer eventuellen Leckage keine Stoffe ins Erdreich und somit ins Wasser gelangen können.

Über 55 Jahre Erfahrung machen die Bauer GmbH zu einem kompetenten Partner rund um die sichere Lagerung umweltgefährdender Stoffe. Je nach Einsatzzweck und Ort bietet das Südlohner Unternehmen eine Vielzahl von Produktlösungen. Für die sichere Lagerung von Fässern und IBCs im Innenbereich sind Auffangwannen in verschiedensten Ausführungen und Größen erhältlich. Mit Hilfe von Regalwannen bzw. Einhängewannen können auch bestehende Regalsysteme wirtschaftlich und schnell gesetzeskonform umgerüstet werden, so dass wassergefährdende Stoffe gelagert werden können. Für den Außenbereich sind geschlossene Regalcontainer mit Flügel -oder Schiebetoren und integrierten Auffangwannen die erste Wahl.

BAUER® SÜDLOHN

Kontakt
BAUER GmbH
www.bauer-suedlohn.com

CEMO
für sicheres Lagern

Akku-Lade- und Lagerschränke
mit Explosionsschutz

standardisierter **Batterie-brandtest**
nach VDMA Einheitsblatt 24994:2024-08

Schutz ohne Zeitlimit

Keine Kompromisse. Keine Zeitgrenze.
Hält Batteriebränden vollständig stand.
Kein Austritt von Flammen oder Funken.

Live Talk 25.09.2025 | 9:30 Uhr

Wiley Industry Talks: Anforderungen an Ladeschränke für Li-Io-Batterien in 2025.
events.bizzabo.com/730766

CEMO GmbH
www.cemo.de/lockex

Innovative Zukunftstechnik trifft Tradition: Die Fels-Werke nutzen für das Management ihrer Gasmessgeräteflotte beim Abbau von Kalkstein und dessen Weiterverarbeitung die cloudbasierte Softwarelösung Gas Detection Connect von Dräger

GASMESSUNG

Digitale Gasmesstechnik in der Kalkindustrie

Mehr Schutz und Effizienz durch smarte Vernetzung

Digitales Gasmonitoring und die automatisierte Geräteverwaltung über eine Cloudsoftware sind mögliche Meilensteine auf dem Weg, Sicherheitsprozesse zu optimieren und neues Wissen zu erzeugen. Schon heute bieten vernetzte Hardware-Systeme und Datenplattformen mehr Transparenz über den Zustand von Industrieanlagen und Arbeitsplätzen. Diese und weitere Smart-Safety-Lösungen können für einen sicheren, transparenten und effizienten Betrieb in der Rohstoffwirtschaft und Prozessindustrie sorgen.

Digitalisierte Gasmesstechnik überwacht traditionelles Kalkbrennen

Beim Betrieb der Kalkschachtöfen der Fels-Werke GmbH treffen jahrhundertealtes Materialwissen und Zukunftstechnik aufeinander: Kalkbrennen, die Herstellung von Calciumoxid (CaO), ist seit der Antike bekannt und wurde seither immer wieder weiterentwickelt. Dabei wird Calciumcarbonat (CaCO3) in der Form von Kalkstein durch einen festen, flüssigen oder gasförmigen Brennstoff auf rund 1.000 Grad Celsius erhitzt. So entsteht Branntkalk, der durch das Löschen mit Wasser zu Löschkalk (Ca(OH)2) wird.

Während der Produktion sorgen mobile Gasmessgeräte für eine hohe Arbeitssicherheit. Hier hat das vor 85 Jahren unter dem Namen „Stein und Erden GmbH“ gegründete Unternehmen aus Goslar seit 2021 eine digitale Transformation vorgenommen: Die Fels-Werke nutzen für das Management ihrer Gasmessgeräteflotte die cloudbasierte Softwarelösung Gas Detection Connect von Dräger.

„Smart Safety“ steht für die Digitalisierung von sicherheitsrelevanten Prozessen und Aufgaben. Sie basiert grundsätzlich auf der Verfügbarkeit von vielfältigen Daten, die zu einem wertvollen Wissensvorsprung im Geschäftsbetrieb werden. Innovative Services rund um Messtechnik, Schutzausrüstung und Zubehör schaffen auf Basis

von Gerätedaten, Sensorwerten, Bild- und Kartenmaterial oder lokalen Informationen einen Mehrwert und eine Entlastung für die Anwender. Das bestätigt Thomas Ullrich, wenn er von seinem täglichen Umgang mit der Dräger-Gasmesstechnik berichtet. Als Messtechniker ist er in den Fels-Werken für eine über sechs Standorte verteilte Flotte von rund 150 Dräger-Gasmessgeräten und X-dock-Prüfstationen verantwortlich.

Dieser Bestand wird seit zwei Jahren mit Gas Detection Connect verwaltet. „Mit diesem System kann man sekundenschnell nachvollziehen, dass ein Mitarbeiter bei einem bestimmten Einsatz das Gasmessgerät genutzt hat, dass es vorher getestet wurde und dass es einsatzbereit ist“, sagt Ullrich.

Alle Komponenten der cloud-basierten Softwarelösung Gas Detection Connect von Dräger

Kontinuierliche Gasüberwachung in der Weiterverarbeitung

Die digital vernetzte Gasmesstechnik soll die Sicherheit durch die Nutzung von Echtzeitdaten weiter erhöhen. „In unseren fünf Tagebau-Betrieben, in denen Kalkstein abgebaut wird, stellen Gase meist kein Problem dar“, berichtet Thomas Ullrich. „Wichtiger ist die kontinuierliche Überwachung der Atmosphäre während der Weiterverarbeitung in den 37 aktuell betriebenen Kalkschachtöfen.“ Diese Anlagen werden in fortlaufender Verbrennung betrieben. Solange sie glühen, ist Gasmesstechnik essenziell, vor allem zum Schutz der Arbeitskräfte vor Kohlenstoffmonoxid. Dessen Konzentration wird daher kontinuierlich mit Eingaswarngeräten vom Typ Dräger Pac überwacht. „Ohne diese Geräte darf niemand die Gicht – so heißt der obere Teil des Schachtofens – betreten“, erklärt Ullrich.

Konnektive Prüfroutine über die Sicherheitsstandards hinaus

Getestet werden die Gasmessgeräte bei den Fels-Werken nicht nur arbeitstäglich, sondern vor jedem einzelnen Einsatz. „Damit übertreffen wir die Anforderungen der Merkblätter T 021 und T 023 der BG RCI“, sagt Messtechniker Ullrich. T 021 („Gaswarneinrichtungen und -geräte für toxische Gase/Dämpfe und Sauerstoff – Einsatz und Betrieb“) sowie T 023 („Gaswarneinrichtungen und -geräte für den Explosionsschutz – Einsatz und Betrieb“) definieren in Deutschland den Standard für die Verwendung von Gasmessgeräten für die Arbeitsplatzsicherheit. Diese unternehmerische Entscheidung ist ein echtes Plus für die Arbeitssicherheit, die durch vernetzte Teststationen mit digitaler Infrastruktur erleichtert wird. Insgesamt acht Dräger-Dockingstationen und passende Prüfgase stehen bei den Fels-Werken für die Prüfungen, auch Bumptests genannt, zur Verfügung. Die Stationen übertragen nicht nur die Datenlogger aller mobilen Gaswarngeräte und die Ergebnisse der Prüfungen an die Cloudsoftware, sondern übertragen auch Firmware-Updates aus der Cloud an die Gasmessgeräte.

Die X-dock-Stationen beziehen ihre eigenen Firmware-Updates ebenfalls von der Cloudsoftware Gas Detection Connect – per Knopfdruck

Arbeitsplatzüberwachung mit digitalem Live-Monitoring

Stellt die digitale Verwaltung der Messgeräteflotte einen Qualitätssprung im Management der Technik dar, so führt das Smart-Safety-Portfolio mit seinen Live-Monitoring-Systemen zu einer erheblichen Steigerung der Sicherheit. Die Überwachung einer Variante, eines Gases und einer Kontamination erfolgt dabei ebenfalls mit der Gas Detection Connect Software: Gasmessgeräte werden via Bluetooth mit einem explosionsgeschützten Smartphone oder dem smarten Datengateway ConHub gekoppelt. Diese senden je nach betrieblichen Regelungen Daten wie Messwerte, GPS-Koordinaten, Alarme und auf Wunsch den Namen des Geräteträgers über eine mobile App an die Cloud. Der Vorteil: Wird ein Alarm ausgelöst, läuft dieser in Echtzeit in der Messwarte, im Gasschutzwesen, in der Gruben- oder Werksfeuerwehr auf und wird auf einer Karte visualisiert. So lassen sich Gasvorkommen, Leckagen, Vorfälle, Arbeitsplatzbelastung und Kontamination schnell von allen relevanten Personen bewerten und automatisch dokumentieren. GIT

Drägerwerk AG & Co. KGaA
www.draeger.com


© Christoph Ryll

ROBOTIK-SAFETY

Führerschein für den Greifarm

Roboterführerschein, Normenentwicklung und Sicherheitsanforderungen: Wie neue Standards die Qualifizierung in der Robotik verändern

Die Robotik entwickelt sich rasant – von stationären Industrierobotern über kollaborative Systeme bis hin zu mobilen Plattformen und humanoiden Robotern. Mit dem Roboterführerschein des Deutschen Robotik Verbands entsteht erstmals ein standardisiertes Qualifizierungsformat für den sicheren Umgang mit Robotern. Unser Interview mit Christoph Ryll, Geschäftsführer bei Robotics Consulting und Fachmann für gesetzliche Vorgaben, Normung und Sicherheitsfragen in der Robotik beim Deutschen Robotik Verband (DRV), beleuchtet regulatorische Entwicklungen, Herausforderungen in der Risikoanalyse und die Rolle des Roboterführerscheins für die Sicherheitsbranche.

Was war der Impuls für die Entwicklung des Roboterführerscheins durch den Deutschen Robotik Verband?

Christoph Ryll: Wir haben den DRV gegründet, weil wir an die Robotik als Zukunftstechnologie glauben. Und wir glauben auch weiterhin an den Standort Deutschland. Kurz gesagt, Robotik aus Deutschland und für Deutschland. Für die Sicherung des Wohlstands und einer technologischen Überlegenheit ist die Aus- und Weiterbildung essenziell. Die Robotik ist sehr vielfältig. Wenn ein potenziell neuer Mitarbeiter mit einem Zertifikat um die Ecke kommt, dann weiß der Arbeitgeber oft nicht, was diese Person tatsächlich tun und ob man den Menschen neben oder mit dem Roboter arbeiten lassen kann. Wir möchten hier mehr Klarheit bringen und den Arbeitgebern mehr Sicherheit verschaffen. Es soll ein einheitliches Aus- und Weiterbildungssystem entstehen – daher auch der Zusatz Führerschein. Wenn eine Person den Führerschein der Klasse B besitzt, dann ist jedem klar, dass sie einen Pkw lenken, aber deshalb dennoch nicht als Busfahrer arbeiten kann.

Welche Zielgruppen sollen mit dem Roboterführerschein konkret angesprochen werden – und warum?

Christoph Ryll: Zu unseren Zielgruppen gehören sowohl Robotikneulinge als auch bereits erfahrene Experten, die sich weiterbilden oder ihr Wissen in einem bestimmten Gebiet auffrischen möchten. Die primäre Zielgruppe sind jedoch Anfänger, bzw. Robotikanwender mit leicht fortgeschrittenen Kenntnissen. Denn diese Personen können das meiste aus dem DRV-Roboterführerschein rausholen.

In nächster Zukunft, davon bin ich überzeugt, wird alles auf irgendeiner Art und Weise mit Robotik zu tun haben. Hier bin ich ganz bei Jensen Huang, dem CEO von Nvidia. Wir brauchen nicht nur in der Industrie ein viel besseres Verständnis für die Robotik, sondern auch in der breiten Masse der Bevölkerung. Prinzipiell wäre es wünschenswert, wenn die Grundlagen der Robotik, hierzu würde ich auch das Programmieren zählen, bereits in der Schule vermittelt werden. Neben der Ausbildung bietet der Roboterführerschein auch Weiterbildungsmöglichkeiten für erfahrene Industrieexperten, die einen Auffrischungskurs benötigen, oder sich über die neuesten Entwicklungen oder Gesetzesänderungen informieren möchten.

Wie ist der Roboterführerschein strukturiert und welche Inhalte decken Pflicht- und Wahlmodule ab?

Christoph Ryll: Unser Ziel mit dem Roboterführerschein des Deutschen Robotik Verbands ist es, Robotik für alle verständlich und zugänglich zu machen. Jeder der möchte sollte „Robotisch“ sprechen können. Daher gehört zu den Grundlagen, alles kennen zu lernen, was die Robotik ausmacht. Neben der Industrierobotik umfasst das auch Themen wie Service Robotik, Humanoide und natürlich kollaborative Robotik.

Auch Quereinsteiger, die noch nichts von der Robotik gehört haben, sollen sich hier wiederfinden und von Anfang an lernen, was Robotik bedeutet. Zum Pflichtteil gehören daher unter anderem die Einführung in die Geschichte der Robotik sowie die Vermittlung der Grundlagen der Regularien und der Robotersicherheit.

Selbstverständlich muss man es auch „begreifen“. Somit ist auch der praktische Umgang, das Angreifen/Anfassen und etwas mit dem Roboter selbst zu tun, essenziell. Zu den Pflichtgrundlagen gehört daher auch ein Programmierkurs, der mehrere Tage umfasst. Jeder Teilnehmer soll einen Roboter bewegt und einfache Programme selbst erstellt haben.

Nach diesem Grundkurs oder Pflichtteil steht es jedem frei, in Form seines eigenen individuellen Führerscheins seine Spezialisierung zu erlernen. Möchte man z. B. eher in die Richtung Projektmanagement gehen, dann sollten Effizienz und rechtliche Grundlagen weiter vertieft werden. Geht man hingegen den Weg des Servicetechnikers oder Instandhalters, ist es sinnvoll, sich auf weitere Hardwarekomponenten in der Robotik zu konzentrieren.

Beim Roboterführerschein gehen wir so weit, dass wir den akademischen Teil mithilfe unserer Partner-Universitäten und Hochschulen auch komplett abdecken können. Robotik für Akademiker ist somit ebenfalls ein fester Bestandteil des deutschen Robotik Führerscheins. Dies war auch von Anfang an unser Ziel. Wir wollten die Grundsteine legen, also das Basiswissen vermitteln und gleichzeitig gewährleisten, dass sich die Teilnehmer individuell weiterentwickeln können.

Welche Rolle spielen aktuelle Normen und regulatorische Entwicklungen – etwa in der MVO – für die Gestaltung der Inhalte?

Christoph Ryll: Gerade jetzt ändert sich sehr viel in den Regularien. Wir werden ab 2027 eine neue Maschinenverordnung (MVO) haben. Zugleich haben sich mit Februar 2025 die Roboternormen erneuert und lösen die 2011 publizierten harmonisierten Normen ab. Der Umfang der Roboternormen ist dabei von 90 Seiten auf circa 250 Seiten angestiegen. Und speziell das Kapitel Sicherheitsfunktionen und deren Eigenschaften erstreckt sich nun auf über 8 Seiten.

Gegenwärtig sind jedoch noch die Vorgaben der Maschinenrichtlinie 2006/42/EG anzuwenden. Hierzu gehören auch die beiden harmonisierten Normen EN ISO 10218 Teil 1 und Teil 2. Wer also heute ein Robotersystem entwickeln, konstruieren, bauen, oder am Markt bereitstellen möchte, wird diese Rechtslage und Normenlage verwenden müssen.

Gleichzeitig müssen wir aber aufzeigen, was demnächst passieren wird. Entsprechend werden auch die Vorgaben der neuen Maschinenverordnung beim Roboterführerschein berücksichtigt.

Ganz ähnlich verhält es sich mit der neuen Roboternorm. Sie ist als ISO Norm im Februar 2025 publiziert worden und wird so auch demnächst als Europäische Norm übernommen werden. Entsprechend sind sowohl die bestehende Maschinenrichtlinie, die neue Maschinenverordnung und die neue Roboternorm fester Bestandteil des Roboterführerscheins.

Wie verändert sich die Risikoanalyse bei kollaborativen oder mobilen Robotern im Vergleich zu klassischen Industrierobotern?

Christoph Ryll: Die Risikobeurteilung bei kollaborativen Robotern ist etwas aufwändiger als bei klassischen Industrierobotern. Bei der klassischen Industrierobotik greift man auf eine seit 50 Jahren bewährte Risikominderungsmaßnahme – die trennende Schutzeinrichtung zumeist in Form eines Zauns – zurück. Roboter und Mensch bleiben dadurch physisch getrennt.

Bei den sogenannten kollaborativen Robotersystemen oder in der mobilen Robotik gibt es solche trennenden Schutzeinrichtungen hingegen nicht. Hier ist es auch vollkommen egal, ob Mensch und Roboter tatsächlich kollaborativ, also sprichwörtlich Hand in Hand arbeiten oder man einfach nur ohne Zaun arbeiten will. In beiden Fällen ist es jederzeit möglich, von allen Seiten zum Roboter zu gelangen – ob gewollt oder ungewollt.

Bei der Risikobeurteilung muss man jedoch noch genauer ins Detail gehen. So gibt es sehr viele Einsatzszenarien und dem gemäß auch sehr viele Möglichkeiten, wie man zum jeweiligen Roboter gelangen kann. Noch vielfältiger sind die möglichen Scherstellen oder Stellen, an denen es zu Kollisionen bzw. Quetschungen kommen kann.

Auch das Wie spielt dabei eine große Rolle: Es macht einen großen Unterschied, ob man nur mit einer Hand oder mit dem ganzen Kopf in die Applikation hineingelangen kann. Grob gesagt, benötigt man für eine Risikobeurteilung für ein kollaboratives respektive zaunloses System etwa 30 bis 40 % mehr Zeit, da man im Vergleich zu einem Industrierobotersystem viel mehr Einzelaspekte betrachten muss.

Bitte umblättern ▶

Der Roboterführerschein enthält neben der Theorie auch einen praktischen Teil direkt am Roboter. Hier ein UR 3 mit dem Kraftmessgerät GTE-KMG75

Wie wird mit dem Spannungsfeld zwischen KI-gestützten Robotern und sicherheitsgerichteten Anforderungen umgegangen?

Christoph Ryll: Hier haben wir ein sehr spannendes, aber auch schwieriges Thema.

Erst dank künstlicher Intelligenz (KI) war es möglich, eine Vielzahl von Aktoren zur gleichen Zeit anzusteuern und diese Bewegungen effizient umzusetzen. Für einen Programmierer war es zuvor sehr zeitintensiv diese Anzahl von Aktoren zu synchronisieren. Dank der Unterstützung von KI ist dies nun sehr effizient möglich.

Jedoch sehe ich persönlich im Bereich der Maschinensicherheit Hürden, die noch nicht geklärt sind. Wenn ich ein Robotersystem validieren möchte, so muss ich Bewegungen und Gefährdungen vorhersagen können und speziell bei Gefährdungen und Verletzungen beurteilen, wann und mit welcher Wahrscheinlichkeit diese statistisch eintreten werden. KI in der Maschinensicherheit erlaubt mir diese Vorhersage nicht.

In der Ansteuerung der Bahnplanung der Aktorik, also im Programmteil, liegt für mich die einzige sinnvolle und mögliche Anwendung von KI in der Robotik. Und diese künstliche Intelligenz im Programmteil muss durch statische klassische Sicherheitsfunktionen abgesichert sein. Darunter fallen z. B. Limitierungen wie die maximale Geschwindigkeit oder die Größe des Arbeitsraums. In der kollaborativen Robotik kommen weitere Parameter für eine solche Sicherheitsfunktion hinzu, z. B. mit welcher Kraft und mit welcher Leistung der Roboter betrieben werden darf.

Welche Perspektiven sehen Sie für humanoide Roboter – und wie bereitet der Roboterführerschein auf diese Entwicklungen vor?

Christoph Ryll: Meiner Meinung nach werden uns humanoide Roboter schneller „überrennen“, als wir es uns aktuell vorstellen können.

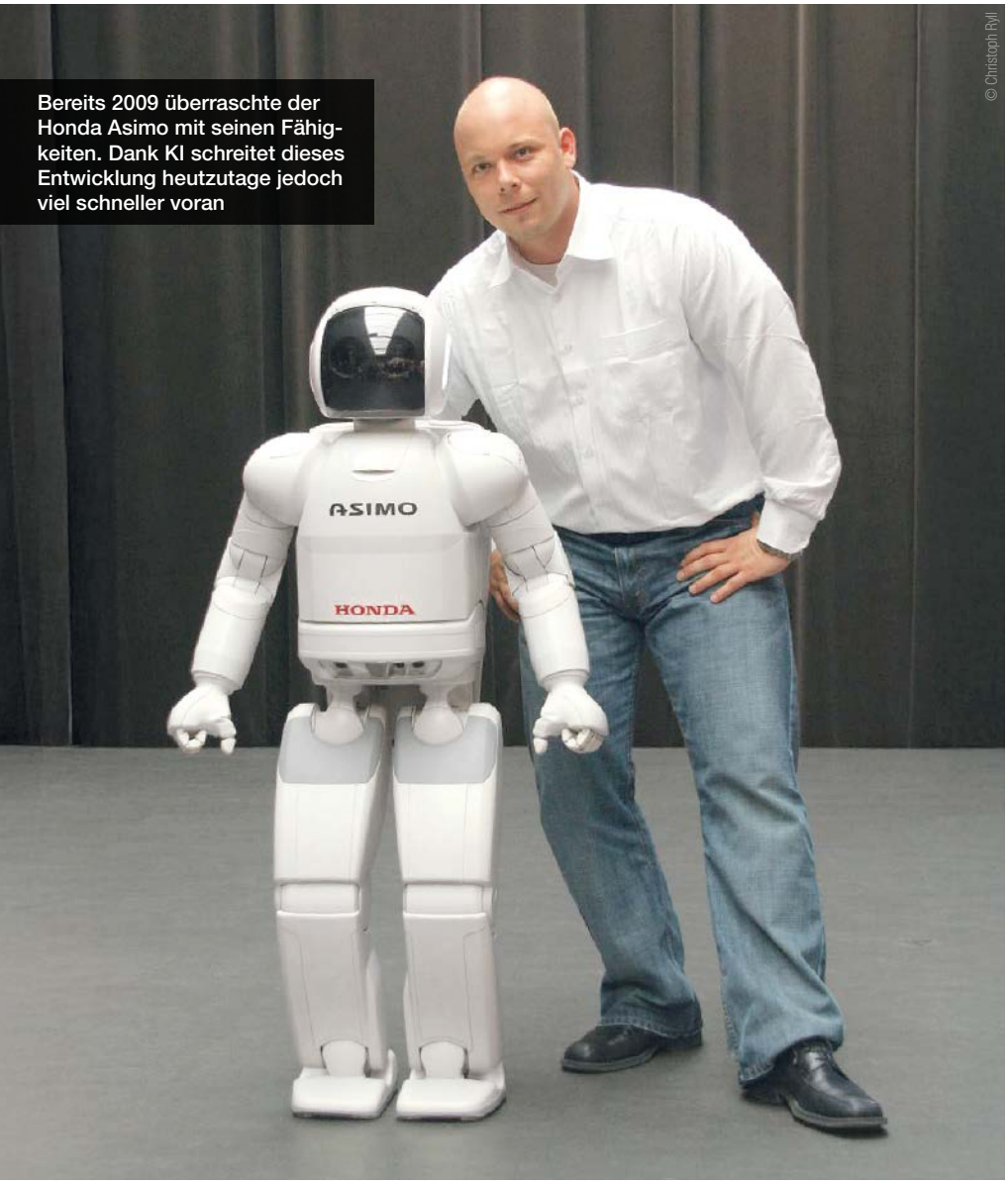
Aktuell gibt es zwar immer noch erst einigen Prototypen, die in kontrollierten Umgebungen vor allem für Marketingzwecke gute Dienste leisten. Andererseits haben sich die Entwicklungszeiten für solche Humanoide massiv verkürzt, da wir dank der künstlichen Intelligenz die Vielzahl der Aktoren synchron bewegen können.

Humanoide Roboter sind nach meinem Verständnis die nächste Evolutionsstufe des mechanisierten Helfers. Man bedenke nur, welche Voraussetzungen wir aktuell schaffen müssen, um Industrieroboter oder kollaborative Roboter in das für Menschen geschaffene Umfeld zu integrieren. Da ist der dem Menschen nachempfundene Humanoide klar im Vorteil. Er passt perfekt in unsere Umwelt.

Ich selbst durfte im Jahre 2009 den Honda Asimo sehen und war damals schon überrascht, was alles möglich war. Mit dem heutigen Wissen ist das aber absolut nicht zu vergleichen. Denn der Asimo wurde aus dem Hinterzimmer mit einer Vielzahl an Programmierern und Entwicklern gesteuert. Heutige Humanoide können tausendmal mehr.

Der Roboterführerschein kann diesbezüglich aktuell da auch nur einen Ausblick geben und die aktuellen Trends aufzeigen. Tatsächliche Anwendungsfälle gibt es leider noch nicht und wenn dann sind diese rein in der Entwicklung oder Forschung zu verorten.

Aber auch im Deutschen Robotik Verband hören wir, wenn wir dieses Thema beim Roboterstammtisch, welcher jeden zweiten Dienstag im Monat stattfindet, ansprechen, dass diese Technologie eine rege Diskussion verursacht. Viele sind begeistert, es gibt aber auch viele Fragen, Ängste und Sorgen. Ob man will oder nicht – humanoide Roboter stehen derzeit im Mittelpunkt des öffentlichen und fachlichen Interesses. Ich persönlich denke, die Humanoiden haben das Thema MRK (Mensch Roboter Kollaboration) oder Industrie 4.0 aus jedem Vortrag erfolgreich abgelöst und sind aktuell der ganz große Hype. Ich bin mir sicher, dass wir in fünf, spätestens aber in zehn Jahren das als gegebene Technik ansehen werden, so wie heute die Cobots. GIT



Bereits 2009 überraschte der Honda Asimo mit seinen Fähigkeiten. Dank KI schreitet dieses Entwicklung heutzutage jedoch viel schneller voran

Mehr zum Roboterführerschein

Deutscher Robotik Verband e.V. (DRV)
https://robotikverband.de

Korrektionsschutzbrille

Bollé Safety präsentiert mit der STKS 420 das neueste Produkt seiner Korrektionsschutzbrillenserie für den industriellen Bereich. Mit seinem modernen Design passt sich das Modell unterschiedlichsten Situationen an und bietet hohen Tragekomfort – auch bei längerem Einsatz. Korrektionsschutzbrillen werden oft als unattraktiv und unbequem empfunden. Deshalb hat Bollé Safety die STKS 420 entwickelt: eine trendige Schutzbrille, die moderne Technologien und langlebige Materialien für hohen Tragekomfort und maximale Widerstandsfähigkeit vereint. Das Modell STKS 420 wurde speziell für die Anforderungen in industriellen Umgebungen entwickelt. Die Brille zeichnet sich durch ein modernes Design aus und spiegelt den wachsenden Trend auf dem PSA-Markt wider, Stil und Persönlichkeit auch bei der Arbeit zu verbinden. Sie eignet sich für den ganztägigen Einsatz und bietet zertifizierten Schutz nach Norm EN 166.

© Bollé Safety | Semaphore&Co

www.bollesafety.com/de

Fristads Neuheiten auf der A+A

Ab September 2025 präsentiert Fristads neue Produkte – mit innovativen Materialien, neuen Schnitten und Funktionen, die sich an jede Arbeitssituation anpassen. Im Mittelpunkt stehen die ATHF Stretch-Kollektion mit umfassendem Multinorm-Schutz in Kombination mit optimaler Bewegungsfreiheit sowie die Tyresta-Kollektion mit neuen Arbeitshosen, die mit flexiblen Werkzeugtaschen individuell kombinierbar sind – sicher und fest dank Magnetsystem. Ergänzt werden die Kol-lektionen durch weitere praxisorientierte Modelle. Das leichte, weiche Stretchge-webe (265 g/m²) der Flamestat Multinorm Stretch-Kollektion besteht aus Modacryl, Baumwolle, Polyamid, Elastan und antistatischer Faser. Es ist inhärent flammhemmend – die Schutzeigenschaften bleiben über die gesamte Lebensdauer erhalten. Ob Multinorm-Schutz mit Stretchkomfort oder modulare Workwear mit Magnetsystem – die Fristads Neuheiten 2025 sind live auf der A+A Messe in Düsseldorf zu sehen.

© Fristads

A+A: Halle 15, Stand F46

www.fristads.com/de

Fristads setzt auf inklusive Arbeitskleidung

Wer hart arbeitet, braucht Ausrüstung, die funktioniert – unabhängig von Geschlecht, Körperbau oder Konfektionsgröße. Fristads verfolgt daher konsequent eine klare Strategie: Arbeitskleidung muss für alle passen. Mit einem der breitesten Größensortimente der Branche, geschlechtsspezifischen Schnitten und Speziallösungen wie Umstandshosen geht das Unternehmen neue Wege im Bereich Inklusion – funktional, praxisnah und nachhaltig. Werkzeugtaschen zu hoch, Kniepolster an der falschen Stelle: Was zunächst wie ein Designfehler wirkte, entpuppte sich als falsch gewählte Größe. Solche Situationen zeigen, wie wichtig die Passform für Sicherheit, Bewegungsfreiheit und den Tragekomfort ist. „Sie entscheidet über die Alltagstauglichkeit unserer Kleidung – deshalb legen wir auf die Passform größten Wert“, sagt Anastasios Lappas, Head of Design & Innovation bei dem schwedischen Workwear-Hersteller Fristads.

www.fristads.com/de

Psychische Belastungen am Arbeitsplatz nehmen zu – ein Trend, der durch Digitalisierung, ständige Erreichbarkeit und steigende Komplexität der Arbeitswelt verstärkt wird. Im Interview mit der Arbeitspsychologin Ivon Ames, Arbeitspsychologin, Wissenschaftlerin an der FernUniversität Hagen und Geschäftsführerin EVAO GmbH, beleuchtet GIT SICHERHEIT die Ursachen, Auswirkungen und präventiven Maßnahmen im Kontext moderner Arbeitsgestaltung. Besonderes Augenmerk liegt auf der Rolle psychologischer Expertise im betrieblichen Arbeitsschutz sowie den Herausforderungen und Chancen für Unternehmen im Umgang mit psychischer Gefährdungsbeurteilung.

© Ivon Ames

ARBEITSSCHUTZ

Wenn Arbeit krank macht – und was Unternehmen dagegen tun können

Arbeitspsychologin Ivon Ames spricht über die Bedeutung präventiver Maßnahmen

GIT SICHERHEIT: Frau Ames, erzählen Sie uns bitte zunächst etwas über Ihren persönlichen Werdegang und wie Sie zur Arbeitspsychologie gekommen sind.

Ivon Ames: Ich habe zunächst Betriebswirtschaftslehre studiert und war über 12 Jahre in der Automobilindustrie tätig, vor allem in strategischen Funktionen. Dabei wurde mir zunehmend bewusst, wie stark Arbeitsbedingungen die Gesundheit und auch Leistungsfähigkeit beeinflussen. Das hat mich zum Psychologie-Studium geführt. Heute bin ich Arbeits- und Organisationspsychologin, forsche an der FernUniversität in Hagen zur gesundheitsförderlichen Arbeitsgestaltung und berate mit meinem Team in unserer Ausgründung EVAO Unternehmen zu genau zu diesen Themen. Im Berufsverband Deutscher Psychologinnen und Psychologen engagiere ich mich zudem im Vorstand der Sektion Wirtschaftspsychologie.

Psychische Belastungen am Arbeitsplatz nehmen zu – woran liegt das aus Ihrer Sicht und wie äußert sich das in der Praxis?

Ivon Ames: Der Wandel der Arbeitswelt – etwa durch die zunehmende Digitalisierung hat zu einer Zunahme der Arbeitsverdichtung, ständigen Erreichbarkeit und Komplexität der Arbeitsaufgaben geführt. Mitarbeitende berichten von erhöhtem Zeit- und Leistungsdruck und häufigeren Arbeitsunterbrechungen. Das kann zur Erschöpfung, sinkender Motivation oder auch zu vermehrten Konflikten im Team führen. Die Folgen sind nicht immer sofort sichtbar, wirken sich aber natürlich langfristig auf unsere Gesundheit und Leistung aus.

Mit der Novellierung der DGUV Vorschrift 2 rücken psychische Belastungen stärker in den Fokus des Arbeitsschutzes. Was sind aus Ihrer Sicht die wichtigsten Neuerungen?

Ivon Ames: Die aktuelle Novellierung ist ein wichtiger Schritt in die richtige Richtung. Es ist sehr zu begrüßen, dass die interdisziplinäre Zusammenarbeit im Arbeitsschutz dadurch nun gestärkt wird. Das entspricht den realen Anforderungen in der Arbeitswelt. Gleichzeitig erleben wir in der Praxis, dass arbeitspsychologische Fachkompetenz, insbesondere in der Gestaltung psychischer Belastungsfaktoren,

noch nicht überall dort ankommt, wo sie gebraucht wird. In den Regelwerken, aber auch in der konkreten Umsetzung, gibt es aus meiner Sicht noch Potenzial, psychologische Expertise stärker zu nutzen. Es braucht heute stärker denn je passgenaue Unterstützung, um Unternehmen und Beschäftigte wirksam zu begleiten.

Wie hat sich die Integration psychologischer Aspekte in den Arbeitsschutz historisch entwickelt – und was war der Auslöser für diesen Wandel?

Ivon Ames: Lange Zeit lag der Fokus im Arbeitsschutz auf physischen Gefährdungen, das muss man schon so festhalten. Mit der zunehmenden Erkenntnis, dass psychische Belastungsfaktoren ähnlich negative Folgen auf die Gesundheit haben können, begann ein Umdenken. Ein Meilenstein war hier eindeutig die Novellierung des Arbeitsschutzgesetz im Jahr 2013 – seitdem sind auch psychische Belastungsfaktoren als Gefährdungsquelle eindeutig benannt, die damit Unternehmen in Ihrer regelmäßigen Gefährdungsbeurteilung berücksichtigen müssen.

Wie gut sind Unternehmen – insbesondere kleine und mittlere – aktuell aufgestellt, wenn es um die Gefährdungsbeurteilung psychischer Belastungen geht?

Ivon Ames: Es gibt Fortschritte. Aber gerade KMUs tun sich oft schwer mit der Umsetzung. Gründe sind häufig fehlende personelle Ressourcen, Unsicherheiten im Vorgehen und natürlich auch mangelnde Fachkenntnis. Das Thema wirkt komplex, man hat Sorge, dass die Anforderungen unrealistisch hoch sind. Dabei geht es überhaupt nicht um das rosarote Wolkenschloss der perfekten Arbeitsbedingungen, sondern im Grunde erst einmal darum, dass Mitarbeitende ohne Störungen und Hindernisse Ihren Job gut machen können. Daher sind niedrigschwellige Angebote, klare Leitlinien und externe Unterstützung entscheidend.

Welche Rolle spielen arbeitspsychologische Fachkräfte im betrieblichen Arbeitsschutzkonzept – insbesondere im Zusammenspiel mit Betriebsärzten und Sicherheitsfachkräften?

Ivon Ames: Die Art und Weise, wie Menschen ihren Arbeitsalltag erleben, wie sich dies auf die physische und psychische Gesundheit auswirkt, ist seit jeher ein zentraler Forschungsschwerpunkt in der Arbeitspsychologie. Arbeitspsychologinnen und -psychologen verfügen daher über spezifisches Wissen zu den komplexen Wirkmechanismen, die im Arbeitsalltag auf die Menschen einwirken. Im Zusammenspiel mit anderen Arbeitsschutzakteuren entsteht ein ganzheitliches Bild, das alle Risiken berücksichtigt. Dieses Zusammenspiel ist meines Erachtens essenziell für eine zeitgemäße Prävention.

© mpix-foto - stock.adobe.com

Was sind aus Ihrer Sicht die häufigsten psychischen Belastungsfaktoren in modernen Arbeitsumgebungen – und wie wirken sich diese auf die Gesundheit aus?

Ivon Ames: Das ist natürlich situativ ganz unterschiedlich, aber häufige Belastungsfaktoren sind Zeitdruck, unklare Rollenverteilung, mangelnde Anerkennung sowie verschwimmende Grenzen und ständige Erreichbarkeit. Auf Dauer führen solche Faktoren bei ungünstiger Gestaltung zu Erschöpfung, Schlafproblemen und weiteren gesundheitlichen Beeinträchtigungen bis hin zu kardiovaskulären Beschwerden und Diabetes. Eine frühzeitige Intervention kann hier sehr viel bewirken.

Wie beeinflussen neue Arbeitsformen wie Homeoffice oder der Einsatz von KI die psychische Belastung und das Sicherheitsgefühl am Arbeitsplatz?

Ivon Ames: Mobiles Arbeiten bietet ohne Frage viele Vorteile, wie mehr Flexibilität oder Autonomie. Gleichzeitig kann es aber auch zu Entgrenzung, fehlender sozialer Einbindung oder einer geringeren emotionalen Bindung zum Team führen. Hier ist es entscheidend, dass Führung und Teams aktiv gestalten, wie Zusammenarbeit auf Distanz funktioniert, damit die positiven Effekte wirklich auch zur Geltung kommen.

Beim Einsatz von KI beobachten wir eine neue Form der Umverteilung von Aufgaben. Wenn z. B. KI Systeme einzelne Teilaufgaben übernehmen, besteht die Gefahr, dass ursprünglich ganzheitlich gestaltete Aufgaben nun als unvollständig wahrgenommen werden. Damit das oder auch andere negative Auswirkungen auf die Belastungsprofile der Mitarbeitenden nicht passieren, ist eine prospektive Arbeitsgestaltung wichtiger denn je. Damit meine ich die bewusste, vorausschauende Gestaltung von Arbeitsprozessen mit dem Menschen im Mittelpunkt. KI darf unterstützen, aber ohne zu entwerten. Das gelingt aber nur, wenn psychische Belastungsfaktoren von Anfang an mitgedacht werden.

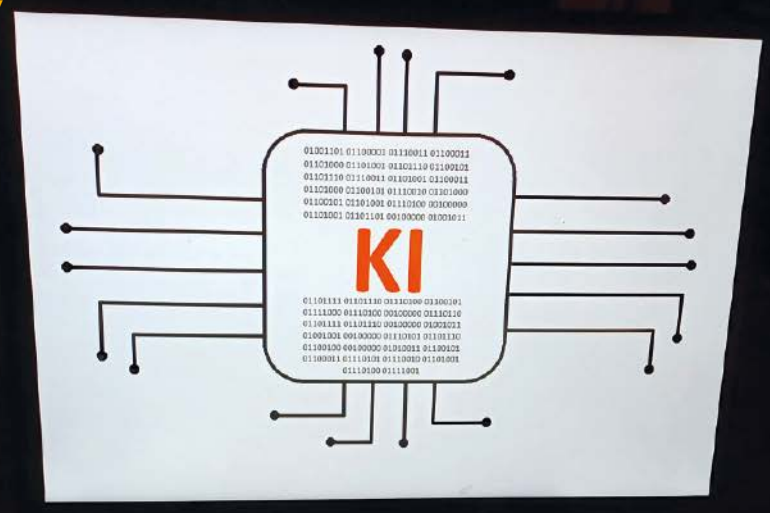
Welche konkreten Maßnahmen können Unternehmen ergreifen, um psychische Belastungen frühzeitig zu erkennen und präventiv gegenzusteuern?

Ivon Ames: Zentrale Maßnahmen sind in erster Linie eine regelmäßige Messung und Beurteilung der Arbeitsbedingungen über die Gefährundungsbeurteilung. Das ist ein zentraler Punkt, da diese eine ganzheitliche Standortbestimmung der Arbeitsbedingungen liefern. Man erfährt, welche Arbeitsbedingungen aktuell sehr gut gestaltet sind. Diese gilt es zu sichern und, wo dies nicht der Fall ist, Optimierungspotenziale zu heben. Weiterhin sind Schulungen für Führungskräfte zur gesundheitsförderlichen Arbeitsgestaltung zentral, ebenso wie die Förderung einer offenen Kommunikationskultur. Auch ein strukturiertes Fehlzeitenmanagement und psychosoziale Unterstützungsangebote können präventiv wirken.

Wie steht Deutschland im internationalen Vergleich da, wenn es um die strukturelle Verankerung psychologischer Expertise im Arbeitsschutz geht?

Ivon Ames: Deutschland hat in den letzten Jahren wichtige Schritte unternommen, insbesondere durch die Novellierung des Arbeitsschutzgesetzes. Das Thema ist europaweit wichtig und auch andere Länder habe die Bedeutung schon längst erkannt und entsprechende Strukturen verankert. Hier können wir voneinander lernen. Insbesondere im Hinblick auf die flächendeckende Verfügbarkeit psychologischer Expertise in Betrieben haben wir in Deutschland noch unausgeschöpftes Potenzial. GIT

BDP e.V.
www.bdp-verband.de



© Siemens AG

Holger Laible, Senior Safety Expert bei Siemens AG

© Siemens AG

Maximilian Korff, Senior Safety Expert bei Siemens AG

Die digitale Vernetzung und die Verwendung neuer Technologien wie Künstliche Intelligenz (KI) stellen den Maschinen- und Anlagenbau, seine Komponentenzulieferer und Maschinenbetreiber in Sachen Funktionale Sicherheit vor neue Herausforderungen. Maschinen und Anlagen werden deutlich flexibler und bieten neue Möglichkeiten. Gleichzeitig wächst die Komplexität der Applikationen. Cybersecurity-Bedrohungen und neue Regularien stellen erhöhte Anforderungen. Wie können wir dem begegnen?

Eine Artikel-Serie in Kooperation von VDMA, ZVEI und GIT SICHERHEIT.

Die Ansprechpartner: Birgit Sellmaier betreut im VDMA-Fachverband Elektrische Automation Technik- und Technologiethemen wie Steuerungstechnik und Funktionale Sicherheit in der Anwendung im Maschinenbau. Dr. Markus Winzenick ist zuständig für den Fachbereich Schaltgeräte, Schaltanlagen, Industriesteuerungen im ZVEI Fachverband Automation.

VDMA Elektrische Automation

GIT SICHERHEIT

zvei electrifying ideas

MASCHINEN- UND ANLAGENSICHERHEIT

Maschinensicherheit im Kontext von KI und Security

Potection against corruption: Neue Sicherheitsanforderungen in der Maschinenverordnung

Im exklusiven Interview mit der GIT SICHERHEIT sprechen Holger Laible und Maximilian Korff, Safety und Security Experten bei Siemens, über die weitreichenden Auswirkungen der neuen Maschinenverordnung (MVO, Verordnung (EU) 2023/1230) auf die Industrie. Die Integration des Aspekts „Schutz vor Korrumpierung“ stellt Hersteller vor neue Herausforderungen und erfordert eine umfassende Anpassung der Risikobewertungen und Sicherheitsmaßnahmen. Erfahren Sie, wie Unternehmen sich auf diese Veränderungen vorbereiten können.

GIT SICHERHEIT: Welche Auswirkungen hat die Integration des Aspekts „Schutz vor Korrumpierung“ in die Maschinenverordnung (MVO)?

Holger Laible: Es wird zu einem Paradigmenwechsel im Sinne der Produkthaftung kommen. Diese Änderung hat große Tragweite, das können wir schon heute sagen, auch wenn momentan noch einiges unklar ist. Die Industrie wartet auf den Leitfaden zur MVO, an dessen Erstellung auch der VDMA beteiligt ist. Praktisch von Bedeutung ist, dass nun auch bei vorsätzlichen böswilligen Handlungen unbekannter Dritter der Hersteller in die Haftung genommen werden könnte, falls er einschlägige Schutzmechanismen nicht implementiert hat.

Zur technischen Bedeutung dieses neuen Abschnitts (1.1.9 der MVO) gibt es die unterschiedlichsten Sichtweisen, da der Regulierungstext stark interpretierbar ist. Ein Aspekt wäre zum Beispeil, ob auch die Manipulation von Gerätschaften innerhalb von zugangs-kontrollierten Fertigungsanlagen abzudecken ist, oder ob es in erster Linie um die externe Anbindung an öffentliche Datennetze (zwecks Fernwartung, Cloud-Computing, ...) geht. Das wäre dann nur für Maschinen relevant, die entweder per Fernwartung erreichbar oder permanent mit der Cloud verbunden sind.

Es wäre begrüßenswert, wenn der offizielle Leitfaden zur MVO sich zu diesen Fragen positionieren würde. Die Zeitstrecke liegt allerdings parallel zum europäisch initiierten Normungsprojekt der EN 50742 (Safety of Machinery – Potection against corruption), weshalb es zu Inkonsistenzen in der Auslegung kommen kann. Die Aufgabe der EN 50742 liegt in der Erarbeitung einer gemeinsamen Sicht auf die MVO-Ergänzungen zum Thema „Korrumpierung“. Das Substitut „Korrumpierung“ wurde im Abschnitt 1.1.9 anstelle von Begriffen wie „Security“ oder „Informationssicherheit“ gewählt, um vermutlich Überschneidungen mit anderen Regulierungen zu vermeiden. Auch wegen weiterer Regulierungen wie dem Cyber Resiliance Act (s. GIT SICHERHEIT 7-8/2025, ab S. 78), die 2027 verbindlich werden, können sich die Hersteller diesen neuen Anforderungen nicht mehr verschließen. Da es sich um komplexe Themen handelt, sind KMUs besonders auf Beratung und den branchenübergreifenden Erfahrungsaustausch (zum Beispiel in Industrieverbänden) angewiesen.

Müssen Maschinenhersteller zukünftig neben der Safety Risikobewertung auch eine eigene Security Bedrohungs- und Risikoanalyse durchführen?

Maximilian Korff: Die Betrachtung zur Korrumpierung ist der Startpunkt einer Security-Betrachtung und es wäre sinnvoll, diese Bewertung zu allen Security-Aspekten durchzuführen, so wie diese im CRA angedacht sind, und es nicht nur bezogen auf die MVO zu tun. Praktisch ist es schwierig, einen Teil der Security-Betrachtung isoliert zu definieren, der sich mit den Safety-Auswirkungen alleine beschäftigt. Denn die Zielrichtung von Angriffen kann in der Regel nur forensisch und damit im Nachhinein bestimmt werden.

Holger Laible: Im Bereich der Normung haben wir diese Entwicklung erkannt und haben bereits durch verschiedene Publikationen (wie IEC TR 63069 oder IEC TS 63074) hilfreiche Informationen erarbeitet. Diese Dokumente haben sich auf allgemeingültiger und Maschinenebene mit dem Thema Security und Funktionale Sicherheit auseinandergesetzt. Von Seiten der EU-Kommission wurde im Gesetzgebungsverfahren zum CRA betont, dass die Methoden übereinstimmen sollen.

Maximilian Korff: Entscheidend für ein Risiko Assessment sind allerdings die Randbedingungen, über die, wie zuvor erwähnt, ebenfalls noch diskutiert wird. So ist es beim Thema Security wichtig, sich auf Annahmen stützen zu können, die sich aus der Anwen-

Bitte umblättern ▶

Gemeinsamkeiten von Safety und Security

Safety	Security
Risikobewertung: Die Basis	
ISO 12100 Ermittelt das Risiko der Maschine für den Menschen Ermittlung PL/SIL	IEC 62443 / ISO 27005 Betrachtet Risko für Menschen durch Manipulation der FuSi Security Level (SL)
Konzeption von Maßnahmen	
Sicherheitskonzept (Safety Concept) Z.B. Zugang, Zugriffsmanagement, Abstandsschutz, Lichtgitter	Sicherheitskonzept (Security Concept) Z.B. Schutz vor unberechtigtem Zugriff, auch über Zugriffsmanagement und physischen Zugang
Umsetzung	
Schutzmaßnahmen z.B. Zaun, Lichtgitter im Abstand von 5cm und Höhe von 2m, aber auch IAM	Z.B. Segmentierung des Netzes, Benutzer-Management, IAM, „IT“-artige Maßnahmen bei der Integration beim Betreiber
„Ergonomie“	
Behindern Maßnahmen, werden sie umgangen	Behindern Maßnahmen, werden sie umgangen
Verifikation / Validierung	
Qualitativ und quantitativ Gut definierte normative Vorgaben für beides	Verifikation der korrekten Maßnahmenumsetzung möglich Umfängliche Validierung der Maßnahmen schwierig
Zyklus	
Update und Veränderungen nur bei Veränderung der Maschine Menschliche Evolution langsam Jährliche Sicherheitsunterweisung	Schwachstellen werden täglich gefunden Neue Angriffswege entstehen laufend Risikobewertung „veraltet“ (Jährliche) Sicherheitsunterweisung
Patchmanagement	
Bei Safety-kritischen Fehlern Zusammenspiel Maschinenbauer-Maschinenbetreiber	Bei Schwachstellen die Auswirkungen auf die Safety haben Zusammenspiel Maschinenbauer-Maschinenbetreiber

Zur Illustration ein Beispiel aus der Lieferantenselbstauskunft:

Risikomanagement		
SRM	Führen Sie eine Risikobewertung Ihrer Komponenten/ Maschine/Anlage durch, die die im Betrieb zu erwartenden IT-Sicherheitsrisiken abdeckt?	Beispiel: Beschreiben, welche Schutzziele (Verfügbarkeit, Integrietät, Vertraulichkeit) berücksichtigt und welche Annahmen zum Betrieb getroffen wurden.
SRM	**Wenn JA:** Gehen Sie nach allgemein anerkannten Verfahren vor (z.B. nach IEC 62443, TRBS 1115 Teil 1 für MSR-Einrichtungen, VDE 2182)?	Nennung der angewendeten anerkannten Verfahren, ggf. mit Nachweis
SRM	Werden Gefährdungen der Safety durch Cyberrisiken gem. MVO beurteilt?	Nach Maschinenverordnung Annex III, Part B, Beurteilung "cyber-safety". **Hinweis:** Gilt die Betrachtung auch für den Schutz der Safety-Komponenten bei Fernzugängen?

Quelle VDMA

dung ergeben. Zudem ist entscheidend, welches Niveau der Schutzmaßnahmen praktisch vernünftig erscheint. Denn die Systeme gegen einen Zugriff auf höchstem Niveau absichern zu wollen – also gegen jeden denkbaren Angriff –, ist praktisch unmöglich. Das gilt schon deshalb, weil Backdoors und Zugriff über den Faktor Mensch nicht in jedem Fall abzusichern sind. So trägt auch das grundlegende Konzept der vier verschiedenen Security Level in der IEC 62443 diesem Umstand Rechnung, dass Risikomanagement immer eine Kosten- / Nutzenabwägung bleibt.

Welche Teile einer Anlage sind besonders von den neuen Security-Anforderungen betroffen?

Holger Laible: Das hängt von den Randbedingungen und den Ergebnissen der Risikobewertung ab. Es gibt Stimmen, die den notwendigen Umfang gerne auf die in der Anlage befindlichen Safety-Produkte reduzieren möchten. In der MVO steht jedoch, dass es um Auswirkungen geht, die einen gefährlichen Zustand hervorrufen und das ist nicht immer einzig auf Komponenten der Funktionalen Sicherheit bezogen. Ein Beispiel wäre die Betriebsanleitung, die nach neuer MVO auch digital zur Verfügung gestellt werden kann und risikoreduzierende Nutzerinformationen enthält. Sollte diese Betriebsanleitung sich elektronisch auf einer Maschine befinden und inhaltlich korrumpiert werden, könnte eine gefährliche Situation für den Nutzer die Folge sein. Dies wäre genauso außerhalb von Systemen der Funktionalen Sicherheit, wie softwareunterstützte Sensoren, die beispielsweise auch in Sicherheitsfunktionen eingebunden werden könnten und damit ebenfalls gegen Angriffe abzusichern wären, um in der Folge gefährliche Auswirkungen zu verhindern.

Gleichzeitig ist zu erkennen, dass gezielte (Cyber-)Angriffe auf Systeme der Funktionalen Sicherheit zwar selten stattfinden, aber wenn, dann mit höchstem Angriffsniveau. Letztendlich ist es wichtig, Anlagen in Betrieb zu halten, also deren Verfügbarkeit abzusichern, was zu wesentlich breiteren Maßnahmen in der Praxis führt, als es in der MVO angedacht ist.

Wie können Maschinenhersteller sich in relevante Security-Aspekte einarbeiten?

Maximilian Korff: Ein Einstieg zum Know-how-Aufbau sind zum Beispiel die zweitägigen Seminare der VDMA Academy. Dort wird insbesondere auf den sicheren Entwicklungsprozess gemäß IEC 62443-4-1 eingegangen. Vertiefend sei auf die einschlägigen Publikationen, Events und Arbeitskreise im VDMA zum Thema Industrial Security hingewiesen. Zum „Stand der Technik“ in Maschinen und Anlagen, bieten der TÜV und viele Automatisierungshersteller „Security Gap-Assessments“ an.

VDMA Academy Seminar „Security by Design für Maschinen und Anlagen“ Product Security nach IEC 62443

VDMA Expertenseite „Cybersecurity“

Welche Maßnahmen sollten Maschinenhersteller ergreifen, um security-relevante Funktionen von Zukauf-Komponenten zu gewährleisten?

Maximilian Korff: Was industrielle Akteure in der Lieferkette voneinander erwarten können, ist in den einschlägigen Checklisten des VDMA-Arbeitskreises Industrial Security beschrieben, die sowohl Technikern als auch Einkäufern zu empfehlen sind: Sie fangen an mit Leitfragen für eine generelle Lieferantenselbstauskunft und gehen weiter auf den konkreten Beschaffungsprozess kompletter Maschinen (aus Betreibersicht) oder Komponenten (aus Sicht des Maschinenherstellers) ein.

VDMA Dokumentenreihe „Supply Chain Security“ Checklisten – Mindestempfehlungen, Lieferantenselbstauskunft, Lastenhefte

Wie ist die Integration von maschinellem Lernen und autonomem Verhalten in die MVO zu bewerten?

Holger Laible: Aus meiner Sicht wollte man hier den Zeitgeist aufgreifen, denn hinsichtlich der Sicherheit von Maschinen bleibt auch in der MVO gültig und richtig, dass die Funktionalitäten und Betriebsarten der Maschine oder Anlage im Vorfeld in der Risikobetrachtung zu bewerten sind (siehe Teil B 1e) der MVO). Damit ist es nur schwer begründbar, wie sich zur Laufzeit der Maschine ein Verhalten autonom entwickeln kann, sofern es für die Sicherheit der Maschine relevant ist.

Natürlich können Daten gesammelt werden, die durch spätere sicherheitsrelevante Updates von Maschinen im Feld zu einer Weiterentwicklung führen. Eine umfassende sicherheitstechnische Bewertung ist allerdings auch künftig nur unter Mitwirkung und abschließender Bewertung durch den Menschen umsetzbar. Die Möglichkeit nicht-sicherheitsrelevante Performance einer Maschine zur Laufzeit automatisch durch maschinelles Lernen zu entwickeln, war auch schon mit der noch geltenden Maschinenrichtlinie gegeben.

Im Rahmen der Arbeiten im ISO/IEC JTC 1/SC 42/JWG 4 zur Funktionalen Sicherheit von KI Systemen wurden bereits im ISO/IEC TR 5469 erste Schritte zur Bewertung solcher Systeme aufgezeigt und aktuell in die technischen Spezifikationen der ISO/IEC TS 22440-Reihe überführt und weiter ausgearbeitet. Ein wichtiger Schritt besteht in der Klassifizierungder der eingesetzten KI-Technologie im Hinblick auf ihre Sicherheitsrelevanz. Dabei wird deutlich, dass es eine ganze Reihe von Möglichkeiten gibt, diese Technologie einzusetzen, beispielsweise um die Performance von Maschinenbewegungen im nicht-sicherheitskritischen Kontext zu verbessern. GIT

Siemens AG
www.siemens.com

Ion-Line Ultra um Präsenzsensor erweitert

Die Asecos GmbH ergänzt den Ion-Line Ultra Sicherheitsschrank zum Lagern und Laden von Lithium-Akkus um eine intelligente Erweiterung: Optional ist der Sicherheitsschrank nun mit einem Präsenzsensor erhältlich. Ziel ist es, hohe Sicherheit mit bestmöglichem Bedienkomfort zu kombinieren.

Der Ultra, das Premium-Modell der Ion-Line Produktreihe, erfüllt höchste Sicherheitsstandards. Der Sicherheitsschrank, der zum Lagern und Laden von Lithium-Akkus vorgesehen ist, ist er nach VDMA 24994:2024-08 in der Klasse I/O 90 zertifiziert. Zusätzlich wurde das Modell nach den Anforderungen des GS-Prüfgrundsatzes EK5/AK4 22-01 konstruiert und geprüft.

Basierend darauf ist der Schrank im Sinne des Explosionsschutzes mit einer automatischen Türschließung ausgestattet. Sie gewährleistet, dass sich die Türen nach jedem Öffnungsvorgang – aus jeder beliebigen Position – selbstständig und innerhalb kürzester Zeit schließen.

Mit der Integration des Präsenzsensors reagiert der Ultra intelligent auf die Anwesenheit von Nutzern im Türbereich. Der Sensor erkennt Personen im Schwenkbereich der Türen und ermöglicht dadurch einen komfortablen Zugriff auf den Schrankinhalt. Die automatische Schließung der Türen sowie das dazugehörige akustische Warnsignal werden so lange verzögert, wie es im Arbeitsalltag für das Be- oder Entladen des Schranks nötig ist.

Der Vorteil: Trotz des erhöhten Bedienkomforts bleibt die zusätzliche Schutzebene durch die automatische Türschließung vollumfänglich erhalten. **www.asecos.com**

Moxa erhält Cybersicherheits-Zertifikate für Wireless-Portfolio

Moxa Europe GmbH hat die EU-Baumusterprüfbescheinigung nach der Funkanlagen-Richtlinie (Radio Equipment Directive Delegated Act, RED DA) für industrielle Netzwerkgeräte erhalten. Unter den zertifizierten Produkten sind die Mobilfunkrouter der Serie Moxa OnCell G4300-LTE4, die fortschrittlichen IIoT-Gateways der AIG-302-Serie und die APs/Bridges/Clients der Serie AWK Wi-Fi 6. Die EN-18031-Serie (RED DA), die in die harmonisierte Norm der RED aufgenommen wurde, tritt am 1. August 2025 in Kraft. Ziel ist es, die Cybersicherheit, den Schutz personenbezogener Daten und die Privatsphäre für alle drahtlosen Geräte und Produkte zu verbessern, die in der EU auf den Markt kommen. Die Zertifizierungsprüfungen und das Audit wurden vom TÜV Rheinland durchgeführt, einem führenden Prüf- und Zertifizierungsunternehmen und einer benannten Stelle der EU für 2014/53/EU RED. **www.moxa.com**

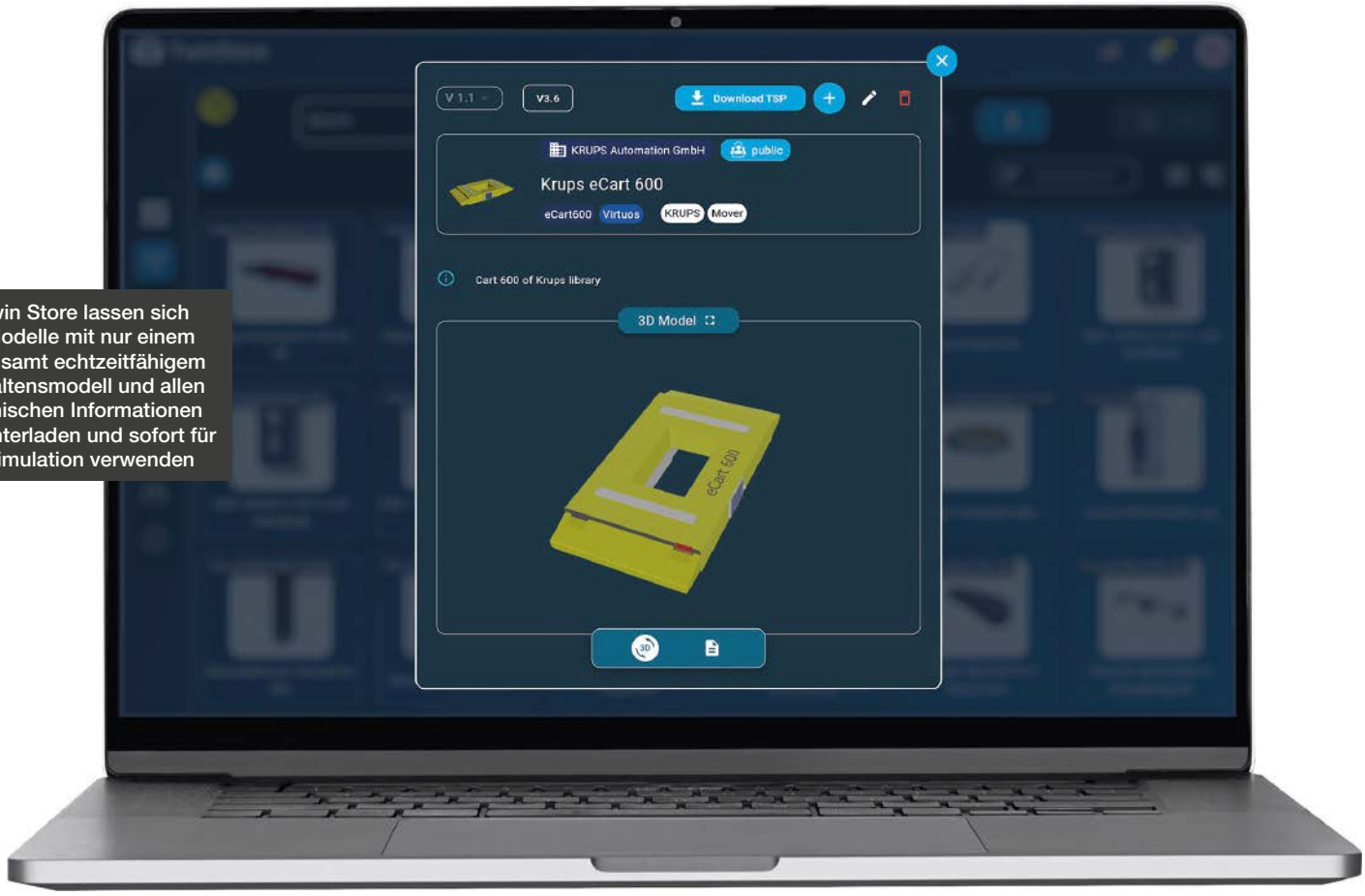
Bernhard Wiedemann wechselt ins Privatleben

Bernhard Wiedemann (links) und Jochen Bihl

Bei der Bihl+Wiedemann GmbH vollzieht sich ein personeller Wechsel: Bernhard Wiedemann, Mitgründer, Geschäftsführer und langjähriger Entwicklungsleiter, zieht sich nach über 30 Jahren erfolgreicher Tätigkeit aus dem operativen Geschäft zurück und beginnt einen neuen Abschnitt im Privatleben. Die alleinige Geschäftsführung übernimmt fortan Mitgründer Jochen Bihl – er steht für Kontinuität in der Führung und wird das Unternehmen auch weiterhin mit voller Tatkraft leiten. Bernhard Wiedemann habe mit seinem technischen Know-how, seiner Weitsicht und seinem Engagement maßgeblich dazu beigetragen, dass das Unternehmen heute als Technologieführer im Bereich AS-Interface gelte, so Jochen Bihl. „Er verlässt ein hervorragend aufgestelltes Unternehmen – und ich freue mich darauf, diesen erfolgreichen Weg gemeinsam mit unserem erfahrenen Team fortzuschreiben." **www.wiedemann.de**

Pepperl+Fuchs Box Thin Clients jetzt IGEL Ready-certified

Nachdem Pepperl+Fuchs dem IGEL Ready-Programm als Technologiepartner beigetreten ist, sind die Box Thin Clients von Pepperl+Fuchs IGEL Ready-certified. Die industriellen Box Thin Clients BTC22 und BTC24 sind die einzigen robusten Thin Clients, die als IGEL Ready-certified Produkte erhältlich sind, so das Unternehmen. Das bedeutet, dass die Geräte von IGEL getestet und qualifiziert wurden und der gesamte Support über die Firma IGEL abläuft. Damit auch Anwender Linux-basierter Systeme von den Vorteilen der Box Thin Clients und VisuNet-Serie profitieren können, bietet Pepperl+Fuchs die Hardware mit vorinstalliertem IGEL OS (die Lizenz für das Betriebssystem ist direkt bei IGEL zu erwerben) an. Das plattformunabhängige Betriebssystem für Thin Clients ermöglicht einen einfachen, intelligenten und sicheren Zugriff auf virtuelle Anwendungen, Desktops und Cloud-Arbeitsplätze. **www.pepperl-fuchs.com**



Im Twin Store lassen sich 4D-Modelle mit nur einem Klick samt echtzeitfähigem Verhaltensmodell und allen technischen Informationen herunterladen und sofort für die Simulation verwenden

DIGITALER ZWILLING

Vertrauen ist gut, Verifizierung ist besser

Digitale Zwillinge: Wie geprüfte 4D-Modelle die Virtuelle Inbetriebnahme belastbar machen

Digitale Zwillinge ermöglichen durch Virtuelle Inbetriebnahme und simulationsgestützte Entwicklung kürzere Time-to-Market und höhere Prozesssicherheit. Setzt man jedoch unvollständige oder angenäherte Simulationsmodelle ein, sinkt die Aussagekraft der digitalen Zwillinge, und das Risiko kostspieliger Fehleinschätzungen steigt. Hier setzt Twin Store an.

Die Virtuelle Inbetriebnahme (VIBN) ist eine zentrale Methode, um Entwicklungs- und Inbetriebnahmezeiten bei Maschinen und Anlagen deutlich zu verkürzen. Doch für belastbare, verlässliche Ergebnisse braucht es präzise digitale Zwillinge, die das physische System realitätsgetreu abbilden. Doch genau hier stehen viele Unternehmen vor einer Herausforderung: Für zahlreiche Komponenten wie Antriebe, Sensoren oder Greifer fehlen herstellerverifizierte 4D-Simulationsmodelle.

In der Praxis bedeutet das: Entweder müssen fehlende Komponenten mit erheblichem Zeitaufwand selbst modelliert werden oder man greift, wenn vorhanden, auf vorgefertigte Simulationsmodelle zurück, wie sie manche Softwarehersteller in ihren Bibliotheken anbieten. In beiden Fällen gibt es keine Gewähr auf realistisches Verhalten.

Ob ein angenähertes 4D-Modell ausreicht, hängt stark vom Anwendungsfall ab. Für einfache Bewegungsabläufe mag eine Annäherung genügen. Doch sobald z. B. sicherheitsrelevante Funktionen im Rahmen der VIBN getestet werden sollen, ist höchste Modelltreue gefragt. Bereits geringe Abweichungen zwischen dem simulierten und realen Komponentenverhalten können zu fehlerhaften Freigaben führen, mit potenziell kostspieligen Folgen im späteren Betrieb.

Vorgefertigte 4D-Modelle

Um der Herausforderung fehlender verifizierter Simulationsmodelle zu begegnen

Ob Robotik, Sensorik oder Antriebstechnik: Im Twin Store finden Sie eine große Auswahl an vorgefertigten 4D-Modellen direkt vom Hersteller für unterschiedlichste Anwendungen

und die Prozesssicherheit zu erhöhen, ist der direkte Weg über den Komponentenhersteller unerlässlich. Genau hier setzt Twin Store an. In enger Zusammenarbeit mit Unternehmen wie z. B. Sick, Balluff, Krups Automation, KEB Automation oder Weiss wird deren Produktportfolio Schritt für Schritt in simulationsfähige 4D-Modelle überführt. Diese stehen anschließend über den Online Store „Twin Store" zur Verfügung.

Für die Nutzer bedeutet das: Statt generischer Modelle erhalten sie sofort einsetzbare, validierte 4D-Modelle direkt vom Hersteller. Durch die integrierte Firmware bilden diese die reale Komponente nicht nur optisch, sondern auch funktional exakt ab. Eine weitere technische Besonderheit ist das enthaltene echtzeitfähige Verhaltensmodell. Hierdurch liefern die 4D-Modelle nicht nur in Model- oder Software-in-the-Loop-, sondern auch in Hardware-in-the-Loop Simulationsszenarien mit Zykluszeiten bis zu 1 ms deterministische und somit verlässliche Ergebnisse.

Darüber hinaus verfügt jedes auf dem Twin Store bereitgestellte 4D-Modell eine detaillierte technische Dokumentation und lässt sich dank standardisierter Austauschformate wie AASX oder FMU flexibel in unterschiedliche Simulationsumgebungen integrieren, ohne zusätzlichen Aufwand.

Für Unternehmen ergibt sich daraus ein klarer Mehrwert: geringere Modellierungsaufwände und -fehler, verlässliche Ergebnisse und höhere Aussagekraft der VIBN z. B. bei Machbarkeitsstudien. Das hilft, die Prozesssicherheit zu steigern und potenzielle Fehler bereits in der Simulation und nicht erst in der realen Inbetriebnahme zu erkennen.

Win-Win-Win-Situation

Der Twin Store bietet Mehrwert für alle Beteiligten entlang der Wertschöpfungskette:

- Komponentenhersteller erhalten die technische und organisatorische Infrastruktur, um ihre 4D-Modelle bereitzustellen. Dies unterstützt ihre Kunden bei der VIBN und schafft zugleich neue digitale Geschäftsmodelle.
- Maschinen- und Anlagenbauer profitieren von der höheren Verfügbarkeit verifizierter 4D-Komponentenmodelle. Der Modellierungsaufwand sinkt deutlich, gleichzeitig steigt die Aussagekraft und Qualität der Simulation.
- Anlagenbetreiber nutzen die validierten 4D-Modelle zur realitätsnahen Mitarbeiterschulung, zur Fehlersimulation und zur risikofreien Prüfung von Funktionsupdates, ganz ohne Maschinenstillstand.

Co-Working-Plattform

Der Twin Store ist längst mehr als ein reiner Online Store für 4D-Modelle. Mit dem letzten großen Update im letzten Jahr hat sich die Plattform zu einem Co-Working-Space für das Digitale Engineering weiterentwickelt. Anwender können nun nicht nur auf herstellerverifizierte 4D-Modelle zugreifen, sondern unter anderem auch eigene projektspezifische Modellbibliotheken erstellen und diese direkt mit Teammitgliedern oder externen Partnern teilen.

Diese Bibliotheken dienen aber nicht nur der kollaborativen Projektarbeit, sondern bilden auch die Grundlage für eine automatisierte Modellgenerierung. Durch die nahtlose Integration des Twin Store in Simulationsumgebungen wie z. B. ISG-virtuos lassen sich die eigenen Bibliotheken automatisiert nach benötigten 4D-Modellen durchsuchen. Verfügbare 4D-Modelle werden dann automatisch an der richtigen Stelle in den digitalen Zwilling eingefügt.

Auf diese Weise entstehen komplexe digitale Zwillinge ganzer Anlagen und Maschinen in deutlich kürzerer Zeit und der Prozess der Virtuellen Inbetriebnahme kann entsprechend früher beginnen. GIT

TwinStore auf der SPS in Nürnberg: Halle 6 Stand 338

In den kommenden Artikeln dieser Serie in der GIT SICHERHEIT geben Komponentenhersteller aus der Twin Store Community praxisnahe Einblicke: Wie entsteht aus einem CAD-Modell ein simulationsfähiges 4D-Modell? Wie läuft die Integration in VIBN-Projekte ab? Und welche Rolle spielt dabei der Twin Store für durchgängige Prozesssicherheit?

TwinStore GmbH
www.twinstore.de

Liebe Leserinnen und Leser,

In BusinessPartner, dem „Who is who in Sachen Sicherheit", präsentieren sich Ihnen die kompetentesten Anbieter aus allen Sicherheitsbereichen. Die hier vertretenen Firmen legen Wert auf den Kontakt mit Ihnen. Alle Einträge finden Sie auch in www.git-sicherheit.de/buyers-guide mit Links zu den Unternehmen!

Sie gehören selbst zu den wichtigen Anbietern und wollen mit jeder Ausgabe 30.000 Entscheider direkt erreichen? Dann kontaktieren Sie uns für eine Aufnahme.

SICHERHEITS MANAGEMENT

Sicherheitsmanagement

barox
Switche für Video

barox Kommunikation GmbH · 79540 Lörrach
Tel.: +49 7621 1593 100
www.barox.de · mail@barox.de
Cybersecurity, Videoswitch, PoE Power-over-Ethernet, Medienkonverter, Extender

Sicherheitsmanagement

FREIHOFF 24 GRUPPE

Freihoff Sicherheitsservice GmbH
Herzogstraße 8 · 40764 Langenfeld
Tel.: 02173 106 38-0
info@freihoff.de · www.freihoff-gruppe.de
Einbruchmeldeanlagen, Brandmeldeanlagen, Videoüberwachung, Zutrittskontrolle, Notruf- und Serviceleitstelle

Sicherheitsmanagement

BOSCH

Bosch Building Technologies
Fritz-Schäffer-Straße 9 · 81737 München
Tel.: 0800/7000444 · Fax: 0800/7000888
Info.service@de.bosch.com
www.boschbuildingtechnologies.de
Produkte und Systemlösungen für Einbruchmelde-, Brandmelde-, Sprachalarm- und Managementsysteme, professionelle Audio- und Konferenzsysteme. In ausgewählten Ländern bietet Bosch Lösungen und Dienstleistungen für Gebäudesicherheit, Energieeffizienz und Gebäudeautomation an.

Sicherheitsmanagement

nsc Sicherheitstechnik GmbH

NSC Sicherheitstechnik GmbH
Grete-Hermann-Str. 6
33758 Schloß Holte-Stukenbrock
Tel.: +49 (0) 5257 97799-0
Fax: +49 (0) 5257 97799-29
info@nsc-sicherheit.de · www.nsc-sicherheit.de
Brandmeldetechnik, Videotechnik, Sprach-Alarm-Anlagen

Sicherheitsmanagement

ABUS Security Tech Germany

ABUS Security-Center GmbH & Co. KG
Linker Kreuthweg 5 · D-86444 Affing
Tel.: +49(0)8207/95990-0
Fax: +49(0)8207/95990-100
info.de@abus-sc.com · www.abus.com
ABUS Security-Center ist Hersteller innovativer Alarmanlagen, Videoüberwachungssysteme und Zutrittskontrollsysteme. Als Teil der ABUS Gruppe ist das Unternehmen sowohl auf branchenspezifische Sicherheitsbedürfnisse, als auch auf die Anforderungen von Privatanwendern spezialisiert.

Sicherheitsmanagement

DAITEM

Daitem / Atral Security Deutschland GmbH
Eisleber Str. 4 · D-69469 Weinheim
Tel.: +49(0)6201 94 330-40
info.de@daitem.com · www.daitem.com
Funk-Einbruch- und Brandschutzlösungen vom Technologieführer. Vertrieb über qualifizierte Sicherheitsfacherrichter.

Sicherheitsmanagement

Security Robotics®

Security Robotics Development & Solutions GmbH
Mühlweg 44 · 04319 Leipzig
Tel.: 0341-2569 3369
info@security-robotics.de · www.security-robotics.de
Robotics, Sicherheitstechnik, Autonomie, Qualitätssteigerung, Künstliche Intelligenz, Vernetzte Zusammenarbeit, SMA Unterstützung

Sicherheitsmanagement

ASSA ABLOY
Opening Solutions

ASSA ABLOY Sicherheitstechnik GmbH
Bildstockstraße. 20 · 72458 Albstadt
www.assaabloy.com/de · albstadt@assaabloy.com
Das Unternehmen entwickelt, produziert und vertreibt unter den traditionsreichen und zukunftsweisenden Marken IKON, effeff und KESO hochwertige Produkte und vielseitige Systeme für den privaten, gewerblichen und öffentlichen Bereich.

Sicherheitsmanagement

deister electronic

deister electronic GmbH
Hermann-Bahlsen-Str. 11
D-30890 Barsinghausen
Tel.: +49(0)5105/516-111 · Fax: +49(0)5105/516-217
info.de@deister.com · www.deister.com
Zutritts- und Zufahrtskontrollsysteme; biometrische Verifikation; Wächterkontrollsysteme; Verwahrung und Management von Schlüsseln und Wertgegenständen

Sicherheitsmanagement

VSW Vereinigung für die Sicherheit der Wirtschaft e.V.

Vereinigung für die Sicherheit der Wirtschaft e.V.
Lise-Meitner-Straße 1 · 55129 Mainz
Tel.: +49 (0) 6131 - 57 607 0
info@vsw.de · www.vsw.de
Als Schnittstelle zwischen den Sicherheitsbehörden und der Wirtschaft in allen Fragen der Unternehmenssicherheit steht die gemeinnützige Vereinigung seit 1968 der Wirtschaft als unabhängige Organisation zur Verfügung.

GEBÄUDE SICHERHEIT

VIDEO ÜBERWACHUNG

Gebäudesicherheit

deister electronic GmbH
Hermann-Bahlsen-Str. 11
D-30890 Barsinghausen
Tel.: +49(0)5105/516-111 · Fax: +49(0)5105/516-217
info.de@deister.com · www.deister.com
Zutritts- und Zufahrtskontrollsysteme; biometrische Verifikation; Wächterkontrollsysteme; Verwahrung und Management von Schlüsseln und Wertgegenständen

Gebäudesicherheit

Süd-Metall Beschläge GmbH
Sägewerkstraße 5 · D - 83404 Ainring/Hammerau
Tel.: +49 (0) 8654 4675-50 · Fax: +49 (0) 8654 4675-70
info@suedmetall.com · www.suedmetall.com
Funk-Sicherheitsschlösser made in Germany, Mechanische & elektronische Schließsysteme mit Panikfunktion und Feuerschutzprüfung, Zutrittskontrollsysteme modular und individuell erweiterbar, Systemlösungen, Fluchttürsteuerung

Videoüberwachung

ABUS Security-Center GmbH & Co. KG
Linker Kreuthweg 5 · D-86444 Affing
Tel.: +49(0)8207/95990-0
Fax: +49(0)8207/95990-100
info.de@abus-sc.com · www.abus.com
ABUS Security-Center ist Hersteller innovativer Alarmanlagen, Videoüberwachungssysteme und Zutrittskontrollsysteme. Als Teil der ABUS Gruppe ist das Unternehmen sowohl auf branchenspezifische Sicherheitsbedürfnisse, als auch auf die Anforderungen von Privatanwendern spezialisiert.

Gebäudesicherheit

Dictator Technik GmbH
Gutenbergstr. 9 · 86356 Neusäß
Tel.: 0821/24673-0 · Fax: 0821/24673-90
info@dictator.de · www.dictator.de
Antriebstechnik, Sicherheitstechnik, Tür- und Tortechnik

Gebäudesicherheit

TAS Sicherheits- und Kommunikationstechnik
Telefonbau Arthur Schwabe GmbH & Co. KG
Langmaar 25 · D-41238 Mönchengladbach
Tel.: +49 (0) 2166 858 0 · Fax: +49 (0) 2166 858 150
info@tas.de · www.tas.de
Übertragungsgeräte, Alarmierungs- und Konferenzsysteme, Remote Services für sicherheitstechnische Anlagen, vernetzte Sicherheitslösungen

Videoüberwachung

Ihr Value Added Distributor für Videosicherheitstechnik „Made in Germany“

Dallmeier Components GmbH
Hoheluftchaussee 108 | 20253 Hamburg
Tel. +49 40 47 11 213-0 | Fax +49 40 47 11 213-33
info@d-components.com | www.d-components.com

Gebäudesicherheit

DOM Sicherheitstechnik GmbH & Co. KG
Wesselinger Straße 10-16 · D-50321 Brühl / Köln
Tel.: + 49 2232 704-0 · Fax: + 49 2232 704-375
dom@dom-group.eu · www.dom-security.com
Mechanische und digitale Schließsysteme

Gebäudesicherheit

Uhlmann & Zacher GmbH
Gutenbergstraße 2-4 · 97297 Waldbüttelbrunn
Tel.: +49(0)931/40672-0 · Fax: +49(0)931/40672-99
contact@UundZ.de · www.UundZ.de
Elektronische Schließsysteme, modular aufgebaut und individuell erweiterbar

Videoüberwachung

Dallmeier electronic GmbH & Co. KG
Bahnhofstraße 16 · 93047 Regensburg
Tel.: 0941/8700-0 · Fax: 0941/8700-180
info@dallmeier.com · www.dallmeier.com
Videosicherheitstechnik made in Germany: Multifocal-Sensortechnologie Panomera®, IP-Kameras, Aufzeichnungsserver, intelligente Videoanalyse, Videomanagementsoftware

Gebäudesicherheit

frogblue · Smart Building Technology
Luxemburger Straße 6 · 67657 Kaiserslautern
Tel: +49-631-520829-0
info@frogblue.com · www.frogblue.com/de/
Frogblue ist führend in der Entwicklung von drahtlosen, auf Bluetooth® basierenden Elektroinstallationslösungen für den professionellen Einsatz, die vollständig in Deutschland produziert werden. (Sicherheit, SmartHome, energieeffiziente Gebäudetechnik, Zutrittskontrolle)

PERIMETER SCHUTZ

Videoüberwachung

EIZO Europe GmbH
Belgrader Straße 2 · 41069 Mönchengladbach
Tel.: +49 2161 8210 0
info@eizo.de · www.eizo.de/ip-decoding
Professionelle Monitore und Lösungen für den 24/7-Einsatz in der Videoüberwachung, IP-Decoder-Lösungen mit einfacher Installation und computerlosem Betrieb.

Gebäudesicherheit

SimonsVoss Technologies GmbH
Feringastr. 4 · 85774 Unterföhring
Tel.: 089 992280
marketing-simonsvoss@allegion.com
www.simons-voss.com
Digitale Schließanlagen mit Zutrittskontrolle, kabellose und bohrungsfreie Montage, batteriebetrieben, keine Probleme bei Schlüsselverlust.
Digital Schließen ist neu für Sie? Rufen Sie an: 089 99228-555

Perimeterschutz

Berlemann Torbau GmbH
Ulmenstraße 3 · 48485 Neuenkirchen
Tel.: +49 5973 9481-0 · Fax: +49 5973 9481-50
info@berlemann.de · www.berlemann.de
INOVA ist die Marke für alle Komponenten der Freigeländesicherung aus einer Hand! Als Qualitätshersteller für Schiebetore, Drehflügeltore, Zaun-, Zugangs- und Detektionssysteme haben Sie mit INOVA auf alle Fragen des Perimeterschutzes die passende Antwort.

Videoüberwachung

Hanwha Techwin Europe Limited
Kölner Strasse 10
65760 Eschborn
Tel.: +49 (0)6196 7700 490
hte.dach@hanwha.com · www.hanwha-security.eu/de
Hersteller von Videoüberwachungsprodukten wie Kameras, Videorekorder und weiteren IP-Netzwerkgeräten. Sowie Anbieter von Software-Lösungen wie beispielsweise Videoanalyse, Lösungen für den Vertical-Market und Videomanagementsoftware (VMS).

Zeit + Zutritt

AZS System AG
Mühlendamm 84 a · 22087 Hamburg
Tel.: 040/226611 · Fax: 040/2276753
www.azs.de · anfrage@azs.de
Hard- und Softwarelösungen zu Biometrie, Schließ-, Video-, Zeiterfassungs- und Zutrittskontrollsysteme, Fluchtwegsicherung, Vereinzelungs- und Schrankenanlagen, OPC-Server

Zeit + Zutritt

dormakaba Deutschland GmbH
DORMA Platz 1 · 58256 Ennepetal
T: +49 (0) 2333/793-0
info.de@dormakaba.com · www.dormakaba.de
Umfassendes Portfolio an Produkten, Lösungen und Services rund um die Tür sowie den sicheren Zutritt zu Gebäuden und Räumen aus einer Hand. Dies umfasst Schließsysteme, voll vernetzte elektronische Zutrittslösungen, physische Zugangs- und automatische Türsysteme, Türbänder, Beschläge, Türschließer, Zeiterfassung inkl. ERP-Anbindungen, Hotelschließsysteme und Hochsicherheitsschlösser.

Videoüberwachung

HIKVISION Deutschland GmbH
Flughafenstr. 21 · D-63263 Neu-Isenburg
Tel.: +49 (0) 69/40150 7290
sales.dach@hikvision.com · www.hikvision.com/de
Datenschutzkonforme Videoüberwachung, Panorama-Kameras, Wärmebild-Kameras, PKW-Kennzeichenerkennung

Zeit + Zutritt

Bird Home Automation GmbH
Uhlandstr. 165 • 10719 Berlin
Tel. +49 30 12084824 • pr@doorbird.com
Zutrittskontrolle; Tür- und Tortechnik; Türkommunikation; Gebäudetechnik; IP Video Türsprechanlage; RFID; Biometrie; Fingerabdruck; Made in Germany

www.doorbird.com

Zeit + Zutritt

ELATEC GmbH
Zeppelinstr. 1 · 82178 Puchheim
Tel.: +49 89 552 9961 0
info-rfid@elatec.com · www.elatec.com
Anbieter von Benutzerauthentifizierungs- und Identifikationslösungen. Unterstützung der digitalen Transformation von Kunden und Partnern durch das Zusammenspiel von universellen Multifrequenz-Lesegeräten und fortschrittlicher Authentifizierungssoftware, Service und Support.

Videoüberwachung

i-PRO EMEA B.V.
Laarderhoogtweg 25 · 1101 EB Amsterdam
Netherlands
https://i-pro.com/eu/en
Hochwertige CCTV-Lösungen (IP & analog), Video-Automatisierung und KI, Technologien für hohe Ansprüche (FacePro, Personen-Maskierung), Schutz vor Cyber-Attacken im Einklang mit DSGVO, VMS: Video Insight

Zeit + Zutritt

CDVI GmbH
Dahlweg 105 / Tor 2 · D-48153 Münster
Tel.: +49 (0)251 798 477-0
info@cdvi.de · www.cdvi.de
Zutrittskontrolle, Zutrittskontrollsysteme, Zutritt mittels Smartphone, Biometrische Systeme, Türautomation, Komponenten für Türen+Tore

Zeit + Zutritt

FEIG ELECTRONIC GMBH
Industriestr. 1a · 35781 Weilburg
Tel.: +49(0)6471/3109-375 · Fax: +49(0)6471/3109-99
sales@feig.de · www.feig.de
RFID-Leser (LF, HF, UHF) für Zutritts- und Zufahrtskontrolle, Geländeabsicherung, Bezahlsysteme u.v.m.

Videoüberwachung

Zeit + Zutritt

Cichon+Stolberg GmbH
Wankelstraße 47-49 · 50996 Köln
Tel.: 02236/397-200 · Fax: 02236/61144
info@cryptin.de · www.cryptin.de
Betriebsdatenerfassung, Zeiterfassung, cryptologisch verschlüsselte Zutrittskontrolle

Zeit + Zutritt

GANTNER Electronic GmbH
Bundesstraße 12 · 6714 Nüziders · Österreich
Tel.: +43 5552 33944
info@gantner.com · www.gantner.com
Systemlösungen in Zutrittskontrolle/Biometrie, Zeiterfassung, Betriebsdatenerfassung, Schließsysteme, Zugriffsschutz, Schrankschließsysteme

ZEIT
ZUTRITT

Zeit + Zutritt

deister electronic GmbH
Hermann-Bahlsen-Str. 11
D-30890 Barsinghausen
Tel.: +49(0)5105/516-111 · Fax: +49(0)5105/516-217
info.de@deister.com · www.deister.com
Zutritts- und Zufahrtskontrollsysteme; biometrische Verifikation; Wächterkontrollsysteme; Verwahrung und Management von Schlüsseln und Wertgegenständen

Zeit + Zutritt

Gunnebo Deutschland GmbH
Carl-Zeiss-Str. 8 · 85748 Garching
Tel.: +49 89 244163500
info@gunnebo.de · www.gunnebo.de
Tresore und Schränke, Tresorräume, Tresortüren, Hochsicherheitsschlösser, Elektronische Schlösser

Zeit + Zutritt

AceProx Identifikationssysteme GmbH
Bahnhofstr. 73 · 31691 Helpsen
Tel.: +49(0)5724-98360
info@aceprox.de · www.aceprox.de
RFID-Leser für Zeiterfassung, Zutrittskontrolle und Identifikation

Zeit + Zutritt

DNAKE (Xiamen) Intelligent Technology Co., Ltd.
No.8, Haijing North 2nd Rd., Xiamen, Fujian, China
Tel.: +86 592-5705812
sales01@dnake.com, www.dnake-global.com
Intercom System, IP Video Intercom, 2-Wire IP Intercom, Cloud Intercom Service, Access Control

Zeit + Zutritt

PCS Systemtechnik GmbH
Pfälzer-Wald-Straße 36 · 81539 München
Tel.: 089/68004-0 · Fax: 089/68004-555
intus@pcs.com · www.pcs.com
Zeiterfassung, Gebäudesicherheit, Zutritts- und Zufahrtskontrolle, Biometrie, Video, Besuchermanagement, SAP, Handvenenerkennung

Zeit + Zutritt

phg
Peter Hengstler GmbH + Co. KG
D-78652 Deißlingen · Tel.: +49(0)7420/89-0
datentechnik@phg.de · www.phg.de
RFID und Mobile Access: Leser für Zutrittskontrolle, Zeiterfassung, BDE, Türkommunikation, Besuchermanagement, Parksysteme, Zufahrtskontrolle, Vending, ... Terminals, Einbaumodule, Kartenspender, Tischlesegeräte, Leser für Markenschalterpogramme, Identifikationsmedien, ... einfach und komfortabel zu integrieren.

Notruf- und Service-Leitstelle

HWS Wachdienst Hobeling GmbH
Am Sportpark 75 · D-58097 Hagen
Tel.: (0 23 31) 47 30 -0 · Fax: -130
hobeling@hobeling.com · www.hws-wachdienst.de
VdS-Notruf- und Service-Leitstelle, Alarmempfangsstelle DIN EN 50518, Alarmprovider, Mobile Einsatz- und Interventionskräfte, Objekt- und Werkschutz

Brandschutz

WAGNER Group GmbH
Schleswigstraße 1–5 · 30853 Langenhagen
Tel.: +49 (0)511 97383 0
info@wagnergroup.com · www.wagnergroup.com
Brandfrüherkennung und Brandmeldeanlagen, Brandvermeidung, Brandbekämpfung, Gefahrenmanagement

Zeit + Zutritt

primion Technology GmbH
Steinbeisstraße 2-4 · 72510 Stetten a.K.M.
Tel.: 07573/952-0 · Fax: 07573/92034
info@primion.de · www.primion.de
Arbeitszeitmanagement, Zugangsmanagement, Personaleinsatzplanung, grafisches Alarmmanagement, SAP-Kommunikationslösungen, Ausweiserstellung, Biometrie

Notruf- und Service-Leitstelle

FSO Fernwirk-Sicherheitssysteme Oldenburg GmbH
Am Patentbusch 6a · 26125 Oldenburg
Tel.: 0441-69066 · info@fso.de · www.fso.de
Alarmempfangsstelle nach DIN EN 50518
Alarmprovider und Notruf- und Service Leitstelle nach VdS 3138, zertifiziertes Unternehmen für die Störungsannahme in der Energieversorgung.

ARBEITS SICHERHEIT

Zeit + Zutritt

Record Türautomation GmbH | Part of ASSA ABLOY
Otto-Wels-Straße 9 · 42111 Wuppertal
Tel: +49 202 60901 130 · Fax: +49 202 60901 11
sec.de@assaabloy.com · www.assaabloyentrance.de
Speedgates, Durchgangs- und Sicherheitsschleusen, Drehkreuze, Schwenktüren, Sicherheits-Karusselltüren und -Portale für die Sicherheits-Zutrittskontrolle und Personenvereinzelung.

BRAND SCHUTZ

Arbeitssicherheit

ELTEN GmbH
Ostwall 7–13 · 47589 Uedem
Tel.: 02825/8068
www.elten.com · service@elten.com
Sicherheitsschuhe, Berufsschuhe, PSA, ELTEN, Berufsbekleidung, Sicherheit

Zeit + Zutritt

SALTO Systems GmbH
Schwelmer Str. 245 · 42389 Wuppertal
Tel.: +49 202 769579-0 · Fax: +49 202 769579-99
info.de@saltosystems.com · www.saltosystems.de
Vielseitige und maßgeschneiderte Zutrittslösungen – online, offline, funkvernetzt, Cloud-basiert und mobil.

Brandschutz

DENIOS SE
Dehmer Straße 54-66
32549 Bad Oeynhausen
Fachberatung: 0800 753-000-3
Gefahrstofflagerung, Brandschutzlager, Brandschutz für Lithium-Akkus, Wärme- und Kältekammern, Containment, Auffangwannen, Arbeitsschutz, sicherheitsrelevante Betriebsausstattung, Gefahrstoff-Leckage-Warnsystem

Arbeitssicherheit

Hailo-Werk
Rudolf Loh GmbH & Co. KG
Daimlerstraße 8 · 35708 Haiger
www.hailo-professional.de
professional@hailo.de
Steig-/Schachtleitern, Steigschutzsysteme, Schachtabdeckungen, Servicelifte, Schulungsangebote

Zeit + Zutritt

TKH Security GmbH
Heinrich-Hertz-Straße 40 | D-40699 Erkrath
Tel.: +49 211 247016-0 | Fax: +49 211 247016-11
info.de@tkhsecurity.com | https://tkhsecurity.com/de/
Zugangskontrolle, Zutrittssteuerung, Cloudlösungen, Schließanlagen, Videoüberwachung, Sicherheitsmanagement

Brandschutz

Hertek GmbH
Landsberger Straße 240
12623 Berlin
Tel.: +49 (0)30 93 66 88 950
info@hertek.de · www.hertek.de
Hertek: ein Unternehmen im Bereich Brandschutzlösungen. Branchenspezifisches Fachwissen mit hochwertigen Brandschutzkomponenten vereint zu einem sicheren und verlässlichen Brandschutz. Flankiert wird dies mit Fachschulungen und einem umfangreichen, lösungsorientierten Kundenservice.

GEFAHRSTOFF MANAGEMENT

NOTRUF SERVICE LEITSTELLE

Brandschutz

Securitas Technology GmbH
SeTec Sicherheitstechnik
Haupstr. 40 a · 82229 Seefeld
Tel.: +49(0)8152/9913-0 · Fax: +49(0)8152/9913-20
info@setec-security.de · www.setec-security.de
Handfeuermelder, Lineare Wärmemelder, Feuerwehr Schlüsseldepots, Feuerwehr, Schlüsselmanager, Feuerwehrperipherie, Feststellanlagen, Störmeldezentralen

Gefahrstoffmanagement

asecos GmbH
Sicherheit und Umweltschutz
Weiherfeldsiedlung 16–18 · 63584 Gründau
Tel.: +49 6051 9220-0 · Fax: +49 6051 9220-10
info@asecos.com · www.asecos.com
Gefahrstofflagerung, Umwelt- unad Arbeitsschutz, Sicherheitsschränke, Chemikalien- und Umluftschränke, Druckgasflaschenschränke, Gefahrstoffarbeitsplätze, Absauganlagen, Raumluftreiniger uvm.

Gefahrstoffmanagement

BAUER GmbH
Eichendorffstraße 62 · 46354 Südlohn
Tel.: + 49 (0)2862 709-0 · Fax: + 49 (0)2862 709-156
info@bauer-suedlohn.com · www.bauer-suedlohn.com
Auffangwannen, Brandschutz-Container, Fassregale, Gefahrstofflagerung, Regalcontainer, Wärmekammern, individuelle Konstruktionen

MASCHINEN ANLAGEN SICHERHEIT

Gefahrstoffmanagement

DENIOS SE
Dehmer Straße 54-66
32549 Bad Oeynhausen
Fachberatung: 0800 753-000-3
Gefahrstofflagerung, Brandschutzlager, Brandschutz für Lithium-Akkus, Wärme- und Kältekammern, Containment, Auffangwannen, Arbeitsschutz, sicherheitsrelevante Betriebsausstattung, Gefahrstoff-Leckage-Warnsystem

Maschinen + Anlagen

EUCHNER GmbH + Co. KG
Kohlhammerstraße 16
D-70771 Leinfelden-Echterdingen
Tel.: 0711/7597-0 · Fax: 0711/753316
www.euchner.de · info@euchner.de
Automation, MenschMaschine, Sicherheit

Gefahrstoffmanagement

SÄBU Morsbach GmbH
Zum Systembau 1 · 51597 Morsbach
Tel.: 02294 694-23 · Fax: 02294 694-38
fladafi@saebu.de · www.fladafi.de
Gefahrstofflagerung, Gefahrstoffcontainer, Arbeits- & Umweltschutz, Auffangwannen, Gasflaschenlagerung, Gasflaschencontainer, Gasflaschenbox, Kleingebinderegale
Besuchen Sie unseren Online-Shop: www.fladafi.de

Maschinen + Anlagen

IBF Solutions GmbH
Bahnhofstr. 8 · 6682 Vils - AT
Tel. +43 (0) 5677 53 53 - 30
sales@ibf-solutions.com · www.ibf-solutions.com
Führender Anbieter von Softwaresystemen und Consulting-Leistungen im Bereich Maschinensicherheit. Unser Fokus liegt auf der Unterstützung nationaler und internationaler Kunden bei der CE-Kennzeichnung und Risikobeurteilung von Maschinen, Anlagen und elektrischen Geräten.

Maschinen + Anlagen

Pepperl+Fuchs SE
Lilienthalstraße 200 · 68307 Mannheim
Tel.: 0621/776-1111 · Fax: 0621/776-27-1111
fa-info@de.pepperl-fuchs.com
www.pepperl-fuchs.com
Sicherheits-Sensoren, Induktive-, Kapazitive-, Optoelektronische und Ultraschall-Sensoren, Vision-Sensoren, Ident-Systeme, Interface-Bausteine

GASMESS TECHNIK

Maschinen + Anlagen

K.A. Schmersal GmbH & Co. KG
Möddinghofe 30 · 42279 Wuppertal
Tel.: 0202/6474-0 · Fax: 0202/6474-100
info@schmersal.com · www.schmersal.com
Sicherheitszuhaltungen und Sicherheitssensoren, optoelektronische Sicherheitseinrichtungen wie Sicherheitslichtschranken sowie Sicherheitsrelaisbausteine, programmierbare Sicherheitssteuerungen und die Safety Services des Geschäftsbereichs tec.nicum

Maschinen + Anlagen

Pizzato Deutschland GmbH
Brienner Straße 55 · 80333 München
Tel.: 01522/5634596 · 0173/2936227
info@pizzato.com · www.pizzato.com
Automatisierung, Maschinen- und Anlagensicherheit: Sensorik, Schalter, Zuhaltungen, Module, Steuerungen, Mensch-Maschine-Schnittstelle, Positions- und Mikroschalter, Komponenten für die Aufzugsindustrie, u.v.m.

Gasmesstechnik

GfG Gesellschaft für Gerätebau mbH
Klönnestraße 99 · D-44143 Dortmund
Tel.: +49 (0)231/56400-0 · Fax: +49 (0)231/56400-895
info@gfg-mbh.com · GfGsafety.com
Gaswarntechnik, Sensoren, tragbare und stationäre Gasmesstechnik

Maschinen + Anlagen

Leuze electronic GmbH & Co. KG
In der Braike 1 · D-73277 Owen
Tel.: +49(0)7021/573-0 · Fax: +49(0)7021/573-199
info@leuze.com · www.leuze.com
Optoelektronische Sensoren, Identifikations- und Datenübertragungssysteme, Distanzmessung, Sicherheits-Sensoren, Sicherheits-Systeme, Sicherheits-Dienstleistungen

Maschinen + Anlagen

SSP Safety System Products GmbH & Co. KG
Max-Planck-Straße 21 · DE-78549 Spaichingen
Tel.: +49 7424 980 490 · Fax: +49 7424 98049 99
info@ssp.de.com · www.safety-products.de
Dienstleistungen & Produkte rund um die Maschinensicherheit: Risikobeurteilung, Sicherheitssensoren, -Lichtvorhänge, - Zuhaltungen, -Steuerungen sowie Schutzumhausungen, Zustimmtaster uvm.

Sicherheit komplett

aus dem Wiley Verlag

NEWSLETTER
GIT-SICHERHEIT.de
Jetzt kostenfrei registrieren

www.git-sicherheit.de/newsletter

WILEY
Industry Talks

Mit **Profis, Macherinnen und Entscheidern** in Sachen Sicherheit

Ausgabe ONLINE lesen

Mit unseren digitalen und gedruckten Medien sind Sie immer bestens informiert – über alle Themen der Sicherheit.

Probeabos, Mediadaten, Kontakt: GIT-GS@wiley.com

WILEY

DIE VIP LOUNGE

© Pirelli

Benjamin Schneider

Head of Security Pirelli Deutschland GmbH

- Ehemaliger Bundeswehroffizier (Dienstgrad Hauptmann)
- Dipl. Sportwissenschaftler
- M.A. Security Management
- Deputy Head of Physical Security HypoVereinsbank
- Seit 2018 Head of Security Pirelli Deutschland

Ihr Berufswunsch mit 20 war: Bereits damals wollte ich Verantwortung übernehmen. Das habe ich als Fahnenjunker bei der Bundeswehr in die Tat umgesetzt und konnte dort erste Führungserfahrungen sammeln.

Was hat Sie dazu bewogen, eine Aufgabe im Bereich Sicherheit zu übernehmen? Familiär vorgeprägt war mir schon früh klar, dass ich Verantwortung für andere übernehmen wollte. Nach dem Abitur und meiner Zeit bei der Bundeswehr wollte ich mich in der Privatwirtschaft weiterentwickeln und mich im Bereich Sicherheit engagieren.

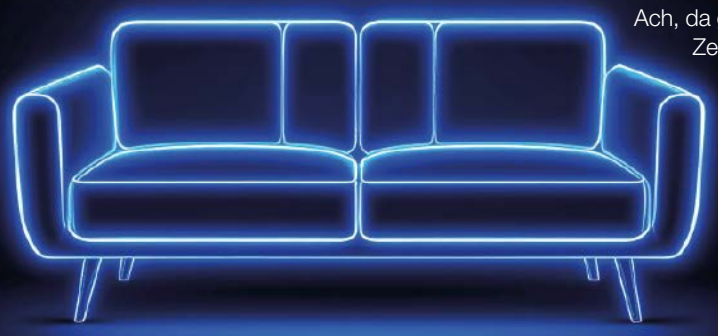
Welche sicherheitspolitische Entscheidung oder welches Projekt sollte Ihrer Meinung nach schon längst umgesetzt sein? Aus sicherheitstechnischer Sicht sind Investitionen in moderne Infrastrukturen, Energieversorgung und Digitalisierung unerlässlich. Hier ist Tempo gefragt – auch, um Unternehmen zukunftssicher aufzustellen.

Ein Erfolg, den Sie kürzlich errungen haben, war: Mit meinem Team einen Beitrag zum Gelingen des Motorrad Testivals 2025 zu leisten – eine komplexe Aufgabe mit vielen sicherheitsrelevanten Details.

Welche Reform bewundern Sie am meisten? Die Einführung eines systematischen, risikobasierten Sicherheitsmanagements in Unternehmen – kombiniert mit dem verstärkten Einsatz moderner Technologien wie Videoanalyse, Zutrittskontrollsystemen oder digitalem Incident Management. Diese Entwicklungen haben das Berufsbild im Sicherheitsbereich nachhaltig professionalisiert.

Wer hat Ihrer Meinung nach eine Auszeichnung verdient? Alle, die im Hintergrund für Sicherheit und Stabilität sorgen – und dabei oft wenig Sichtbarkeit erhalten. Das gilt für viele Berufsgruppen und Menschen, aber insbesondere für jene, die sich bei der Feuerwehr, in der Rettungsmedizin, bei der Polizei oder beim Technischen Hilfswerk für andere einsetzen.

Worüber können Sie sich freuen? Ach, da gibt es vieles: Wenn ich Zeit mit meiner Familie und Freunden verbringen, am Wochenende ausschlafen oder anderen eine Freude machen kann.



Wobei entspannen Sie? Auf meiner Hollywoodschaukel mit einem erfrischenden Getränk, und natürlich beim Sport.

Welchen Urlaubsort können Sie empfehlen? Das Gute liegt oft so nahe: Deutschland hat viele unterschätzte Reiseziele – Mosel, Müritz oder Dresden. Im Ausland zieht es mich immer wieder an den Gardasee oder nach Mailand.

Wie würde ein guter Freund Sie charakterisieren? Loyal, zuverlässig, witzig. Und wenn es um Sicherheit geht, mit einem Blick für Details.

Welche Zeitschriften lesen Sie regelmäßig? Ich lese gerne Magazine mit Technikbezug oder zu meinen Hobbys, etwa Motorräder, Uhren und Finanzen. Feste Rituale habe ich dabei keine.

Die GIT SICHERHEIT ist für mich wichtig, weil sie relevante Themen kompakt, praxisnah und mit einem Blick über den Tellerrand vermittelt.

Welches Buch haben Sie zuletzt gelesen? Die Kunst des guten Lebens: 52 überraschende Wege zum Glück.

Welche Musik hören Sie am liebsten? Je nach Gemütszustand gerne etwas Ruhiges, Electro oder Rock.

Was motiviert Sie? Es ist immer schön zu sehen, wenn ich mit meinem Team einen Beitrag leisten kann, der für das Unternehmen einen echten Mehrwert bringt. Mein Motto: I like to bring the company forward with knowledge, experience, passion and the right attitude.

Worüber machen Sie sich Sorgen? Mich bewegt, wenn der gesellschaftliche Zusammenhalt nachlässt. Denn Sicherheit beginnt für mich auch mit gegenseitigem Respekt und Vertrauen.

Die beste Erfindung im Bereich Sicherheit ist Ihrer Meinung nach: Im Bereich Fahrzeugsicherheit gibt es viele Meilensteine: Airbag, ABS, Totwinkelwarner oder Notbremsassistenten – sie retten tagtäglich Leben und sind nicht mehr wegzudenken.

Ihre gegenwärtige Geistesverfassung ist: Gut gelaunt und bereit für die kommenden Herausforderungen – privat und beruflich.

atlas®

MADE TO RESIST

XT 550 BOA GTX

Besuchen Sie uns in
Halle 13 | Stand D71

A+A
4-7 NOVEMBER 2025
DÜSSELDORF, GERMANY