

GIT

SICHERHEIT

MAGAZIN FÜR SAFETY UND SECURITY



Titelthema Seite 64:

Es geht auch ohne Smartphone

Assa Abloy stellt ersten Schlüssel mit
integrierter Mobilfunkverbindung vor



MESSE-AUSGABE

SCHWERPUNKT KRITIS

Drohnen, Sabotage, Cyberangriffe:

Wie Betreiber kritischer Infrastrukturen
ihre Resilienz stärken

ab S. 8/48

BRANDSCHUTZ

Funkbasierte Brandwarnanlagen,

IoT-Melder und digitale Prüfprozesse

ab S. 74



VIP

Hans-Peter Stuch, Gruppen-
leiter Drohnenabwehr im
Fraunhofer FKIE

S. 114



security
essen

HEFT IM HEFT



VIDEO

ab S. 36



Ausgabe
ONLINE lesen

WILEY

Wir schärfen den Blick für kritische Risiken.

Nicht jedes Risiko springt direkt ins Auge. Deshalb unterstützt Bosch Building Technologies Unternehmen dabei, Sicherheitslücken frühzeitig zu erkennen und geeignete Schutzmaßnahmen zu ergreifen – von der ersten Analyse bis zum sicheren Betrieb.

Schaffen Sie jetzt Klarheit auf: go-to-bosch.de/kritis-analyse



**Erstanalyse vereinbaren
und KRITIS-ready werden!**

Sorgen für Ihre Resilienz: Patricia Reinhard, Dr. Timo Gimbel, Sylvia Heider, Miryam Reubold, Matthias Erler, Steffen Ebert, Claudia Vogel (v. l.). Nicht im Bild, dafür im Home Office für Sie aktiv: Tina Renner (Assistenz), Dr. Michael Leising (Media) und Dr. Ralf Schlichting (Online). Standesgemäß ins Bild gesneakt: Layouter Andi Kettenbach

Resilienz mit Reichweite

Der September ist in der Branche ein Monat der Orientierung – und in diesem Jahr kommt die Security Essen als internationale Leitmesse der Sicherheitswirtschaft hinzu. Doch kreisen die Gespräche und Diskussionen des Jahres 2026 nicht allein um Innovationen und Technologien. Bedrohungen wie der Drohnenvorfall am Flughafen Leipzig/Halle Ende Juli sind keine abstrakten Szenarien mehr. Infrastrukturen stehen zunehmend im Fokus von Sabotage, Ausspähung und Cyberangriffen. Politik, Betreiber und Sicherheitswirtschaft sind gleichermaßen gefordert, die Resilienz wichtiger Systeme spürbar zu stärken.

Das Titelthema dieser Spätsommerausgabe der GIT SICHERHEIT zeigt freilich auch, wie etablierte und ausgereifte Technologien immer noch weiterentwickelt und ausgebaut werden: Auf Seite 64 stellen wir in der Titelstory den eCliq Flash von Assa Abloy vor, den ersten Schlüssel mit integrierter Mobilfunkverbindung.

Wie groß die Herausforderungen im Bereich Kritischer Infrastrukturen geworden sind, zeigen mehrere Beiträge des Schwerpunkts KRITIS. Ab Seite 8 erläutern Dirk H. Bürhaus und Fritz Rudolf Körper von Kötter, weshalb Sicherheit zunehmend zur strategischen Führungsaufgabe wird.

Direkt daran knüpft der Beitrag von Ulrich Dieckert ab Seite 10 an. Er analysiert die rechtlichen und technischen Defizite bei der Abwehr unbemannter Luftfahrzeuge und macht deutlich, wo dringender Handlungsbedarf besteht.

Unser Innentitel ab Seite 50 führt den Gedanken technologischer Resilienz im Bereich KRITIS fort. Clemens Pohl von AP Sensing erklärt, wie Glasfaserkabel zu Sensoren werden, die Pipelines, Stromtrassen oder Offshore-Windparks überwachen.

Im Heft im Heft ab Seite 36 werfen wir zudem einen Blick auf die Zukunft der Videotechnologie. Von Global-Shutter-Kameras für Verkehrsanwendungen bis hin zu KI-gestützten Analysen wird deutlich, wie sich Videotechnik vom Beobachter zum intelligenten Sensor entwickelt.

Auch der Brandschutz bleibt in Bewegung. Ab Seite 74 zeigen unsere Gesprächspartner von Detectortesters und Datolution, wie digitale Prüfprozesse Transparenz schaffen und Wartungsabläufe effizienter machen können.

Im Safety-Bereich zeigt sich, wie eng Sicherheit, Vernetzung und Verfügbarkeit zusammenhängen. Im Rahmen unserer VDMA-Reihe beleuchten wir auf Seite 90 das Thema Time-Sensitive Networking (TSN). Der dritte Beitrag der Reihe zeigt, wie deterministische, hochverfügbare Kommunikationsnetze künftig die Grundlage für sichere und skalierbare Automatisierungslösungen bilden können – von der industriellen Fertigung bis hin zu komplexen Produktionsnetzwerken.

Resilienz entsteht nicht erst in der Krise, sondern lange bevor diese eintritt.

In diesem Sinne wünschen wir von GIT SICHERHEIT Ihnen eine erkenntnisreiche und sichere Lektüre. **GIT**

 **pizzato**



**MAXIMUM TECHNOLOGY
IN THE MINIMUM VOLUME**

**Der weltweit kleinste
RFID Sicherheitsschalter
mit Zuhaltung**





TITELTHEMA

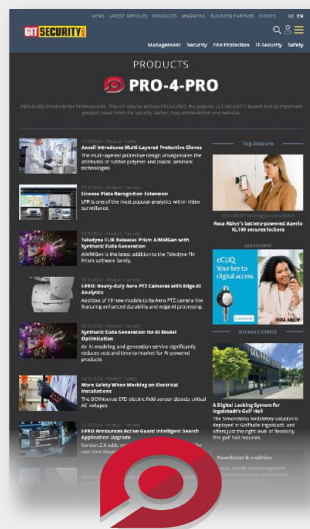
Es geht auch ohne Smartphone

Assa Abloy stellt ersten Schlüssel mit integrierter Mobilfunkverbindung vor

ab Seite 64



PRO-4-PRO
für 2026/2027



GIT-SICHERHEIT.DE/DE/PRODUKTE
PRODUCTS FOR PROFESSIONALS

Produkt- und Lead-Plattform
für Sicherheit



Dirk H. Bürhaus



Andreas Dannöhl



Ferdinand Gehring



Annick Gauthier

3 Editorial

Team GIT SICHERHEIT

MANAGEMENT

KRITIS

8 Hybride Risiken

„Sicherheit schafft Wertschöpfung für Firmen und KRITIS-Betreiber“

10 Sprengstoff-Drohne am Flughafen!

Wie lassen sich kritische Infrastrukturen ausreichend schützen? Ein Beitrag von Ulrich Diekert. Teil 1: Bedrohungslage, rechtliches Dilemma, Lösungsvorschläge

14 Nicht länger warten!

„KRITIS-Konformität beginnt mit einer fundierten Gefahren- und Risikoanalyse.“

16 Bedingt vorbereitet

Deutsche Szenarien in bedrohlichen Zeiten

20 Für die neue Risikolandschaft

Vernetzte Sicherheit: Wie integrierte Sicherheitslösungen Risiken steuern und regulatorische Anforderungen erfüllen

KRITIS

22 Wenn der Zaun nicht reicht

Kritische Infrastrukturen im Visier: 6 Erkenntnisse für KRITIS-Betreiber

MESSEN

26 Hotspot für sichere Kommunikation

PMRExpO 2026 in Köln

VERBÄNDE

28 Neue Technologien für die Unternehmenssicherheit

Der BVS Innovation Hub

WEITERBILDUNG

30 Schutz, Rettung, Sicherheit

vfdB-Akademie: Weiterbildung für die Praxis

VERANSTALTUNGEN

32 Ein Ökosystem der Sicherheit

Secsolutionforum 2026 in Bologna

AK SIBE BW

33 Treffen in Konstanz

ASW-BW-Fachtagung des Arbeitskreises der Sicherheitsbevollmächtigten

SICHERMACHER

34 Converged Security

Warum integrierte Sicherheit zur Pflicht wird

HEFT IM HEFT – VIDEO

VIDEOTECHNOLOGIE

36 Wenn jede Millisekunde zählt

Netzwerkcameras: Global Shutter für moderne Verkehrsanwendungen

SICHERMACHER

39 Vom Kamerahersteller zum Plattformanbieter

Ein Gespräch mit Maximilian Galland, Sales Manager DACH bei Axis Communications

VIDEOTECHNOLOGIE

42 Baustein der Sicherheitstechnologie

Künstliche Intelligenz made in Germany

VIDEOTECHNOLOGIE

44 Videosensoren und Intelligente Videoanalyse im Perimeterschutz

Teil 1 – Entwicklung und technische Grundlagen. Von Hans-Peter Büttner und Ronald Guldner

SECURITY MANAGEMENT

46 Wenn Videodaten zu belastbaren Beweisen werden

Coda Video 9.2 von Octave: Wie Smart Evidence Management Videoanalyse, Ermittlungen und Sicherheitsprozesse effizienter machen soll



Aljona Ijoschina



Jürgen Hövelmann



Xaver Schmidt



Philipp Heinemann

SECURITY

INNENTITEL

49 Überwachung des Unüberschaubaren

Glasfaser als Sensoren zum Schutz von kritischen Infrastrukturen

ZAUNSICHERHEIT

56 Übersteigen, Durchdringen, Untergraben

Bewertung von Zaunanlagen

GIT TEST SERIE – TEIL 3

60 Perspektivwechsel am Perimeter

Neue Möglichkeiten, praxisnah bei Optex getestet: Distributed Acoustic Sensing (DAS)

TITELTHEMA

64 Es geht auch ohne Smartphone

Assa Abloy stellt ersten Schlüssel mit integrierter Mobilfunkverbindung vor

ZUTRITT

66 Integriertes Sicherheits-Ökosystem

KRITIS-konform bei Berlin-Chemie

SCHLISSFACHLÖSUNGEN

68 Kontrollierter Zugriff

Sicherheitskritische Assets verwahren

CYBER-SECURITY

MANAGED SECURITY

70 Bevorzugte Ziele

Wie KMU ihre IT-Sicherheit sofort verbessern können

BRANDSCHUTZ

DIGITALE PRÜFFPROZESSE

74 Intelligenter, transparenter, schneller

Digitale und vernetzte Prüfprozesse im Brandschutz

SICHERMACHER

78 „Innovation ist unser Motor“

GIT SICHERHEIT im Gespräch mit Jürgen Hövelmann von EPS

LITHIUM-IONEN-AKKUS

80 Tausend Grad und mehr

Lithium-Ionen-Akkus: wachsende Herausforderung für den Brandschutz

BRANDMELDETECHNIK

82 Brandmeldeanlagen mobil überwachen

App für den Fernzugriff

JUBILÄEN

84 50 Jahre Wagner

Vom Ingenieurbüro zur internationalen Unternehmensgruppe

AUTONOME GEBÄUDE

88 IoT-ernetzt in die Zukunft

Wie sich Brandschutz im Zeitalter autonomer Gebäude verändert

SAFETY

MASCHINEN- UND ANLAGENSICHERHEIT

90 Time-Sensitive Networking – TSN in der Anwendung

Skalierbare und präzise Produktionsnetze mit PROFINET und TSN

CYBER RESILIENCE ACT

94 CRA-Readiness für Maschinen und Anlagen

Cyberresilienz in der Automatisierung

SICHERHEITSARCHITEKTUR

98 Alles Gute kommt von oben – Sicherheit auch

Normgerechte Kranmodernisierung

SCHUTZHANDSCHUHE

100 Die 11,5-Milliarden-Euro-Frage

Warum PSA nicht automatisch schützt

KNIESCHUTZ

104 Stabil im Knien, beweglich im Einsatz

Knieschutz für Baustelle und Montage

EVENT

106 Arbeitsschutz Aktuell 2026

Wenn Sicherheit zur Chefsache wird

INDEX

QUICK-FINDER

ORGANISATIONEN, INSTITUTIONEN UND UNTERNEHMEN IM HEFT

Advancis	27, 54
AFAG	6
AG Neovo	47
AP Sensing	50
Asecos	72, 105, 107
Assa Abloy	Titel, 55, 64, 69
ASW BW	6, 33
Automatic Systems	41
Axis Communications	36, 39, 59
B.I.N.S.S.	44
Barox	39
BDLS	6
BDSW	6, 19
BG Bau	102
Bihl+Wiedemann	94
Bläkläder	103, 107
Bosch Building Technologies	U2, 14
BVSW	28
Coredinate	19
Dallmeier	33, 42, 54
Datolution	74, 87
Detector testers	74, 81
Dräger	107
Eagle Eye	U4
Eks Engel FOS	21
Eneo	52
EPS	78, 83
Fiera Bologna	32
FireAngel	82
Fraunhofer (IDMT / FKIE)	12, 114
FTI Consulting	16
Geutebrück	41
Geze	83
GfS	55
Hanwha Vision	57
Haus der Technik	73
HB Protective Wear	105
HID Global	U3
Hikvision	59
Hinte Expo	106
Hirsch Secure	45
Hymer-Steigtechnik	105
Infirotec	80
Inotec	83
Keba	41, 59, 68, 97
Kentix	71
Klüh	7, 19, 20
Koelnmesse	26
Krause-Werk	102
Kötter	8
Labor Strauss	79, 82
Leuze	107
Lokavis	22
Lünendonk	12, 72
Messe Essen	13, 29
Miele Professional	87
Mobotix	41
Munk	97, 105
Nierhaus	104
Nobix Group	70
NSTR.security by LivEye	15
Octave	46
Optex	60
Paxton	17
PCS Systemtechnik	37, 66, 69
Phg Peter Hengstler	35
Phoenix Contact	90, 97
Pilz	98
Pizzato	3
Primion	34
Sachverständigenbüro Markus Pendl	22, 60
Salto Systems	51
Security Robotics	63
SimonsVoss	55
Schmersal	93
Secunet	72
Securiton	13
Showa	100
Siemens	87, 88, 90
Telenot	Beilage
Uhlmann & Zacher	55
VDMA	90
Vfdb	30
VfS	56
VSW-Mainz	25
Wagner Group	81, 84
Walaris	11
Werma Signaltechnik	93
Wibu-Systems	97
Videor	53
Zenitel	72



SicherheitsExpo München 2026

Die SicherheitsExpo München 2026 stellte an zwei Tagen aktuelle Themen, Entwicklungen und Trends rund um Sicherheitstechniken in den Mittelpunkt. Die Messe überzeugte mit hochkarätigen Fachvorträgen, namhaften Ausstellern und einer hohen Dichte an Entscheidern, die sich gezielt auf den Messebesuch vorbereitet haben. Die Aussteller und Besucher zeigten sich mit der diesjährigen SicherheitsExpo München sehr zufrieden. Die nächste Ausgabe der SicherheitsExpo München findet am 30. Juni und 1. Juli 2027 im MOC München statt. Rund 3.500 Besucher kamen zur SicherheitsExpo München 2026, um die Angebote der über 120 Aussteller für sich zu entdecken. Die beiden Fachforen und die Möglichkeiten zum Netzwerken wurden sehr gut angenommen. Die SicherheitsExpo München hat in diesem Jahr einen Flächenzuwachs verzeichnet und konnte darüber hinaus mehr Besucher als bei der Vorveranstaltung begrüßen.

www.afag.de

Drohnenvorfall: Sicherheitsverbände fordern entschlossenes Handeln

Der Bundesverband der Sicherheitswirtschaft (BDSW) und der Bundesverband der Luftsicherheitsunternehmen (BDLS) sehen in dem schwerwiegenden Drohnenvorfall am Flughafen Leipzig/Halle ein deutliches Warnsignal an die Politik. Die Ereignisse machen erneut sehr deutlich, dass Deutschland bei der Abwehr unbemannter Luftfahrzeuge vor einer neuen sicherheitspolitischen Herausforderung steht. Der Vorfall markiert eine neue Dimension der Bedrohung Kritischer Infrastrukturen und muss ein Weckruf für die Politik sein. „Wir haben eine neue sicherheitspolitische Realität“, sagt Cornelius Tousaint, Vizepräsident des BDSW und Vorsitzender des Fachausschusses Drohnen. „Drohnen sind heute ein Werkzeug für Spionage, Sabotage und Kriminalität – und die bestehenden gesetzlichen Rahmenbedingungen reichen nicht aus, um diese Bedrohung wirksam zu adressieren.“

www.bdsw.de

Travel Risk Management 2026

Das Expertenforum Travel Risk Management 2026 der Allianz für Sicherheit in der Wirtschaft Baden-Württemberg in Kooperation mit der Safeture AB widmet sich am 29. September 2026 in der Westspitze Tübingen aktuellen Herausforderungen. Auf der Agenda stehen unter anderem Travel Risk Management und Duty of Care, Cyber, Crime und Crisis, geopolitische Risiken, Business Travel Security sowie Compliance und Immigration.

Geschäftsreisen führen zunehmend in ein komplexes Risikoumfeld. Geopolitische Spannungen, Cyberbedrohungen, Kriminalität und unvorhersehbare Krisen stellen Unternehmen vor die Frage, wie sie ihre Mitarbeiter unterwegs wirksam schützen und gleichzeitig ihrer Fürsorgepflicht gerecht werden können. Das Expertenforum Travel Risk Management 2026 greift zum inzwischen vierten Mal seit 2023 diese Entwicklungen auf und bringt Fachleute aus unterschiedlichen Bereichen zum Austausch zusammen.



Travel Risk Management hat sich längst von der reinen Reiseorganisation zu einem wichtigen Bestandteil von Unternehmenssicherheit und Risikomanagement entwickelt. Unternehmen müssen Risiken frühzeitig bewerten, geeignete Maßnahmen definieren und im Krisenfall schnell reagieren können. Gleichzeitig steigen die Anforderungen an Duty of Care, Compliance und die Absicherung internationaler Geschäftsaktivitäten.

Dabei geht es nicht nur um theoretische Betrachtungen. Erfahrungsberichte aus der Praxis, Fachvorträge und Diskussionen sollen unterschiedliche Perspektiven aufzeigen und konkrete Anregungen für den Unternehmensalltag geben. Themen wie die Auswirkungen geopolitischer Entwicklungen auf Geschäftsreisen oder der Umgang mit Krisen und Sicherheitsrisiken stehen dabei genauso im Fokus wie Fragen rund um Visa, Immigration und die zunehmenden Compliance-Anforderungen.

Zu den angekündigten Beiträgen gehören unter anderem „Smarter Than Risk? KI im Travel Risk Management“, „Cyber, Crime & Crisis: Was Reisende heute erwartet“, „Weltunordnung 2030+“, „Beyond Compliance: Modernes TRM in der Praxis“ und „No Visa, No Entry, No Business“. Damit reicht das Themenspektrum von technologischen Entwicklungen über geopolitische Risiken bis hin zu konkreten Herausforderungen im internationalen Geschäftsreiseumfeld.

Bereits am 28. September 2026 findet ein Vorabendevent statt, das Gelegenheit für persönlichen Austausch und Networking bietet. Das Expertenforum richtet sich an Verantwortliche und Fachleute, die sich mit Travel Risk Management, Unternehmenssicherheit, Geschäftsreisen, Krisenmanagement, Compliance und der Fürsorgepflicht gegenüber Mitarbeitern beschäftigen.

www.asw-bw.com



Wir denken Sicherheit neu.

Risiken verändern sich. Bedrohungen wie Cyberangriffe, technische Ausfälle, Lieferkettenunterbrechungen oder auch Extremwetterereignisse stellen Unternehmen, Institutionen und Anlagenbetreiber vor Herausforderungen.

Wir bündeln die verschiedenen Systeme auf einer herstellernerutralen Plattform. Qualifiziertes Personal überwacht rund um die Uhr aus unserer zertifizierten, intelligenten Leitstelle sämtliche sicherheitsrelevanten Prozesse Ihres Unternehmens.

www.klueh.de



Dirk H. Bürhaus
Geschäftsführender Direktor in der Kötter Security Gruppe und u. a. Geschäftsführer von Kötter Cyber Security



Fritz Rudolf Körper,
Mitglied des Kötter Sicherheitsbeirates und ehemaliger Parlamentarischer Staatssekretär im Bundesministerium des Innern

KRITIS

Hybride Risiken

„Sicherheit schafft Wertschöpfung für Firmen und KRITIS-Betreiber“

Hybride Risiken aus Sabotage und Spionage setzen Wirtschaft und Kritische Infrastrukturen (KRITIS) unter Druck. Aktuelles Beispiel ist der Drohnenvorfall an einem deutschen Logistikdrehkreuz. Dazu kommt die wachsende Zahl von Cyberangriffen, deren Gefährlichkeit durch die kriminelle Nutzung von Künstlicher Intelligenz (KI) massiv forciert wird. GIT SICHERHEIT sprach mit Dirk H. Bürhaus, u. a. Geschäftsführer von Kötter Cyber Security, sowie Fritz Rudolf Körper, Mitglied des Kötter Sicherheitsbeirates.

■ GIT SICHERHEIT: Herr Bürhaus, Herr Körper, der jüngste Drohnenvorfall an einem deutschen Großflughafen hat die Bedrohungslage durch hybride Risiken auf eine neue Stufe gehoben, so das Urteil vieler Experten. Was resultiert hieraus?

D. H. Bürhaus: Das Ereignis hat nachdrücklich unterstrichen, dass die Bedrohung durch Drohnen in den letzten Jahren rasant zugenommen hat. Unabhängig von diesem konkreten Fall gilt daher seit Langem: Drohnerkennung und -abwehr müssen für jedes Unternehmen und jeden KRITIS-Betreiber weit oben auf der Agenda stehen – unter Einbeziehung spezialisierter Dienstleister.

F. R. Körper: Gleichzeitig ist die Politik gefordert. Denn wir brauchen straffe behördliche Strukturen statt des Flickenteppichs an administrativen Zuständigkeiten ebenso wie einen wirklich umfassenden Rechtsrahmen für die Drohnenabwehr. Er sollte neben staatlichen Institutionen, KRITIS-Betreibern und Unternehmen auch die Sicherheitswirtschaft einbeziehen sowie diesen Akteuren effektive und rechtssichere Handlungsmöglichkeiten verschaffen. Dazu gehört auch eine Ausweitung der privatrechtlichen Hausrechtsausübung im Luftraum, durch die sich Betroffene gesetzeskonform gegen unautorisierte Drohnenüberflüge zur Wehr setzen können.

Das ist aber bei weitem nicht alles an hybriden Risiken: Insolvenzen infolge von Cyberattacken, Produktionsstillstände nach Brandanschlägen und Sabotageakte auf die Verkehrsinfrastruktur. Wie groß sind die Bedrohungen insgesamt?

D. H. Bürhaus: Riesig – und die Gefahren nehmen stetig weiter zu. Das zeigen folgende Zahlen: Gemäß Bitkom-Studie sind knapp neun von zehn Unternehmen in Deutschland durch analoge und digitale Spionage sowie Sabotage betroffen. Das jährliche Schadensvolumen hat sich in zehn Jahren mehr als verfünffacht auf mittlerweile 289 Milliarden Euro – mehr als das Doppelte des NRW-Lan-

deshaushaltes. Besonders prägnant zudem: Rund 70 % hiervon, also allein schon knapp über 200 Milliarden Euro, entfallen auf KI-forcierte Cybercrime, das Wirtschaftsrisiko Nummer 1.

Die Politik hat hierauf mit KRITIS-Dachgesetz und NIS2-Richtlinie reagiert...

F. R. Körper: Beide Gesetze senden das eindeutige Signal an Wirtschaft und KRITIS-Betreiber, dass Sicherheit oberste Priorität haben muss. Physischer Schutz und Cybersecurity sind jetzt Unternehmens-Kernpflicht. Rund 2.000 Betreiber kritischer Infrastrukturen in Deutschland fallen unter das KRITIS-Dachgesetz. Der Wirkungskreis der NIS2-Richtlinie ist noch weitgehend: Sie betrifft hierzulande knapp 30.000 Unternehmen aus 18 Branchen und Sektoren.

D. H. Bürhaus: Mit dem KRITIS-Dachgesetz werden beide Sektoren erstmals eng miteinander verknüpft. Dieser Allgefahrenansatz hat größte Relevanz, da Sicherheit immer integrativ zu betrachten ist. Unternehmen müssen das Silodenken überwinden, bei dem eine Abteilung den physischen Schutz steuert und eine andere die Cyberabwehr übernimmt.

Was sind aus Ihrer Sicht die inhaltlichen Kernelemente?

F. R. Körper: Erstens: Alle betroffenen Akteure unterliegen einer Registrierungspflicht – gemäß KRITIS-Dachgesetz beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK, und entsprechend NIS2 beim Bundesamt für Sicherheit in der Informationstechnik, BSI. Zweitens: Sie müssen über ein funktionierendes Business-Continuity-Management verfügen – also nachhaltige Strukturen zur Aufrechterhaltung des Betriebes in der Folge eines Notfalls implementieren. Und das inklusive aktivem Krisenmanagement. Drittens: Aus dieser Architektur resultieren konkrete Anforderungen an physischen und IT-Schutz, aber auch Vorschriften zu Meldepflichten, Dokumentationen oder Audits.

D. H. Bürhaus: NIS2 richtet den Fokus zum Beispiel auf die häufig vernachlässigte Kontrolle von Beschaffungsprozessen. Sie ist gerade bei IT-Komponenten von elementarer Relevanz, da diese meist aus dem Ausland kommen und damit Einfallstor für Spionage sind. Weiteres Beispiel: NIS2 verpflichtet Firmen zu Kryptografie, also Verschlüsselung, als Bestandteil des Risikomanagements.

Was müssen Resilienzanalysen sowie daraus folgende BCM-Bausteine zum Beispiel umfassen?

D. H. Bürhaus: Bevor Sicherheitsmaßnahmen greifen, braucht es ein präzises Bild der Ausgangslage. Basis ist daher immer eine Asset-basierte Risikoanalyse. Sie zeigt auf, welche Prozesse und Ressourcen – von Gebäudekomponenten bis zu IT-Systemen – verwundbar sind und wie sie abgesichert werden können. Daraus leiten wir passgenaue Schutzkonzepte ab. Diese reichen von Sicherheitsdiensten und -technik wie etwa Streifengängen und Zutrittskontrollsystemen über Social-Media-Monitoring und Cyber-Defense bis zu Awareness-Schulungen, Notfallübungen und Penetrations-Tests. Im Krisenfall können wir zudem die operative, reversionssichere Lageführung übernehmen, inklusive Notfallkommunikation.

F. R. Körper: All dies ist notwendig, weil der Nachholbedarf in Sachen Sicherheit gerade im Mittelstand riesig ist. Beispiele: Auf vielen Arealen weisen IP-Kameras solche Sicherheitslücken auf, dass Kriminelle sie hacken können, die Steuerung übernehmen oder sich im Zweifel weiteren Zugang zum Netzwerk verschaffen. Ähnlich sieht es bei digital gesteuerten Aufzügen aus. Gleichzeitig haben Brandanschläge auf Strommasten und Kabelbrücken nachhaltig verdeutlicht, wie physisch verwundbar unsere Infrastrukturen sind und welche weitgehenden Folgen daraus resultieren.

Welche physischen Schutzbausteine folgen daraus explizit – etwa für die Sicherheit von Umspannwerken oder Produktionen?

D. H. Bürhaus: Priorität hat die gezielte bauliche Sicherung durch Mauern, Zäune etc. mit geeigneter Sicherheitstechnik inklusive Leitstellen-Aufschaltung. Ziel: Tätern den Zugang zu erschweren und damit einen Sabotageakt zu behindern. Gleichzeitig gewinnen Verantwortliche so nach der Täter-Detektion wertvolle Zeit für Intervention und Notfallmaßnahmen. Dies reduziert Schadensrisiken genauso wie „Security by Design“, also Sicherheitsmaßnahmen bereits bei Standortplanungen. Diese Komponenten wirken nicht allein gegen physische Angriffe, sondern auch gegen Cybercrime und damit ganz im BCM-Sinn.

Spannender Brückenschlag. Worin liegt der hohe Stellenwert physischer Komponenten gegen Cyberangriffe, etwa bei einer Klinik?

F. R. Körper: Cybercrime erfolgt nicht allein aus dem Web heraus. Vielen Attacken gehen physische Delikte voraus: etwa, indem Kriminelle unzureichende Zugangskontrollen zu Stations- oder sogar Serverräumen ausnutzen und dort mit präparierten Sticks

das Netzwerk manipulieren. Nur einer von vielen Aspekten, weshalb ein krisensicheres BCM gerade für Krankenhäuser und Kliniken von höchstem Stellenwert ist – denn sowohl im Alltag als noch mehr in Krisensituationen sind sie elementar für die Versorgungssicherheit.

... und was ist zusätzlich gefordert?

D. H. Bürhaus: Direkten Netz-Angriffen muss ebenfalls größte Aufmerksamkeit gelten, da diese das Gesundheitswesen und andere KRITIS-Sektoren, aber auch Betriebe immer stärker treffen. Es geht darum, solche Attacken in Echtzeit zu registrieren und die Ausbreitung zu verhindern. Daher hat die 24/7-Überwachung von IT-Systemen, wie wir sie mit dem Security Operations Center bieten, zentrale Bedeutung. Im Sinne integraler Sicherheit kooperiert das SOC auch aufs Engste mit Werkschutz-Mitarbeitern, beispielsweise, wenn es Anomalien im Datenverkehr registriert und dann zur Gefahrenabwehr Serverräume zusätzlich gesichert werden.

All diese Anforderungen bereiten vielen Unternehmern aber Sorge mit Blick auf Umsetzbarkeit und Haftungsrisiken. Was raten Sie Firmenchefs?

F. R. Körper: Umfassend in ganzheitliche Sicherheit zu investieren. Denn nicht oder nur halbherzig zu handeln, wird am Schluss doppelt so teuer – in Form massiver Schäden plus Haftungsfolgen, die bis zu 2 % des weltweiten Umsatzes reichen können. Trotzdem ist die Unternehmer-Sorge nachvollziehbar: Zahlreiche Anforderungen sind gerade für kleine und mittelständische Firmen in Eigenregie kaum zu managen. Aber hier besteht gezielte externe Unterstützung.

Zudem ergibt sich hieraus, dass Sicherheit Chefsache sein muss – egal, ob bei physischem Schutz oder Cybersecurity?

F. R. Körper: Exakt. Unternehmensschutz muss immer strategische Führungsaufgabe sein. Denn Prävention und integrierte Sicherheit stärken die Stabilität in einem immer unkalkulierbarer werdenden Umfeld. Sie zahlen damit ganz entscheidend auch auf das Kundenvertrauen ein. 



Kötter

www.koetter.de

KRITIS

Sprengstoff-Drohne am Flughafen!

Wie lassen sich kritische Infrastrukturen ausreichend schützen?

Ein Beitrag von Ulrich Dieckert. Teil 1:

Bedrohungslage, rechtliches Dilemma, Lösungsvorschläge

Der Drohnenvorfall am Flughafen Leipzig Ende Juli 2026 hat das Bewusstsein für eine Bedrohung geschärft, die längst in Deutschland angekommen ist. Nur durch Zufall wurde dort eine mit Sprengstoff beladene Drohne entdeckt. Und Anfang August musste wieder einmal ein Verkehrsflughafen (Hannover) wegen einer Drohnensichtung stundenlang gesperrt werden. In einem zweiteiligen Beitrag für GIT SICHERHEIT geht der Berliner Rechtsanwalt Ulrich Dieckert der Frage nach den – insbesondere rechtlichen – Möglichkeiten im Umgang mit derartigen Vorfällen nach.



Dr. Ulrich Dieckert Rechtsanwalt in Berlin und Mitherausgeber des Werks „Drohnen – Betrieb, Recht und Technik“ (Reguvis Verlag, 2. Auflage 2025)

■ Nach einer Studie des Deutschen Zentrums für Luft- und Raumfahrt (DLR) wurden 2025 insgesamt 116 Drohnenstörfälle an 25 deutschen Verkehrsflughäfen erfasst. Die Folgen – Betriebsunterbrechungen in München über mehrere Tage, umfassende Störungen am Frankfurter Flughafen – summierten sich auf einen geschätzten Schaden von mindestens 60 Millionen Euro. Und für das erste Halbjahr 2026 registrierte die für die Flugsicherung zuständige DFS bereits 145 unerlaubte Drohneneinflüge auf deutschen Flughäfen.

Für Anlagen der Energie- und Wasserwirtschaft, bei denen ein Angriff katastrophale Kaskadeneffekte auslösen kann, existieren vergleichbare Statistiken bislang nicht. Dabei war bisher eine Zuordnung zu den Piloten und Betreibern dieser Drohnen und deren Absichten durch die Sicherheitsbehörden oder die Anlagenbetreiber praktisch nicht möglich.

Der Gesetzgeber hat die Bedrohungslage zwar durchaus erkannt, in letzter Zeit aber lediglich bei den Befugnissen der Sicherheitsbehörden nachgebessert. Des Weiteren hat der Bundesinnenminister im August ein neues Forschungszentrum eröffnet, das auch gezielte Abwehrmöglichkeiten entwickeln soll (mehr dazu in Teil 2 dieses Beitrags in der Oktoberausgabe der GIT SICHERHEIT). Diese Maßnahmen sind zwar begrüßenswert, lösen aber das Kernproblem nicht. Denn bei der Vielzahl von Anlagen der kritischen Infrastruktur

(man denke nur an die leitungsgebundenen Einrichtungen der Versorgungswirtschaft) können weder die Bundes- noch die Landespolizei einen flächendeckenden Schutz gewährleisten. Die extrem kurzen Reaktionszeiten bei Drohnenangriffen – im Bereich weniger Minuten vom Anflug bis zur Wirkung – machen ein rechtzeitiges Eintreffen behördlicher Kräfte faktisch unmöglich.

Rechtliches Dilemma

Der Gesetzgeber mutet den Betreibern kritischer Infrastrukturen eine paradoxe Situation zu. Wie im zweiten Teil dieses Artikels dargestellt wird, sind diese zwar durch eine Vielzahl von Normen zur umfassenden Sicherung ihrer Anlagen verpflichtet. Andererseits fehlt es aber an tauglichen Ermächtigungsgrundlagen für eine effektive Drohnenabwehr. „Weiche“ Abwehrmethoden wie z. B. Jamming erfordern eine aktive Frequenznutzung, die nach § 55 TKG einer Zuteilung bedarf. Nach Auffassung der Bundesnetzagentur ist eine Nutzung, die ausschließlich darauf angelegt ist, eine andere Funknutzung (nämlich die Drohnensteuerung) zu stören, mit dem Grundsatz der störungsfreien Frequenznutzung aus § 2 Abs. 2 Nr. 8 TKG nicht vereinbar. Ein Verstoß kann nach §§ 126, 149 TKG untersagt und als Ordnungswidrigkeit geahndet werden.

Und bei „harten“ Abwehrmaßnahmen wie dem Abschuss von Drohnen riskiert der Verteidiger Schadensersatzansprüche sowie eine Strafbarkeit wegen Sachbeschä-

digung (§ 303 StGB, § 823 BGB), und gegebenenfalls sogar eine Strafbarkeit wegen gefährlichen Eingriffs in den Luftverkehr (§ 315 StGB). Wie ebenfalls im zweiten Teil dieses Artikels dargelegt, könnte sich der Anlagenbetreiber im Angriffsfall zwar auf die Rechtfertigungstatbestände der Notwehr (§ 227 BGB, § 32 StGB) bzw. des Notstandes (§ 228 BGB, § 34 StGB) berufen, diese stellen jedoch keine taugliche Rechtsgrundlage für eine systematische Abwehr dar, zumal die Beweislast für das Vorliegen einer Notwehrlage beim Verteidiger liegt.

Es ist dem Sicherheitspersonal einer KRITIS-Anlage schlicht nicht zumutbar, in Sekundenbruchteilen hochkomplexe rechtliche Abwägungen treffen zu müssen, während eine nicht identifizierbare Drohne mit hoher Geschwindigkeit auf sicherheitsrelevante Anlagenteile zufliegt. Wer sich hier irrt, riskiert strafrechtliche Verfolgung und zivilrechtliche Inanspruchnahme – trotz objektiv verantwortungsvollen Handelns.

Beleihung und Sicherheitspartnerschaften als Lösung

Betreiber kritischer Infrastrukturen benötigen entweder eine Sicherheitspartnerschaft mit den zuständigen Ordnungsbehörden oder – wo deren permanente Präsenz nicht realisierbar ist – eine Beleihung, die ihnen unter strikten rechtlichen Vorgaben eigene Abwehrbefugnisse verleiht.

Das Vorbild der Sicherheitspartnerschaft ist schon seit langem bei Verkehrsflughäfen

bekannt. Dort ist die DFS Deutsche Flugsicherheitsbehörde als beliehenes Unternehmen gemäß §§ 27c, 31b LuftVG für die sichere, geordnete und flüssige Abwicklung des Flugverkehrs im kontrollierten Luftraum zuständig. Nach einer Übereinkunft der zuständigen Ministerien aus dem Jahr 2019 gehören dazu auch die Detektion und Verifikation gefährlicher Drohnen, wozu die DFS entsprechende Gerätschaften vorzuhalten hat. Für die Abwehr solcher Drohnen zuständig ist hingegen die – auf Flughäfen dauerpräsent – Bundespolizei, der nach den einschlägigen Vorschriften des Bundespolizeigesetzes bzw. des Luftverkehrsgesetzes der Schutz vor Angriffen auf die Sicherheit des Luftverkehrs obliegt. Seit dieser Abstimmung wurden zwar eine Reihe von Tests durchgeführt, taugliche Detektions- und Abwehrsysteme sind nach meiner Kenntnis aber – vermutlich aus Kostengründen – erst auf den Flughäfen Frankfurt und München installiert. Auf dem Flughafen Leipzig wurde nach dem Vorfall Ende Juli 2026 in aller Eile eine mobile Detektionstechnik nachgerüstet.

Übertragen auf die Drohnenabwehr bei anderen Anlagen der kritischen Infrastruktur hieße das: Die Betreiber schaffen Detektions- und Abwehrsysteme an; die Sicherheitsbehörden bedienen diese im Angriffsfall aus eigener Kompetenz und in eigener rechtlicher Verantwortung. Dieses Modell funktioniert grundsätzlich aber nur dort, wo Behörden permanent vor Ort sein können – etwa bei Großkraftwerken oder zentralen Netzverteilanlagen. (Zur Möglichkeit des Zugriffs aus der Ferne, siehe den Kommentar von David Sonntag im Kasten).

Für die flächendeckende Absicherung dezentraler Infrastrukturen bedarf es jedoch des Beleihungsmodells. Der Bundesverband der Energie- und Wasserwirtschaft (BDEW) hat in einem Positionspapier vom Oktober 2025 praxistaugliche Vorschläge hierzu unterbreitet. Beleihung ist ein im deutschen Verwaltungsrecht bewährtes Instrument, welche gerade im Bereich des Luftverkehrs nicht unbekannt ist; so überträgt § 16a Luftverkehrsgesetz bereits heute bestimmte Aufgaben auf private Luftverkehrsunternehmen unter hoheitlicher Aufsicht.

Vorstellbare gesetzliche Vorgaben

Für die Drohnenabwehr wären – auch unter Berücksichtigung der von den Drohnenverbänden UAV DACH und BVZD aufgestellten Forderungen – folgende gesetzliche Vorgaben vorstellbar:

- Schaffung eines einheitlichen Luftlagebildes im unteren Luftraum, kombiniert mit der verbindlichen Einführung eines automatischen Funkprotokolls zur Unterscheidung zwischen legalem und illegalem Drohnenbetrieb
- Einrichtung von verbindlichen Flugverbotszonen über konkret definierte KRITIS-Anlagen, integriert in U-Space-Systeme und durch Geo-Fencing technisch abgebildet, sodass jede nicht autorisierte Drohne in diesen Zonen per se rechtswidrig unterwegs ist (flächendeckende Verbotszonen wären für die zivile Drohnenwirtschaft hinderlich)
- Schaffung einer spezialgesetzlichen Grundlage, welche die Betreiber kritischer Infrastrukturen im Wege der Beleihung ermächtigt, gefährliche Drohnen unter

Bitte umblättern ▶

Belastbare Entscheidungsgrundlage

■ Eine Sicherheitspartnerschaft zwischen KRITIS-Betreibern und Behörden bedarf eines technisch belastbaren und geprüften Gesamtsystems. Ein Kommentar von David Sonntag, Senior Director Business Development Walaris.

Kein einzelner Sensor kann alle Drohnen unter sämtlichen Einsatzbedingungen sicher erfassen. Radarsysteme bieten Reichweite und eine kontinuierliche Verfolgung, liefern allein aber nicht immer die erforderlichen Informationen zur eindeutigen Identifikation. Funkfrequenzsensoren, Remote-ID, ADS-B, Akustik und optische Systeme ergänzen das Lagebild jeweils um wichtige Informationen. Erst die intelligente Fusion dieser Daten in einem Command-and-Control-System (kurz C2) schafft eine belastbare Entscheidungsgrundlage.

Drohne, Vogel oder Hubschrauber?

Eine zentrale Rolle spielt dabei die von Walaris entwickelte Computer Vision AI. Sie wertet die Bilder angeschlossener Kameras automatisiert aus und hilft, erkannte Flugobjekte sicher zu verifizieren und zu klassifizieren. Das C2 muss unterscheiden können, ob es sich tatsächlich um eine Drohne, einen Vogel, einen Hubschrauber oder ein anderes Objekt handelt. Gleichzeitig unterstützt die KI dabei, Bewegungen zu verfolgen, Auffälligkeiten zu erkennen und den Verantwortlichen ein nachvollziehbares Lagebild bereitzustellen. So wird aus

einer zunächst unspezifischen Sensormeldung eine qualifizierte und dokumentierte Bewertung.

Möglichst eindeutige Informationen

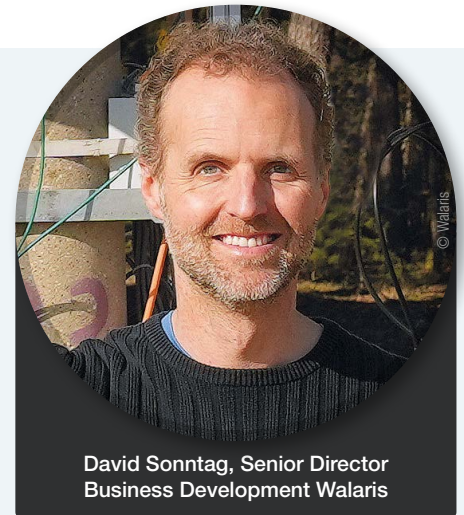
Eine Behörde darf nicht auf der Grundlage eines einzelnen, möglicherweise fehlerhaften Alarms über weitreichende Maßnahmen entscheiden. Sie benötigt möglichst eindeutige Informationen darüber, welches Objekt sich wo befindet, wie es sich bewegt und warum von ihm eine konkrete Gefahr ausgehen könnte. Die Kombination mehrerer Sensoren mit der Computer Vision AI reduziert Fehlalarme und verdichtet die einzelnen Meldungen zu einem gemeinsamen Lagebild.

Standortbezogen geplant

Ein System zur Drohnen-Detektion und Drohnen-Abwehr muss standortbezogen geplant, aufgebaut und unter realistischen Bedingungen getestet werden. Dabei sollten unabhängige Sachverständige von Beginn an einbezogen werden. Erst nach einer unabhängigen Prüfung und Abnahme sollte das Gesamtsystem den zuständigen Behörden vorgestellt und gemeinsam in die vorgesehenen Alarm- und Reaktionsprozesse eingebunden werden.

Zugriff in Echtzeit

Im Rahmen einer Sicherheitspartnerschaft könnte die zuständige Behörde dann über eine sichere VPN-Verbindung im Alarmfall



David Sonntag, Senior Director Business Development Walaris

auf das Lagebild zugreifen. Sie erhält in Echtzeit Zugriff auf verifizierte Sensormeldungen, Kamerabilder, Flugspuren und die dokumentierte Bewertung. Bei einer bestätigten Bedrohung könnte sie – im Rahmen der jeweiligen gesetzlichen Befugnisse – selbst geeignete Abwehrmaßnahmen aus der Ferne auslösen oder die erforderlichen Entscheidungen treffen.

Denkbar ist außerdem, dass die technische Durchführung innerhalb einer gesetzlich geregelten Sicherheitspartnerschaft auf besonders qualifizierte und beliehene Dienstleister übertragen wird. Die hoheitliche Entscheidungs- und Kontrollstruktur bliebe dabei eindeutig festgelegt, während geschulte Kräfte vor Ort die erforderlichen Maßnahmen ohne vermeidbaren Zeitverlust umsetzen könnten. **GIT**

www.walaris.com

Einhaltung strenger Vorgaben selbst abzuwehren

- Definierte Vorgaben zur räumlichen Eingrenzung des Abwehrbereichs sowie die Pflicht zur vorherigen Detektion und Identifikation gefährlicher Drohnen durch Einsatz fusionierter Sensoren. Beschränkung auf verhältnismäßige Wirkmittel

- Bedienung der Abwehreinrichtungen nur durch geschultes Personal. Verpflichtung zu Fail-Safe-Mechanismen und hinreichender Transparenz wie z. B. lückenlose Protokollierung der jeweiligen Einsätze

- Haftungsüberleitung auf den Staat nach den Grundsätzen der Amtshaftung (Art. 34 GG, § 839 BGB), verbunden mit einer gesetzlichen oder vertraglichen Begrenzung des Rückgriffs gegenüber dem Beliehenen

Des Weiteren sollte das Telekommunikationsgesetz so geöffnet werden, dass beliehene Betreiber unter definierten Auflagen auf die Funkverbindung gefährlicher Drohnen zugreifen dürfen (z. B. Jamming). Im Strafgesetzbuch könnte – wie vom BDEW gefordert – ein neuer Tatbestand des „gefährlichen Eingriffs in die kritischen Inf-

rastrukturen der Energie- und Wasserwirtschaft“ – analog zu § 315 StGB – geschaffen werden, während gleichzeitig klargestellt wird, dass rechtmäßige Drohnenabwehr über KRITIS-Anlagen weder einen gefährlichen Eingriff in den Luftverkehr noch eine Sachbeschädigung darstellt.

Schließlich sollten die entstehenden – nicht unerheblichen – Investitionen zumindest für die Versorgungswirtschaft über Entgelte und Gebühren refinanzierbar sein. Denn nicht nur die Anschaffung von Detektions- und Abwehrtechnik, sondern deren laufende Bedienung verursachen einen hohen Aufwand, an dem sich der Staat auch deshalb beteiligen sollte, weil er den KRITIS-Betreibern hohe Verpflichtungen zum Schutz ihrer Infrastruktur auferlegt. Ansonsten steht zu befürchten, dass viele Betreiber auf eine Inanspruchnahme der ihnen verliehenen Abwehrbefugnisse verzichten.

Zusammenfassung

Der Gesetzgeber hat die Betreiber kritischer Infrastrukturen jahrelang juristisch im Regen stehen lassen. Er verpflichtet sie

zur Sicherung, verweigert ihnen aber die Mittel zur wirksamen Abwehr. Der Verweis auf Notwehr und Notstand ist keine Alternative, weil diese Rechtsinstitute für eine systematische Drohnenabwehr ungeeignet sind. Auch reicht es nicht, allein die Ordnungsbehörden mit erweiterten Befugnissen auszustatten und darauf zu hoffen, dass diese schon rechtzeitig vor Ort sein werden. Vielmehr muss der Bund jetzt die rechtlichen, technischen und finanziellen Grundlagen für eine wirksame Drohnenabwehr bei kritischen Infrastrukturen schaffen – sei es über Sicherheitspartnerschaften, über streng reglementierte Beleihungsmodelle oder über eine Kombination beider Ansätze.

Der zweite Teil dieses Beitrags erscheint in der Oktoberausgabe und befasst sich detailliert mit den Abwehrbefugnissen der Behörden, der unzureichenden Rechtslage bei KRITIS-Betreibern und den technischen Voraussetzungen für die Errichtung einer tauglichen Sicherheitsinfrastruktur. **GIT**



Dr. Ulrich Dieckert Rechtsanwalt
www.dieckert.de

Fraunhofer IDMT: Akustische Drohnenerkennung

Das Fraunhofer IDMT Oldenburg hat eine akustische Sensorlösung entwickelt, die Drohnen anhand ihres Klangmusters erkennt und lokalisiert, auch ohne Sichtkontakt. Wenn sich ein unbemanntes Luftfahrzeug einem sensiblen Bereich nähert, zählt jede Sekunde. Sicherheitskräfte müssen möglichst früh erkennen, ob eine Drohne im Anflug ist, wo sie sich befindet und wie sich die Situation entwickelt. Klassische Detektionsverfahren liefern dafür wichtige Informationen, sind aber nicht in jeder Umgebung gleichermaßen zuverlässig: Sichtverbindungen können fehlen, Funkverbindungen gestört sein. Akustische Sensorik eröffnet hier einen zusätzlichen Zugang. Als Ergänzung zu und in Verbindung mit Radar, Kamera und Lidar kann sie bestehende Sicherheitssysteme robuster machen und auch dort Hinweise liefern, wo optische oder funkbasierte Verfahren an Grenzen stoßen. www.idmt.fraunhofer.de



Drohnen hören, bevor man sie sieht: Die Lösung des Fraunhofer IDMT detektiert und lokalisiert Drohnen auch außerhalb des Sichtfeldes mittels intelligenter akustischer Sensorik

Lünendonk: Schwache Konjunktur bremst Wachstum führender Sicherheitsdienstleister

Die 25 nach Umsatz führenden Sicherheitsdienstleister in Deutschland haben ihren Umsatz im Geschäftsjahr 2025 im Durchschnitt um 4,6 Prozent gesteigert. Das Wachstum liegt damit unter dem Vorjahreswert und zeigt, dass die schwache Konjunktur auch im Sicherheitsdienstleistungsmarkt angekommen ist. Für die Jahre 2026 bis 2030 blicken die Dienstleister optimistisch nach vorn und erwarten ein jährliches Umsatzwachstum zwischen 6,7 und 7,6 Prozent, getrieben unter anderem durch die voraussichtlich steigende Nachfrage im Zuge der KRITIS-Regulatorik. Das sind erste Ergebnisse der neuen Lünendonk-Studie „Sicherheitsdienstleistungen in Deutschland“, die im September 2026 erscheint.

Die 25 führenden Sicherheitsdienstleister erwirtschafteten im Geschäftsjahr 2025 einen sicherheitsrelevanten Umsatz in Höhe von 5.628,1 Millionen Euro und repräsentieren damit rund 40 Prozent des Marktvolumens (ohne Geld- und Wertlogistik). Im Segment Sicherheit beschäftigen sie insgesamt 97.400 Mitarbeiter und damit rund ein Drittel aller Beschäftigten der deutschen Sicherheitswirtschaft.

Die deutsche Landesgesellschaft des schwedischen Sicherheitskonzerns Securitas behauptet sich mit einem Umsatzwachstum von 2,4 Prozent auf insgesamt 1.239,1 Millionen Euro an der Spitze der Lünendonk-Liste. Als einziges Unternehmen erzielt Securitas einen Umsatz von mehr als einer Milliarde Euro und bildet damit knapp neun Prozent des deutschen Sicherheitsdienstleistungsmarktes ab, mit deutlichem Abstand zum Verfolgerfeld.

Auf Rang zwei folgt die Kötter Unternehmensgruppe mit Hauptsitz in Essen. Kötter erzielte im Sicherheitsdienstleistungssegment ein Umsatzwachstum von 8,6 Prozent auf 659,0 Millionen Euro. Daneben erbringt der Dienstleister auch Facility Services und erreicht in Deutschland einen Gesamtumsatz von 770,0 Millionen Euro.

www.luenendonk.de

Security Essen 2026: Vernetzte Sicherheit im Fokus

Die Sicherheitswirtschaft befindet sich in einem tiefgreifenden Wandel. Künstliche Intelligenz sorgt für rasante Innovationsimpulse und der Schutz Kritischer Infrastrukturen gewinnt angesichts wachsender Cyberbedrohungen und geopolitischer Entwicklungen weiter an Bedeutung. Gleichzeitig steigen die Anforderungen an Unternehmen, Behörden und Betreiber, physische und digitale Sicherheit ganzheitlich zu denken. Wie diese Entwicklung die Branche verändert und welche Lösungen den Markt künftig prägen werden, zeigt die Security Essen vom 22. bis 25. September 2026 in der Messe Essen.

Als internationale Leitmesse der Sicherheitswirtschaft bringt sie rund 500 Aussteller aus 40 Nationen zusammen und bietet Fachbesuchern einen umfassenden Überblick über aktuelle Technologien, Innovationen und Trends.

Dabei bildet die Fachmesse erneut die gesamte Bandbreite moderner Sicherheitslösungen ab. Das Angebot reicht von Zutrittskontrolle, Mechatronik und mechanischen Sicherungssystemen über Brand- und Einbruchschutz, Perimetersicherung und Videoüberwachung bis hin zu Dienstleistungen, Sonderschutzfahrzeugen sowie Lösungen für Bevölkerungsschutz und zivile Verteidigung.

Besonders deutlich zeigt sich dabei ein Trend: Die Grenzen zwischen den einzelnen Bereichen verschwimmen zunehmend. Moderne Gefahrenmanagementsysteme verknüpfen Videotechnik, Zutrittskontrolle und Einbruchmeldetechnik auf einer gemeinsamen Plattform. Künstliche Intelligenz unterstützt Sicherheitsverantwortliche dabei, Risiken schneller zu erkennen und Ereignisse effizienter zu bewerten. Cloudbasierte Anwendungen ermöglichen die standortübergreifende Steuerung komplexer Sicherheitsinfrastrukturen, während intelligente Sensorik und Automatisierung neue Maßstäbe bei Prävention und Reaktionsgeschwindigkeit setzen.

Diese Entwicklung spiegelt sich auch auf der Security Essen wider. Unternehmen wie Advancis oder Milestone präsentieren Lösungen für modernes Sicherheits- und Gefahrenmanagement. Assa Abloy, Dormakaba, Salto und Telenot zeigen Innovationen rund um Zutrittskontrolle und Gebäudesicherheit. Im Bereich intelligenter Video- und Perimetersicherheit gehören unter anderem Axis Communications, Dallmeier und Strops zu den Ausstellern.

Ergänzt wird das Angebot durch zahlreiche weitere Marktführer, Spezialisten, innovative Unternehmen und Start-ups aus allen Bereichen der Sicherheitswirtschaft.

Der Austausch zwischen den unterschiedlichen Akteuren der Sicherheitswirtschaft findet dabei nicht nur an den Messeständen statt. Mit ihrem umfangreichen Rahmenprogramm schafft die Security Essen zusätzliche Plattformen für Wissenstransfer, Diskussionen und Networking zwischen Herstellern, Anwendern, Wissenschaft, Verbänden und Behörden.

Neue Synergien durch die parallele Eudex

Erstmals findet die Security Essen parallel zur Eudex – Euro Defence Expo statt. Die neue Fachmesse für die Verteidigungsindustrie ergänzt die Security Essen um Themen, die angesichts aktueller sicherheitspolitischer Entwicklungen an Bedeutung gewinnen.



Auf der Security Essen präsentieren vom 17. bis 20. September 2024 rund 500 Aussteller ihre Innovationen aus den Bereichen „Dienstleistungen“, „Zutritt, Mechatronik, Mechanik und Systeme“, „Perimeter“, „Video“, „Brand, Einbruch und Systeme“, „Bevölkerungsschutz“, „Sonderschutzfahrzeuge“ sowie „Digital Networking Security“

Der Schutz Kritischer Infrastrukturen, Bevölkerungsschutz, Krisenvorsorge und resiliente Sicherheitskonzepte lassen sich heute nur noch im Zusammenspiel von Wirtschaft, Behörden und Streitkräften denken. Durch die parallele Durchführung beider Veranstaltungen entstehen neue Möglichkeiten für den fachlichen Austausch und die Zusammenarbeit zwischen ziviler Sicherheitswirtschaft und Verteidigungsindustrie.

Davon profitieren insbesondere Fachbesucher, die sich mit ganzheitlichen Sicherheitsstrategien beschäftigen und Schnittstellen zwischen physischer Sicherheit, Cybersecurity, Bevölkerungsschutz und Verteidigung

in den Blick nehmen möchten. Die Kombination beider Messen schafft damit eine einzigartige Plattform für Innovation, Wissenstransfer und Networking.

www.messe-essen.de

security
essen 26

22. - 25. September
Halle 7 Stand F12

60 **IPS** Intelligent
Video Software

Alarmsituationen erkennen,
bevor sie entstehen.

Videosicherheit ist intelligente
Videoüberwachung mit IPS-Faktor.

Besonders. Sicher.
www.securiton.de/ips-faktor

SECURITON

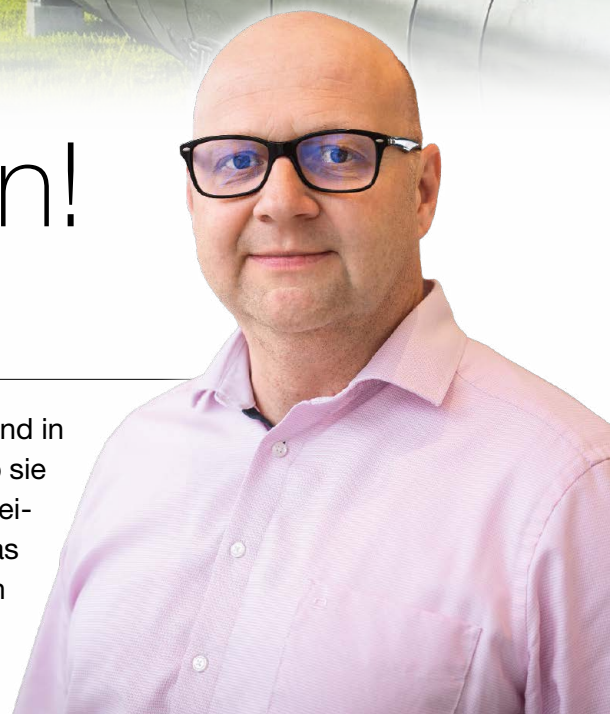


KRITIS

Nicht länger warten!

„KRITIS-Konformität beginnt mit einer fundierten Gefahren- und Risikoanalyse.“

Am 17. März dieses Jahres ist das KRITIS-Dachgesetz in Deutschland in Kraft getreten. Viele Unternehmen wissen aber noch nicht genau, ob sie KRITIS-relevant sind und welche Maßnahmen sie in diesem Fall ergreifen müssten. Im Gespräch mit GIT SICHERHEIT erläutert Andreas Dannöhl, KRITIS-Experte und Branchenmanager Industrie bei Bosch Building Technologies, wie Unternehmen ihre KRITIS-Relevanz erkennen und womit sie in die Umsetzung starten können.



■ GIT SICHERHEIT: Herr Dannöhl, das Thema KRITIS gewinnt an Brisanz. Welche Fragen werden Ihnen als Experten am häufigsten gestellt?

Andreas Dannöhl: Am Anfang steht meistens die Frage: Sind wir überhaupt KRITIS-relevant? Gerade im Mittelstand gibt es hier noch Unsicherheiten. Vor allem weniger offensichtliche Sektoren wie die Lebensmittelindustrie oder technische Zulieferer von Infrastruktur-Betreibern fühlen sich oft nicht angesprochen.

Das heißt, hier ist noch Aufklärungsarbeit zu leisten?

Andreas Dannöhl: Auf jeden Fall, insbesondere bei den kleineren Unternehmen, die Teil einer größeren Versorgungskette sind. Denn jede Kette ist nur so stark wie ihr schwächstes Glied. Im Grunde genommen

sollten sich alle Unternehmen, die Teil einer solchen Kette sind, mit KRITIS beschäftigen.

Welche Unterstützung können Sie dabei leisten?

Andreas Dannöhl: Wir stellen zunächst fest, ob ein Unternehmen von der KRITIS-Gesetzgebung betroffen ist. Das ist immer der Startpunkt. Diese Beratungsleistung bieten wir sehr niedrigschwellig an: Der Einstieg erfolgt – völlig unverbindlich – über ein kostenloses ein- bis zweistündiges Gespräch vor Ort beim Unternehmen.

Und was ist der nächste Schritt, wenn das Unternehmen KRITIS-relevant ist?

Andreas Dannöhl: Dann folgt eine ausführliche Analysephase. Sie besteht aus einer Gefahren- und Risikoanalyse und bildet die Grundlage für die spätere Erstellung

eines richtlinienkonformen Schutzkonzepts. In dieser Phase erfragen wir zum Beispiel auch, ob bereits ein Sicherheitskonzept besteht und ob es anhand der potenziellen Eintrittswahrscheinlichkeit von Zwischenfällen ausreichend ist.

Können Sie diese Analysephase etwas genauer beschreiben?

Andreas Dannöhl: Die Analysephase basiert auf einem dreistufigen, methodischen Prozess. Sie beginnt mit einer detaillierten Gefahren- und Schwachstellenanalyse, die Bedrohungsszenarien und Täterprofile anhand von Standort, Technik und Organisation identifiziert. Danach werden diese Risiken nach Eintrittswahrscheinlichkeit und Schadensausmaß bewertet und als priorisierte Risiko-Matrix dargestellt. Das Ergebnis ist ein an die ISO 31000 angelehntes Lastenheft, das konkrete bauliche,

technische und organisatorische Sicherungsmaßnahmen definiert.

Wie werden die Analyseergebnisse in konkrete Maßnahmen umgesetzt?

Andreas Dannöhl: Wir erstellen ein richtlinienkonformes Schutzkonzept, das Unternehmen als Anleitung dient, um KRITIS-konform zu werden. Darin sind alle Schutzmaßnahmen aufeinander abgestimmt und es ist festgelegt, welche technischen Komponenten und Systeme implementiert werden müssen. Danach folgt dann die konkrete bauliche, technische und organisatorische Umsetzung.

Bosch Building Technologies verfügt über langjährige Expertise in der physischen Absicherung komplexer Infrastrukturen, beispielsweise mit Perimeterschutz. Denken Sie in Ihren Analysen zusätzlich auch das Thema Cybersicherheit mit?

Andreas Dannöhl: Die Cybersicherheit ist inzwischen eng mit der physischen Sicherheit verzahnt. Zum Beispiel hat jede Überwachungskamera auch Softwarekomponenten, die mit anderen Systemen im Unternehmen vernetzt sind. Oder nehmen Sie das Thema Cloud: Es ist durchaus relevant, in welchem Land die Server dafür stehen.

Das heißt, Sie sind auch Spezialisten für die NIS2-Verordnung, die das Thema Cybersicherheit gesetzlich regelt?

Andreas Dannöhl: Beim Schutz von Netz- und Informationssystemen arbeiten wir eng mit unserem erfahrenen Kooperationspartner T Security zusammen. Das

01 Analyse	02 Schutzkonzept	03 Umsetzung und Betrieb
■ Betroffenheit klären ■ Risiken bewerten ■ Schwachstellen identifizieren ■ Handlungsfelder festlegen	■ Schutzziele bestimmen ■ Roadmap erstellen ■ Maßnahmen festlegen ■ Umsetzungsplanung	■ Implementierung ■ Monitoring ■ Kontinuierliche Optimierung ■ Wartung
Ergebnis: Transparenz	Ergebnis: Klarheit	Ergebnis: Resilienz

KRITIS-Konformität entsteht Schritt für Schritt. Schon in der Analysephase steht Bosch Building Technologies Kunden als kompetenter Beratungspartner zur Seite

Tochterunternehmen der Deutschen Telekom übernimmt – falls es vom Kunden zusätzlich gewünscht wird – den NIS2-Beratungsansatz und prüft unter anderem das IT-Sicherheitsmanagementsystem beim Kunden. Damit ergänzt T Security unser Angebot zur physischen Sicherheit optimal.

Warum haben Sie sich für diese Kooperation entschieden?

Andreas Dannöhl: Mit T Security arbeiten wir bereits seit Jahren eng zusammen. T Security ist auch Teil des Bosch Sicherheitsnetzes, kurz BoSiNet genannt. Dabei handelt es sich um ein Netzwerk für die verschlüsselte Alarm- und Datenübertragung. Wir kennen und schätzen uns aus dieser langjährigen Zusammenarbeit.

Heißt das, Ihre Risikoanalysen umfassen ab jetzt immer KRITIS und NIS2?

Dannöhl: Nicht unbedingt, der Kunde hat hier die freie Wahl. Er kann nur eine Analyse der physischen Sicherheit vornehmen lassen, oder nur den Bereich Cybersicherheit

abdecken, oder beides im Paket. Es war uns wichtig, das Angebot so flexibel wie möglich zu gestalten. Im Endeffekt geht es vor allem darum, die von KRITIS und NIS2 betroffenen Unternehmen bei allen Schritten eng zu begleiten.

Noch eine praktische Frage: Was raten Sie Unternehmen, die wissen wollen, ob ihre Organisation KRITIS-relevant ist?

Andreas Dannöhl: Unser wichtigster Rat ist, nicht länger zu warten. Analyse und Umsetzung brauchen Zeit, und die haben wir angesichts der derzeitigen Gefährdungen nicht. Deshalb ist es existenziell, möglichst schnell zu wissen, ob man überhaupt vom Thema KRITIS betroffen ist und welche Maßnahmen in diesem Fall für eine höhere Resilienz getroffen werden müssen. **GIT**



Bosch Building Technologies
www.boschbuildingtechnologies.com

© Bilder: Grafik: Bosch Building Technologies

NSTR.SECURITY BY LIVEYE

NSTR.security by LivEye sichert Firmengelände mit autarken KI-Multikameras und einer aktiven deutschen Leitstelle, die live eingreift, bevor Schaden entsteht. Keine Großinvestition, sondern Sicherheit als planbares Abo: Hardware, KI, 24/7 Leitstelle und Dokumentation aus einer Hand, Made in Germany.

Erleben Sie live, wie aktive Videoüberwachung Diebstahl, Vandalismus und Sabotage verhindert auf der Security Essen Messe | 22. - 25. September 2026 | Halle 5, Stand 5A29



Jetzt scannen &
Termin am Stand sichern!
nstr.security

LivEye

NSTR
SECURITY





KRITIS

Bedingt vorbereitet

Deutsche Szenarien in bedrohlichen Zeiten

Sich einen klaren Blick auf die Lage zu verschaffen – das ist in Krisen oberstes Gebot, wenn man rational handeln und sich nicht lähmen lassen will. Ferdinand Gehring und Johannes Steger erläutern in ihrem Buch „Deutschland im Ernstfall“, was eigentlich genau passiert, wenn Deutschland angegriffen wird – auch durch die viel besprochenen hybriden Bedrohungen und Sabotageakte etwa gegen kritische Infrastrukturen. Wie robust und handlungsfähig sind wir im Fall der Fälle? GIT SICHERHEIT hat mit Ferdinand Gehring gesprochen.

■ GIT SICHERHEIT: Herr Gehring, Sie sind ein vielbeschäftigter Experte und beraten als solcher beispielsweise Politiker und Organisationen zu Themen wie Cybersicherheit und hybriden Bedrohungen sowie zur Sicherheit der so im Fokus stehenden kritischer Infrastrukturen. Geben Sie uns zunächst einmal einen Einblick zu Ihrem Hintergrund?

Ferdinand Gehring: Ich komme aus der Schnittstelle von Sicherheit, Technologie und Geopolitik und verbinde dabei technische, strategische und regulatorische Perspektiven. Inhaltlich arbeite ich vor allem zum Schutz kritischer Infrastrukturen, Cybersicherheit und hybriden Bedrohungen sowie dazugehöriger Resilienz. Neben der sicherheitspolitischen Praxis habe ich auch einen juristischen Hintergrund, der insbesondere bei Fragen von Regulierung, staatlichen Eingriffsbefugnissen und der rechtlichen Einordnung von Krisen- und Konfliktszenarien eine wichtige Rolle spielt. Diese Kombination erlaubt es mir, sowohl operative Schwachstellen als auch strategische und rechtliche Implikationen ganzheitlicher zu analysieren und entsprechend zu beraten.

Zusammen mit Johannes Steger haben Sie das Buch „Deutschland im Ernstfall“ geschrieben. Seitdem ist zwar gar

nicht so viel Zeit vergangen, aber dennoch ist die Welt seit dem Krieg in der Golfregion nicht mehr dieselbe. Was hat sich für Deutschland aus Ihrer Sicht verändert?

Ferdinand Gehring: Die sicherheitspolitische Lage hat sich weiter verdichtet: Konflikte sind vernetzter, schneller und komplexer geworden. Deutschland ist seit der Veröffentlichung unseres Buches spürbar stärker von hybriden Angriffen betroffen. Gleichzeitig zeigt die Lage im Mittleren Osten die Verwundbarkeit globalisierter Lieferketten und digitalisierter Infrastrukturen.

Zunehmend zentral ist zudem die Ressourcenfrage – auch mit Blick auf den Krieg in der Ukraine: Hoher Materialverbrauch, insbesondere auf Seiten der USA, bindet Kapazitäten, während die Ukraine zugleich durch ihre Drohnenexpertise neue Unterstützer gewinnen kann. Russland und China beobachten diese Dynamiken sehr genau.

Inzwischen stellt man sich ja sogar die Frage, ob iranische Raketen Deutschland erreichen könnten?

Ferdinand Gehring: Ausschließen können wir das nicht – technisch ist es grundsätzlich möglich, insbesondere mit weiterentwickelten Trägersystemen und

ballistischen Raketen entsprechender Reichweite. Der jüngste Abschuss einer iranischen ballistischen Rakete auf den gemeinsamen US-britischen Militärstützpunkt Diego Garcia im Indischen Ozean verdeutlicht diese Fähigkeiten. Allerdings ist unklar, ob der Start tatsächlich von Land aus erfolgte; ebenso denkbar ist ein Abschuss von einer Plattform in geringerer Distanz, etwa von einem Schiff.

Für Deutschland ist derzeit jedoch weniger ein direkter Angriff wahrscheinlich als vielmehr eine indirekte Bedrohung über Eskalationsdynamiken und asymmetrische Mittel, etwa durch iranische Proxys. Zudem verfügt Iran über ausgeprägte Cyberfähigkeiten, die zuletzt erneut sichtbar geworden sind.

Ausgangspunkt für Ihr Buch ist der Ernstfall, also die Vorstellung eines tatsächlichen Angriffs gegen Deutschland. Bevor wir dazu kommen: Wir werden ja schon von Russen und Chinesen nach Strich und Faden ausspioniert und sabotiert – auf guerillahafte Weise mit Hilfe von „Low-level-Agenten“. Außerdem gibt es Desinformationskampagnen per Social Media. Wie genau ist das eigentlich erfasst?

Ferdinand Gehring: Wir erfassen die verschiedenen Formen der hybriden Einflussnahme noch nicht ausreichend. Vielmehr

beginnen wir gerade erst damit, Spionage- und Sabotagefälle systematisch zu erfassen. Anfang des Jahres haben wir erstmalig bundesweite Zahlen zu den Sabotageverdachtsfällen (321 Fälle) bekommen. Die Sicherheitsbehörden arbeiten oft isoliert, erstellen individuelle Lagebilder und teilen Informationen nur zurückhaltend – das muss sich angesichts der aktuellen Bedrohungslage schnell ändern. Gleichzeitig müssen wir besser darin werden, Muster zu erkennen, operative Maßnahmen zu ergreifen, Fälle zu analysieren und Unternehmen stärker einzubinden. Besonders gegen „Low-Level“-Agents laufen Ermittlungen zu häufig noch leer und Täter werden kaum gefasst. Das bestärkt Russland derzeit darin, eher weiter darauf zu setzen.

Lassen Sie uns jetzt mal die Szenarien durchspielen, mit denen Deutschland reagieren würde. Es gibt den Zustimmungsfall – dann den Spannungsfall, der in die Notwendigkeit der Gesamtverteidigung mündet...?

Ferdinand Gehringer: Ich habe derzeit eher den Eindruck, dass wir politisch zu spät reagieren würden. Der Zustimmungsfall und der Spannungsfall sollen es

Deutschland ermöglichen, frühzeitig auf Bedrohungen zu reagieren und stärkere Sicherheitsmaßnahmen zu ergreifen. Konkret sieht die deutsche Notstandsverfassung eine abgestufte Abfolge vor: Im Zustimmungsfall kann die Regierung einzelne vorbereitende Maßnahmen treffen. Im Spannungsfall, also im Vor-Verteidigungsfall, können schon weitreichende Maßnahmen der Gesamtverteidigung aktiviert, etwa die Mobilisierung von Ressourcen, die Einbindung von Behörden und Unternehmen sowie die Anpassung der zivilen Infrastruktur. Der Verteidigungsfall kann ausgerufen werden, wenn Deutschland bspw. direkt angegriffen wird. Er erlaubt umfassende staatliche Eingriffe zur Landesverteidigung. Dann gibt es noch den Bündnisfall, der dann erklärt werden kann, wenn ein Nato-Partner angegriffen wird. Vorher muss die Nato Artikel 5 des Nato-Vertrages aktivieren; Deutschland unterstützt dann die Verteidigung des Bündnisses.

Derzeit fürchte ich, dass wir die Vorbereitungsphase, die ein Zustimmungsfall oder Spannungsfall ermöglichen würde, verschlafen. Deutschland wird im Ernstfall vermutlich erst reagieren, wenn ein Nato-Partner unmittelbar und direkt und auch nicht „nur hybrid“ angegriffen wird. Auf

hybride Angriffe reagieren wir politisch noch zu zurückhaltend: Die Sorge politischer Entscheidungsträger, der Bevölkerung zu viel zuzumuten, ist groß. Ich bin aber der Meinung, dass wir unserer Bevölkerung deutlich mehr zumuten können und sie nicht unterschätzen sollten. Sie verfolgen die Sicherheitslage genau.

Nun gibt es zwei Säulen der Verteidigung, die militärische und die zivile. Könnten Sie das zunächst einmal überschlägig definieren?

Ferdinand Gehringer: Die militärische Säule umfasst den Einsatz von Heer, Luftwaffe und Marine, also alles, was direkt Angriffe abwehrt und das Land schützt. Die zivile Säule sorgt dafür, dass der Staat, die Wirtschaft und die Gesellschaft funktionsfähig bleiben – etwa durch sichere Strom- und Wasserversorgung, Notfallpläne für Krankenhäuser oder die Koordination von Logistik und Krisenstäben. Beide Säulen greifen ineinander: Militärische Maßnahmen funktionieren nur, wenn die zivilen Strukturen stabil bleiben, und die zivile Verteidigung kann ohne militärische Unterstützung im Ernstfall schnell an ihre Grenzen stoßen.

Bitte umblättern ▶

Der **NEUE** weiterentwickelte **PaxLock Pro2**

Robust konstruiert. Zuverlässig im Schutz.

Zertifiziert. Bewährt. Sicher.

Der neueste Funk-Türdrücker mit Zutrittskontrollfunktion von Paxton.



Entdecken Sie PaxLock Pro2

bei unseren exklusiven Webinaren

Jetzt anmelden



Paxton

Herr Gehringer, lassen Sie uns nun etwas näher betrachten, was eine solche Lage für kritische Infrastrukturen bedeutet. Sie analysieren ja in Ihrem Buch auch ausführlich deren Schwachstellen. Wo liegen hier vor allem die Probleme aus Ihrer Sicht?

Ferdinand Gehringer: Die zentralen Probleme liegen vor allem in der hohen Vernetzung und Komplexität kritischer Infrastrukturen. Viele Systeme sind nicht ausreichend segmentiert und stark voneinander abhängig. Große Betreiber sind in Sachen Cybersicherheit bereits gut aufgestellt, mittlere und kleinere Anbieter haben hier noch deutliche Defizite. Angriffe auf die Lieferkette und auf Dienstleister können sofort Auswirkungen auch auf gut geschützte Betriebe haben.

Der physische Schutz kritischer Infrastruktur ist häufig noch unzureichend – etwa Perimeterschutz, Zugangskontrollen oder Sicherheitsüberprüfungen des Personals. Viele Betriebe sind nicht ausreichend auf Stromausfälle vorbereitet, verfügen über unzureichende Notstromversorgung und Dieselvorräte. Der wirtschaftliche Druck der Unternehmen verzögert notwendige Sicherheitsinvestitionen. Regelmäßige Übungen, auch gemeinsam mit Behörden und der Bevölkerung, finden bisher kaum statt.

Kommen wir also zum Ernstfall. Wie werden die kritischen Infrastrukturen – nehmen wir als Beispiel einmal die Stromversorgung – geschützt? Und wogegen lassen sie sich überhaupt schützen?

Ferdinand Gehringer: Zunächst ist es wichtig, dass wir Ausfälle akzeptieren und uns darauf gesellschaftlich vorbereiten. Kritische Infrastrukturen wie die Stromversorgung werden durch ein Bündel technischer, organisatorischer und personeller Maßnahmen geschützt. Dazu gehören Redundanzen in der Versorgung, physischer Schutz von Anlagen, Cyberabwehr und Notfallpläne für den Betriebsausfall. Komplette Verhinderung lassen sich Angriffe nie – der Schutz reduziert Risiken, erschwert Angriffe und begrenzt die Auswirkungen.

Perspektivisch wird es für uns darum gehen, Ausfälle realistischer einzuplanen, die Bevölkerung besser vorzubereiten und vor allem die Wiederanlaufphase deutlich zu verkürzen. Das umfasst zum Beispiel den besseren Schutz kritischer Kabelverläufe, schnelle Reparaturen durch Vorratshaltung von Ersatzteilen, flächendeckende Schnelleingreifteams und eine deutlich größere Anzahl mobiler Notstromaggregate. In der Ukraine setzt man auf mobile Umspannwerke und kleine Kraftwerke, um schnell

und flexibel die Netze wiederherzustellen. Da können wir noch viel lernen.

Man muss ja offenbar davon ausgehen, dass die Russen jeden Stein und jede Zuständigkeit und jeden Prozess dank vorheriger Spionage bereits ausbalanciert haben – das dürfte den Schutz nicht gerade erleichtern?

Ferdinand Gehringer: Ja, viele Informationen über Kabelverläufe und Strukturen sind frei zugänglich im Internet. Dazu kommen noch gezielte Spionageoperationen bspw. durch den Einsatz von Low-Level-Agents oder über Cyberangriffe. Da haben wir es Russland und auch China bisher zu einfach gemacht. Unsere Sicherheitskultur muss sich dahingehend ändern. Transparenz ist dabei aber auch ein wichtiges Gut der Demokratie. Sie sollte aber mit dem Schutzinteresse genau abgewogen werden.

Wie sieht die Rollenverteilung dabei aus? Die Kritischen Infrastrukturen selbst sind ja durch das neue Kritis-Dachgesetz und NIS2 besonders gefordert, was die Eigensicherung betrifft. Was verändert sich im Ernstfall?

Ferdinand Gehringer: Im Normalbetrieb liegt die Verantwortung für Sicherheit und Resilienz weitgehend bei den Betreibern selbst. Das Kritis-Dachgesetz und NIS2 verpflichten sie, ihre Systeme abzusichern, Risiken zu analysieren und Vorfälle zu melden. Im Ernstfall kann sich die Rollenverteilung verschieben: Staatliche Stellen koordinieren die Gesamtlage. Die Bundeswehr kann besonders wichtige Anlagen für die Landes- und Bündnisverteidigung sichern, verfügt im Ernstfall jedoch nicht über ausreichend Personal, um flächendeckend alle kritischen Infrastrukturen zu schützen. Der Heimatschutz ist darauf ausgerichtet, wenige zentrale Infrastrukturen zu sichern, die Hauptverantwortung für den Betrieb und Schutz bleibt aber weiterhin bei den Betreibern selbst.

Auch Unternehmen, die selbst keine kritischen Infrastrukturen sind, können im Ernstfall verpflichtet werden. Was kann das alles sein? Sind die Unternehmen auf ein solches Szenario vorbereitet?

Ferdinand Gehringer: Auch Unternehmen, die nicht offiziell zu den kritischen Infrastrukturen zählen, können im Ernstfall verpflichtet werden, Leistungen bereitzustellen. Das kann zum Beispiel die Bereitstellung von Logistikkapazitäten durch Speditionsfirmen, Produktionskapazitäten in der Lebensmittel- oder Pharmaindustrie oder IT-Ressourcen und Personal zur Unterstützung von Kommunikations- und

Steuerungssystemen betreffen. Unternehmen sind auf ein solches Szenario bisher nicht vorbereitet.

Herr Gehringer, Künstliche Intelligenz ist in unseren Tagen das Buzz-Word schlechthin. Da ist es kein Wunder, dass auch der Einsatz von KI in Krisenstäben diskutiert wird. KI kann, so wird gesagt, krisenrelevante Daten schnell analysieren, Szenarien simulieren und Entscheider entlasten. Wie weit sind wir hier schon?

Ferdinand Gehringer: In der Bundeswehr sind wir beim Einsatz von Künstlicher Intelligenz für Krisen- und Lageanalysen bisher noch nicht weit. Im Vergleich setzen die US-Streitkräfte bereits intensiv auf KI, und auch die Ukraine nutzt Systeme wie „Lancelot“, um Szenarien zu simulieren und Entscheidungen zu unterstützen. In Unternehmen ist die Akzeptanz von KI noch nicht groß genug, obwohl sie bereits bei der Datenanalyse eingesetzt wird. Für Simulationen kommt sie hingegen bisher nur vereinzelt zum Einsatz. Künftig wird der gezielte Einsatz von KI in Krisenstäben und die Nutzung von digitalen Zwillingen für den Ausbau der Resilienz gewinnbringend sein.

Inwieweit sprechen Halluzinationen, Verzerrungen, und „Adversarial Attacks“ dagegen? Und da gibt es ja auch noch das Black-Box-Problem: Die KI zeigt sich anscheinend eher bockig, wenn es darum geht, ihre Empfehlungen richtig zu begründen?

Ferdinand Gehringer: KI-Systeme bringen enorme Potenziale, aber auch zentrale Risiken mit sich. Halluzinationen oder Verzerrungen können dazu führen, dass die KI falsche Schlüsse zieht, und „Adversarial Attacks“ – also gezielt manipulierte Eingaben – können die Analyse unterlaufen. Das Black-Box-Problem erschwert zusätzlich die Nachvollziehbarkeit von Empfehlungen, weil die KI oft nicht erklären kann, wie sie zu einem Ergebnis gekommen ist. Deshalb darf KI in Krisenstäben nie die menschliche Entscheidung ersetzen. Sie kann jedoch Daten schnell aufbereiten, Muster erkennen und Entscheidungsprozesse unterstützen – die Verantwortung und die kritische Bewertung liegen immer beim Menschen. **GIT**



FTI Consulting
Ferdinand Gehringer, Director,
Lead Defense & Security
www.fticonsulting.com



Personalleiterin Viktoria Kaiser (l.) und Employer Branding Managerin Katrin Albrecht bei der Best-Recruiters-Auszeichnung in Düsseldorf

Klüh auf Platz 1 der größten Recruiting-Studie Deutschlands

Der Multiservice-Anbieter Klüh ist Sieger der renommierten Best Recruiters-Studie 2025/26 des career Institut & Verlags. Das Düsseldorfer Familienunternehmen erreichte sowohl den 1. Platz in der Branche „Facility-/Security-Services“ als auch den 1. Platz im Gesamtranking aller 517 untersuchten Arbeitgeber in Deutschland. Damit zeichnet die größte Recruiting-Studie im deutschsprachigen Raum Klüh für die höchste Recruiting-Qualität Deutschlands aus. Best Recruiters untersucht jährlich die Recruiting-Performance von mehr als 1.400 Arbeitgebern in Deutschland, Österreich, der Schweiz und Liechtenstein. Im Studienjahrgang 2025/26 wurden allein in Deutschland 517 Unternehmen anhand von 330 wissenschaftlich fundierten Kriterien bewertet. Für seine herausragende Recruiting-Qualität erhielt Klüh das goldene Best Recruiters-Siegel.

www.klueh.de

BDSW: Viktoria Nees ist neue Vorsitzende Fachausschuss Bundeswehr

Der BDSW-Fachausschuss Bundeswehr hat nach 28 Jahren Vorsitz von Gunnar Vielhaack, Geschäftsführer VSU Vereinigte Sicherheitsunternehmen GmbH, eine neue Vorsitzende gewählt. Zukünftig wird Viktoria Nees, Geschäftsführerin ESD Sicherheitsdienst GmbH, den Vorsitz des Ausschusses übernehmen. Aus dem mit 19 Teilnehmern gestarteten Ausschuss ist über die Jahre ein reger Teilnehmerkreis von 38 Unternehmensvertretern geworden, die sich mit Themen rund um die Private Sicherheitswirtschaft im Bereich Bundeswehrliegenschaften befassen. Der Fachausschuss Bundeswehr wurde am 23.04.1998 gegründet. Nach eingehender Diskussion der damaligen Teilnehmer setzte er sich zum Ziel die Lobbyarbeit für die private Sicherheit beim Bundesverteidigungsministerium, den Diensthundeschulen und Wehrbereichsverwaltungen zu etablieren. Zudem sollte Kontakt zu den betreffenden Bundeswehrstellen aufgenommen und gepflegt werden.

www.bdsw.de



(v. l.): Nikolaus Danner, Helmut Grönheim, Viktoria Nees, Jörg Schultz, Bernd Petersen

COREDINATE
by nomadia

Nie mehr alleine auf Rundgang.

Mit **COREDINATE** haben Sie immer einen Assistenten dabei!



Kontrollpunkte erfassen



Vorfälle dokumentieren



Alleinarbeit absichern



Berichte automatisieren

Besuchen Sie uns auf der Messe in Essen • Stand 8E14 • Halle 8





KRITIS

Für die neue Risikolandschaft

Vernetzte Sicherheit: Wie integrierte Sicherheitslösungen Risiken steuern und regulatorische Anforderungen erfüllen

Geopolitische Spannungen, hybride Bedrohungen, Cyberangriffe, Vandalismus und steigende Anforderungen an die Resilienz von Organisationen verändern die Rahmenbedingungen, unter denen Sicherheitskonzepte entwickelt und umgesetzt werden müssen. Gleichzeitig wächst der regulatorische Druck. Die AES/NSL von Klüh Security erfüllt mit Zertifizierungen nach VdS 3137/DIN EN 50518, VdS 3138, DIN EN 17483-1 sowie ISO 27001 zentrale Anforderungen an Leitstellenbetrieb, KRITIS-Schutz und Informationssicherheit.

■ Vorgaben wie NIS-2, das KRITIS-Dachgesetz oder Anforderungen an Datenschutz und Informationssicherheit erhöhen die Verantwortung von Unternehmen, Sicherheitsprozesse nicht nur wirksam umzusetzen, sondern auch nachvollziehbar zu dokumentieren. Sicherheit wird damit zunehmend zu einem Thema der Unternehmenssteuerung.

„Die Fragen, die Kunden heute an uns stellen, sind andere als noch vor fünf Jahren“, sagt Sven Horstmann, Geschäftsführer von Klüh Security. „Es geht nicht mehr nur darum, wer nachts ein Gelände kontrolliert. Unternehmen wollen wissen, wer den Überblick behält, wenn gleichzeitig unterschiedliche Ereignisse eintreten und wie daraus schnell die richtigen Entscheidungen abgeleitet werden können.“

Vom Sicherheitsdienst zur integrierten Sicherheitssteuerung

Die zunehmende Komplexität moderner Gebäude und Infrastrukturen macht

deutlich: Einzelne Sicherheitsmaßnahmen reichen heute häufig nicht mehr aus. Videoüberwachung, Zutrittskontrolle, Gefahrenmeldetechnik, Gebäudetechnik und operative Sicherheitsdienste müssen miteinander verbunden werden, damit aus einzelnen Informationen ein belastbares Lagebild entsteht.

Genau hier setzt Klüh Security mit seinem integrierten Sicherheitskonzept an: Das Unternehmen verbindet personelle Sicherheitsdienstleistungen mit moderner Technologie und digitalen Steuerungsprozessen. Ziel ist es, Sicherheit nicht isoliert zu betrachten, sondern als integriertes System aus Menschen, Technik und klar definierten Abläufen.

Eine zentrale Rolle spielt dabei die eigene Alarmempfangsstelle (AES) und Notruf- und Serviceleitstelle (NSL). Die Leitstelle bündelt sicherheits- und betriebsrelevante Informationen aus unterschiedlichen Systemen und ermöglicht eine strukturierte Bewertung von Ereignissen rund um die Uhr.

„Eine technische Anlage meldet einen Alarm. Eine besetzte Leitstelle bewertet ihn und handelt“, erklärt Horstmann. „Der Unterschied liegt darin, dass aus einer einzelnen Meldung ein Gesamtbild entsteht, auf dessen Grundlage Entscheidungen getroffen werden können.“

Über eine herstellerneutrale Plattform werden unter anderem Videoüberwachung, Zutrittskontrolle, Einbruch- und Brandmeldetechnik sowie technische Meldungen zusammengeführt. Ereignisse können dadurch schneller verifiziert, priorisiert und dokumentiert werden. Für Kunden entsteht mehr Transparenz – und gleichzeitig eine höhere Sicherheit im operativen Betrieb.

Technologie als Verstärkung menschlicher Kompetenz

Die Digitalisierung verändert die Sicherheitsbranche grundlegend. Künstliche Intelligenz, intelligente Sensorik, IoT-Anbindungen und automatisierte Analyseverfahren

ren unterstützen dabei, große Mengen an Informationen effizient auszuwerten.

Dabei geht es nicht darum, den Menschen zu ersetzen. Vielmehr verschieben sich die Aufgabenprofile. Routineprozesse können automatisiert werden, während qualifizierte Sicherheitskräfte stärker für Bewertung, Entscheidungsfindung und Intervention eingesetzt werden.

Auch Robotik und Drohnentechnologie gewinnen an Bedeutung. Bei der Überwachung großer Areale, der Kontrolle schwer zugänglicher Bereiche oder der schnellen Lagebewertung können solche Systeme einen zusätzlichen Mehrwert bieten. Die finale Einschätzung und das Handeln in kritischen Situationen bleiben jedoch Aufgabe erfahrener Fachkräfte.

„Sicherheit ist und bleibt ein Geschäft, das sich um Menschen dreht. Technik unterstützt, aber Menschen treffen die Entscheidungen“, so Horstmann.

Zertifizierte Prozesse schaffen Vertrauen

Gerade in sensiblen Bereichen wie Energieversorgung, Gesundheitswesen, Flughäfen oder Rechenzentren sind nachvollziehbare Prozesse und geprüfte Strukturen entscheidend. Die AES/NSL von Klüh Security erfüllt mit Zertifizierungen nach VdS 3137/DIN EN 50518, VdS 3138, DIN EN 17483-1 sowie ISO 27001 zentrale Anforderungen an Leitstellenbetrieb, KRITIS-Schutz und Informationssicherheit.

Für Kunden bedeutet das eine geprüfte Infrastruktur, die technische Leistungsfähigkeit mit klar definierten Prozessen verbindet. Gleichzeitig bleibt das Modell flexibel: Unternehmen können eigene Strukturen ergänzen, einzelne Leistungen auslagern oder die Leitstelle als Erweiterung ihrer bestehenden Sicherheitsorganisation nutzen.

„Zertifizierungen sind für uns kein Selbstzweck. In regulierten Umgebungen

”

Die Fragen, die Kunden heute an uns stellen, sind andere als noch vor fünf Jahren

Sven Horstmann, Geschäftsführer von Klüh Security



schaffen sie Vertrauen und geben unseren Kunden die Sicherheit, dass Prozesse belastbar und nachvollziehbar funktionieren“, erklärt Horstmann.

Dabei bleibt trotz aller technologischen Entwicklungen eines unverändert: Sicherheit entsteht durch das Zusammenspiel von Technik, Prozessen und qualifizierten Menschen. Moderne Leitstellen unterstützen Mitarbeitende dabei, relevante Informationen schneller zu bewerten und fundierte Entscheidungen zu treffen. Deshalb investiert Klüh Security kontinuierlich in die Weiterentwicklung seiner Fachkräfte und bereitet sie auf die steigenden technischen und organisatorischen Anforderungen der Branche vor.

Security Essen als Plattform für den Austausch

Die Security Essen 2026 steht vor diesem Hintergrund ganz im Zeichen vernetzter Sicherheit. Als internationale Leitmesse der Sicherheitswirtschaft bringt sie Hersteller, Dienstleister, Anwender und Entscheider zusammen, um aktuelle Entwicklungen und Lösungen für die Herausforderungen der kommenden Jahre zu diskutieren.

Auch Klüh Security nutzt die Messe vom 22. bis 25. September 2026 als Plattform für den Austausch mit Kunden, Partnern und Fachbesuchern. Im Mittelpunkt stehen integrierte Sicherheitskonzepte, intelligente Leitstellenlösungen und die Frage, wie Unternehmen ihre Sicherheitsorganisation zukunftsfähig aufstellen können.

„Die Zukunft der Sicherheitsbranche liegt nicht in einzelnen Maßnahmen, sondern im Zusammenspiel aller Komponenten“, fasst Sven Horstmann zusammen. „Entscheidend ist, Risiken frühzeitig zu erkennen, Informationen sinnvoll zusammenzuführen und daraus die richtigen Entscheidungen abzuleiten.“

Damit entwickelt sich Sicherheit zunehmend von einer reaktiven Dienstleistung zu einem strategischen Bestandteil moderner Unternehmensführung. Klüh Security versteht sich dabei als Partner, der Technologie, operative Erfahrung und qualifizierte Menschen zu einem ganzheitlichen Sicherheitsmodell verbindet. **GIT**



Klüh Service Management GmbH
www.klueh.de

© Bilder: Klüh



Wir freuen uns auf Sie:
Besuchen Sie uns in Essen,
Halle 5, Stand B31.

Für sichere Datenverbindungen

Wir bieten Glasfaser-Systeme für Industrie-Anwendungen:

- Höchste Bandbreiten und Echtzeitkommunikation
- Mehr Sicherheit – nicht abhörbar, manipulationsarm
- Störungsfrei auch bei EMV-belasteten Umgebungen
- Sehr große Reichweiten, geringe Verluste
- Zukunftssicher und hochverfügbar

Für maximale Performance und Resilienz beraten wir Sie unverbindlich.

Tel. +49 2762 9313-600
vertrieb@eks-engel.de





BfV-Präsident Sinan Selen und Bundesinnenminister Alexander Dobrindt: Verfassungsschutzbericht 2025 vorgestellt: BfV verteidigt Demokratie in Deutschland gegen Angriffe von außen und innen

© BMJ/Hemmer

KRITIS

Wenn der Zaun nicht reicht

Kritische Infrastrukturen im Visier: Einbruch, Wirtschaftsspionage, Ausspähung und Sabotage – und 6 Erkenntnisse für KRITIS-Betreiber

Eine Auswertung des Verfassungsschutzberichts und der Polizeilichen Kriminalstatistik 2025 mit Folgerungen für den Schutz kritischer Infrastrukturen.

■ Als Alexander Dobrindt, Bundesinnenminister, und Sinan Selen, Präsident des Bundesamts für Verfassungsschutz, am 30. Juni 2026 den Verfassungsschutzbericht 2025 vorstellten, zeichnete sich erneut ein klares Bild ab: Die Gefährdungslage für Deutschland bleibt angespannt. Bereits zuvor hatten Alexander Dobrindt, der Vorsitzende der Innenministerkonferenz Andy Grote sowie BKA-Präsident Holger Münch die Polizeiliche Kriminalstatistik (PKS) 2025 präsentiert.

Für KRITIS-Betreiber, Industrieunternehmen und Sicherheitsverantwortliche ergibt sich daraus eine zentrale Erkenntnis: Physische Angriffe, Ausspähung, Wirtschaftsspionage und Sabotage lassen sich nicht mehr isoliert betrachten. Vielmehr verschwimmen die Grenzen zwischen klassischer Krimina-

lität und strategisch motivierten Angriffen zunehmend.

Einbruchdiebstahl

2025 wurden bundesweit 82.920 Wohnungseinbruchdiebstähle einschließlich Versuchen registriert. Im Vorjahr waren es 78.436 Fälle. Die Aufklärungsquote lag bei rund 14 Prozent. Auffällig bleibt der hohe Anteil gescheiterter Taten. Bereits 2024 lag die Versuchsquote bei 46 Prozent, und auch die Zahlen für 2025 deuten darauf hin, dass viele Einbrüche im Ansatz scheitern.

Dieser Befund unterstreicht die Bedeutung mechanischer Sicherungen, moderner Einbruchmeldetechnik, Videoüberwachung und einer frühzeitigen Wahrnehmung verdächtiger Aktivitäten. Gleichzeitig zeigt die Statistik, dass Einbrüche keineswegs nur

nachts stattfinden. Täter nutzen häufig vorhersehbare Abwesenheitszeiten während der Arbeitszeit, beim Einkaufen oder in den frühen Abendstunden.

Neben Wohnungseinbrüchen erfasst die PKS auch Delikte in Dienst- und Büroräumen, Werkstätten, Produktionsbetrieben, Lagern, Verkaufsstellen, Baustellen, öffentlichen Einrichtungen sowie Energie- und Versorgungseinrichtungen. Damit berühren die Zahlen unmittelbar Bereiche, die auch für kritische Infrastrukturen relevant sind.

Einbruch und Sabotage

Für Markus Piendl vom Sachverständigenbüro Markus Piendl in München reicht die Betrachtung eines Einbruchs als reine Eigentumskriminalität häufig nicht mehr aus.

CHECKLISTE: 6 Schlüsselfaktoren für wirksamen Perimeterschutz

Die Auswertung dokumentierter Sicherheitsvorfälle zeigt, dass nicht einzelne Komponenten, sondern das Zusammenspiel von Technik, Prozessen und Intervention über die Wirksamkeit eines Sicherheitskonzepts entscheidet. Daraus ergeben sich sechs Schlüsselfaktoren für einen wirksamen Perimeterschutz.

- Detektion ohne wirksame Alarmbearbeitung und Intervention bietet keine ausreichende Schutzwirkung.
- Hohe Falschalarmraten können dazu führen, dass Systeme deaktiviert oder Alarmmeldungen ignoriert werden.
- Fehlende Videoverifikation erschwert eine schnelle Lagebeurteilung.
- Schwachstellen an Übergängen, Zufahrten, Fenstern, Dächern, Wasserwegen oder Baustellen müssen gesondert betrachtet werden.
- Stromversorgung und Kommunikationswege sind kritische Abhängigkeiten.
- Perimetersicherheitslösungen sollten regelmäßig unter realistischen Bedingungen getestet werden.
- Im Mittelpunkt steht dabei stets die vollständige Sicherheitskette aus Detektion, Übertragung, Anzeige, Verifikation, Entscheidung, Intervention und Dokumentation.

„Bei gewerblichen Objekten lassen sich Einbruch, Ausspähung und Sabotage nicht immer klar voneinander trennen“, erklärt der Sachverständige. Neben dem Diebstahl von Wertgegenständen oder Betriebsmitteln können Täter unter anderem Betriebsunterbrechungen verursachen, Maschinen manipulieren, Energie- oder Datenleitungen beschädigen, vertrauliche Unterlagen entwenden, Überwachungsgeräte platzieren oder gezielt Sicherheitsmaßnahmen ausundschaften.

Problematisch dabei: Nach außen wirken solche Vorfälle häufig wie gewöhnliche Einbrüche oder Sachbeschädigungen. Erst vertiefte Ermittlungen und eine behördenübergreifende Bewertung lassen mögliche Auftraggeber, Motivlagen oder strategische Hintergründe erkennen. Je nach Tatmotiv können solche Vorfälle zudem als politisch motivierte Kriminalität oder Staatsschutzsachverhalt eingeordnet werden.

Schlussfolgerungen des Experten

Zwar lassen sich die Zahlen des Wohnungseinbruchdiebstahls nicht unmittelbar auf kritische Infrastrukturen übertragen, dennoch zeigen sie nach Ansicht von Markus Piendl, dass das Überwinden baulicher und technischer Schutzmaßnahmen weiterhin ein relevantes Kriminalitätsphänomen darstellt.

Während mittelständische Unternehmen durch Produktionsausfälle oder Know-how-Verlust in ihrer Existenz gefährdet sein können, stehen bei KRITIS-Betreibern häufig andere Ziele im Fokus: Ausspähung, Manipulation oder Sabotage.

Vom Lagebild zur Umsetzung

Die eigentliche Herausforderung beginnt dort, wo Sicherheitskonzepte im operativen Alltag funktionieren müssen. Perimeter-

schutz umfasst sämtliche baulichen, technischen und organisatorischen Maßnahmen, die das unbefugte Überwinden einer definierten Grundstücks- oder Objektgrenze erkennen, verzögern oder verhindern sollen.

Die Lokavis Sicherheitstechnik GmbH mit Sitz in Eggenfelden hat sich auf die Absicherung solcher Perimeter spezialisiert und vertreibt Lösungen des US-Herstellers Southwest Microwave in Deutschland, Österreich und der Schweiz.



Fatmir Kalmendi (l. und Thomas Friedlmeier (r.) vor Lokavis-Testgelände, das GIT SICHERHEIT demnächst ebenfalls genauer unter die Lupe nehmen wird



Sachverständiger Markus Piendl im Einsatz bei einem Zauntest

Für Betriebsleiter Thomas Friedlmeier bestätigen die aktuellen Sicherheitsberichte die Erfahrungen aus der Praxis. Deutschland stehe unter Druck, und gerade im Bereich des Perimeterschutzes könnten Planungsfehler, ungeeignete Technologien, Installationsmängel oder eine mangelhafte Abstimmung einzelner Komponenten die tatsächliche Schutzwirkung deutlich reduzieren.

Gemeinsame Lösungsfindung

Ein prägendes Praxisbeispiel erlebte Thomas Friedlmeier vor mehr als 15 Jahren bei einer Photovoltaikanlage in Italien, bei der Kupferdiebstähle einen sechsstelligen Schaden verursachten: „Gemeinsam mit Markus Piendl wurde die Ursache untersucht. Die Analyse deckte eine überbrückte Manipulationssicherung auf, durch die die Täter unerkannt eindringen konnten. Anschließend wurde die Sicherheitstechnik unter anderem mit Lösungen von Dallmeier electronic verbessert“, so Friedlmeier.

Vor dem Hintergrund des im März 2026 in Kraft getretenen KRITIS-Dachgesetzes ließ Lokavis gemeinsam mit dem Sachverständigen zahlreiche dokumentierte Sicherheitsvorfälle auswerten, um typische Schwachstellen bei Planung, Installation und Betrieb von Perimetersicherheitslösungen

Bitte umblättern ►

Detektiert ist nicht verhindert

fünf reale Sicherheitsvorfälle und die Schwachstellen in der Sicherheitskette

Fall	Projekt	Technik vor Ort	Kurzbeschreibung	Fehler	Bewertung
Fall 1	Nuklear-beziehungsweise Hochsicherheitsanlage	Es kamen mehrere Zaunlinien, technische Perimeterdetektion, Kameras und bewaffnete Sicherheitskräfte zum Einsatz.	Drei Aktivisten drangen durch mehrere Zaunlinien bis an ein Hochsicherheitsgebäude vor.	Die vorhandenen Sicherungsmaßnahmen verhinderten nicht, dass die Aktivisten bis an das Hochsicherheitsgebäude vordrangen.	Es ist zu unterscheiden, ob und warum Detektionssysteme nicht auslösten, Meldungen nicht erkannt wurden oder die anschließende Reaktion unzureichend war. Detektion allein genügt nicht, wenn Alarmübertragung, Lagebewertung, Videoverifikation und Intervention nicht zuverlässig ineinandergreifen.
Fall 2	Flughafen	Radar, Kameras mit videobasierter Bewegungserkennung sowie sensorisch überwachte Zaunsysteme kamen zum Einsatz.	Ein Mann überstieg die Zäune, lief über zwei Landebahnen und wurde erst im weiteren Verlauf bemerkt.	Nach den ausgewerteten Informationen wurden mögliche Alarm- oder Videoereignisse offenbar nicht rechtzeitig operativ bewertet.	Detektions- und Sichtlücken müssen im Rahmen einer systematischen Abdeckungs- und Schwachstellenanalyse identifiziert und geschlossen werden. Erforderlich sind eine Priorisierung nach Schutzzonen, die Korrelation von Sensor- und Videodaten, definierte Alarmbearbeitungs- und Reaktionszeiten, eindeutige Zuständigkeiten sowie abgestufte Interventionsmaßnahmen.
Fall 3	Justizvollzugsanstalt	Ein mechanisches Zaunsystem, Bewegungsmelder, Wachdienst und Kameras kamen zum Einsatz.	Zwei Insassen flohen durch eine seit Tagen bekannte Zaunöffnung. Die Flucht wurde erst viele Stunden später entdeckt.	Die Bewegungsmelder waren wegen häufiger Fehlalarme über einen langen Zeitraum deaktiviert. Zudem war eine bekannte Beschädigung des mechanischen Zaunsystems weder beseitigt noch durch geeignete Ersatzmaßnahmen kompensiert worden.	Dauerhaft deaktivierte Sensoren erzeugen eine gefährliche Scheinsicherheit. Beschädigungen mechanischer Zaunsysteme müssen unverzüglich bewertet, provisorisch gesichert und dauerhaft instand gesetzt werden. Das Sicherheitskonzept und die eingesetzten Systeme sind regelmäßig auf ihre Funktionsfähigkeit zu prüfen.
Fall 4	Museum	Zum Einsatz kamen eine Gebäudeaußenhaut- und Fensterabsicherung, eine Einbruchmeldeanlage, Kameras sowie Interventionskräfte.	Täter legten Feuer, unterbrachen die Stromversorgung und Beleuchtung, drangen über ein Fenster ein und begingen einen Diebstahl.	Die Unterbrechung der Stromversorgung und Beleuchtung beeinträchtigte offenbar Teile der Außenhautüberwachung beziehungsweise der visuellen Verifikation. Die kurze Tatzeit und das im Verhältnis dazu zu lange Interventionsintervall erschwerten eine rechtzeitige Reaktion.	Kritische Komponenten sind durch eine geeignete unterbrechungsfreie Stromversorgung, Ersatz- beziehungsweise Notstromkonzepte sowie Manipulationsschutz abzusichern. Darüber hinaus muss die Verifikationsfähigkeit auch bei einem Ausfall der regulären Beleuchtung erhalten bleiben.
Fall 5	Wertschutzanbieter mit mehreren Tresoren innerhalb eines Gebäudes	Zum Einsatz kamen eine Einbruchmeldeanlage, die Aufschaltung auf eine Leitstelle sowie eine innere Einbruchdetektion beziehungsweise eine zusätzliche Detektionslinie innerhalb des Gebäudes.	Täter bohrten sich über ein verlängertes Wochenende durch die Tresorwand und leerten mehrere Schließfächer.	Ein Einbruchalarm wurde gemeldet, jedoch nicht wirksam verifiziert und verfolgt. Insbesondere erfolgte keine Außenkontrolle durch den Interventionsdienst.	Ein ausgelöster Alarm entfaltet keine ausreichende Schutzwirkung, wenn er nicht qualifiziert bewertet, verifiziert und erforderlichenfalls eskaliert wird.

Quelle: Daten und Bewertungen: Markus Pendl/SMP/Lokavis

gen zu identifizieren (*siehe Tabelle oben: „Detektiert ist nicht verhindert“*.)

Fazit

Für Fatmir Kalmendi, Geschäftsführer von Lokavis, ist die Lage eindeutig: „Die aktuelle Bedrohungslage erfordert einen ganzheitlichen Sicherheitsansatz. Die Risiken reichen von klassischem Einbruch über Wirtschaftsspionage bis zu gezielter Sabotage. Moderne Sicherheitskonzepte müssen daher physische und digitale Schutzmaßnahmen verbinden und Daten aus unterschiedlichen Detektionssystemen zu einem belastbaren Lagebild zusammenführen.“ Kalmendi ergänzt: „Gerade in sicherheitskritischen Umgebungen wie Flughäfen, Justizvollzugsanstalten, Energieanlagen, militärischen Einrichtungen oder anderen KRITIS-Standorten entscheidet nicht die einzelne Komponente über den Schutzgrad, sondern das reibungslose Zusammenspiel aller Systeme, Prozesse und Verantwortlichkeiten.“ **GIT**



Sachverständigenbüro Markus Pendl
www.markuspiendl.com

Lokavis Sicherheitstechnik GmbH
www.lokavis-sicherheit.de

CHECKLISTE: 6 Erkenntnisse für KRITIS-Betreiber

Für Unternehmen und Betreiber kritischer Infrastrukturen ergeben sich aus den aktuellen Bedrohungslagen sechs zentrale Handlungsfelder, die bei der Planung, Bewertung und Weiterentwicklung von Sicherheitskonzepten berücksichtigt werden sollten.

■ Sicherheitsvorfälle ganzheitlich bewerten

Vorfälle sollten nicht ausschließlich nach dem unmittelbaren Sach- oder Entwendungsschaden beurteilt werden.

■ Anzeichen für Ausspähung ernst nehmen

Wiederholte Zutrittsversuche, verdächtige Beobachtungen, Drohnenüberflüge oder Manipulationsspuren können Hinweise auf vorbereitende Ausspähungsmaßnahmen sein.

■ Physische und digitale Sicherheit verzahnen

Cybersecurity und physische Sicherheit müssen organisatorisch und prozessual zusammengeführt werden.

■ Ein gemeinsames Lagebild schaffen

Perimeterschutz, Zutrittskontrolle, Videoanalyse, Einbruchmeldetechnik und Drohnenerkennung sollten in ein integriertes Sicherheits- und Lagebild einfließen.

■ Auch gescheiterte Angriffe auswerten

Erfolgreiche Einbruchs- oder Manipulationsversuche sind systematisch zu dokumentieren und auf mögliche Zusammenhänge zu analysieren.

■ Melde- und Eskalationswege definieren

Klare interne und externe Meldewege sind Voraussetzung für eine schnelle und koordinierte Reaktion auf Sicherheitsvorfälle.

2026



Verband für Sicherheit
in der Wirtschaft

Hessen – Rheinland-Pfalz – Saarland

VSW-Sicherheitstag

Komplexe Risiken - Klare Strategien

Sicherheit ganzheitlich denken. Resilienz wirksam gestalten.

30. September 2026



Vertrauen - **S**icherheit - **W**irtschaftsschutz

Schloss Waldthausen
Im Wald 1
55257 Budenheim

www.vsw.de



MESSEN

Hotspot für sichere Kommunikation

Im November lädt die PMRExpo 2026 nach Köln ein

Die PMRExpo ist die europäische Leitmesse für sichere Kommunikation und ein zentraler Treffpunkt für alle, die sich mit einsatz- und geschäftskritischer Kommunikation beschäftigen. Vom 24. bis 26. November 2026 bringt sie in Köln Anwender, Hersteller, Dienstleister, Netzbetreiber und Beschaffer zusammen.

Im Mittelpunkt stehen auch 2026 Lösungen für Behörden und Organisationen mit Sicherheitsaufgaben (BOS), Kritische Infrastrukturen (KRITIS) sowie Unternehmen aus sicherheits- und versorgungsrelevanten Wirtschaftssektoren. An drei Messtagen präsentieren Aussteller aus aller Welt Innovationen, Produkte, Lösungen und Anwendungen. Das Spektrum reicht von Applikationslösungen über Leitstellen- und Sicherheitstechnik bis zu Kommunikationsinfrastrukturen, Netzdiensten, Endgeräten und Zubehör. Die Veranstaltung knüpft an die starke Resonanz der Vorjahresveranstaltung an: 2025 präsentierten 268 Aussteller aus 29 Ländern ihre Lösungen vor rund 6.000 Besuchenden aus 59 Ländern.

Schmalband, Breitband und 5G

Die Fachmesse greift zentrale Entwicklungen auf, die die Zukunft sicherer einsatz- und geschäftskritischer Kommunikation prägen. Dazu gehört insbesondere die zunehmende Verbindung von Schmalband- und Breitbandkommunikation: Bewährte professionelle Kommunikationsnetze werden durch leistungsfähige Breitbandtechno-

logien wie LTE und 5G ergänzt. So lassen sich neben Sprache auch große Datenmengen, Bilder, Videos und Lageinformationen zuverlässig übertragen.

Auch private Breitbandnetze und 5G-Campusnetze gewinnen an Bedeutung. Sie ermöglichen Unternehmen, Behörden und Betreibern Kritischer Infrastrukturen eigene leistungsfähige Kommunikationsnetze, die auf Anforderungen wie Datensouveränität, Verfügbarkeit, Sicherheit und Prozessflexibilität ausgerichtet sind. Die PMRExpo zeigt, wie diese Technologien zu resilienten Kommunikations- und Datenökosystemen für BOS, KRITIS und Industrie zusammenwachsen.

Moderne Leitstellen und Künstliche Intelligenz

Leitstellen zählen zur DNA der PMRExpo. Sie entwickeln sich von reinen Sprachkommunikationszentralen zu umfassenden digitalen Informations-, Kommunikations- und Führungsplattformen. Neben sicheren Sprachdiensten gewinnen Breitbandkommunikation, Video, Echtzeitdaten, mobile Anwendungen und die Integration unterschiedlicher Kommunikationssysteme an Bedeutung.

Damit rücken auch Modernisierungsprojekte, die Einbindung breitbandiger Anwendungen und die Nutzung Künstlicher Intelligenz in den Fokus. KI kann große Datenmengen analysieren, bei der Lagebewertung unterstützen, Informationen priorisieren, Störungen frühzeitig erkennen und Einsatz- sowie Betriebsabläufe effizienter gestalten. Für Leitstellen, Lagezentren, KRITIS-Betreiber und Industrieunternehmen wird KI so zum praktischen Werkzeug für mehr Effizienz, Sicherheit und Entscheidungssouveränität.

BOS, Kritische Infrastrukturen und Cyberresilienz

Für Polizei, Feuerwehr, Rettungsdienste und andere Organisationen mit Sicherheitsaufgaben ist zuverlässige Kommunikation eine zentrale Voraussetzung für Handlungsfähigkeit. Die PMRExpo zeigt aktuelle Lösungen für den professionellen Digitalfunk ebenso wie Entwicklungen bei LTE- und 5G-basierten Breitbanddiensten.

Auch für Kritische Infrastrukturen gewinnt die Resilienz der Kommunikationsinfrastruktur an Bedeutung. Energieversorgung, Verkehr, Wasserwirtschaft, Industrie

und andere kritische Bereiche müssen auch bei Cyberangriffen, Sabotage, technischen Störungen oder Extremwetter arbeitsfähig bleiben. Sichere, hochverfügbare und flexible Kommunikationsnetze leisten dazu einen wesentlichen Beitrag.

Cybersicherheit ist integraler Bestandteil resilienter Kommunikations- und Sicherheitsarchitekturen. Von Kommunikationsnetzen der Polizei über vernetzte Leitstellen bis zu IoT-Systemen in Kritischen Infrastrukturen zeigt die PMRExpo 2026, wie Cyberresilienz in umfassende Sicherheits- und Betriebskonzepte eingebunden werden kann.

Critical IoT und vernetzte Systeme

Mit Critical IoT rückt die Vernetzung von Maschinen, Sensoren und intelligenten Systemen in den Mittelpunkt. Industrielle Robotik, autonome Fahrzeuge, fahrerlose Transportsysteme sowie zeitkritische Fernüberwachungs- und Steuerungslösungen stellen hohe Anforderungen an Verfügbarkeit, Sicherheit und Leistungsfähigkeit der Kommunikation.

Neben 5G spielen dabei auch LPWAN-Technologien wie NB-IoT, LTE-M, LoRa oder MIOTY eine Rolle. Die PMRExpo zeigt, wie diese Technologien in kritischen Anwendungen eingesetzt werden können – etwa in Produktion, Logistik, Infrastrukturüberwachung, Betriebsführung und Gefahrenabwehr.

Drohnen als vernetzte Einsatz- und Informationssysteme

Unbemannte Systeme gewinnen im Umfeld von BOS, Katastrophenschutz, KRITIS und Verteidigung weiter an Bedeutung. Drohnen können Lagebilder aus der Luft liefern, die

Suche nach vermissten Personen unterstützen oder schwer zugängliche Infrastrukturen erkunden. Entscheidend ist dabei die sichere, stabile und latenzarme Datenübertragung zwischen Drohne, Bodenstation, Leitstelle und Führungsstruktur. Die PMRExpo zeigt entsprechende Systeme, Integrationslösungen und Kommunikationsschnittstellen – einschließlich Anwendungen für Drohrendetektion und Drohnenabwehr.

Satellitenkommunikation und Non-Terrestrial Networks

Eine wachsende Bedeutung haben zudem Satellitenkommunikation und Non-Terrestrial Networks (NTN). Sie können Kommunikationsmöglichkeiten dort erweitern, wo terrestrische Netze nicht verfügbar, überlastet oder ausgefallen sind. Im Zusammenspiel mit PMR, LTE, 5G und privaten Netzen entstehen hybride Kommunikationsarchitekturen, die Reichweite, Verfügbarkeit und Ausfallsicherheit erhöhen. Für BOS, Katastrophenschutz, KRITIS, mobile Einsatzlagen, abgelegene Standorte und temporäre Lagezentren eröffnen sich damit zusätzliche Möglichkeiten für resiliente Kommunikationsstrukturen.

Zivil-militärische Zusammenarbeit und PMRExpo Symposium

Ein weiterer wichtiger Schwerpunkt der PMRExpo 2026 ist die zivil-militärische Zusammenarbeit. Großschadenlagen, Bevölkerungsschutz, der Schutz Kritischer Infrastrukturen und komplexe Kooperationslagen machen deutlich, wie wichtig interoperable Kommunikationssysteme, gemeinsame Lagebilder, belastbare Schnittstellen und robuste Kommunikationswege sind.

Das PMRExpo Symposium supported by CPM Verlag stellt 2026 die resiliente

Einsatzkommunikation im Kontext der zivil-militärischen Zusammenarbeit in den Mittelpunkt. Im Fokus steht die Frage, wie Organisationen in Großschadenlagen, beim Schutz Kritischer Infrastrukturen und in komplexen Kooperationslagen sicher kommunizieren, Lageinformationen teilen, Entscheidungen koordinieren und handlungsfähig bleiben. Das Format richtet sich an Fach- und Führungskräfte, die Kommunikation, Führung, Betriebssicherheit oder Resilienz in kritischen Einsatz- und Betriebsumgebungen strategisch, technisch oder operativ verantworten.

PMRExpo Summit

Begleitet wird die Messe vom PMRExpo Summit. Hochkarätige Branchenexperten diskutieren dort aktuelle technologische Entwicklungen, sicherheitspolitische und regulatorische Fragestellungen sowie konkrete Anwendungs- und Modernisierungsperspektiven. Der Summit ergänzt die Ausstellung um eine strategische Perspektive und bietet Gelegenheit, die technologischen, organisatorischen und gesellschaftlichen Veränderungen der Branche zu diskutieren.

Gemeinsam die Zukunft der einsatz- und geschäftskritischen Kommunikation gestalten – unter diesem Leitgedanken wird die PMRExpo 2026 erneut zum Treffpunkt einer Branche, deren Technologien überall dort unverzichtbar sind, wo Kommunikation zuverlässig, sicher und auch unter schwierigen Bedingungen funktionieren muss. **GIT**



Koelnmesse
www.pmrexpo.com

Organisieren Sie Ihre Sicherheit.

Mit unseren Softwarelösungen
AIM und WinGuard.

advancis.de

BESUCHEN SIE UNS!



22. - 25. September
Halle 8, Stand 8A15

advancis

VERBÄNDE

Neue Technologien für die Unternehmenssicherheit

Der BVSW Innovation Hub

Die Anforderungen in der Unternehmenssicherheit wachsen. Gleichzeitig eröffnen digitale Technologien neue Möglichkeiten, um Sicherheitsaufgaben zuverlässiger und effizienter zu bewältigen. Mit dem BVSW Innovation Hub will der Bayerische Verband für Sicherheit in der Wirtschaft junge Unternehmen und etablierte Akteure zusammenbringen.



Der BVSW Innovation Hub soll junge Unternehmen und etablierte Akteure zusammenbringen

BVSW
Vernetzung. Innovation. Vertrauen.

■ In den vergangenen Jahren sind die Aufgaben in der Unternehmenssicherheit deutlich vielfältiger geworden. Neben klassischen Risiken müssen Sicherheitsverantwortliche heute zahlreiche weitere Bedrohungen im Blick behalten. Dazu zählen etwa Cyberangriffe, die Folgen geopolitischer Spannungen und des Klimawandels sowie eine stärkere Abhängigkeit von vernetzten Systemen. Zugleich werden die gesetzlichen Vorgaben umfangreicher und die Anforderungen an Dokumentation und Transparenz steigen.

Doch auch auf technologischer Seite gibt es viel Bewegung: In immer kürzeren Abständen entstehen neue digitale Technologien und junge Unternehmen bieten Lösungen an, mit denen sich die Herausforderungen in der Sicherheit bewältigen lassen.

Austausch zwischen Start-ups und Sicherheitsverantwortlichen

Aus dieser Situation heraus entstand die Idee des BVSW Innovation Hubs. Die Initiative soll Start-ups mit Sicherheitsverantwortlichen etablierter Unternehmen zusammenbringen und den direkten Austausch fördern. „Mit dem BVSW Innovation Hub wollen wir junge Unternehmen dabei unterstützen, ihre Lösungen auf dem Markt zu etablieren“, sagt BVSW-Geschäftsführerin Caroline Eder. „Über den BVSW Innovation Hub erhalten Gründerinnen und Gründer Zugang zu rund 200 Entscheidungsträgern mit Sicherheitsverantwortung.“

Dabei profitieren beide Seiten von dem Austausch: Start-ups lernen die Anforderungen der Unternehmenssicherheit aus erster Hand kennen und können ihre Lösungen gezielt daran ausrichten. Im Gegenzug erhalten die BVSW-Mitgliedsunternehmen frühzeitig Einblick in neue Technologien und die Möglichkeit, diese auf ihre Praxistauglichkeit zu prüfen, um sie eventuell in ihre Sicherheitskonzepte zu integrieren.

Mehr Sicherheit und Effizienz durch neue Lösungen

Welche Möglichkeiten sich daraus ergeben, zeigen die Start-ups, die über die Initiative bereits Mitglied beim BVSW geworden sind: Das Schweizer Unternehmen Laelaps AI entwickelt eine Security-Intelligence-Plattform, die stationäre Sicherheitsinfrastruktur und autonome Robotikplattformen zu einem einheitlichen Lagebild zusammenführt. Damit können kritische Ereignisse schneller sichtbar gemacht werden. Die Lösung von Laelaps AI kommt mittlerweile vor allem bei der Sicherung von kritischen Infrastrukturen zum Einsatz, beispielsweise bei Rechenzentren, Energieanlagen und kritischen Produktionsstätten.

Dr. Sophia Belser, CEO von Laelaps AI, schätzt vor allem den Austausch innerhalb des Verbands: „Ich finde es sehr spannend, dass der BVSW so viele unterschiedliche Branchen zusammenbringt, von Unternehmen aus dem militärischen und sicherheitstechnischen Bereich bis hin zu Anwenderunternehmen.“



Dr. Sophia Belser,
CEO von Laelaps AI

Gleichzeitig hat mir gefallen, dass der Verband Unternehmen von ganz unterschiedlichen Größen offensteht, DAX-Unternehmen sind ebenso vertreten wie kleinere Betriebe. Für uns als junges Unternehmen ist es wichtig, Kontakte in die Sicherheitsbranche zu knüpfen und uns mit anderen auszutauschen. BVSW bietet hier viele Möglichkeiten.“

Außer zur Optimierung von Sicherheitsprozessen eignet sich Künstliche Intelligenz auch zur Automatisierung von Arbeitsabläufen, um die Effizienz zu steigern. ForceHub, seit Juni Mitglied im BVSW, hat eine Plattform entwickelt, die Sicherheitsdienstleister bei Dokumentation, Schulung und Onboarding unterstützt. Insbesondere in diesem Bereich, der von hohen Anforderungen an die Dokumentation und vielen Mitarbeitenden mit internationalem Hintergrund

geprägt ist, lassen sich darüber administrative Prozesse vereinfachen.

Auch für ForceHub-Gründer Henry Burkert bietet der enge Austausch die Möglichkeit, Lösungen gezielt an den Anforderungen der Sicherheitsbranche auszurichten. „Uns ist ein Punkt bei der Entwicklung von ForceHub wichtig: Wir wollen keine Lösung im stillen Kämmerchen entwickeln, sondern getreu dem Motto „mit der Branche für die Branche“. Der direkte Austausch, das Netzwerken auf Augenhöhe und das gegenseitige Lernen von- und miteinander sind für uns unverzichtbar, um eine Plattform zu bauen, die den Betrieben im Alltag auch wirklich hilft. Der BVSW bietet mit seinem starken



Henry Burkert,
Gründer von ForceHub

Netzwerk und seiner tiefen Branchenkompetenz dafür die absolut optimalen Bedingungen für uns als junges Unternehmen.“

50 Jahre BVSW: Neue Impulse für die Zukunft

Die Gründung des BVSW Innovation Hub fällt dabei in ein besonderes Jahr: 2026 feiert der BVSW sein 50-jähriges Bestehen. Dass der Verband das Jubiläum nicht nur für einen Rückblick nutzt, sondern gleichzeitig eine Initiative zur Förderung junger Unternehmen startet, unterstreicht seinen Anspruch, die Veränderungen in der Sicherheitsbranche aktiv mitzugestalten.

Denn eines haben die zurückliegenden fünf Jahrzehnte gezeigt: Sicherheit ist eine Aufgabe, die sich ständig weiterentwickelt. Mit den Anforderungen wächst auch der Bedarf an neuen Ideen und technologischen Lösungen. **GIT**



Bayerischer Verband für Sicherheit
in der Wirtschaft e. V.
www.bvsw.de

© Bilder: BVSW

22. – 25. September 2026

SECURE YOUR BUSINESS



Die Leitmesse für Sicherheit

JETZT TICKET SICHERN!

Zum 1. Mal parallel:
die EURO DEFENCE EXPO –
die neue internationale
Fachmesse der
Verteidigungsindustrie



www.GIT-SICHERHEIT.de

www.security-essen.de



GIT SICHERHEIT 9/2026

WEITERBILDUNG

Schutz, Rettung, Sicherheit

vfdb-Akademie bietet Weiterbildung für die Praxis

Die VFDB-Akademie soll als zentrale Plattform für den Wissenstransfer dienen – mit praxisnahen, wissenschaftlich fundierten Schulungen sowie Fachveranstaltungen. Die Leitung übernimmt die Erwachsenenbildnerin Annick Gauthier. GIT SICHERHEIT hat mit ihr gesprochen.

■ GIT SICHERHEIT, Frau Gauthier, können Sie zunächst einmal etwas über das generelle Programm der vfdb-Akademie sagen? Was möchten Sie bieten, was es auf dem Weiterbildungsmarkt noch nicht gibt?

Annick Gauthier: Die vfdb-Akademie besitzt ein wirkliches Alleinstellungsmerkmal: Sie versteht sich als unabhängige und neutrale Transferplattform, die Forschung, Regelwerksarbeit und praktische Anwendung miteinander verbindet. Unser Anspruch ist es, das aktuelle Wissen aus den Fachreferaten der vfdb, aus Forschungsprojekten sowie aus dem breiten Expertennetzwerk von Schutz, Rettung und Sicherheit in hoch-

wertige, unmittelbar praxisrelevante Weiterbildungsangebote zu überführen.

Der Weiterbildungsmarkt ist bereits sehr vielfältig und es gibt qualitativ hochwertige Angebote – und vielfach bilden die Richtlinien und Merkblätter der vfdb die Grundlage für diese Weiterbildungsangebote. Neu ist nun, dass wir mit der vfdb-Akademie die direkte Vermittlung anbieten: Die Expertinnen und Experten, die unsere Richtlinien erarbeitet haben, vermitteln sie auch.

Welche Themen sind derzeit aktuell in der Akademie?

Annick Gauthier: In den letzten Monaten haben wir Merkblätter zu den Themenkomplexen „Löschwasserzusätze bei Vegetati-

onsbränden“, „Einsatz von Bodycams bei der nichtpolizeilichen BOS“, „Wiederkehrende Prüfung von Vollkomposite-Atemluftflaschen (Typ 4)“ und „Empfehlungen zur Vorgehensweise bei der Implementierung eines Human-Biomonitoring-Systems für Einsatzkräfte“ herausgegeben. Hinzu kommen der Technische Bericht 07-01 „Leitfaden zur Erstellung von georeferenzierten Feuerwehrplänen“ und die Richtlinie 08-30 „Schulung zum Umgang mit PSA (Leitfaden für die Aus- und Fortbildung)“. Diese Auswahl zeigt, dass es ein großes Potenzial an verfügbaren Seminarinhalten gibt.

Darüber hinaus fließen bei uns auch die Erkenntnisse aus Forschungsergebnissen in die Seminare ein. Damit entsteht ein unmittelbarer Transfer von der fachlichen Erarbeitung in die Anwendungspraxis – schnell, unabhängig und qualitätsgesichert. Gleichzeitig schaffen wir einen Raum, in dem sich Fachleute aus Feuerwehren, Hilfsorganisationen, Behörden, Wissenschaft, Wirtschaft und weiteren sicherheitsrelevanten Bereichen begegnen. Die Akademie ist damit weit mehr als ein Bildungsanbieter: Sie ist eine neutrale Plattform, die alle relevanten Stakeholder zusammenführt und einen übergreifenden Austausch ermöglicht.

Sie haben die Leitung der Akademie übernommen. Welche strategischen Ziele verfolgen Sie in dieser Funktion?

Annick Gauthier: Mein Ziel ist es, die vfdb-Akademie als eine zentrale und anerkannte Bildungsplattform für die Themen Schutz,



Die Schulungsinhalte orientieren sich an realen Fragestellungen aus Einsatzpraxis, Planung, Ausbildung



Die vfdb-Akademie soll als zentrale Bildungsplattform für Schutz, Rettung und Sicherheit etabliert werden

Rettung und Sicherheit zu etablieren. Dabei stehen für mich drei Aspekte im Vordergrund: Qualität, Aktualität und Praxisnutzen.

Wir wollen ein Angebot schaffen, das wissenschaftlich fundiert ist, gleichzeitig aber auch auf die konkreten Herausforderungen in den Feuerwehren, Hilfsorganisationen, Firmen und Behörden eingeht. Dazu gehört auch, neue Lernformate zu entwickeln, die Präsenzveranstaltungen, digitale Angebote und interaktive Trainings sinnvoll miteinander verbinden.

Ein weiteres strategisches Ziel ist der Ausbau eines starken Partnernetzwerks. Nehmen wir ein Beispiel. Die Herausforderungen im Bevölkerungsschutz werden immer komplexer und auch dynamischer; diverse Aspekte und Akteure sind involviert. Da macht es aus meiner Sicht absolut Sinn, nach Kooperationspartnern zu schauen, mit denen wir möglichst passgenaue Angebote entwickeln können.

Wir sind im vergangenen Jahr gestartet und konnten bereits erste Veranstaltungen erfolgreich umsetzen. Ich bin überzeugt, dass wir in den kommenden Jahren noch viele Potenziale nutzen können.

Die Praxisnähe wird bei Ihnen besonders betont. Wie soll diese erreicht werden?

Annick Gauthier: Praxisnähe beginnt bereits bei der Themenauswahl. Unsere Inhalte orientieren sich an realen Fragestellungen aus Einsatzpraxis, Planung, Ausbildung. Unsere Referentinnen und Referenten verfügen selbst über umfangreiche Erfahrungen in den Feuerwehren und Hilfsorganisationen, der Verwaltung, Forschung oder auch der Industrie.

Darüber hinaus setzen wir auf anwendungsbezogene Formate. Neben Fachvorträgen sollen Fallstudien, Workshops, Übungen und Erfahrungsaustausche eine wichtige Rolle spielen. Ein Beispiel dafür sind Veranstaltungen, die auf vfdb-Merkblättern oder



Bei der vfdb-Akademie werden gleichermaßen digitale und präsenzbasierte Weiterbildungsformate angeboten

Forschungsergebnissen aufbauen und deren Inhalte direkt in praktischen Szenarien erprobt werden können. Ein gutes Beispiel ist unser unlängst durchgeführtes Seminar zu Straßenbahnunfällen. Es basiert auf dem Merkblatt 06-14 „Technische Hilfeleistung bei Unfällen mit Straßen- und U-Bahnen“.

Unser Anspruch ist, dass die Teilnehmenden nicht nur Informationen erhalten, sondern konkrete Lösungsansätze und Handlungsempfehlungen für ihren Arbeitsalltag mitnehmen.

Es gibt bereits eine Partnerschaft mit Evac Train. Worin besteht sie? Wird es weitere derartige Kooperationen geben?

Annick Gauthier: Die Kooperation mit Evac Train ist ein sehr gutes Beispiel dafür, wie wir wissenschaftliche Expertise und praktische Ausbildung miteinander verbinden möchten. Gemeinsam entwickeln wir digitale und präsenzbasierte Weiterbildungsformate. Darüber hinaus unterstützt Evac Train die Akademie insbesondere bei Themen mit Forschungsbezug und bei der Entwicklung innovativer Trainingskonzepte. Am 9. September führen wir ein Angebot zur Evakuierung von Menschen mit Beeinträchtigungen in Münster durch – ein großes Thema, das bisher noch viel zu

wenig thematisiert wird. Dabei werden wir Tools und Methoden einsetzen, mit denen die Teilnehmenden Beeinträchtigungen am eigenen Körper erleben können und die Herausforderungen von der anderen Seite wahrnehmen lassen. Auf diese Weise wird die Vermittlung deutlich intensiver und nachhaltiger. Für die Zukunft wollen wir weitere Partnerschaften aufbauen. Die vfdb verfügt über ein umfangreiches Netzwerk aus Wissenschaft, Behörden, Organisationen und Unternehmen. Dieses Potenzial möchten wir nutzen, um zusätzliche Kompetenzen einzubinden und das Angebot der Akademie kontinuierlich zu erweitern.

Welche aktuellen Projekte stehen gerade bzw. in der nächsten Zeit an?

Annick Gauthier: Derzeit arbeiten wir am weiteren Ausbau des Akademieprogramms und an der Entwicklung neuer Veranstaltungsformate. Ein Schwerpunkt liegt darauf, aktuelle Erkenntnisse aus Forschung und Regelwerksarbeit in konkrete Bildungsangebote zu überführen. Zu den nächsten Veranstaltungen gehören unter anderem Formate zum Explosionsschutz oder zum „Bau von Feuerwehrehäusern der Zukunft“. Dabei greifen wir gezielt aktuelle Herausforderungen auf und verbinden fachlichen Austausch mit praxisnahen Fragestellungen und Lernmethoden.

Darüber hinaus beschäftigen wir uns intensiv mit der Frage, wie Weiterbildung im Bereich Schutz, Rettung und Sicherheit künftig aussehen muss. Digitalisierung, neue Technologien und sich verändernde Gefahrenlagen werden dabei eine wichtige Rolle spielen. Die vfdb-Akademie soll ein Ort sein, an dem diese Zukunftsthemen frühzeitig aufgegriffen und gemeinsam gestaltet werden. **GIT**

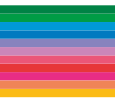


vfdb e.V.
www.vfdb.de

© Bilder: vfdb e.V.



secsolutionforum®
The innovative event for the Security Industry



VERANSTALTUNGEN

Ein Ökosystem der Sicherheit

Secsolutionforum 2026 in Bologna

Am 7. und 8. Oktober trifft sich auf dem Messegelände Bologna Fiere die Fachwelt für physische und digitale Sicherheit. Über 100 Referenten, neun Konferenzräume, mehr als 60 Sponsoren und 4.000 m² Ausstellungsfläche: Das Secsolutionforum 2026 in Bologna positioniert sich als Veranstaltung, die sich nicht nur als Fachmesse, sondern als lebendiges Ökosystem positioniert.

Das diesjährige Secsolutionforum in Bologna erstreckt sich auf über 4.000 m² Ausstellungsfläche und umfasst neun parallel genutzte Konferenzräume. Mehr als 100 Referenten, begleitet von sechs erfahrenen Moderatoren, gestalten das Programm.

Auf der Agenda stehen über 100 Veranstaltungen – von Keynotes und Talkshows über Workshops und Podiumsdiskussionen bis hin zu Fortbildungsangeboten.

Die mehr als 25 Themenbereiche der Messe decken einen Großteil der gesamten Sicherheitsbranche ab: Videoüberwachung, Cybersicherheit, Zutrittskontrolle, regulatorische Rahmenbedingungen sowie technologisch anspruchsvolle Themen wie der Einsatz Künstlicher Intelligenz zum

Schutz von Menschen, Infrastrukturen und Daten.

Treffpunkt der Community

„Die Veranstaltung bestätigt ihre Rolle als zentraler Treffpunkt für Fachleute aus den Bereichen Sicherheit und Cybersicherheit und bietet hochwertige Inhalte sowie erstklassige Möglichkeiten für Networking und Weiterbildung“, erklärt Andrea Sandrolini, CEO der Ethos Media Group. Die Stärke des Secsolutionforum liege nicht nur in der Vielfalt seiner Inhalte, sondern auch in der Breite und Tiefe seiner Community. Mehr als 60 Sponsoren und über 38 Partnerverbände stehen für das Engagement der führenden Akteure des Sicherheitsmarktes.

Zwei Auszeichnungen werden auf der Veranstaltung verliehen: der Secsolutionforum Urban Security Award, mit dem besonders engagierte öffentliche Verwaltungen für ihre Leistungen im Bereich der integrierten urbanen Sicherheit geehrt werden, sowie ein weiterer Preis für herausragende Best Practices von Unternehmen. Teilnehmer an den akkreditierten Fortbildungsveranstaltungen erhalten anerkannte Weiterbildungspunkte. Die Teilnahme an ihnen ist kostenlos. **GIT**



Fiera Bologna
www.secsolutionforum.it



AK SIBE BW

Treffen in Konstanz

Fachtagung des Arbeitskreises der Sicherheitsbevollmächtigten Baden-Württemberg bei der ASW Baden-Württemberg

Im Mittelpunkt der Tagung am 30. Juni und 1. Juli standen aktuelle sicherheitsrelevante Entwicklungen, fachliche Impulse aus Expertenvorträgen sowie organisatorische Entscheidungen zur zukünftigen Ausrichtung des Arbeitskreises.

Zu Beginn gab das Landesamt für Verfassungsschutz Baden-Württemberg einen umfassenden Lageüberblick zu aktuellen Bedrohungen. Thematisiert wurden Cyberangriffe, Spionage, Sabotage und Einflussnahme sowie deren Auswirkungen auf Unternehmen und kritische Wertschöpfungsketten. Die Teilnehmer diskutierten die Bedeutung eines ganzheitlichen Sicherheitsverständnisses, das organisatorische, personelle und technische Maßnahmen gleichermaßen berücksichtigt.

Im weiteren Verlauf rückten sicherheitsrelevante Entwicklungen im Bereich Extremismus und Proliferation in den Fokus. Die Diskussionen befassten sich mit aktuellen Gefährdungslagen und geeigneten Maßnahmen zur Sensibilisierung von Beschäftigten sowie zum Schutz besonders exponierter Unternehmensbereiche.

Ein zusätzlicher Fachvortrag widmete sich den Möglichkeiten und Herausforderungen moderner Cloud-Lösungen für die Verarbeitung schutzbedürftiger Informationen. Neben technischen Aspekten wurden regulatorische Anforderungen, Sicherheitsarchitekturen und praktische Umsetzungsszenarien beleuchtet.

Organisatorische Entscheidungen

Neben den fachlichen Inhalten wurden im Rahmen der Tagung auch organisatorische Weichen gestellt. Die Teilnehmenden verständigten sich auf künftige Arbeitsschwerpunkte und Maßnahmen zur Stärkung des internen Wissenstransfers. Zudem wurde der Vorstand neu gewählt, der künftig gemeinsam mit der ASW Baden-Württemberg die inhaltliche und organisatorische Vorbereitung der kommenden Sitzungen und Veranstaltungen übernehmen wird.

Bedeutung für den Wirtschaftsschutz

Die Veranstaltung verdeutlichte, dass wirksamer Wirtschaftsschutz zunehmend von enger Zusammenarbeit, kontinuierlichem Informationsaustausch und gemeinsamen Standards abhängt. Angesichts komplexer Bedrohungslagen gewinnen vernetzte Fachkompetenzen und regelmäßige Erfahrungsaustausche weiter an Bedeutung. Die Tagung leistete hierzu einen wichtigen Beitrag und stärkte die Resilienz der beteiligten Unternehmen und Organisationen. **GIT**



Allianz für Sicherheit in der Wirtschaft
Baden-Württemberg e. V. (ASW-BW)
www.asw-bw.com



Dallmeier

PANOMERA® V8
GRAND VIEW. INFINITE INSIGHTS.



GRAND VIEW
8 Linsen kombiniert in einer Ansicht



180°-ABDECKUNG
> 10.000 m² ohne toten Winkel



INSIGHTS

Vielfältige KI-Anwendungen
mit vertrauenswürdigen Datenschutz



JETZT MEHR ERFAHREN.

Francis Cepero, CEO von Primion
(rechts), Steffen Ebert vom Team
GIT SICHERHEIT (links)



© GIT SICHERHEIT/Wiley

SICHERMACHER

Converged Security

Warum integrierte Sicherheit zur Pflicht wird

Sicherheitssysteme waren früher klar getrennt: Zutritt, IT und Betrieb liefen in eigenen Silos. Heute sind selbst Klimaanlage vernetzt – und damit angreifbar. Francis Cepero, CEO von Primion, erklärt im Interview mit GIT SICHERHEIT, warum konvergente Sicherheit zur strategischen Notwendigkeit geworden ist, wie Identitäten Prozesse steuern und weshalb digitale Souveränität für Unternehmen immer wichtiger wird.

■ GIT SICHERHEIT: Herr Cepero, Sie sprechen häufig von konvergenter Sicherheit als strategischer Notwendigkeit. Was hat sich in den letzten Jahren so grundlegend verändert, dass Unternehmen Sicherheit nicht mehr in getrennten Einheiten denken können?

Francis Cepero: Zunächst einmal hat sich die Vernetzung radikal verändert. Heute ist selbst die Klimaanlage vernetzt und von außen steuerbar. Auch die Sauerstoffversorgung im Krankenhaus ist elektronisch kontrollierbar. Zutrittssysteme sind digital, Videoüberwachung hängt im Netzwerk, Maschinensteuerung ebenso. Sobald all diese Systeme verbunden sind, entsteht eine gemeinsame Angriffsfläche. Das sind keine separaten Disziplinen mehr. Die ISO 27001 beschreibt im entsprechenden Abschnitt klar, dass diese Bereiche zusammengeführt werden müssen – zu einem ganzheitlichen Informations- und Sicherheitskonzept.

Worin liegt konkret das Risiko der alten Fragmentierung zwischen IT-Sicherheit, physischer Sicherheit und Betrieb?

Francis Cepero: Wenn Sie Endgeräte schützen, ist das gut. Wenn Sie Türen schützen, ist das gut. Aber entscheidend ist die Identität.

Ein Mitarbeiter darf nur die Maschinen bedienen, für die er qualifiziert ist und nur während seiner Schicht. Selbst wenn er Passwörter hätte, darf er außerhalb dieser Zeit keinen Zugriff haben. Die Integration dieser Identitätslogik über alle Systeme hinweg – das ist der Kern von Converged Security.

Wie übersetzt sich diese Entwicklung in die Strategie von Primion?

Francis Cepero: Unsere Mission lautet: vorbeugen, schützen, bewahren. Wir beraten Unternehmen, analysieren Sicherheitskonzepte, erstellen neue und integrieren in bestehende Strukturen. Wir wollen nicht alles herausreißen und neu bauen, sondern Werte erhalten. Primion ist ein Integrator: Wir binden Geräte verschiedenster Hersteller ein und verbinden physische Sicherheit, IT- und OT-Sicherheit zu einem holistischen Konzept.

Im Zentrum steht aber weiterhin die Tür, der Zutritt...?

Francis Cepero: Natürlich kommen wir aus der physischen Sicherheit. Aber wir erweitern das Konzept: Identitäten gelten nicht nur für Personen, sondern auch für Maschinen und Assets. So lassen sich Beziehungen zwischen diesen Identitäten

abbilden. Sicherheit wird damit nicht nur Compliance, sondern ein Effizienzfaktor. Ein Unternehmen ist besser, wenn es sicher ist.

Können Sie ein konkretes Beispiel nennen, wo Converged Security im Alltag echten Mehrwert schafft?

Francis Cepero: Einer unserer Kunden, ein großer Logistiker mit 14.000 Mitarbeitern, nutzt ein System, das sich dynamisch an Schichten und Funktionen anpasst. 8.000 temporäre Mitarbeiter erhalten genau die Zugriffe, die sie für ihre Aufgaben brauchen – nicht mehr und nicht weniger. Das Sicherheitskonzept passt sich den Geschäftsprozessen an, nicht umgekehrt.

Und ein Beispiel aus einem ganz anderen Sektor?

Francis Cepero: In der Produktion geht es oft um Compliance: Wer darf welche Maschine bedienen? Ist die Person qualifiziert? Ist die Zertifizierung aktuell? Wir motivieren Unternehmen, Sicherheit nicht als abstraktes Konzept zu sehen, sondern als Schutz für Menschen und Prozesse. Wir arbeiten zudem an virtualisierten Controllern und „Policy as Code“, um Berechtigungen flexibel und zeitlich begrenzt zu vergeben.

Mit wem sprechen Sie zuerst, wenn Sie Unternehmen von diesem Ansatz überzeugen wollen?

Francis Cepero: Es gibt zwei Wege: Entweder wir erklären Unternehmen proaktiv, wie die Systeme ineinandergreifen. Oder wir werden von Kunden hineingeführt – oft von Verantwortlichen, die Sicherheit als Wertschöpfungsfaktor verstehen. Sicherheit kann EBIT-relevant sein.

Kritische Infrastrukturen stehen besonders unter Druck. Wird Sicherheit durch die Vernetzung nicht unfassbar komplex?

Francis Cepero: Ja, es ist komplex. Die Angriffsfläche wächst exponentiell: IoT-Geräte, Fremdmitarbeiter, Endgeräte. Aber mit identitätsbasierten Systemen und Prinzipien wie Zero Trust lässt sich das kontrollieren. Wir kommen aus der physischen Welt, also wissen wir: Eine Tür muss nicht nur geschlossen sein, sie muss im Ernstfall verriegelt werden. Diese Logik übertragen wir auf digitale Identitäten.

Sie haben Physik studiert. Wie sehr hilft Ihnen Ihr technischer Hintergrund?

Francis Cepero: Sehr. Ich habe immer Technologieteams geführt – bei SAP, bei A1 in Österreich, jetzt bei Primion. Die technologische Welt verändert sich extrem schnell. Vor zwei Jahren war generative KI irrelevant. Heute können Angreifer mit KI hochstrukturierte Angriffe fahren. Tools wie Flipper Zero ermöglichen Netzwerkzugriffe in kürzester Zeit. Das muss man verstehen, um gute Sicherheitskonzepte zu bauen.

Kürzlich wurde bekannt, dass Anthropic seine KI für Nicht-US-Unternehmen einschränkt. Betrifft Sie das?

Francis Cepero: Nein. Primion sieht sich als europäisches Unternehmen. Wir wollen digitale Souveränität garantieren und keine Abhängigkeit von Hyperscalern oder extraterritorialen Gesetzen wie dem US Cloud Act. Deshalb sind wir auf eine europäische Cloud migriert. Kunden fragen das aktiv nach.

Wie flexibel sind Sie bei der Bereitstellung Ihrer Lösungen?

Francis Cepero: Sehr. Wenn ein Kunde eine europäische Cloud möchte, bekommt er sie. Wenn er global ist und eine amerikanische oder chinesische Cloud braucht, können wir das ebenfalls. Und wenn er alles On-premises im eigenen Rechenzentrum betreiben will, machen wir das auch. Wir wachsen mit unseren Kunden.

Wie tragen Sie das Thema Converged Security in die interne und externe Welt?

Francis Cepero: Wir schulen unsere Mitarbeitenden intensiv und zeigen neue Strukturen und Plattformen. Unser klassisches Portfolio – Zutritt, Zeit, Video, Besuchermanagement – wird durch starke Softwareplattformen ergänzt: Geräteintegration, Prozessintegration, Logistikprozesse, SAP-Anbindung. Wir wollen nicht nur Zutrittskontrolle liefern, sondern einen echten Mehrwert schaffen. **GIT**



Primion
<https://primion.io>



Erfahren Sie mehr auf der Security 2026:

Erleben Sie bei phg die READERSPHERE – den Treffpunkt mit der Leser-Vielfalt auf der Security!

- Für jeden Einsatzbereich den richtigen Leser
- Für jede Umgebung die richtige Technologie
- Für jede Anforderung die richtige Beratung
- Mit Sicherheit CRA-ready
- Messe-Premiere: der neue VOXIO-C easy

Als Spezialist für Leser ist phg für Systemintegratoren die richtige Verbindung. Wir freuen uns auf Ihren Besuch!

phg Peter Hengstler GmbH + Co. KG
Tel. +49 7420 89-0 • datentechnik@phg.de



22. - 25. September 2026
Halle 6 Stand 6E17

phg
Die richtige Verbindung

Wenn jede Millisekunde zählt

Netzwerkcameras: Global Shutter für moderne Verkehrsanwendungen

Auf Autobahnen und Schnellstraßen spielt die Global-Shutter-Technologie ihre Stärken besonders aus



Mit seiner P1486-LE Global Shutter Camera hat Axis Communications erstmals eine Bullet-Kamera mit Global-Shutter-Technologie vorgestellt, die speziell für die präzise Erfassung schnell bewegter Fahrzeuge und Kennzeichen entwickelt wurde. Ein Beitrag von Jochen Sauer. Er ist seit 2022 bei Axis Communications als Architect & Engineering Manager für Errichter und Planer in Deutschland verantwortlich.

Bildes gleichzeitig und vermeidet dadurch weitgehend die für Rolling-Shutter-Sensoren typischen geometrischen Verzerrungen bei schnellen Bewegungen. Das Ergebnis sind besonders präzise und konsistente Bilddaten als Grundlage für automatisierte Verkehrsanalysen. Netzwerk-Kameras entwickeln sich damit zunehmend vom

■ Ob automatische Kennzeichenerkennung, Fahrzeugklassifizierung oder Verkehrsflussanalyse: Moderne Verkehrsmanagementsysteme basieren zunehmend auf KI-gestützten Videoanalysen. Bildinformationen werden dabei nicht mehr ausschließlich von Menschen ausgewertet, sondern automatisiert durch Algorithmen verarbeitet. Damit diese Anwendungen zuverlässig funktionieren, müssen die zugrunde liegenden Bilddaten konsistent und präzise sein. Gerade bei schnell bewegten Fahrzeugen stoßen herkömmliche Bildsensoren jedoch an physikalische Grenzen. Bewegungen können zu geometrischen Verzerrungen führen und die automatisierte Auswertung erschweren.

Genau hier setzt die Global-Shutter-Technologie an: Sie belichtet alle Pixel eines

Die Axis P1486-LE Global Shutter Camera wurde für Anwendungen entwickelt, bei denen schnell bewegte Fahrzeuge und Kennzeichen auch unter anspruchsvollen Bedingungen präzise und verzerrungsfrei erfasst werden müssen





Jochen Sauer ist seit 2022 bei Axis Communications als Architect & Engineering Manager für Errichter und Planer in Deutschland verantwortlich

reinen Bildgeber zum intelligenten Sensor innerhalb vernetzter Verkehrsinfrastrukturen. Sie liefern kontinuierlich Daten für Verkehrsleitstellen, automatisierte Kontrollsysteme und datengetriebene Verkehrsmanagementlösungen.

Präzise Bilddaten als Grundlage intelligenter Verkehrssysteme

Kommunen setzen auf intelligente Verkehrssteuerung, um Verkehrsflüsse effizienter zu lenken und Staus frühzeitig zu erkennen. Betreiber kritischer Infrastrukturen wiederum möchten Zufahrten automatisiert kontrollieren, Fahrzeuge zuverlässig identifizieren und Verkehrsbewegungen in Echtzeit erfassen. Die hierfür notwendigen Entscheidungen basieren zunehmend auf automatisiert ausgewerteten Bilddaten. Entsprechend gewinnen Konsistenz und Präzision der erfassten Bildinformationen weiter an Bedeutung.

Gerade im Verkehrswesen entstehen jedoch besonders anspruchsvolle Bildsituationen: Fahrzeuge bewegen sich mit hoher Geschwindigkeit, die Lichtverhältnisse

können sich innerhalb kürzester Zeit ändern und Kennzeichen müssen auch bei schnellen Vorbeifahrten zuverlässig erfasst werden. Herkömmliche Bildsensoren können dabei physikalisch bedingt an ihre Grenzen stoßen. Bewegungsverzerrungen beeinträchtigen unter Umständen die Bildqualität und somit auch die Genauigkeit automatisierter Auswertungen.

Hier spielt die Global-Shutter-Technologie ihre Stärken aus. Im Gegensatz zur weit verbreiteten Rolling-Shutter-Technologie belichtet diese alle Pixel eines Bildes gleichzeitig. Dadurch entstehen auch bei schnellen Bewegungen Aufnahmen ohne die für Rolling Shutter typischen geometrischen Verzerrungen. Dies ist insbesondere dort ein Vorteil, wo Bilddaten nicht nur betrachtet, sondern automatisiert ausgewertet werden.

Rolling oder Global Shutter?

Die meisten Netzwerk-Kameras arbeiten heute mit einem sogenannten Rolling-Shutter-Sensor. Dabei werden die Pixel eines Bildes nicht gleichzeitig, sondern zeilenweise von oben nach unten ausgelesen. Dieser Vorgang dauert nur Bruchteile einer Sekunde und fällt bei statischen Szenen kaum ins Gewicht.

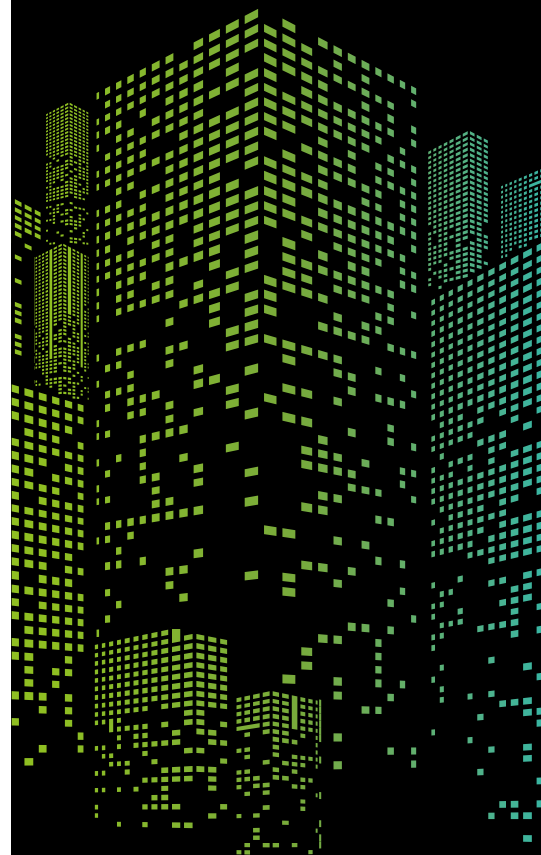
Bewegen sich Objekte jedoch schnell durch das Bild, können typische Rolling-Shutter-Verzerrungen entstehen. Fahrzeuge erscheinen beispielsweise schräg, gerade Linien wirken verzogen oder Objekte werden gestaucht beziehungsweise gestreckt dargestellt. Für das menschliche Auge

Bitte umblättern ▶



Hochwertige und verzerrungsfreie Bilddaten unterstützen die zuverlässige Erfassung von Bewegungen und Aktivitäten im urbanen Raum

pcs



- Sichere Zutritts- und Zufahrtskontrolle
- Moderne Zeiterfassung
- Cloud- & SaaS-Lösungen
- Einfache Integration

◆◆ Treffen Sie uns vor Ort:
Security Essen
22.-25.09.2026

Zeit für Sicherheit.



Netzwerk-Kameras mit Global-Shutter-Technologie liefern auch in öffentlichen Bereichen wie Parks, Plätzen oder Freizeitanlagen eine konsistente Bildgrundlage für Sicherheits- und Analyseanwendungen

sind diese Effekte häufig nur geringfügig sichtbar. Für KI-basierte Analysefunktionen können sie jedoch relevant sein.

Moderne Analyseanwendungen erkennen, klassifizieren und verfolgen Objekte automatisiert auf Basis der erfassten Bildinformationen. Je konsistenter die Darstellung eines Objekts ist, desto zuverlässiger können nachgelagerte Analysen arbeiten. Werden Fahrzeuge durch Bewegungsverzerrungen geometrisch verändert dargestellt, kann dies die Qualität der automatisierten Auswertung beeinträchtigen. Verzerrungsfreie Bilddaten schaffen daher eine verlässlichere Grundlage für Anwendungen wie Fahrzeugklassifizierung, Kennzeichenerkennung oder Verkehrszählungen.

Global-Shutter-Sensoren verfolgen einen anderen Ansatz. Hierbei werden alle Pixel gleichzeitig belichtet und anschließend gemeinsam ausgelesen. Das gesamte Bild entsteht somit exakt zum gleichen Zeitpunkt. Dadurch werden die für Rolling Shutter typischen Bewegungsartefakte weitgehend vermieden. Selbst schnell fahrende Fahrzeuge lassen sich dadurch ohne geometrische Verzerrungen erfassen.

Global Shutter ist jedoch nicht in jeder Anwendung die bessere Technologie. In vielen klassischen Sicherheits- und Verkehrsanwendungen liefern Rolling-Shutter-Sensoren ausgezeichnete Ergebnisse und bieten häufig Vorteile hinsichtlich Auflösung, Lichtempfindlichkeit oder Wirtschaftlichkeit. Ihre besonderen Stärken spielt die Global-Shutter-Technologie vor allem in dynamischen Szenen aus, in denen kurze Belichtungszeiten und eine geometrisch präzise Abbildung entscheidend sind. Damit schafft sie optimale Voraussetzungen für KI-gestützte Analysen und Anwendungen, die auf möglichst konsistente Bilddaten angewiesen sind.

Relevanz für moderne Verkehrsanwendungen

Die Rolle von Netzwerk-Kameras im Verkehrsmanagement hat sich in den vergangenen Jahren grundlegend verändert. Während sie früher hauptsächlich der visuellen Beobachtung und Beweissicherung dienten, liefern sie heute wertvolle und zunehmend strukturierte Informationen für intelligente Verkehrssysteme. Mithilfe von Videoanalysen lassen sich Fahrzeuge erkennen, Fahrzeugtypen unterscheiden, Kennzeichen erfassen und Verkehrsströme nahezu in Echtzeit analysieren. Die Kamera entwickelt sich damit zunehmend von einem reinen Bildgeber zu einer intelligenten Datenquelle für automatisierte Verkehrsanwendungen.

Entscheidend für die Leistungsfähigkeit dieser Anwendungen ist die Qualität der zugrunde liegenden Bilddaten. Bewegungsverzerrungen können dazu führen, dass Fahrzeuge weniger eindeutig klassifiziert oder Kennzeichen schlechter erkannt werden. Insbesondere bei höheren Geschwindigkeiten steigt dieses Risiko. Für KI-basierte Analyseverfahren sind jedoch möglichst konsistente und präzise Bildinformationen entscheidend.

Global-Shutter-Sensoren schaffen hierfür eine besonders zuverlässige Datengrundlage. Durch die Reduzierung Rolling-Shutter-bedingter geometrischer Verzerrungen stehen Analyseanwendungen möglichst originalgetreue Bildinformationen für die Erkennung, Klassifizierung und Auswertung von Fahrzeugen, Kennzeichen und weiteren relevanten Merkmalen zur Verfügung.

Global Shutter und intelligente Beleuchtung

Besonders interessant wird die Technologie in Kombination mit kurzen Belichtungszeiten und gepulster Infrarotbeleuchtung.

Da beim Global Shutter alle Pixel gleichzeitig belichtet werden, lassen sich kurze Lichtimpulse präzise mit der Bildaufnahme synchronisieren. Die verfügbare Lichtleistung kann dadurch gezielt während der eigentlichen Belichtungszeit eingesetzt werden. Dies verbessert die Erfassung schnell bewegter Fahrzeuge auch bei Dunkelheit und ermöglicht detailreiche Aufnahmen von Fahrzeugen und Kennzeichen. Gleichzeitig lassen sich Energieverbrauch und Wärmeentwicklung der Beleuchtung reduzieren.

Gerade für anspruchsvolle Verkehrsanwendungen eröffnet dies neue Möglichkeiten. In Verbindung mit leistungsstarken IR-Impulsstrahlern können selbst bei hohen Fahrzeuggeschwindigkeiten und schwierigen Lichtverhältnissen relevante Fahrzeugdetails zuverlässig erfasst werden. Dazu zählen beispielsweise Fahrzeugmerkmale, Kennzeichen sowie weitere für Verkehrsüberwachung und Verkehrssicherheit wichtige Informationen.

Mit dem weiteren Ausbau intelligenter Verkehrssysteme wird die Qualität der zugrunde liegenden Bilddaten zunehmend zum Erfolgsfaktor automatisierter Analyseprozesse. Technologien wie Global Shutter tragen dazu bei, auch unter anspruchsvollen Bedingungen eine verlässliche Datengrundlage für moderne Verkehrsmanagement- und Sicherheitsanwendungen bereitzustellen.

Typische Einsatzbereiche

Die technologischen Eigenschaften des Global Shutters machen die Axis P1486-LE insbesondere für Anwendungen interessant, bei denen schnell bewegte Objekte zuverlässig erfasst werden müssen. Typische Anwendungen sind beispielsweise:

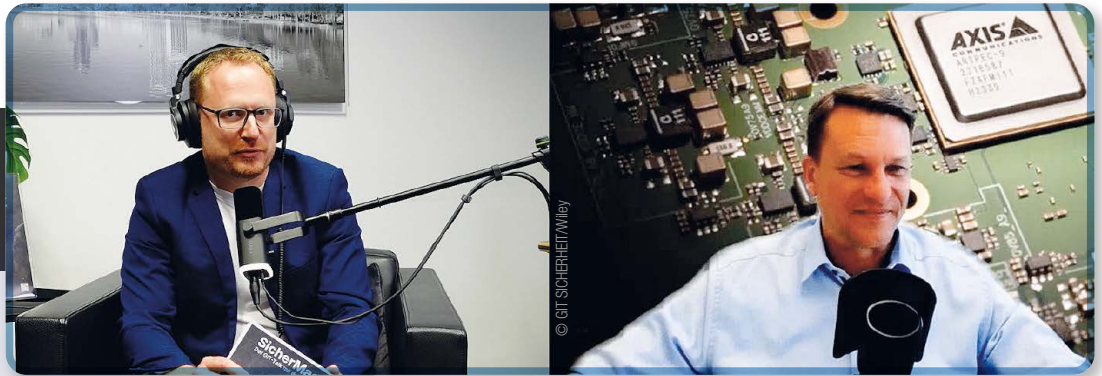
- Verkehrserfassung an Kreuzungen und auf Hauptverkehrsstraßen
- Tunnel- und Autobahnanwendungen
- Zufahrtskontrollen zu Betriebsgeländen oder kritischen Infrastrukturen
- Maut- und Zufahrtskontrollsysteme
- Busspuren, Umweltzonen
- intelligente Verkehrsmanagementsysteme

Auch außerhalb klassischer Verkehrsanwendungen bietet die Global-Shutter-Technologie Vorteile – etwa in der Fördertechnik, der Paketlogistik oder automatisierten Produktionsprozessen. Überall dort, wo schnell bewegte Objekte präzise erfasst und analysiert werden müssen, kann die Technologie einen deutlichen Mehrwert bieten. **GIT**



Axis Communications
www.axis.com

Maximilian Galland, Sales Manager DACH bei Axis Communications (rechts), Dr. Timo Gimbel vom Team GIT SICHERHEIT (links)



SICHERMACHER

Vom Kamerahersteller zum Plattformanbieter

Ein Gespräch mit Maximilian Galland, Sales Manager DACH bei Axis Communications

Axis hat sich vom reinen Netzwerk-Kamera-Pionier zu einem Anbieter integrierter Sicherheitsplattformen entwickelt. Maximilian Galland, Sales Manager DACH, spricht über diesen Wandel, die Bedeutung eigener Chipsätze, KI auf der Edge, Cybersecurity-Regulatorik, neue Sensortechnologien und die Frage, wie Video, Zutritt und Audio künftig zusammenwachsen. Ein Blick in die Zukunft der vernetzten Sicherheit.

GIT SICHERHEIT: Herr Galland, schön, dass Sie bei uns sind. Stellen Sie sich und Ihre Rolle bei Axis bitte kurz vor.

Maximilian Galland: Sehr gerne. Ich bin seit etwas über vier Jahren bei Axis und verantworte den Vertrieb für Deutschland, Österreich und die Schweiz. Wir arbeiten im Two-Tier-Modell mit Distribution, Channel-Partnern und Endkunden. Zusätzlich haben wir ein Team, das TGA-Planer und Planungsbüros unterstützt – Architects & Engineers. Unser Ziel ist es, Projekte und Kunden in der gesamten DACH-Region bestmöglich zu begleiten.

Axis war lange klar als Kamerahersteller positioniert. Heute sprechen Sie von integrierten Sicherheitslösungen. Wie hat sich diese Rolle verändert?

Maximilian Galland: Wir feiern dieses Jahr 30 Jahre Axis IP-Video. 1996 haben wir mit der Neteye 200 die erste Netzwerk-Kamera auf den Markt gebracht. Seitdem hat sich viel getan. Video bleibt unser Kerngeschäft, aber die Anforderungen der Kunden haben sich seitdem fortlaufend verändert. Heute geht es darum, eine Plattform aus Hard- und Software aus einer Hand bereitzustellen, die Integrationsaufwand reduziert und eine zentral steuerbare Sicherheitsinfrastruktur ermöglicht. Unser Videomanagement-

barox



Light Core Switch

RY-LGSO38-10

Für strukturierte Netze mit hoher Datenlast

- Speziell für Anwendungen mit hoher Datenlast (Video-over-IP und Video-Streaming)
- Realisation grosser Netzwerkprojekte mit den neuesten Kameramodellen möglich
- Umfangreiche Sicherheitsfunktionen für den Schutz des Switches und des Netzwerkes
- Durch vielseitige Verwaltungsoptionen werden selbst die komplexesten Netzwerkanforderungen erfüllt

barox Kommunikation GmbH

Weiler Strasse 7 | 79540 Lörrach | 07621 1593 100 | www.barox.de

system Axis Camera Station ist dabei das Herzstück. Gleichzeitig bleiben wir offen: Wir wollen keinen Lock-in, sondern ein Ökosystem, das auch andere VMS- oder Gefahrenmanagementsysteme einbindet.

Axis ist einer der wenigen Hersteller, die eigene Chipsätze entwickeln. Warum?

Maximilian Galland: Das stimmt. Unser System-on-Chip Artpac, aktuell in der 9. Generation, ist ein zentraler Baustein. Er optimiert die Bildqualität und ermöglicht KI-Anwendungen direkt auf der Edge. Es gibt nicht viele Hersteller, die eigene Chipsätze entwickeln – das ist eine große Aufgabe. Aber sie erlaubt uns, Hardware und Software perfekt aufeinander abzustimmen. Wenn die Kamera ein optimiertes Bild liefert, kann KI oder Forensik viel besser arbeiten. Wenn die Hose grau erscheint, weil die Lichtverhältnisse schlecht sind, kann ich nicht nach einer roten Hose suchen. Und nicht zuletzt ermöglicht uns der eigene, inhouse entwickelte Chip, unsere Cybersicherheitsstrategie konsequent umzusetzen. Diese orientiert sich von Beginn an am Secure-by-Design-Ansatz und ist damit fest in unserer Produktentwicklung verankert.

Woran arbeitet Axis aktuell besonders?

Maximilian Galland: KI wird zum Standard. Prozesse sollen automatisiert werden, Analysen ebenfalls. Wir erweitern unser Sensorportfolio fortlaufend: Video wird durch Radar, Thermal und weitere Technologien ergänzt. Auch Zutritt und Audio spielen eine immer größere Rolle. Dazu kommen Themen wie Cybersecurity, Nachhaltigkeit und Total Cost of Ownership.

Blieben wir beim Thema Cybersecurity. Europa hat neue Regulatorik: KRITIS-DACH, NIS2, Cyber Resilience Act. Was tut Axis, um Security by Design sicherzustellen?

Maximilian Galland: Cybersecurity beginnt für uns lange bevor ein Produkt auf den Markt kommt – schon bei der Auswahl der Komponenten. Bereits bei der Auswahl der Komponenten achten wir auf höchste Sicherheitsstandards und vermeiden potenzielle Risiken in der Lieferkette. In der Entwicklung verfolgen wir konsequent den bereits erwähnten Secure-by-Design-Ansatz: Dazu gehören verschlüsselte Kommunikation, hardwarebasierte Sicherheitsmechanismen sowie der Schutz von Geräten, Daten und Identitäten über den gesamten Produktlebenszyklus hinweg.

Ein zentrales Element jeder Axis-Lösung ist unser Axis Edge Vault. Dabei handelt es sich um ein hardwarebasiertes Sicherheitsmodul in der Kamera, das kryptografische Schlüssel und sensible Identitätsdaten zuverlässig schützt. Ergänzt wird dies durch Funktionen wie Secure Boot, signierte Firmware und abgesicherte Software-Lieferketten, um die Integrität unserer Produkte jederzeit sicherzustellen.

Ebenso wichtig ist für uns die langfristige Sicherheit im Betrieb. Deshalb bieten wir kontinuierliche Sicherheitsupdates und ein umfassendes Patch-Management, damit unsere Kunden auch über viele Jahre hinweg geschützt bleiben.

Seit Frühjahr 2025 tragen alle neuen Produkte das IT-Sicherheitskennzeichen des BSI. Mit aktuell mehr als 240 zertifizierten Produkten verfügt Axis über das mit Abstand umfangreichste entsprechend gekennzeichnete Portfolio in der Videosicherheitsbranche.

Und wo sehen Sie die größten Schwachstellen auf Nutzerseite?

Maximilian Galland: Ganz klar: bei der Umsetzung. Wir können Fort Knox liefern – aber wenn ein schlechtes Passwort verwendet wird, hilft das beste Produkt nichts. Die größte Herausforderung liegt häufig nicht in der Technologie selbst, sondern in ihrer konsequenten Anwendung.

Cybersecurity ist eine gemeinsame Verantwortung entlang der gesamten Wertschöpfungskette – vom Hersteller über den Integrator bis hin zum Endanwender. Deshalb unterstützen wir unsere Kunden nicht nur mit sicheren Produkten, sondern auch mit Schulungen, Best Practices und Tools, die die sichere Inbetriebnahme und den sicheren Betrieb erleichtern. Letztlich kann eine Sicherheitslösung jedoch nur so stark sein wie ihre Umsetzung im täglichen Betrieb.

KI, Edge Computing, Cloud – welche technologischen Trends werden für Axis besonders wichtig?

Maximilian Galland: KI auf der Edge ist zentral. Wir erzeugen Metadaten direkt auf der Kamera, um Server und Netzwerk zu entlasten. Gleichzeitig bleiben wir offen für hybride Modelle, wenn Kunden Analysen lieber auf dem Server oder in der Cloud durchführen möchten. Unser Artpac-Chip ermöglicht KI-Anwendungen und optimiert die Bildqualität, insbesondere bei schwierigen Lichtverhältnissen. Dazu kommt der neue Videostandard AV1, der den Bandbreitenbedarf reduziert. Ereignisbasiertes Streaming statt kontinuierliches Streaming spart zudem Speicherplatz und Kosten.

Außerdem arbeiten wir an neuen Sensortechnologien wie Global-Shutter-Sensoren, die insbesondere bei Verkehrsanwendungen Vorteile bieten, sowie an Bisppektralkameras, die optische und thermische Bilddaten in einem Gerät kombinieren.

Welche Vorteile ergeben sich, wenn man Videosicherheit und Zutrittsmanagement gemeinsam plant?

Maximilian Galland: Wer Videoüberwachung und Zutrittsmanagement gemeinsam plant, erhält ein deutlich umfassenderes Lagebild. Zwei bislang getrennte Systeme werden zu einer integrierten Lösung. Dadurch lassen sich Prozesse und Workflows automatisieren, die Komplexität im Betrieb reduzieren und neue Business-Intelligence-Anwendungen erschließen: Besucherströme analysieren, Flächennutzung optimieren, Prozesse verbessern.

Blicken wir fünf Jahre nach vorn: Wie wird sich Axis positionieren, und wie wird sich der Markt entwickeln?

Maximilian Galland: KI wird zum Standard werden – nicht nur zur Entlastung von Sicherheitsverantwortlichen, sondern auch zur Automatisierung und Optimierung von Prozessen. Echtzeitanalytik wird dabei eine immer größere Rolle spielen. Gleichzeitig wird sich die Sensorik weiterentwickeln, etwa durch Radar, Perimeterdetektion über große Distanzen oder die Detektion von Drohnen. Kameras werden sich zunehmend zu intelligenten Sensoren entwickeln, die weit über klassische Sicherheitsanwendungen hinausgehen. Sie unterstützen dabei, operative Prozesse in Echtzeit zu optimieren und liefern die Grundlage für fundierte, datenbasierte Business-Intelligence-Entscheidungen. Parallel dazu wird die Bedeutung von Cybersecurity und entsprechender Regulierung weiter zunehmen. Auch Themen wie Nachhaltigkeit und Total Cost of Ownership werden bei Investitionsentscheidungen noch stärker in den Fokus rücken. Insgesamt wird Sicherheit vernetzter, intelligenter und stärker automatisiert. **GIT**



SicherMacher
Der GIT-Talk mit den Marktführern



Jetzt ansehen:
das vollständige
Interview in unserem
Video-Podcast



Axis Communication
www.axis.com



Automatic Systems und Geutebrück GmbH kooperieren

Automatic Systems und die auf Videoüberwachungslösungen spezialisierte Geutebrück GmbH haben ihre Technologiepartnerschaft bekannt gegeben. Dank eines neuen Plug-ins für die Schnittstelle „G-Connect“ lassen sich die SlimLane Sensorschleusen von Automatic Systems nun nahtlos in die Geutebrück-Systemwelt einbinden. Die einfache Integration in das Video-Management des Unternehmens – speziell in die Plattformen G-SIM und G-Core – ermöglicht, dass Alarime und Bedienfunktionen der Sensorschleusen direkt in den Leitstand übertragen werden, ohne dass gesonderte Lösungen nötig sind. Die Operatoren sehen den Zustand jeder einzelnen SlimLane in Echtzeit und können prüfen, ob sie im Normalbetrieb läuft, gesperrt ist oder offengehalten wird. Ereignisse wie etwa ein unberechtigter Durchgang, das Passieren in Gegenlaufrichtung oder Manipulationsversuche werden als Alarime im Leitstand angezeigt, sodass die Bediener unmittelbar reagieren können.

www.automatic-systems.com/de

Mobotix erweitert One-Plattform

Mit der Mobotix c One erweitert die Mobotix AG ihre One-Plattform um ein intelligentes, ultrakompaktes Sensorsystem für professionelle Indoor-Anwendungen. Die neue Kamera vereint 180°-Hemispheric-Technologie, 4K-Bildqualität, integrierte Videoanalyse, Audiofunktionen sowie IR- und Weißlichtbeleuchtung in einem nur 120 Millimeter großen Gehäuse. Damit ermöglicht sie eine leistungsfähige 360°-Raumerfassung mit reduziertem Installations- und Betriebsaufwand. Mit der c One verfolgt Mobotix konsequent das Ziel, komplexe Sicherheitslösungen einfacher zu machen. Das neue System bündelt Funktionen, die in vielen Anwendungen bislang über mehrere Einzelkomponenten abgebildet wurden, in einem einzigen intelligenten Sensor. Das vereinfacht Planung, Installation und Betrieb und schafft zugleich die technologische Basis für aktuelle und zukünftige KI-basierte Anwendungen.

www.mobotix.com



Protect what matters.

24/7 authorized access, secure storage and full traceability of every asset.



Visit us at
Security Essen 2026
22-25 September
Hall 6 Booth E36

Schedule an appointment now and get a free ticket

www.keba.com



keba.com/en/news/asset-management/security-essen

KEBA

Automation by innovation.

VIDEOTECHNOLOGIE

Baustein der Sicherheitstechnologie

Künstliche Intelligenz made in Germany



Künstliche Intelligenz ist für Dallmeier ein zentraler Baustein moderner Sicherheitstechnologie. Die KI-Modelle des Unternehmens werden auf eigenen Servern in Regensburg trainiert, außerdem verfügt es über ein firmeneigenes Testgelände für Optimierungen unter realen Einsatzbedingungen. Dr. Maximilian Sand-Kraus, Teamleader Artificial Intelligence bei Dallmeier, erläutert die Hintergründe und Vorteile dieses Ansatzes.

■ GIT SICHERHEIT: Herr Dr. Sand-Kraus, wie relevant ist das Thema KI in Ihren Entwicklungen – und wie stellen Sie Qualität und Transparenz sicher?

Maximilian Sand-Kraus: Künstliche Intelligenz ist für uns kein kurzfristiger Trend, sondern ein wesentlicher Bestandteil unserer technologischen Entwicklung. Qualität und Transparenz erreichen wir, indem wir den gesamten Entwicklungs- und Trainingsprozess konsequent selbst kontrollieren. Deshalb verlassen wir uns nicht allein auf große, generische Datensätze, sondern erweitern unsere Datenbasis gezielt um hochwertige, praxisnahe Daten, die ausschließlich auf eigenen Servern in Deutschland verarbeitet werden.

Die Qualität der Trainingsdaten ist ein entscheidender Faktor für leistungsfähige KI-Systeme. Genau hier setzen wir an: Auf unserem firmeneigenen Testgelände in

Regensburg können wir reale Einsatzbedingungen und konkrete Anwendungsszenarien kontrolliert simulieren. Dadurch optimieren wir unsere KI gezielt für spezifische Markt- und Kundenanforderungen in unterschiedlichen Sicherheitsanwendungen. So entstehen praxisnahe und zuverlässige KI-Lösungen.

Sämtliche Trainingsprozesse erfolgen somit innerhalb unserer eigenen Infrastruktur in Deutschland. Sensible Daten verlassen zu keinem Zeitpunkt die kontrollierte Umgebung von Dallmeier oder gelangen in externe Cloud-Systeme. Gleichzeitig ist unser Training konsequent darauf ausgelegt, optimal mit den KI-Chips in unseren Kameras zusammenzuarbeiten. So entsteht eine leistungsfähige, sichere und exakt auf unsere Systemarchitektur abgestimmte KI-Lösung.

Dieser ganzheitliche Ansatz sorgt für eine hohe Praxisnähe und Zuverlässigkeit der Anwendungen und schafft die Grundlage

für vertrauenswürdige KI. Kurz gesagt: Wir setzen auf „AI trained by Dallmeier“.

Was bedeutet „trainierte KI“ bei Dallmeier konkret im praktischen Einsatz?

Maximilian Sand-Kraus: Unsere neuronalen Netze werden vollständig bei uns trainiert und anschließend auf die Kameras übertragen. Auf der Kamera selbst findet ausschließlich die Ausführung des trainierten Modells statt – ein automatisches Nachlernen im Betrieb erfolgt nicht. Stattdessen nutzt das vortrainierte neuronale Netz sein gelerntes Wissen, um unbekannte Live-Bilder zu analysieren und Objekte zuverlässig zu detektieren – beispielsweise Personen, Fahrzeuge wie Autos oder LKW sowie Tiere.

Diese klare Trennung zwischen Training und Anwendung schafft eine hohe Stabilität und Vorhersagbarkeit im Systemverhalten. Gleichzeitig erhöht sie auch den Schutz gegenüber Manipulationen, da das KI-Modell im Einsatz nicht durch manipulierte Daten im Betrieb kompromittiert werden kann.

Auch im Hinblick auf regulatorische Anforderungen ist dieser Ansatz relevant: Das Systemverhalten ist definiert und wird im Betrieb nicht dynamisch verändert – ein zentraler Aspekt im Kontext aktueller EU-KI-Regularien.

Worin unterscheidet sich dieser Ansatz von klassischen Verfahren wie die Mustererkennung?

Maximilian Sand-Kraus: Ein wesentlicher Unterschied liegt im Funktionsprinzip: Klassische Pattern-Matching-Verfahren basieren typischerweise auf vordefinierten Merkma-



Auf dem firmeneigenen Testgelände kann Dallmeier reale Einsatzbedingungen und konkrete Anwendungsszenarien kontrolliert simulieren.

len und stoßen bei variierenden oder unbekannten Erscheinungsformen schneller an Grenzen. Neuronale Netze hingegen lernen während des Trainings abstrakte Merkmale und Zusammenhänge aus den Daten. Dadurch sind sie in der Lage zu generalisieren. Das heißt: Sie können beispielsweise eine „unbekannte Person“ als Person erkennen, auch wenn genau diese Person nie Teil der Trainingsdaten war. Diese Fähigkeit ist entscheidend für den zuverlässigen Einsatz in realen, dynamischen Umgebungen.

Wie flexibel ist Ihr System im Hinblick auf zukünftige Anforderungen?

Maximilian Sand-Kraus: Unsere Systeme sind so ausgelegt, dass zusätzliche Analysefunktionen oder verbesserte neuronale Netze bei Bedarf ergänzt werden können. Neue Funktionen können per verschlüsseltem Update bereitgestellt und anschließend gezielt aktiviert werden. So bleibt das System langfristig anpassungsfähig, ohne die bestehende Infrastruktur verändern zu müssen.

Ist Ihre KI-Lösung skalierbar?

Maximilian Sand-Kraus: Unsere Lösung ist hochskalierbar. Die Bildanalyse mittels neuronaler Netze erfolgt direkt in der Kamera. Das bedeutet: Es sind keine zusätzlichen Analyse-Server on-premises oder in der Cloud erforderlich – auch das Thema Datenschutz in der Cloud stellt sich somit erst gar nicht. Dieser dezentrale Ansatz reduziert nicht nur die Systemkomplexität, sondern ermöglicht auch eine einfache Erweiterung – beispielsweise durch das Hinzufügen weiterer Kameras, ohne zentrale Ressourcen neu dimensionieren zu müssen.

Inwieweit ist Ihre KI mit bestehenden Sicherheitsplattformen kompatibel?

Maximilian Sand-Kraus: Die Integration in bestehende Sicherheitsinfrastrukturen ist ein zentraler Aspekt. Erkannte Objekte und Analyseereignisse stellen wir standardisiert über ONVIF zur Verfügung. Darüber hinaus sind unsere KI-Lösungen nicht nur in unserer eigenen Videomanagementsoftware Hemisphere Semsy nutzbar, sondern auch kompatibel mit Plattformen anderer Unternehmen wie Genetec, Milestone, Advancis oder Octave. Dadurch können Kunden bestehende Systeme weiter nutzen und gleichzeitig von KI-gestützter Videoanalyse profitieren.

Wie zuverlässig sind die Analyseergebnisse – und welche Rolle spielt der Mensch dabei?

Maximilian Sand-Kraus: Unsere KI liefert eine hohe Genauigkeit und Zuverlässigkeit.



Sie ist darauf ausgelegt, Entscheidungsprozesse zu unterstützen, nicht zu ersetzen. In der Praxis bedeutet das: Ein Supervisor kann auf Basis der generierten Analyseereignisse Entscheidungen treffen, ohne permanent alle Kamerabilder beobachten zu müssen. Die KI reduziert also die Arbeitslast erheblich und lenkt die Aufmerksamkeit gezielt auf relevante Ereignisse.

Gibt es bei Dallmeier „Human-in-the-Loop“-Ansätze?

Maximilian Sand-Kraus: Ja, in einer klar definierten Form. Unsere KI trifft keine autonomen Entscheidungen. Sie dient der Objektdetektion und Ereignisgenerierung. Die eigentliche Bewertung und Entscheidung liegt immer beim Menschen. Anwender können beispielsweise Regeln definieren wie: „Wenn eine Person eine bestimmte Linie überschreitet, wird ein Ereignis ausgelöst.“ Dieses Ereignis wird dann von einem Operator geprüft und bewertet. So bleibt die Kontrolle jederzeit beim Nutzer.

Welche Maßnahmen setzen Sie ein, um Risiken wie Modellabweichungen oder Verzerrungen zu minimieren?

Maximilian Sand-Kraus: Wir setzen auf mehrere Maßnahmen: Zum einen fließen Rückmeldungen aus Projekten oder von Anwendern natürlich in die Weiterentwicklung ein. Zum anderen trainieren wir unsere Modelle regelmäßig mit neuen, sorgfältig geprüften Daten. Ein besonderer Fokus liegt auf der Qualität der Trainingsdaten. Wir achten gezielt auf ausgewogene Datensätze, um systematische Verzerrungen zu vermeiden, und führen umfangreiche Tests sowie Evaluierungen durch. So stellen wir sicher, dass unsere KI auch langfristig zuverlässig und stabil arbeitet.

Welche KI-Analysefunktionen stehen Anwendern heute konkret zur Verfügung?

Maximilian Sand-Kraus: Unsere KI umfasst eine Vielzahl spezialisierter Analysefunktionen für unterschiedliche Einsatzszenarien. Beispiele dafür sind Anwendungen wie die AI Perimeter App, mit der sich Sicherheitsbereiche entlang von Zäunen oder Perimetern überwachen lassen, wobei das speziell trainierte neuronale Netz auch gut vorbereitete Täter erkennt – selbst bei ungewöhnlichen Körperhaltungen, Bewegungsmustern oder Tarnkleidung. Die AI Extended Tamper Detection App identifiziert Manipulationsversuche an Kameras, von direktem Eingriff beispielsweise durch Verdrehen bis hin zu gezielten Störungen durch Lichtquellen oder Nebel. Für stark frequentierte Bereiche ermöglicht die AI High Resolution Counting App eine präzise Zählung von Personen und Fahrzeugen. Ergänzend dazu bestimmt die AI Person Attributes App Merkmale wie den Farbton der Bekleidung und beschleunigt so die Auswertung von Videoaufzeichnungen. Diese Anwendungen zeigen, dass unsere KI gezielt auf konkrete Einsatzszenarien ausgerichtet ist und Betreiber wirkungsvoll unterstützt.

Was ist aus Ihrer Sicht der entscheidende Vorteil von „AI trained by Dallmeier“?

Maximilian Sand-Kraus: Der entscheidende Vorteil liegt in der Kombination aus Datenqualität, technologischer Kontrolle und Transparenz. Wir trainieren unsere KI auf eigener Infrastruktur in Deutschland und nutzen dabei gezielt praxisnahe Trainingsdaten aus realistischen Einsatzszenarien. Dadurch entstehen KI-Lösungen, die stabil, sicher und zuverlässig arbeiten. Das ist die Grundlage für Vertrauen – und Vertrauen ist gerade in sicherheitskritischen Anwendungen ein entscheidender Faktor. **GIT**



Dallmeier
www.dallmeier.com
www.panomera.com

Videosensoren und Intelligente Videoanalyse im Perimeterschutz

Teil 1 – Entwicklung und technische Grundlagen. Von Hans-Peter Büttner und Ronald Güldner

Videosensorik, intelligente Analyse und KI prägen moderne Systeme zur Perimetersicherung. Diese dreiteilige Serie von Hans-Peter Büttner und Ronald Güldner erläutert technische Grundlagen, Analyseverfahren und praktische Testergebnisse. Der folgende erste Teil behandelt die technischen Grundlagen und die Entwicklung der Videosensortechnik.

Die Überwachung großer Areale erfordert Verfahren, die relevante Vorgänge zuverlässig erkennen und gleichzeitig das Wachpersonal entlasten. Videosensoren bilden dafür eine zentrale Grundlage: Sie automatisieren Abläufe, reduzieren monotone Beobachtungsaufgaben und ermöglichen eine präzise Fokussierung auf sicherheitsrelevante Ereignisse. Bereits in analogen Systemen kamen Sensoren unterschiedlicher Qualität zum Einsatz, die später in IP-basierten Systemen weiterentwickelt wurden. Die technische Basis hat sich dabei grundlegend verändert: Während analoge Systeme lediglich Grauwertänderungen zwischen zwei Bildern erfassten, erlauben moderne digitale Verfahren die Analyse

von Bildinhalten und damit eine deutlich differenziertere Bewertung.

Mit dem Übergang zur digitalen Videotechnik wurde es möglich, nicht nur das Erscheinen von Personen und Objekten zu erkennen, sondern auch spezifische Merkmale wie Bewegungsmuster, Farben, Objektklassen oder zeitabhängige Ereignisse. Diese Entwicklung hat die Einsatzmöglichkeiten von Videosensoren erheblich erweitert und bildet die Grundlage für moderne Perimeterschutzsysteme, die auf automatisierte Analyse und schnelle Reaktion angewiesen sind.

Aktivitätsdetektion als Ursprung der Sensortechnik

Die Aktivitätsdetektion (AD) gilt als Ausgangspunkt der Videosensorik. Sie vergleicht Grauwertänderungen zwischen zwei zeitlich aufeinanderfolgenden Bildern. Werden Abweichungen festgestellt, löst das System eine Ereignismeldung aus. Dieses Verfahren ist schnell – Änderungen können innerhalb von 40 bis 80 ms erkannt werden – und eignet sich besonders für Innenbereiche oder geschützte Außenbereiche. Die Geschwindigkeit ist ein zentraler Vorteil, denn sie ermöglicht eine unmittelbare Reaktion auf Veränderungen im Bild.

Um unerwünschte Meldungen zu vermeiden, werden Felder entweder

für die gesamte Bildfläche oder partiell ins Bild eingefügt. Bewegungen in diesen Zonen lösen Ereignisse aus, während andere Bereiche ignoriert werden. Auch richtungsbezogene Detektion ist möglich, indem Felder zeitweise deaktiviert werden. Allerdings stößt die AD bei komplexen Außenbedingungen schnell an Grenzen, da Beleuchtungsänderungen, Schatten oder Witterungseinflüsse zu zahlreichen Falschmeldungen führen können.

Videosensoren: Erweiterte Funktionen und flexible Parametrierung

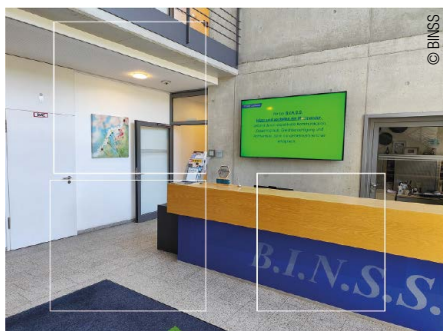
Moderne Videosensoren bieten deutlich mehr Funktionen als die AD. Sie berücksichtigen Beleuchtungsunterschiede, Witterungseinflüsse und komplexe Szenarien. Über 100 frei definierbare Felder können in Größe, Position, Empfindlichkeit und Messzeit angepasst werden. Dadurch lassen sich Kleintiere ausblenden, Fahrzeuge priorisieren oder langsame Bewegungen wie Kriechen erkennen. Die Parametrierung ermöglicht eine sehr feine Steuerung der Detektion und erlaubt es, die Sensorik exakt an die Bedingungen der jeweiligen Liegenschaft anzupassen.

Ein zentrales Prinzip ist die Detektionsschwelle: Nur wenn die Bildänderungen in einem Feld diese Schwelle überschreiten, wird ein Ereignis ausgelöst. So können Personen auf einem Parkplatz ignoriert werden, während Fahrzeuge zuverlässig erkannt werden. Die Empfindlichkeit der Felder kann zudem an die Beleuchtung angepasst werden, sodass auch dunkel gekleidete Personen in schwach beleuchteten Bereichen zuverlässig erkannt werden.

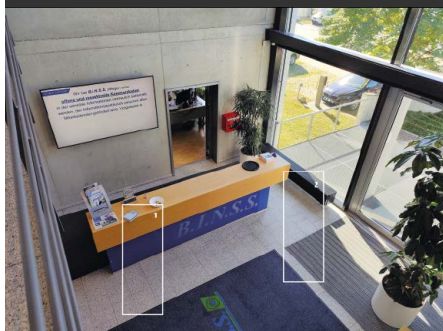
Spezialfunktionen und Szenarien

Sensorfelder können miteinander verknüpft werden, etwa als Vor- und Hauptalarmfelder. Erst wenn ein Objekt beide Bereiche in der richtigen Reihenfolge durchläuft, wird ein Alarm ausgelöst. Auch Sperrfelder, die nachgeordnete Felder temporär stumm schalten, ermöglichen komplexe Szenarien. Diese Funktionen erlauben es, typische Bewegungsmuster innerhalb einer Liegenschaft abzubilden und Falschalarme durch reguläre Vorgänge zu vermeiden.





Beispiele für Aktivitätsdetektion und Feldstrukturen



Witterungseinflüsse wie Regen oder Schnee erzeugen globale Änderungen, die moderne Sensoren ignorieren. Partielle Änderungen – etwa durch eine Person – werden dennoch erkannt. Perspektivische Anpassungen sorgen dafür, dass Objekte unabhängig von ihrer Entfernung zur Kamera gleich bewertet werden. Dies ist besonders wichtig, da Personen im Vordergrund deutlich größer erscheinen als im Hintergrund.

Das Parametrieren spezieller Szenarien wie Tag- und Nachteinstellung, das Einstellen auf Sommer- oder Winterbedingungen erlaubt die weitere detaillierte Anpassung an die Bedingungen der zu überwachenden Szene.

Grenzen der Sensortechnik

Trotz ihrer Flexibilität bleibt die Parametrierung anspruchsvoll. Jahreszeiten, Lichtverhältnisse und Schatten erfordern regelmäßige Anpassungen. Besonders problematisch sind bewegte Schatten durch Wind oder vorbeifahrende Fahrzeuge.

Wärmebildkameras können diese Effekte reduzieren, indem sie unabhängig von Lichtreflexionen arbeiten. Die Kombination aus Videosensorik und Wärmebildtechnik hat sich in vielen Systemen bewährt, da sie die Falschalarmrate deutlich reduziert.

Ein Vorteil bleibt jedoch einzigartig: Die extrem kurze Detektionszeit von maximal 80 ms wird von keiner KI-basierten Analyse erreicht. Diese Geschwindigkeit macht klassische Videosensoren weiterhin zu einem wichtigen Bestandteil moderner Perimeterschutzsysteme.

Relevanz für den Perimeterschutz

Im Perimeterschutz müssen Systeme zuverlässig zwischen relevanten und irrelevanten Ereignissen unterscheiden. Die Videosensorik bietet hierfür eine schnelle und flexible Grundlage. Besonders in Bereichen mit stark wechselnden Lichtverhältnissen oder komplexen Bewegungsmustern ist die Fähigkeit, Felder individuell zu parametrieren, ein entscheidender Vorteil. Die Sensorik kann so eingestellt werden, dass reguläre Bewegungen – etwa von Mitarbeitenden – ignoriert werden, während sicherheitsrelevante Vorgänge zuverlässig erkannt werden.

Die Kombination aus Geschwindigkeit, Flexibilität und der Möglichkeit, komplexe Szenarien abzubilden, macht Videosensoren zu einem unverzichtbaren Bestandteil moderner Sicherheitsarchitekturen. Auch wenn KI-basierte Verfahren zunehmend an Bedeutung gewinnen, bleibt die klassische Sensortechnik aufgrund ihrer Echtzeitfähigkeit ein wichtiges Fundament.

Fazit

Videosensoren haben sich von einfachen Grauwertdetektoren zu hochflexiblen Analysewerkzeugen entwickelt. Ihre Fähigkeit, Szenarien präzise abzubilden und schnell auf Veränderungen zu reagieren, macht sie auch weiterhin zu einem Element im Perimeterschutz. Die Bedeutung KI-basierter Analyseverfahren wird sich weiter erhöhen. Für spezifische Einsatzfälle bleibt die klassische Sensortechnik aufgrund ihrer Detektionsgeschwindigkeit relevant. In der Kombination beider Ansätze findet man eine Lösung, sowohl schnelle als auch komplexe Analysen zu ermöglichen. **GIT**



Hans-Peter Büttner, Freier Berater
Videoüberwachungstechnik
pb.videoplan@t-online.de

Ronald Güldner, Projektleiter,
B. I.N.S.S. GmbH Berlin
rgueldner@innss.de



HIRSCH

Maximale Sicherheit.

Ganz Einfach.

Ihr One-Stop-Shop für Sicherheit.

Vom Perimeter bis zum Desktop.



Security Essen 2026

22. - 25. September
2026 Messe Essen

Stand 6E27

SECURITY MANAGEMENT

Wenn Videodaten zu belastbaren Beweisen werden

Coda Video 9.2 von Octave: Wie Smart Evidence Management Videoanalyse, Ermittlungen und Sicherheitsprozesse effizienter machen soll

Laut Recherchen von GIT SICHERHEIT führt das Hexagon-Spin-off-Unternehmen Octave mit der Version 9.2 seiner Videoplattform Coda Video eine Reihe funktionaler Erweiterungen ein, die darauf abzielen, Reibungsverluste in täglichen Sicherheitsprozessen zu reduzieren sowie Ermittlungen konsistenter und effizienter zu gestalten.

■ Moderne Sicherheitsorganisationen stehen unter wachsendem Druck: Immer größere Mengen an Videodaten müssen ausgewertet werden, während gleichzeitig schnelle, belastbare Ermittlungsergebnisse erwartet werden. Video-Management-Systeme übernehmen dabei längst mehr als reine Aufzeichnungsfunktionen. Sie sind zentrale Werkzeuge, um visuelle Informationen in strukturierte, verwertbare Beweise zu transformieren.

Prozessorientierter Ansatz für Videoermittlungen

Nach Einschätzung von GIT SICHERHEIT markiert Coda Video 9.2 einen wichtigen Entwicklungsschritt innerhalb der Enterprise-Video-Management-Software von Octave. Der Fokus liegt weniger auf ein-

zelnen Features, sondern auf einer konsequent prozessorientierten Betrachtung von Ermittlungsabläufen.

Im Zentrum steht das Konzept des Smart Evidence Management (SEM). Ziel ist es, digitale Beweise effizienter zu erfassen, zusammenzustellen und teamübergreifend bereitzustellen. Gerade in komplexen Sicherheitsumgebungen summieren sich kleine Ineffizienzen schnell: Ermittler verbringen viel Zeit mit der Sichtung von Videomaterial, dem Export einzelner Sequenzen und der Aufbereitung von Beweisen für interne oder externe Stellen.

SEM setzt genau hier an. Durch die Reduktion manueller Zwischenschritte und klar strukturierte Workflows entsteht ein konsistenter Prozess – besonders wertvoll für Organisationen mit hohem Fallaufkommen.

Optimiertes Beweismanagement und mehr Klarheit in Ermittlungen

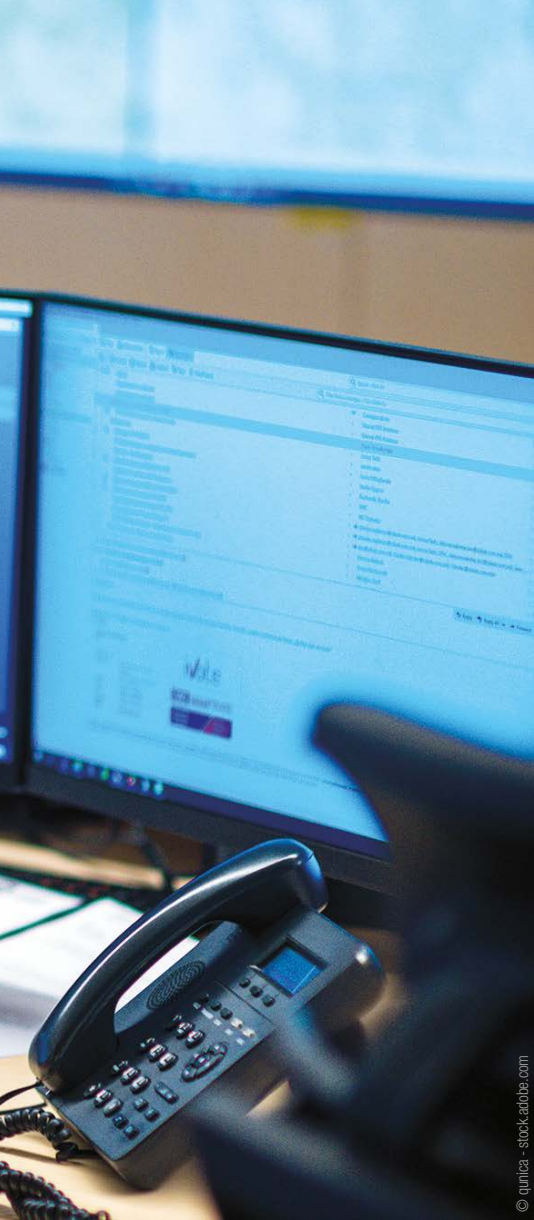
Eine der zentralen Neuerungen in Coda Video 9.2 liegt laut GIT-Recherchen in den erweiterten Möglichkeiten für Videoexporte und View-Navigation. Relevante Videosequenzen lassen sich schneller zusammenstellen und übersichtlich präsentieren.

Das Ergebnis: Beweispakete werden verständlicher, strukturierter und juristisch belastbarer. Sowohl interne Entscheidungsprozesse als auch formale Ermittlungen profitieren von einer klaren Darstellung und lückenlosen Dokumentation.

Durch die verkürzte Zeitspanne vom Rohmaterial bis zum verwertbaren Beweis beschleunigen Sicherheitsteams die Fallbearbeitung – ohne Abstriche bei Konsistenz oder Nachvollziehbarkeit. Gerade in regulierten Umfeldern mit hohen Anforderungen an Auditierbarkeit und Dokumentationsqualität ist das ein entscheidender Vorteil.

Höhere Anzeigeperformance für anspruchsvolle Einsatzszenarien

Effizienz im Sicherheitsbetrieb hängt maßgeblich von der Systemperformance ab. Mit Version 9.2 hat Octave die Darstellungsleis-



anzeigen – ohne Einbußen bei Stabilität oder Reaktionsgeschwindigkeit.

Das reduziert sowohl kognitive als auch operative Belastungen in Leitstellen. Verzögerte oder fragmentierte Videodarstellungen gehören damit der Vergangenheit an. Ein flüssiges, konsistentes Bild unterstützt die schnelle Lageeinschätzung und ermöglicht fundierte Entscheidungen in zeitkritischen Situationen.

Nahtlose Integration multisensorischer Kamerasysteme

Der zunehmende Einsatz von Multisensor-Kameras eröffnet neue Möglichkeiten, stellt Video-Management-Systeme aber auch vor Herausforderungen. Coda Video 9.2 begegnet diesen Anforderungen mit einer nahtlosen Integration multisensorischer Systeme, die große Areale abdecken und gleichzeitig hohe Detailgenauigkeit bieten.

Besonders relevant ist dies für komplexe Infrastrukturen wie Flughäfen, Bahnanlagen oder den öffentlichen Personennahverkehr. Betreiber profitieren von großflächigen Übersichten und der Möglichkeit, einzelne Vorfälle detailliert zu analysieren – ohne Systemwechsel oder Medienbrüche.

Erweiterte Unterstützung für Panorama-Überwachung

Installationen mit Dallmeier Panomera-Kameras beispielsweise profitieren in Coda Video 9.2 von einem erweiterten Funktionsumfang. Automatisches Stitching und verlustfreier Zoom ermöglichen den nahtlosen Wechsel zwischen Überblicks- und Detailansichten innerhalb desselben Bildkontextes.

Das steigert die Situationswahrnehmung erheblich und reduziert manuelle Kamerateilnahmen. Gerade in Umgebungen mit

hoher Personendichte oder dynamischen Bewegungsmustern behalten Operatoren so jederzeit den Überblick.

Vereinfachte Installation und webbasierter Zugriff

Neben den Ermittlungsfunktionen bringt Coda Video 9.2 auch praktische Verbesserungen für Installation und Administration. Ein neuer, einheitlicher Modul-Installer vereinfacht die Bereitstellung sowie Updates und reduziert den Aufwand für IT- und Sicherheitsteams deutlich.

Parallel dazu wurde der Octave Coda Web Client funktional erweitert und in der Bedienbarkeit optimiert. Das erleichtert den browserbasierten Zugriff – insbesondere in verteilten oder standortübergreifenden Sicherheitsarchitekturen.

Grundlage für datenbasierte Sicherheitsentscheidungen

Insgesamt spiegeln die Neuerungen von Coda Video 9.2 einen klaren Trend in der physischen Sicherheit wider: den Übergang zu datengetriebenen Entscheidungsprozessen. Durch reibungsärmere Workflows, verbesserte Visualisierung und die Integration moderner Kameratechnologien unterstützt die Plattform strukturierte, nachvollziehbare Ermittlungen.

Für Organisationen mit steigender Sicherheitskomplexität und wachsendem Verantwortungsdruck wird es damit möglich, Videodaten in konkrete, handlungsrelevante Erkenntnisse zu überführen – ohne zusätzliche operative Belastung. **GIT**

tung im nativen Client deutlich verbessert. Anwender können nun mehr Videostreams gleichzeitig und in höheren Auflösungen



Octave
www.octave.com



RUND UM DIE UHR IM DIENST

AG Neovo Displays mit NeoV™ Glastechnologie -> gebaut für 24/7/365 durch:

- Hochqualitative Selektion aller Komponenten
- Kratz- und stoßfeste NeoV™ Glas-Oberfläche
- Minimierung von Helligkeitsverlusten durch NeoV™
- patentierte Anti-Burn-in™ Technologie
- Solide und Wärme-ableitende Metallgehäuse
- NDAA-Konformität aller Produkte

AG Neovo's Design und jahrzehntelange Erfahrung sichern so verlässlichen Dauerbetrieb für Ihre Displays - unabhängig von Ort und Aufgabe.



Kontakt:
vertrieb@ag-neovo.com
+ 49-2256-6289820



Diesen Monat auf GIT-SICHERHEIT.de

NEWS AKTUELLE INHALTE PRODUKTE MAGAZIN BUSINESS PARTNER EVENTS DE EN

GIT SICHERHEIT

MANAGEMENT SECURITY BRANDSCHUTZ IT-SECURITY SAFETY

SicherMacher
Jetzt ansehen:
Die GIT-Talks mit den Marktführern

GIT SICHERHEIT AWARD
Jetzt für Ihre Favoriten stimmen!

VIP-Interview
Die VIPs in Sachen Sicherheit

Acher
SicherMacher – der GIT-Talk mit den Marktführern:
Aleksej Tokarev, Gründer von Security Robotics
Folge 7: Nächste Evolutionsstufe physischer Sicherheit

BRANDSCHUTZ
SicherMacher – der GIT-Talk mit den Marktführern: Tobias Vathjunker (Kirotec, Priorit)

ANZEIGE • SECURITY
ISO 27001 zertifiziert: CES macht Informationssicherheit zur Managementdisziplin

ANZEIGE
Expertenforum Reisesicherheit
Tübingen · 28.–29. September 2026
Reale Erfahrungen. Relevante Themen. Wertvolle Gespräche.
[Programm ansehen & anmelden →](#)

NEWS

Hikvision erhält die EUCC-Zertifizierung für Netzwerkkameras

SicherheitsExpo München 2026

BSI: Prüfkatalog vertrauenswürdige KI-Systeme

TOP 100-Award: Christian Wulff würdigt Astrum IT

BDSW warnt vor Minijob-Reform

THEMEN

ANZEIGE • TOPSTORY • SECURITY
PIAM-Suite von ID-ware: Physical Identity & Access Management für zentral verwaltete Identitäten, sichere Zutritte, volle Compliance
Physical Identity & Access Management: zentral verwaltete Identitäten, sichere Zutritte, volle Compliance für jedes Unternehmen

TOPSTORY • MANAGEMENT
Hybride Bedrohungen im Fokus: Warum Sicherheit heute Chefsache ist und Resilienz über den Unternehmenserfolg entscheidet
Sicherheit wird zur Chefsache: Warum hybride Bedrohungen, Mensch-Risiken und Resilienz heute über Unternehmensstabilität entscheiden

TOPSTORY • SECURITY
Elektronische Zutrittskontrolle für Kirchen: Flexible Schließlösung von Wilka im Pfarrzentrum Velbert
Elektronische Schließlösung für Kirchengemeinde in Velbert

VIDEO • SECURITY
SicherMacher – der GIT-Talk mit den Marktführern: Aleksej Tokarev, Gründer von Security Robotics
Folge 7: Aleksej Tokarev, Co-Gründer und Geschäftsführer von Security Robotics, über die nächste Evolutionsstufe physischer Sicherheit.

ANZEIGE
SicherMacher
Der GIT-Talk mit den Marktführern

ANZEIGE
SicherMacher
Der GIT-Talk mit den Marktführern

SPECIAL
GIT SICHERHEIT PRO SPECIAL
Schutz für Museum & Kultur
Schwerpunkt rund um den Schutz von Museen, Ausstellungen und wertvollen Kulturgütern.

SICHERMACHER
SicherMacher – der GIT-Talk mit den Marktführern
Die Köpfe hinter den Marktführern. Die Strategien von morgen. Die Themen, die die Sicherheitsbranche bewegen. Jetzt alle SicherMacher-Talks entdecken.

LANDING-PAGE
35 Jahre
GIT SICHERHEIT
Trendberichte, Interviews & Specials
JUBILÄUM
35 Jahre GIT SICHERHEIT
Trendberichte, Interviews und Specials

PRODUKTE

R&S Imager prüft in Echtzeit Qualität verpackter Waren

ppm GmbH erweitert Anti-jamming-Portfolio

Mobotix erhält die ANS/FM 3260-Zulassung

IP-Decoder-Box- und -Monitorlösung von Eizo

Onekey setzt auf „Decision Intelligence“ bei Cybersicherheit

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.-Betw. Steffen Ebert
+49 6201 606 709

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

Dr. Timo Gimbel
+49 6201 606 049

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@vservice.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: DE5501108006161517443

GIT SICHERHEIT

Auflage: s. iww.de

inkl. GIT Sonderausgabe PRO-4-PRO



Abonnement 2026

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 BHE, BDSW, BDGW, BDLS, PMeV, vrbö, VfS, VSW-Bundesverband sowie seiner Regionalverbände 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.

Originalarbeiten

Die namentlich gekennzeichneten Beiträge stehen in der Verantwortung des Autors. Nachdruck, auch auszugsweise, nur mit Genehmigung der Redaktion und mit Quellenangabe gestattet. Für unaufgefordert eingesandte Manuskripte und Abbildungen übernimmt der Verlag keine Haftung.

Dem Verlag ist das ausschließliche, räumlich, zeitlich und inhaltlich eingeschränkte Recht eingeräumt, das Werk/den redaktionellen Beitrag in unveränderter oder bearbeiteter Form für alle Zwecke beliebig oft selbst zu nutzen oder Unternehmen, zu denen gesellschaftsrechtliche Beteiligungen bestehen, sowie Dritten zur Nutzung zu übertragen. Dieses Nutzungsrecht bezieht sich sowohl auf Print- wie elektronische Medien unter Einschluss des Internet wie auch auf Datenbanken/Datenträger aller Art.

Alle etwaig in dieser Ausgabe genannten und/oder gezeigten Namen, Bezeichnungen oder Zeichen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

Gender-Hinweis

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) sowie auf Sonderschreibweisen mit Doppelpunkt oder Genderstern verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Druck

westermann DRUCK | pva

Printed in Germany, ISSN 2751-4536



WILEY

GIT SICHERHEIT

INNENTITEL – SECURITY



Überwachung des Unüberschaubaren

Glasfaser als Sensoren zum Schutz von kritischen
Infrastrukturen und anderen großen Geländen

APSENSING.

FASEROPTISCHE SENSORIK

Überwachung des Unüberschaubaren

Glasfaser als Sensoren zum Schutz von kritischen Infrastrukturen und anderen großen Geländen

AP Sensing überwacht kritische Infrastrukturen mit faseroptischer Sensorik – von Pipelines über Stromnetze bis zu Offshore-Windparks. Clemens Pohl, CEO des in Böblingen südlich Stuttgarts ansässigen Unternehmens, erklärt im Gespräch mit GIT SICHERHEIT, wie Glasfasern als durchgehende Sensoren Fremdeingriffe früh erkennen und die Sicherheit essenzieller Systeme gewährleisten.



■ GIT SICHERHEIT: Herr Pohl, Sie befassen sich bei AP Sensing mit faseroptischen Sensorsystemen. Bevor wir der Frage nachgehen, wie sie genau funktionieren und wozu man sie einsetzt: Könnten Sie uns kurz einmal Ihr Unternehmen vorstellen?

Clemens Pohl: AP Sensing entwickelt Lösungen für die ortsverteilte faseroptische Sensorik. Wir überwachen kritische Infrastrukturen, machen sie effizienter und sicherer. Mit unserer Sensortechnologie können Betreiber Risiken, Fremdeingriffe oder sich anbahnende Systemausfälle frühzeitig erkennen und schnell reagieren. Damit erhöhen wir die Verfügbarkeit wichtiger Anlagen. Unsere Wurzeln reichen bis zu Hewlett-Packard zurück. AP Sensing entstand 2007 aus dem Umfeld der HP-Messtechnologie. Dort wurde bereits seit den 1980er-Jahren an faseroptischen Messtechnologien geforscht und entwickelt.

Heute beschäftigen wir mehr als 180 Mitarbeitende auf fünf Kontinenten. Unsere Lösungen sind bei über 1000 Kunden in mehr als 70 Ländern im Einsatz. Zu unseren Kunden zählen Unternehmen aus der Energieversorgung, der Branderkennung, dem Pipeline Monitoring, der Bahn- und Verkehrsinfrastruktur, dem Perimeterschutz und dem Defence-Bereich.

Das sind vielfach Kritische Infrastrukturen, die ja heute insgesamt stärker im Fokus stehen als noch vor einigen Jahren...

Clemens Pohl: Tatsächlich haben wir in den vergangenen Jahren sehr deutlich gesehen, wie abhängig unsere Gesellschaft von diesen Infrastrukturen ist. Stromnetze, Pipelines, Telekommunikationsverbindungen, Bahnstrecken oder Unterseekabel bilden das Rückgrat unseres täglichen Lebens. Fällt eine dieser Infrastrukturen aus, sind die Auswirkungen oft weit über den eigentlichen Standort hinaus spürbar.

Gleichzeitig haben mehrere Ereignisse gezeigt, dass diese Systeme verwundbar sind. Die Sabotage der Nord-Stream-Pipelines, Beschädigungen von Unterseekabeln in Nord- und Ostsee sowie Angriffe auf die Bahninfrastruktur und Anfang des Jahres der Anschlag in Berlin und vor kurzem in einem Umspannwerk in Reutlingen haben das Thema in den Fokus der Öffentlichkeit gerückt.

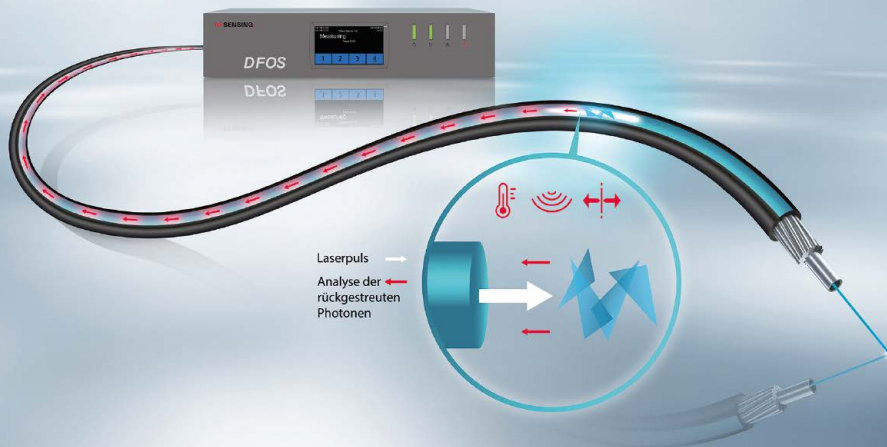
Hinzu kommt, dass unsere Infrastrukturen zunehmend größer und komplexer werden. Im Zuge der Energiewende entstehen neue Offshore-Windparks, Stromtrassen, Batteriespeicher und grenzüberschreitende Energieverbindungen. Viele dieser Anlagen erstrecken sich über Hunderte von Kilometern und verlaufen durch abgelegene oder schwer zugängliche Gebiete.

Das macht ihren Schutz zu einer besonderen Herausforderung. Man kann nicht alle paar Kilometer Personal stationieren oder jede Infrastruktur permanent vor Ort überwachen. Deshalb benötigen Betreiber neue Möglichkeiten, um den Zustand ihrer Anlagen kontinuierlich im Blick zu behalten und Auffälligkeiten sofort zu erkennen. Es geht um die Sicherheit und Zuverlässigkeit von Systemen, auf die wir jeden Tag angewiesen sind.

Zu Ihrem Portfolio gehören die Lineare Wärmedetektion (LHD), Systeme zur verteilten Temperaturmessung (DTS), verteilte akustische Sensorik (DAS) sowie Systeme zur Temperatur- und Dehnungsmessung (DTSS). Können Sie das einmal ein wenig für uns sortieren?

Clemens Pohl: Zunächst einmal basieren all diese Lösungen auf demselben Grundprinzip: Wir nutzen Glasfaserkabel als Sensoren. Dadurch können wir über viele Kilometer hinweg an jeder Stelle des Kabels Informationen erfassen und nicht nur an einzelnen Messpunkten. Der Unterschied zwischen den genannten Produkten liegt darin, welche Informationen wir aus der Glasfaser gewinnen.

Bei der Linearen Wärmedetektion und der verteilten Temperaturmessung messen wir die exakte Temperatur an jedem Meter des Kabels und dies über viele Kilometer hinweg. Die Technologie wird beispielsweise für die



Laserpulse werden durch ein Glasfaserkabel gesendet. Das zurückgestreute Licht wird analysiert, um Temperatur, akustische Signale und Dehnung kontinuierlich zu erfassen

Branderkennung oder die Überwachung von Energiekabeln und Pipelines eingesetzt.

Die verteilte akustische Sensorik erfasst Vibrationen und Geräusche entlang der Glasfaser, vergleichbar zu tausenden von Mikrofonen. Damit lassen sich beispielsweise Arbeiten an Energiekabeln und Pipelines, Fremdeingriffe oder Aktivitäten entlang von Zäunen und anderen kritischen Infrastrukturen erkennen. Darüber hinaus wird sie auch zur Erdbebenforschung und Tsunamiwarnung verwendet.

Bei der Temperatur- und Dehnungsmessung erfassen wir zusätzlich mechanische Veränderungen. Das ist besonders interessant für die Zustandsüberwachung von Bauwerken, Tunneln, Pipelines oder anderen kritischen Anlagen. Darüber hinaus kommt die Technologie auch bei der Überwachung von Dämmen und Deichen sowie in geowissenschaftlichen Anwendungen zum Einsatz, etwa zur Erkennung von Erdrutschen.

Letztlich verfolgen alle diese Technologien dasselbe Ziel: Sie schaffen Transparenz über Zeit und Ort und helfen Betreibern, Bedrohungen frühzeitig zu erkennen und ihre Anlagen sicher zu betreiben.

Können Sie noch mal etwas genauer beschreiben, wie faseroptische Sensorik technisch funktioniert?

Clemens Pohl: Vereinfacht gesagt nutzen wir ein Glasfaserkabel als durchgehenden

Sensor. Ein Messgerät sendet Lichtimpulse in die Faser. Ein sehr kleiner Teil dieses Lichts wird entlang der Faser zurückgestreut und wieder zum Messgerät geführt. Verändert sich die Umgebung der Faser, zum Beispiel durch Wärme, Vibrationen oder mechanische Belastungen, verändert sich auch das zurückgestreute Licht. Diese Veränderungen können wir in Echtzeit messen und auswerten. Dadurch lässt sich sehr genau bestimmen, wo entlang der Faser ein Ereignis auftritt und um welche Art von Ereignis es sich handelt.

Es gibt in der Regel ja ein Spannungsfeld zwischen hoher Detektionsempfindlichkeit und Falschalarmen. Wie schlägt sich diese Technik diesbezüglich?

Clemens Pohl: Das Spannungsfeld gibt es tatsächlich. Eine hohe Empfindlichkeit ist wichtig, damit kritische Ereignisse früh erkannt werden. Gleichzeitig müssen Betreiber darauf vertrauen können, dass Alarmer relevant sind. Falsche Alarmer führen schnell dazu, dass Warnmeldungen nicht mehr ernst genommen werden. Deshalb geht es heute nicht mehr nur um die Leistung der Sensorik selbst, sondern auch um die intelligente Auswertung der Daten.

Moderne Systeme können deutlich besser zwischen kritischen Ereignissen und normalen Umwelteinflüssen unterscheiden als noch vor einigen Jahren. Dabei helfen

salto 
INSPIRED ACCESS



Vielseitige Zutrittslösungen

> HOHE SICHERHEIT

Salto Lösungen basieren auf modernsten Zutritts- und Sicherheitstechnologien, binden sämtliche Zutrittspunkte ein und bieten ein umfassendes Zutrittsmanagement.

> OPTIMIERTE PROZESSE

Salto digitalisiert und automatisiert Abläufe durch die Integration mit Management- und IT-Systemen sowie die Einbindung in Workflows.

> EFFIZIENTER BETRIEB

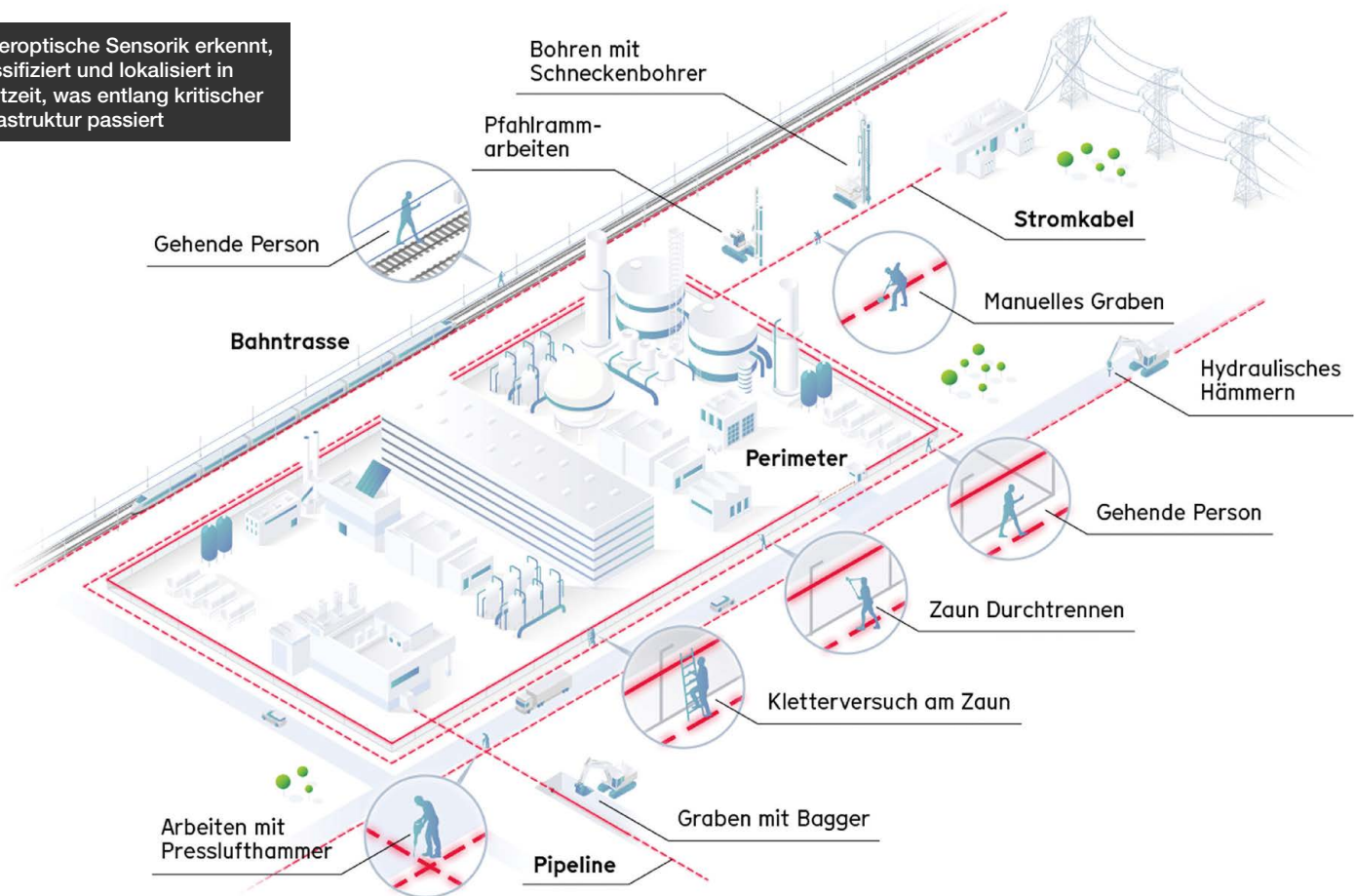
Anwender profitieren von flexibler Raumnutzung, hoher Sicherheit, optimierten Prozessen und niedrigen Lebenszykluskosten.

saltosystems.de

SECURITY ESSEN
22.-25.9.2026
HALLE 6, STAND 6B27

SALTO WECOSYSTEM

Faseroptische Sensorik erkennt, klassifiziert und lokalisiert in Echtzeit, was entlang kritischer Infrastruktur passiert



uns die große Datenbasis aus Tausenden von Installationen weltweit sowie moderne Analyseverfahren und Machine Learning. So erzielen wir eine zuverlässige Detektionsleistung bei gleichzeitig hoher Alarmqualität. Unser Ziel ist nicht nur die zuverlässige Erkennung eines Ereignisses, sondern auch dessen präzise Klassifizierung und Lokalisierung. Erst diese Kombination sorgt dafür, dass Betreiber die richtigen Informationen zur richtigen Zeit erhalten.

Der Markt für faseroptische Systeme wächst stark – getrieben vor allem durch die Entwicklung bei erneuerbaren Energien und normativer Veränderungen im Bereich Kritische Infrastrukturen. Entsprechend haben sich die Technologien bereits in vielen Märkten etabliert. Sie sind in all diesen Bereichen vertreten?

Clemens Pohl: Ja, absolut. Wir sehen in all diesen Bereichen eine steigende Nachfrage nach zuverlässigen Überwachungslösungen. Die Energiewende bringt neue Anforderungen mit sich. Das gilt beispielsweise für den Ausbau von Stromnetzen oder neue Energieinfrastrukturen sowie für Pipelines und Bahntrassen.

Neben technologischen Entwicklungen sehen wir auch regulatorische Treiber. Mit NIS2 und dem KRITIS-Dachgesetz rücken

Resilienz, Transparenz und die frühzeitige Erkennung von Risiken noch stärker in den Fokus. Betreiber müssen heute jederzeit wissen, was entlang ihrer kritischen Infrastruktur passiert und im Ernstfall schnell reagieren können.

Für uns sind diese Entwicklungen nicht neu. Wir unterstützen seit vielen Jahren Kunden dabei, potenzielle Gefahren frühzeitig zu erkennen und fundierte Entscheidungen auf Basis von Echtzeitdaten zu treffen. Wir sehen hier eine langfristige Entwicklung. Es geht nicht nur um einzelne Projekte oder neue Technologien. Vielmehr verändert sich die Art und Weise, wie kritische Infrastrukturen betrieben und geschützt werden.

Können Sie die Arbeitsweise Ihrer Systeme einmal anhand eines besonders aussagekräftigen Beispiels aus dem Bereich Kritische Infrastrukturen vorstellen?

Clemens Pohl: Ja, gerne. Ein gutes Beispiel ist die Überwachung von Gaspipelines. Schon einfache Bauarbeiten in der Nähe der Trasse können ein erhebliches Risiko darstellen. Bei einem großen Pipelineprojekt in Osteuropa überwachen wir nahezu 500 Kilometer Pipeline mit verteilter akustischer Sensorik. Wenn beispielsweise ein Bagger in der Nähe der Leitung arbeitet, erkennt das System die entstehenden Vibrationen und

Geräusche, lokalisiert die Position und informiert den Betreiber in Echtzeit. Dadurch können potenzielle Gefährdungen frühzeitig bewertet werden, bevor Schäden entstehen.

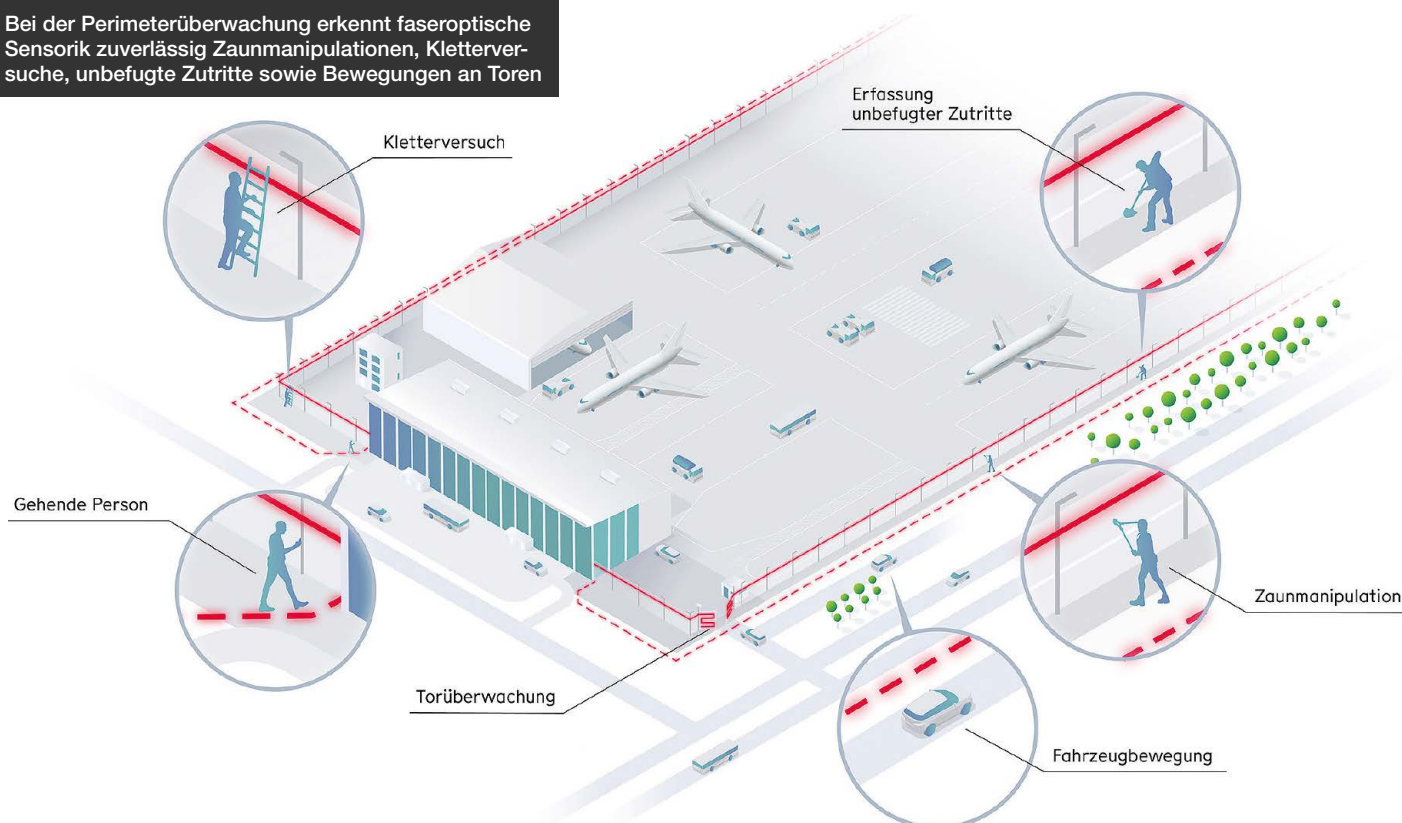
Ein weiteres Beispiel sind Hochspannungsverbindungen zwischen europäischen Ländern. Wir überwachen mehr als 300 Kilometer lange Unterseekabel, die eine wichtige Rolle für die europäische Energieversorgung und die Integration erneuerbarer Energien spielen. Solche Verbindungen sind kritische Infrastruktur im wahrsten Sinne des Wortes. Unsere Systeme erkennen Aktivitäten in der Nähe der Kabelstrecke, beispielsweise wenn Anker über den Meeresboden gezogen werden oder Fischernetze, und unterstützen den Betreiber dabei, diese Risiken frühzeitig zu erkennen und schnell zu reagieren.

Die Beispiele sind unterschiedlich, das Prinzip ist jedoch immer dasselbe. Wir verwandeln eine Glasfaser in einen durchgehenden Sensor, schaffen damit Sichtbarkeit und liefern ein kontinuierliches Lagebild, das auf Echtzeitdaten basiert.

Vielleicht noch ein weiteres Beispiel aus einem anderen Bereich, in dem Sie besonders stark sind?

Clemens Pohl: Ein weiteres gutes Beispiel ist die Überwachung von Exportkabeln bei Offshore-Windparks. Diese unter dem

Bei der Perimeterüberwachung erkennt faseroptische Sensorik zuverlässig Zaunmanipulationen, Kletterversuche, unbefugte Zutritte sowie Bewegungen an Toren



Meer verlaufenden Kabel sind für die Netzanbindung entscheidend. Kommt es hier zu einem Schaden, sind Reparaturen oft sehr aufwendig. Sie erfordern Spezialschiffe und sind von Wetterfenstern abhängig. Entsprechend wichtig ist es, potenzielle Probleme möglichst früh zu erkennen.

Wir haben in Frankreich mehrere Offshore-Windprojekte mit faseroptischer

Sensorik ausgestattet. Dabei werden unterirdische und submarine Exportkabel kontinuierlich überwacht. Zum Einsatz kommen verteilte Temperaturmessung und verteilte akustische Sensorik.

Die Temperaturmessung hilft, Hotspots frühzeitig zu erkennen. Das ist wichtig, weil sich thermische Auffälligkeiten oft langsam entwickeln. In einem konkreten Fall konnte

ein lokaler Temperaturanstieg über mehrere Wochen erkannt werden. Die Ursache war eine landwirtschaftliche Aktivität oberhalb der Kabeltrasse. Der Betreiber konnte reagieren, bevor daraus ein größeres Problem wurde.

Die akustische Sensorik ergänzt diese Überwachung. Sie erkennt zum Beispiel

Bitte umblättern ▶

Verstecken zwecklos.

Die neuen eneo Hybridkameras sehen, was andere übersehen.

- ➔ Thermal detektieren.
- ➔ Optisch verifizieren.
- ➔ Aktiv abschrecken.

Auch bei völliger Dunkelheit und Tarnung.



a VIDEOR brand



Bauarbeiten oder andere Aktivitäten in der Nähe der Kabelroute. Dadurch erhält der Betreiber ein besseres Lagebild und kann bewerten, ob ein Ereignis kritisch ist oder nicht.

Gerade bei Offshore-Wind zeigt sich sehr gut, wozu es uns geht. Es reicht nicht, eine Anlage erst dann zu betrachten, wenn ein Fehler auftritt. Betreiber brauchen kontinuierliche Echtzeitinformationen über ihre Infrastruktur. Nur so können sie kritische Situationen früh erkennen, Wartung besser planen und die Verfügbarkeit der Netzanbindung sichern.

Auch mit militärischen Anwendungen, d. h. im Bereich Verteidigung bzw. Defence, befassen Sie sich bei AP Sensing. Inwiefern unterscheiden sich zivile von militärischen Anwendungen Ihrer Systeme?

Clemens Pohl: Zu konkreten Projekten oder Kunden im Defence-Bereich können wir uns grundsätzlich nicht äußern. Generell sehen wir ein wachsendes Interesse an faseroptischer Sensorik in sicherheitsrelevanten Anwendungen. Hier spielt die Technologie viele ihrer Vorteile aus. Die Faser ist z. B. komplett passiv, d. h. hier kann kein Jamming, Spoofing oder elektromagnetische Störungen durchgeführt werden.

Die Kabel, in denen die Fasern verlaufen, sind meist sehr robust. Sie könnten nicht nur in staubigen, heißen, kalten, sondern auch in radioaktiven Umgebungen immer noch präzise ihre Aufgaben erfüllen. Darüber hinaus kann so ein Kabel sehr schnell an Zäunen angebracht und in den Boden gepflügt werden.

Grundsätzlich geht es auch im Defence-Bereich um die Überwachung kritischer Infrastrukturen und die frühzeitige Erkennung von Aktivitäten entlang sensibler Bereiche.

Faseroptische Sensorik eignet sich dafür besonders gut, weil mit einer einzigen Glasfaser große Entfernungen überwacht werden können. Die Technologie erkennt beispielsweise Bewegungen, Fahrzeuge oder andere Aktivitäten entlang von Grenzen, militärischen Anlagen oder militärischer Kommunikationsinfrastruktur. Betreiber erhalten dadurch ein kontinuierliches Lagebild in Echtzeit.

Die zugrundeliegende Technologie unterscheidet sich dabei nicht von zivilen Anwendungen. Die physikalischen Prinzipien sind dieselben. Wir messen Temperaturveränderungen, Vibrationen oder akustische Signale entlang einer Glasfaser und werten diese Informationen aus.

Der wesentliche Unterschied liegt in den Anforderungen. Im zivilen Umfeld geht es häufig darum, größere Ereignisse wie Bau-

arbeiten, schleifende Anker oder andere potenzielle Gefährdungen in der Nähe einer Infrastruktur zuverlässig zu erkennen. Im Defence-Bereich stehen dagegen oft deutlich subtilere Aktivitäten im Fokus. Dort kann es beispielsweise darum gehen, sehr kleine Bewegungen oder Eingriffe in der Nähe kritischer Infrastrukturen frühzeitig zu detektieren.

Darüber hinaus ist Interoperabilität im Defence-Umfeld von zentraler Bedeutung. Unsere Systeme arbeiten in der Regel nicht isoliert, sondern werden in umfassende Sicherheits- und Lagebildsysteme integriert. Die Fähigkeit, Daten mit anderen Sensoren und Plattformen auszutauschen und in bestehende Führungs- und Überwachungssysteme einzubinden, ist daher oft genauso wichtig wie die eigentliche Sensorik.

Letztlich verfolgen zivile und militärische Anwendungen aber dasselbe Ziel: Betreiber und Sicherheitsverantwortliche benötigen verlässliche Informationen darüber, was entlang ihrer Infrastruktur passiert. Die Unterschiede liegen vor allem in den Bedrohungsszenarien und den daraus resultierenden Anforderungen an die Detektion und Systemintegration. **GT**



AP Sensing
www.apsensing.com

© Bilder: AP Sensing

Advancis öffnet WinGuard: AOP schafft neue Möglichkeiten

Die Advancis Software & Services GmbH präsentiert auf der Security Essen ihre Lösungen für integriertes Sicherheits-, Gebäude- und Identitätsmanagement. Im Mittelpunkt des Messeauftritts stehen die Softwareplattformen WinGuard, AIM (Advanced Identity Manager) sowie der offizielle Marktstart der neuen Advancis Open Platform (AOP). Auf dem Advancis Messestand erhalten Fachbesucher umfassende Einblicke in die neuesten Entwicklungen im integrierten Sicherheits- und Gebäudemanagement. Im Mittelpunkt stehen dabei die beiden Kernlösungen AIM und WinGuard. Mit dem Advanced Identity Manager (AIM) präsentiert das Unternehmen eine leistungsstarke Plattform für Physical Identity & Access Management (PIAM). Die Lösung zentralisiert die Verwaltung von Identitäten, Zutrittsrechten, Besuchern, Fremdfirmen und Genehmigungsprozessen in einer einheitlichen Anwendung. www.advancis.net

Security Essen: Halle 8, Stand 8A15/8B15



Advancis CEO und Co-Founder Jan Meiswinkel

Dallmeier erweitert Softwarewartung auf bis zu zehn Jahre

Dallmeier erweitert sein Angebot für Softwarewartung und bietet ein zusätzliches Wartungspaket für Kameras und Recorder an. Kunden können ihre Videosicherheitssysteme damit bis zu zehn Jahre aktuell halten und profitieren von langfristiger Investitions- und Planungssicherheit. Mehr Sicherheit und Planbarkeit über den gesamten Lebenszyklus. Gerade öffentliche Auftraggeber, Betreiber kritischer Infrastrukturen und Unternehmen mit langfristigen Investitionszyklen legen zunehmend Wert auf verlässliche Planungssicherheit. Mit dem neuen Wartungspaket können Anwender die Softwarewartung um weitere fünf Jahre verlängern und sich so langfristig gegen Sicherheitsrisiken absichern. Das neue Wartungspaket ist für Panomera Systeme, Single-Sensor Kameras sowie Recorder verfügbar. Für Kameras sind bereits heute fünf Jahre Softwarewartung im Lieferumfang enthalten – durch das neue Paket lässt sich dieser Zeitraum auf insgesamt zehn Jahre erweitern. www.dallmeier.com



Bequem auf dem Sofa durch die e-Ausgabe der **GIT SICHERHEIT** blättern: Registrieren Sie sich auf www.git-sicherheit.de/newsletter

Assa Abloy auf der Security Essen 2026

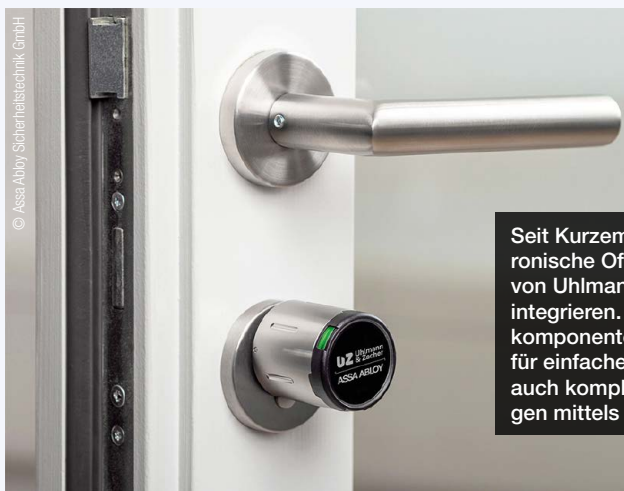
Assa Abloy Sicherheitstechnik GmbH, GfS – Gesellschaft für Sicherheitstechnik mbH und Uhlmann & Zacher präsentieren auf ihrem Messestand auf der Security Essen innovative Produkte und zukunftsfähige Systemlösungen im Bereich digitaler Schließtechnik, Zutrittskontrolle und Fluchtwegsicherung. Auch präsent ist am Stand Traka Deutschland, die über ihre KRITIS-spezifischen Sicherheitslösungen informieren.

Ein besonderes Highlight erwartet die Besucher: Assa Abloy stellt vor Ort eine wegweisende Innovation für das elektronische Schließsystem eCliq vor. Details werden erst auf der Messe enthüllt.

Neu ist die Integration der Offline-Komponenten der Marke Clex public von Uhlmann & Zacher. Die kabellosen, batteriebetriebenen Lösungen eignen sich besonders für Nachrüstungen im Gebäudebestand und erweitern das System um zusätzliche Einsatzmöglichkeiten für Türen, Möbel und andere sensible Bereiche.

Aperio DR100

Mit dem Aperio DR100 erweitert Assa Abloy sein Portfolio digitaler Zutrittslösungen um einen Kartenleser mit integrierten Relais für anspruchsvolle Tür- und Zugangssituationen – etwa an



Seit Kurzem lassen sich auch elektronische Offline-Türkomponenten von Uhlmann & Zacher in Scala net integrieren. Die Clex public Schließkomponenten eignen sich besonders für einfache Nachrüstungen, die auch komplett schlüssellose Öffnungen mittels Transponder erlauben

Neue Cliq Leser und Updater

Die neuen Cliq Leser für den Innen- und Außenbereich sowie der neue Cliq Updater bieten neuen Komfort im eCliq-Schließanlagen-Produktportfolio. Sie ermöglichen die sichere Ansteuerung von Drittgeräten wie Türöffnern, Schranken oder Motorschlössern und lassen sich vollständig in bestehende Cliq-Schließanlagen integrieren. Der neue Cliq Updater aktualisiert Schlüsseldaten komfortabel über eine RS-485-Verbindung – ganz ohne Netzkabel im Außenbereich – und eignet sich dadurch besonders für Nachrüstungen und dezentrale Anwendungen.

Zutrittskontrolle Scala mit Uhlmann & Zacher Integration

Scala net ermöglicht eine vernetzte Zutrittskontrolle mit umfassenden Funktionen wie Zeitsteuerung, Zonenüberwachung oder Aufzugsintegration. Dank des modularen Lizenzmodells lässt sich das System flexibel an wachsende Anforderungen anpassen und unterstützt gängige RFID-Technologien sowie den offenen OSS Standard Offline.

Haupteingängen, Drehsperrern, Toren oder Ladezonen. Die Lösung unterstützt sowohl Online- als auch Offline-Anwendungen und ermöglicht dank der bewährten drahtlosen Aperio-Technologie eine besonders flexible Nachrüstung und Systemerweiterung bestehender Zutrittskontrollsysteme.

GfS Türwächter Go – vernetzte Fluchtwegsicherung

Mit dem Türwächter Go gibt GfS auf der Security Essen einen Ausblick auf die nächste Generation der Fluchtwegsicherung. Die neue Lösung ergänzt den bewährten GfS Türwächter um moderne IoT-Funktionalitäten und ermöglicht unter anderem die mobile Benachrichtigung bei Ereignissen sowie eine automatische Dokumentation mit Zeit- und Standortinformationen. Dank Mobilfunkanbindung können die angebundenen Flucht- und Rettungstüren standortunabhängig überwacht werden. Das modulare Konzept eröffnet zudem Perspektiven für den Einsatz der IoT-Technologie in weiteren GfS Produkten.

www.assaabloy.com/de

Security Essen: Halle 6, Stand C23

FORTLOX
Simply secure



Digitale
Schließlösungen
für Gemeinden,
Städte & Stadtwerke



Mehr Informationen



Dipl.-Ing. Carsten Feddern,
Geschäftsführer VfS

Dipl.-Ing. Matthias Demmel, Geschäftsführer
Prüfzentrum für Bauelemente (PfB)

ZAUNSICHERHEIT

Übersteigen, Durchdringen, Untergraben

Bewertung der Widerstandsfähigkeit von Zaunanlagen

Die Absicherung Kritischer Infrastrukturen erfordert belastbare Perimeter. Für das KRITIS-Dachgesetz werden dokumentierte Widerstandszeiten nötig, um Bestandsanlagen gezielt zu ertüchtigen und sicher zu planen. Der Verband für Sicherheitstechnik und das Prüfzentrum befassen sich vor diesem Hintergrund mit der Entwicklung einer neuen Prüfleitlinie zur Bewertung der Widerstandsfähigkeit von Zaunanlagen. Ein Gespräch mit Dipl.-Ing. Carsten Feddern, Geschäftsführer VfS, und Dipl.-Ing. Matthias Demmel, Geschäftsführer Prüfzentrum für Bauelemente (PfB).

Herr Feddern, was war der Anlass für die Entwicklung einer neuen Prüfleitlinie zur Bewertung der Widerstandsfähigkeit von Zaunanlagen?

Carsten Feddern: In unseren Arbeitskreisen kam immer wieder die Diskussion auf, dass es bislang aufgrund fehlender oder lückenhafter Regulierungen schwergefallen ist, die mechanische Widerstandsfähigkeit und damit die Widerstandszeit einer Perimeterabsicherung (Zaun) zu bestimmen. Gemeinsam mit unserem VfS Beiratsmitglied Matthias Demmel, dem Geschäftsführer des Prüfzentrums für Bauelemente (PfB) aus Rosenheim, ist die Idee für diese Prüfleitlinie entstanden. Insbesondere vor dem Hintergrund der Absicherung Kritischer Infrastrukturen schien uns dieses Thema von zentraler Bedeutung, um entsprechende, zumeist unzureichend

dokumentierte, Bestandsanlagen sinnvoll und angemessen zu ertüchtigen. Spätestens für die Umsetzung des KRITIS-Dachgesetzes werden Widerstandszeiten für Perimeter zur Planung, Ausschreibung und Umsetzung benötigt.

Welche sicherheitsrelevanten Lücken bestehen derzeit im Bereich Perimeter-schutz, die durch bestehende Normen und Regelwerke noch nicht ausreichend abgedeckt sind?

Carsten Feddern: Ganz konkret fehlen Vorgaben zur Widerstandsermittlung gegen Übersteigen, Prüfwerkzeugsatz für Zäune in der Fläche, Vorgaben zur Widerstandsermittlung gegen Untergraben, Widerstandszeiten sowie entsprechende Vorgaben von Widerstandsklassen.

Herr Demmel, wie funktioniert die geplante Prüfung konkret? Welche Angriffsszenarien werden getestet und nach welchen Kriterien bewertet?

Matthias Demmel: Bei dem Entwurf einer Prüfrichtlinie haben wir bewährte Prüfsequenzen aus der Prüfung der Einbruchhemmung von Gitterelementen als Basis herangezogen und auf die speziellen Anforderungen der Zäune adaptiert und erweitert. Es findet eine statische Prüfung gemäß DIN EN 1628, Produktgruppe 4 (Gitter) mit einer speziellen Belastung der Pfosten an den freien Enden statt. Hier wird der Widerstand gegen Umlegen oder Aufspreizen eines Zaunes nachgewiesen. Es erfolgt eine dynamische Prüfung gemäß der EN 1629, jedoch mit einer Belastung von beiden Zaunseiten in allen Widerstandsklassen, um

sowohl ein mehrfaches Anspringen, Anstoßen aber auch ein Rütteln an den Zäunen abzutesten.

Der „manuelle“ Angriff erfolgt sowohl in der Fläche mit bewährten aber anders kategorisierten Werkzeugen der EN 1630, als auch mit dem Versuch des Übersteigens und Untergrabens. Dazu kommen den Widerstandsklassen entsprechende Hilfsmittel zum Einsatz: Für das Übersteigen z. B. Seil, Leiter und Teppich, für das Untergraben Klappspaten, Schaufel, Hacke und Akku-Erdbohrer). Kategorisiert wird getrennt das Übersteigen, Durchsteigen und Untergraben jeweils für drei täterspezifische Widerstandsklassen und 5 Widerstandszeiten: N für keine erreichte Widerstandszeit oder ein statisches bzw. dynamisches Versagen sowie 2, 3, 5 und 10 Minuten Widerstandszeit. Die Klassifizierung erfolgt somit zweckmäßigerweise in einer Matrix und bietet damit ein Spektrum der Widerstandswerte.

Welche Rolle spielen reale Vorfälle – etwa unbefugtes Eindringen auf Flughafengelände für die Entwicklung praxisnaher Prüfverfahren?

Matthias Demmel: Die medienwirksamen Vorfälle an den Flughäfen mit der Startbahnbesetzung, den lahmgelegten Trafostationen und einigen weiteren Fällen waren ausschlaggebend auch im Hinblick auf das KRITIS-DACH-Gesetz, die mechanische Sicherheit von Perimetern und spezifischer Vorgaben zu hinterfragen. Das Ergebnis war, dass es zum einen vereinzelte Prüfkationen einzelner Betreiber gab, zum anderen auf eine britische Norm für einbruchhemmende Elemente zurückgegriffen wurde, die



Der Versuch des Übersteigens ist der Klassiker der versuchten Zaunüberwindung

aber nicht das gesamte Anforderungsprofil der Zäune abdeckt, im wesentlichen nur den Angriff in der Fläche. Somit war die Entwicklung einer zaunspezifischen Richtlinie für den mechanischen Widerstand, die sowohl vom Hersteller zur Entwicklung und Optimierung der Zaunaufbauten als auch dem Betreiber kritischer Infrastruktur für

die Standortbestimmung und Ertüchtigung vor Ort dient, die logische Konsequenz.

Inwiefern unterscheidet sich Ihre Prüfleitlinie von klassischen Normen oder Zertifizierungen, und welchen Mehrwert bietet sie insbesondere für Betreiber kritischer Infrastrukturen?

Bitte umblättern ▶

PROUDLY
KOREAN

VGA KI-Wärmebildkameras mit Teleobjektiv

<16mK Wärmebildpräzision in jeder Umgebung

Hanwha
Vision



Fahrzeug



Person



Schiff



Schiff



Schon bald können Sie die Kamera live in unserem neuen Frankfurter Büro und Showroom besichtigen.



Person

Simuliertes Bild, keine echte Kameraaufnahme.



Viele Werkzeuge – ein Ziel:
Den Zaun zu durchschneiden

Matthias Demmel: Die Richtlinie wurde mit den Merkmalen einer Norm geschrieben, um im Falle einer gewünschten Überführung zu einer DIN TS nicht Zeit für die strukturelle Umarbeitung zu verlieren. Sie basiert auch auf dem Normenwerk der EN 1627 bis EN 1630, um auf Bekanntes zurückzugreifen, damit eine Einordnung für den Betreiber leichter möglich ist. Die Richtlinie wurde aufgrund der Lücke eines Nachweisverfahrens für den mechanischen Widerstand von Zäunen geschrieben, da Zäune nicht im Anwendungsbereich der EN 1627 einbruchhemmender Elemente aufgeführt sind.

Die Richtlinie wurde aus der langjährigen Erfahrung mit einbruchhemmenden Produkten aller Art und der Erfahrung in der Normungsarbeit in unserem Hause (Richtlinie für einbruchhemmende Rollläden und DIN 18106 für Gitter, jetzt jeweils implementiert in die EN 1627 der DIN 18104-1 und -2 für einbruchhemmende Nachrüstprodukte) als Entwurf erstellt, um ohne Verzögerung zum Start des KRITIS-Dachgesetzes eine erste Grundlage zur Bewertung des manuellen Widerstandes von Zäunen vorliegen zu haben und diese zur Erprobung und Diskussion zu stellen.

Eine Zertifizierung benötigt ein die Prüfgrundlage ergänzendes freiwilliges Zertifizierungsprogramm. Das stützt der Prüfgrundlage üblicherweise eine regelmäßige Überwachung der Produktherstellung über. Somit ist die Zertifizierung eine Ergänzung zum Prüfnachweis, die aber erst nach der

Umsetzung des Prüfprogramms als Pfb-Richtlinie erfolgen kann.

Welche Erkenntnisse ergaben sich aus den Praxistests im April – und wie sollen diese Ergebnisse in die Weiterentwicklung der Leitlinie einfließen?

Matthias Demmel: Beim ersten Schreiben einer Richtlinie bleiben erfahrungsgemäß Details unberücksichtigt, die sich bei der Anwendung herausstellen. So zum Beispiel zeigte sich bei der Auswahl der Werkzeuge, dass die Verwendung der elektrischen Gartenschere nicht effektiver als der Bolzenschneider ist und somit aus dem Werkzeugsatz gestrichen werden kann. Beim Übersteigen waren Gewindestangen und Klebeband effektiver als Haken. Das Mitnehmen von Werkzeug beim Übersteigen muss zudem geregelt werden. Diese und weitere Erfahrungen werden wir kurzfristig in einen zweiten Entwurf einarbeiten.

Herr Feddern, welche Folgen hat das KRITIS-Dachgesetz für den Perimeterschutz? Und wie hilft Ihre Initiative dabei, die dort formulierten Anforderungen in die Praxis zu übersetzen?

Carsten Feddern: Im Bereich der Standortsicherheit für Kritische Infrastrukturen ist der Perimeterschutz ja sozusagen die erste physische Verteidigungslinie. Vor diesem Hintergrund kommt dem Perimeterschutz in der aktuellen Bedrohungslage

eine außerordentlich hohe Bedeutung zu. Die Komplexität durch Mechanik, Elektronik sowie organisatorischen und personellen Maßnahmen machen den Perimeterschutz zur zentralen Aufgabenstellung für die physische Sicherheit, deren Ertüchtigung das KRITIS-Dachgesetz fordert. Mit der Prüflinie gibt es aus unserer Sicht einen klaren Praxisbezug auf die in §13 des Gesetzes geforderte Angemessenheit der erforderlichen Maßnahmen.

Herr Demmel, sehen Sie perspektivisch die Entwicklung hin zu einer verbindlichen Norm oder sogar einer Zertifizierung – und welche Schritte sind dafür noch notwendig?

Matthias Demmel: Der Entwurf der Pfb-Richtlinie stellt einen ersten Schritt dar. Der überarbeitete Entwurf wird zur Diskussion in den entsprechenden Arbeitskreisen des Vfs und der Perimeterhersteller gestellt, damit voraussichtlich zum Ende des Jahres eine validierte Prüfrichtlinie zur Verfügung steht. Die Entscheidung über ein Normverfahren obliegt dem DIN. Eine entsprechende Anfrage werden wir, sofern er vom Arbeitskreis des Vfs und den Perimeterherstellern in Ergänzung zum Validierungsprozess der Pfb-Richtlinie befürwortet wird, gerne beim DIN einbringen. Sofern das entsprechende Normengremium dann ein Normungsverfahren befürwortet und dieses beim DIN bestätigt wird, werden wir die Richtlinie dafür gerne zur Verfügung stellen.

Eine Zertifizierung ist ein zusätzliches freiwilliges Verfahren auf Basis eines Zertifizierungsprogrammes. Hier spielt es keine Rolle, ob eine in Fachkreisen validierten Richtlinie oder einer Norm als Basis herangezogen wird. Ein verpflichtendes Zertifizierungsverfahren wie bei Brand- und Rauchschutzelementen auf Basis der MVVTB bzw. der BauPVO mit einem zugeordneten System wird es für den mechanischen Widerstand gegen Angreifer bei Zäunen nicht geben, da die Eigenschaft Security nicht bauaufsichtlich gefordert ist. **GIT**



Verband für Sicherheitstechnik (Vfs)
www.vfs-hh.de

Prüfzentrum für Bauelemente (Pfb)
www.pfb-rosenheim.de



„Protect what matters“: Keba auf der Security Essen 2026

Nach mehreren Jahren ist Keba wieder auf der Security Essen vertreten. Unter dem Leitgedanken „Protect what matters“ zeigt das Unternehmen in Essen Lösungen für sichere Verwahrung, berechtigten 24/7-Zugriff und lückenlose Nachvollziehbarkeit von sicherheitskritischen Assets. Im Mittelpunkt des Messeauftritts stehen automatisierte Übergabe- und Zugriffssysteme für Militär, Polizei, kritische Infrastrukturen, öffentliche Verwaltung, Sicherheitsdienstleister und Industrie. Keba zeigt, wie unterschiedliche Assets zentral verwahrt, gesteuert und bei Bedarf rund um die Uhr an berechtigte Personen ausgegeben und bei Bedarf auch wieder zurückgegeben werden können. Die Kombination aus Depotsystemen, Identifikation, Berechtigungsmanagement und Software sorgt dafür, dass sensible Objekte verfügbar bleiben, ohne die Kontrolle über Ausgabe, Rückgabe und Nutzung zu verlieren. Jede Übergabe wird transparent dokumentiert und kann nachvollzogen werden.

www.keba.com

Security Essen: Halle 6, Stand E36

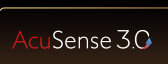
Kamera mit Global-Shutter-Technologie

Axis Communications bringt mit der Axis P1486-LE Global Shutter Camera die erste Axis-Netzwerkamera auf den Markt, die mit Global-Shutter-Technologie ausgestattet ist. Die Global-Shutter-Technologie erfasst das gesamte Bild in einem einzigen Moment synchron, indem sie alle Pixelinformationen des Sensors gleichzeitig ausliest. Auf diese Weise werden selbst bei sehr schnellen Bewegungen – zum Beispiel bei vorbeifahrenden Fahrzeugen – Bewegungsunschärfen vermieden und präzisere Ergebnisse erzielt. Die Axis P1486-LE Global Shutter Camera ist mit einem lichtempfindlichen 1/1.8-Zoll-CMOS-Sensor (Complementary Metal-Oxide Semiconductor) mit Global-Shutter-Technologie ausgestattet. Zusätzlich hat sie eine integrierte und konstante stroboskopische Infrarot-Beleuchtung sowie ein 10–40-Millimeter-Teleobjektiv mit einem horizontalen Sichtfeld von 44 bis 11 Grad. www.axis.com



PRO SERIE MINI-PTRZ-DOME-KAMERAS

Die Dome-Revolution neu definiert – kleine und erschwingliche PTRZ



Kompatibel mit
Licht-Schienensystem



2,8/4 mm Point-to-Point-Zoom

HIKVISION

Jeder Kilometer sicher im Blick



EchoPoint von OPTEX überzeugt im Praxistest mit präziser faseroptischer Detektion und intelligenter Ereignisklassifizierung

Viele Kilometer lange Perimeter gehören zu den anspruchsvollsten Aufgaben moderner Sicherheitstechnik. Auf dem Testgelände von Optex untersuchte GIT SICHERHEIT gemeinsam mit dem Sachverständigen für Sicherheitstechnik Markus Piendl, wie sich mit Distributed Acoustic Sensing, kurz DAS, und dem faseroptischen Detektionssystem EchoPoint Ereignisse über viele Kilometer hinweg per Glasfaserkabel erkennen, lokalisieren und klassifizieren lassen.

Die japanische Optex Group entwickelt seit vielen Jahrzehnten intelligente Sensorik für unterschiedliche Anwendungsbereiche. Zum Portfolio gehören passive Infrarotsensoren, aktive Infrarot-Lichtschranken, LiDAR-Systeme der Redscan-Serie sowie die faseroptischen Lösungen der Tochtergesellschaft Fiber SenSys. Die unterschiedlichen Sensortechnologien lassen sich zu mehrschichtigen Sicherheitskonzepten verbinden.

EchoPoint steht heute im Mittelpunkt dieses GIT-Testberichts. Es übernimmt innerhalb dieses Portfolios die Aufgabe, weitläu-

fige Infrastrukturen über viele Kilometer hinweg kontinuierlich zu überwachen.

Praxis statt Prospekt

Vor Ort auf einem der professionell ausgestatteten Optex-Testgelände. Schon beim Betreten wird deutlich: Stresstest statt Showroom – oder eben Praxis statt Prospekt. Zwischen Zaunanlagen, erdverlegten Glasfasern und unterschiedlichen Versuchsfeldern wird unter realitätsnahen Bedingungen getestet, wie sich DAS im harten, praktischen Einsatz verhält.

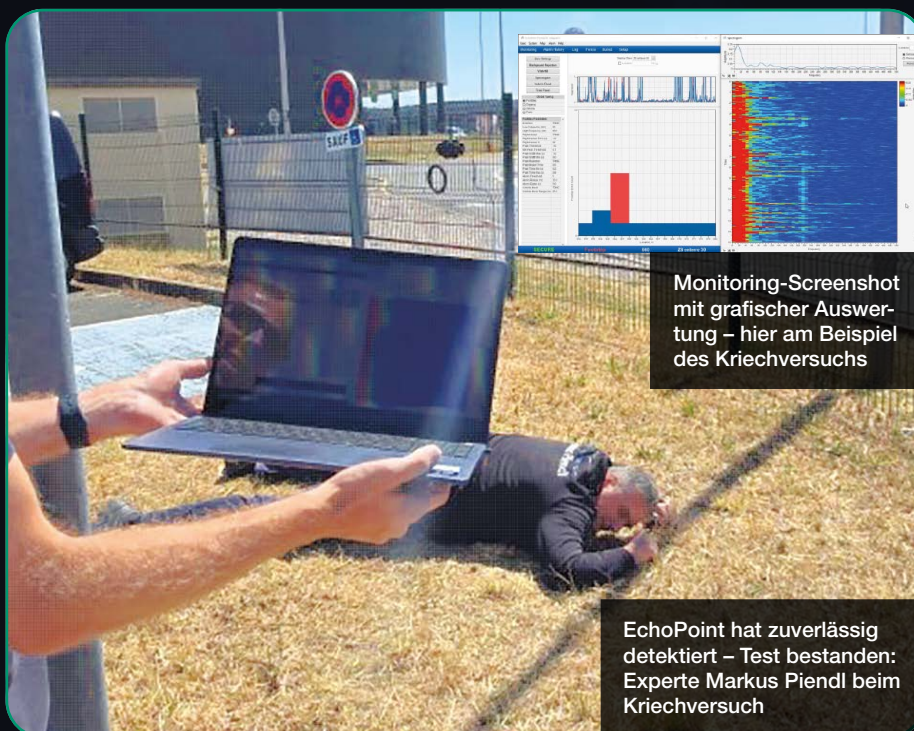
Statt einer klassischen Produktpräsentation erhielt Experte Markus Piendl also einen detaillierten Einblick in Planung, Installation und Inbetriebnahme von EchoPoint. Nach einer technischen Einweisung zu Systemarchitektur, Detektionszonen und Alarmmanagement konnten eigene Fragestellungen direkt auf dem Testgelände untersucht werden. Dabei wurden sowohl die Zaunsensorik als auch die Bodendetektion unter realistischen Bedingungen geprüft.

Aurélien Martin, Technical Pre-Sales Engineer, erläutert zunächst das Grundprinzip der Technologie. Bei Distributed Acoustic Sensing (DAS) dient ein Glasfaserkabel als durchgängiges Sensorelement. Mechanische und akustische Einwirkungen entlang der überwachten Strecke verändern das in der Faser zurückgestreute Licht. Das Perimeterschutz-System EchoPoint wertet diese Veränderungen aus, ordnet sie einem Ereignisort zu und unterstützt die Klassifizierung unterschiedlicher Ereignisarten.

Vorteil: Befestigung am Zaun, im Erdreich und hybrid

Und EchoPoint überzeugt Markus Piendl direkt beim Start in die Test-Szenarien. Denn eine besondere Stärke liege in der flexiblen Installation. Das EchoPoint-Sensorkabel kann je nach örtlichen Bedingungen am Zaun befestigt, im Erdreich verlegt oder innerhalb eines Projekts in einer hybriden Ausführung aus beiden Montagearten eingesetzt werden. „Ein großer Vorteil bei Projekten in der Praxis!“, so der Experte. Pluspunkt.

Was zudem für das System spricht: Glasfaser ist vollständig passiv. Entlang der überwachten Strecke befinden sich keine aktiven



Monitoring-Screenshot mit grafischer Auswertung – hier am Beispiel des Kriechversuchs

EchoPoint hat zuverlässig detektiert – Test bestanden: Experte Markus Piendl beim Kriechversuch

elektronischen Komponenten. Dadurch eignet sich die Technologie, wie Piendl konstatiert, besonders für Anwendungen mit hohen Anforderungen an Zuverlässigkeit, elektromagnetische Verträglichkeit und Blitzfestigkeit. Weiterer Pluspunkt im Testprotokoll.

Im Verlauf des Tests bescheinigt Markus Piendl dem Technical Director bei Optex, Geoffrey Michaud, einen weiteren Vorteil in der kontinuierlichen Überwachung langer Strecken. EchoPoint ermöglicht die Bildung virtueller Detektionszonen und lokalisiert Ereignisse entlang der Sensorfaser mit einer Herstellerangabe von plus/minus 6 Metern. Durch die Zuordnung des Faserverlaufs zu geografischen Positionsdaten lassen sich Alarmmeldungen mit GPS-Koordinaten verknüpfen und auf einer Lagekarte darstellen.

Die Integration in Video-Management-, PSIM- und Leitstellensysteme unterstützt anschließend die gezielte Verifikation und Bearbeitung des Ereignisses. Je nach Systemkonfiguration kann die Überwachung zudem ausfalltolerant oder redundant aufgebaut werden. Noch ein Positiv-Haken in der Checkliste von Tester Piendl.

Intelligente Ereignisklassifizierung

Ein wesentlicher Unterschied zu klassischen Perimetersystemen besteht laut Markus



Test: Empfindlichkeitseinstellungen

Piendl darin, dass Distributed Acoustic Sensing nicht nur feststellt, dass ein Ereignis stattfindet, sondern dass es auch die charakteristischen Schwingungsmuster entlang der Glasfaser analysiert. Unterschiedliche Einwirkungen – beispielsweise Schritte,



Test: Übersteigen mit Leiter und Decke

Fahrzeugbewegungen, Grabungsarbeiten oder Manipulationen an einem Zaun – erzeugen jeweils eigene akustische Signaturen. Dadurch gewinnt die Detektion deutlich an Aussagekraft.

Bitte umblättern ►



Mit EchoPoint überwacht Optex große Perimeter wie Flughäfen oder Industrieanlagen und lokalisiert Eindringversuche präzise entlang der gesamten Zaulinie



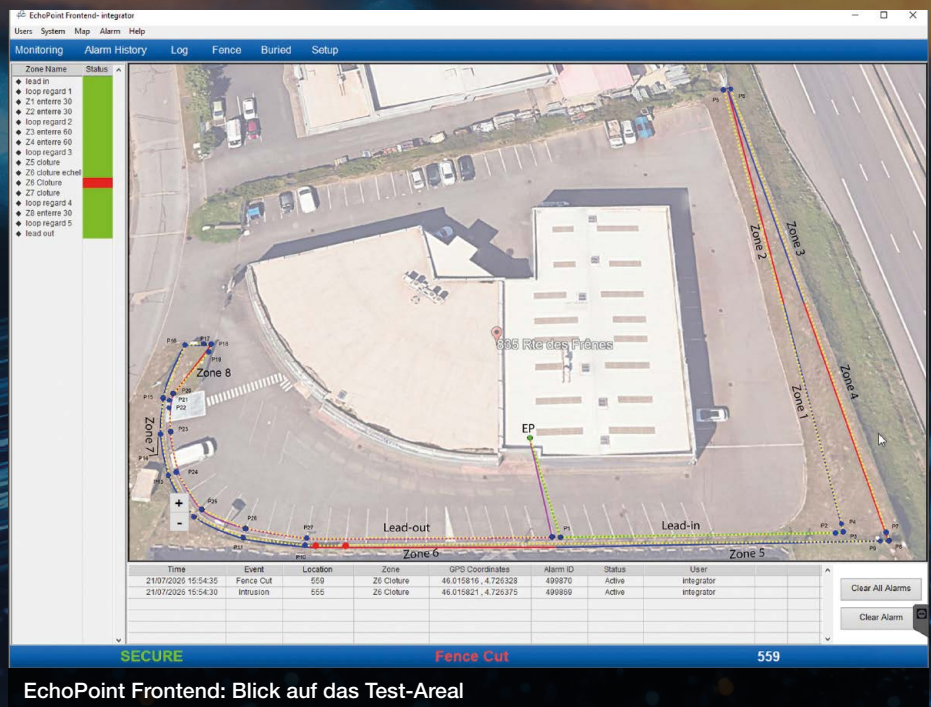
Trumpf im Test: EchoPoint wertet diese Signaturen kontinuierlich aus, ordnet sie einem Ereignisort zu und klassifiziert sie entsprechend ihrer Charakteristik. Dadurch erhält der Sicherheitsverantwortliche neben der Positionsmeldung eine erste Einschätzung, welche Art von Ereignis wahrscheinlich vorliegt.

Dies wiederum erleichtert die Bewertung der Situation und ermöglicht eine schnellere Reaktion. In Kombination mit einer Videoverifikation entsteht ein mehrstufiges Sicherheitskonzept: Die Glasfaser übernimmt die Detektion, während Kameras oder weitere Sensoren das Ereignis bestätigen. Ergebnis: die Nuisance Alarm Rate (NAR) ist reduziert, Einsatzkräfte können gezielter eingesetzt werden.

Ergebnisse und Erkenntnisse

Der Verlauf des Prüfprogramms zeigt es: Experte Piendl ist rundum zufrieden.

- EchoPoint erkannte sämtliche vorbereiteten Angriffsszenarien sowohl an der zaunmontierten als auch an der erdverlegten Sensorstrecke zuverlässig.
- Voralarme, Hauptalarme und Sabotagemeldungen ließen sich in Echtzeit nachvollziehen und den jeweiligen Ereignissen zuordnen.
- Die Auswirkungen veränderter Parametrierungen konnten unmittelbar beobachtet werden.



EchoPoint Frontend: Blick auf das Test-Areal

Die von EchoPoint gemeldeten Ereignispositionen wurden mit den GPS-Koordinaten der Testpunkte abgeglichen. Parallel dazu ermöglichte die Videoverifikation die visuelle Bestätigung der Ereignisse. Fazit: Auch in dieser Hinsicht vollumfänglich bestanden.

Die Anbindung an die Management-Software Milestone XProtect führte anschaulich vor, wie sich Detektion, Verifikation und Alarmbearbeitung sinnvoll miteinander

verbinden lassen – mit EchoPoint als zentralem Baustein.

Mehrwert über den Test hinaus

Rick Wakeham, als Senior Technology Manager EMEA bei Optex ebenfalls Zeuge des unabhängigen Tests, bestätigt Piendl's Einschätzung zur Robustheit faseroptischer Detektion bei weitläufigen Perimetern sowie die kontinuierliche Überwachung großer Schutzstrecken: „Gerade in Zeiten zuneh-

Das Prüfprogramm für EchoPoint

Auf dem Testgelände wurden sowohl die zaunmontierte als auch die erdverlegte Ausführung praktisch untersucht. Die Versuche wurden bei trockenem, wolkenlosem Wetter, einer Temperatur von 28 °C und mäßigem Wind mehrfach durchgeführt. Das Prüfprogramm umfasste folgende Punkte:

Zaundetektion

- Installation und Projektierung der Sensorik
- Parametrierung der Detektionszonen
- Übersteigen des Zauns
- Leiteranstellung, unter anderem mit einer Decke als dämpfender Auflage
- Aufhebeln und Durchtrennen des Zaungeflechts
- Bewertung des Alarmverhaltens

Vollumfänglich bestanden

Bodendetektion

- Gehen entlang der überwachten Strecke
- Laufen im Detektionsbereich
- Kriechen im Detektionsbereich
- Rollende Fortbewegung im Detektionsbereich
- Veränderung der Empfindlichkeit
- Analyse von Vor- und Hauptalarmen
- Bewertung der Lokalisierungsgenauigkeit

Vollumfänglich bestanden

Systemintegration

- Live-Darstellung der Sensordaten
- Videoverifikation
- Alarmbearbeitung
- Integration in Milestone XProtect
- Abgleich der gemeldeten Ereignispositionen mit den GPS-Koordinaten der Testpunkte

Vollumfänglich bestanden



Test: Eingelassene Bodensensorik



Sachverständigenbewertung

Empfehlung für EchoPoint

Laut Markus Piendl hat EchoPoint von Optex alle Testszenarien mit Bravour bestanden. Auch das Testgelände selbst fiel positiv auf, zudem die praxiserichte Installation der EchoPoint-Technologie und die Möglichkeit, eigene Angriffsszenarien unter realistischen Bedingungen durchzuführen. Das ausführliche Urteil des Experten: „EchoPoint reagierte auf alle geprüften Angriffsszenarien nachvollziehbar und zuverlässig. Besonders hilfreich war die Möglichkeit, Voralarme, Hauptalarme und Sabotagemeldungen in Echtzeit zu verfolgen und die gemeldeten Ereignispositionen mit den GPS-Koordinaten der Testpunkte abzugleichen. Die flexible Montage am Zaun, im Erdreich oder als Hybridlösung eröffnet vielfältige Einsatzmöglichkeiten an weitläufigen Perimetern und bietet Infrastruktur-Vorteile. In Verbindung mit der Videoverifikation und dem Video-Management entstand ein vollständiger und praxisnaher Alarmbearbeitungsprozess. Abschließendes Ergebnis und Urteil: EchoPoint gilt für mich als klare Empfehlung für Perimeterschutz-Projekte.“

mender Extremwetterereignisse gewinnen Themen wie Blitz- und Überspannungsschutz immer mehr an Bedeutung. Glasfaserbasierte Systeme bieten hier aufgrund ihres physikalischen Aufbaus entscheidende Vorteile gegenüber konventionellen Sensorlösungen.“

Nützlicher Nebeneffekt der Tests im Sinne der Optex-Kunden: Wakeham zeigte sich insbesondere am Vorschlag Piendl interessiert, Logdateien künftig mithilfe künstlicher Intelligenz automatisiert auszuwerten. Ziel könnte es sein, Errichter

bereits während der Inbetriebnahme bei der Optimierung der Parametrierung und bei der Fehlersuche zu unterstützen.

Auch die Anregung Piendls, Architekten und Fachplaner schon frühzeitig für die Möglichkeiten faseroptischer Bodendetektion zu sensibilisieren, stieß auf Interesse und Zustimmung. Piendl: „Gerade bei schützenswerten Bereichen und Geländen ist es wichtig, bereits in der Planungsphase berücksichtigt zu werden, um einen zusätzlichen Sicherheitsgewinn zu ermöglichen.“ **GIT**

Demnächst
in GIT SICHERHEIT

EchoPoint überzeugt im Test

Die Technologie im Detail



Optex

www.optex-europe.com

**Sachverständigenbüro
Markus Piendl**

www.markuspiendl.com

© Bilder: SMP / OPTEX / GIT SICHERHEIT

Mehr Sicherheit weniger Routine



Robotik & KI Software Spezialist

Mehrwert durch
integrale Vernetzung
intelligenter
Robotersysteme





**TITEL
THEMA**



Es geht auch ohne Smartphone

Assa Abloy stellt ersten Schlüssel mit integrierter Mobilfunkverbindung vor

Mit dem eCliq Flash der Marke Ikon schließt Assa Abloy eine der letzten Medienlücken elektronischer Schließsysteme: Der neue eCliq-Schlüssel ruft Berechtigungen selbst über Mobilfunk ab – ohne Smartphone.

■ Wer 100 wird, darf zurückblicken. Die Traditionsmarke Ikon blickt im Jubiläumsjahr 2026 lieber nach vorn und präsentiert eine Lösung für einen entscheidenden Engpass elektronischer Schließsysteme: Als weltweit erster Schlüssel kommuniziert der Flash direkt über Narrowband Internet of Things (NB-IoT) und Long Term Evolution for Machines (LTE-M) mit der Cloud. Neue Schließberechtigungen gelangen so aus dem Cliq Web Manager unmittelbar auf den Schlüssel.

Wie relevant das im Alltag ist, zeigt eine für Servicetechniker und Facility Manager typische Situation: Bereits auf dem Weg zu einem Objekt trifft die Nachricht ein, dass noch bei einem weiteren Standort nach dem Rechten zu sehen ist. Die passende Berechtigung dafür fehlt jedoch. Bislang hieß das: einen stationären Updater anfahren oder ein Smartphone als Schnittstelle nutzen. Steht beides nicht zur Verfügung, wird aus einem Zusatzauftrag schnell eine zusätzliche Fahrt. Mit dem Flash genügt

dagegen ein Knopfdruck, um die digitalen Schließrechte zu aktualisieren.

Die Berechtigung kommt zum Schlüssel

Damit dreht Ikon das bisherige Prinzip beim Flash um: Nicht mehr der Schlüssel muss zum Updater, sondern die Berechtigung kommt zum Schlüssel. Das ist mehr als ein Komfortgewinn. Speziell bei externen Dienstleistern stoßen smartphonebasierte Verfahren an organisatorische und



Flash ergänzt die vorhandenen Schlüsselvarianten und lässt sich mit unterschiedlichen Zylinderbauformen im Mischbetrieb einsetzen

technische Grenzen. Nicht jeder verfügt über ein geeignetes Firmenhandy, private Geräte sind häufig ausgeschlossen und IT-Richtlinien können App-Installationen verhindern. Hinzu kommen unterschiedliche Betriebssysteme und Softwareversionen bei den Nutzern.

Flash vereinfacht die Handhabung an dieser Stelle. Die Kommunikationskette führt direkt vom Schlüssel über Mobilfunk zur Cloud bis hin zum Cliq Web Manager. In der browserbasierten Software verwalten Administratoren die Schließanlage standortunabhängig, vergeben Schließberechtigungen und protokollieren Ereignisse. Das macht Updates und Validierungsprozesse

nicht nur sicherer, sondern auch effizienter: Je weniger Endgeräte beteiligt sind, desto weniger Aufwand ist für Einrichtung, Einweisung und Fehleranalyse erforderlich.

Stets erreichbar

Die direkte Verbindung zum Mobilfunknetz baut der Flash über NB-IoT und LTE-M auf. Beide Standards sind für vernetzte Geräte mit geringem Energiebedarf ausgelegt und ergänzen sich bei Reichweite und Verfügbarkeit. NB-IoT bietet zudem eine hohe Gebäudedurchdringung. Das verbessert die Erreichbarkeit in Technikräumen sowie Kellern und schafft eine flächendeckende Netzverfügbarkeit auch in dünn besiedelten Gebieten – genau dort, wo viele unter anderem sicherheitskritische Anlagen liegen.

Die Datenübertragung erfolgt bei den eCliq-Schlüsseln generell mit durchgängiger End-to-End-Verschlüsselung und sicherer AES-128-Bit-Technologie. Flash-Nutzer setzen somit bei der Cyber Security auf ein gewohnt hohes Niveau: Ein wichtiges Kriterium angesichts der Tatsache, dass physische und digitale Sicherheit immer mehr zusammenwachsen. Kontinuierlich steigende gesetzliche Anforderungen wie NIS2 oder das KRITIS-Dachgesetz unterstreichen diesen Trend.

Leistungsfähig im täglichen Einsatz

Die Mobilfunkkommunikation benötigt eine eigene Energiequelle. Anders als bisherige eCliq-Schlüssel ist der Flash deshalb mit einem integrierten Akku ausgestattet, der über USB-C geladen wird. Nach einer Entladung um 80 Prozent ist der Akku innerhalb einer Stunde wieder vollständig geladen. Eine Ladung reicht für einen Monat bei 800 Schließungen, hunderte Berechtigungsaktualisierungen und diverse Statusmeldungen. Hoher Wasser- und Staubschutz gemäß IP67 für die Verwendung im Freien sowie optische und akustische Signale runden die Ausstattung ab.

Zudem wurde der Spark technisch und gestalterisch überarbeitet. Der Schlüssel erzeugt seine Energie weiterhin selbst und kommt ohne Batterie oder Akku aus. Neu sind das markante Design, ein Kunststoffschieber und eine weiterentwickelte Funktionsstabilität.

Beide Schlüssel sind noch 2026 über den Fachhandel erhältlich. Ikon feiert sein erstes Jahrhundert mit Lösungen am Puls der Zeit für Kundinnen und Kunden der elektronischen Schließtechnik von morgen. 



Der energieautarke Spark erhielt eine Aktualisierung, um die aktuellen Marktanforderungen vollumfänglich abzudecken. Zusätzlich zum markanten Look wurde bei der neuen Version die Funktionsstabilität gesteigert

ZUTRITT

Integriertes Sicherheits-Ökosystem

KRITIS-konforme Zutrittskontrolle bei Berlin-Chemie



Mit dem KRITIS-Dachgesetz hat die Bundesregierung erstmals einen verbindlichen Rahmen geschaffen, der Betreiber kritischer Infrastrukturen verpflichtet, ihre Resilienz transparent nachzuweisen. Unternehmen aus regulierten Branchen stehen damit vor der Aufgabe, Risiken zu minimieren und auch ihre physische Sicherheit nach aktuellen technischen Standards auszurichten. Zutrittskontrolle wird damit zum zentralen Baustein gesetzlich geforderter Regularien.

Das traditionsreiche deutsche Pharmaunternehmen Berlin-Chemie ist als KRITIS-Betrieb von diesen Regularien betroffen. Es ist seit mehr als 130 Jahren am Markt, mit fünf Standorten in Berlin und rund 5.000 Beschäftigten. Eine abteilungsübergreifende Task Force analysierte das bestehende Zutrittssystem, das sich über viele Jahre hinweg entwickelt hatte. Das Ergebnis zeigt ein Bild, das für viele Bestandsanlagen typisch ist. Schnell wurde deutlich: Hier besteht Handlungsbedarf. Die technische Basis war geprägt durch ein veraltetes RS485-Bussystem, das gebäudeübergreifend installiert war. Dadurch kam es zu Störanfälligkeiten, Spannungsschwankungen führten zu Ausfällen und zu einer instabilen Protokollierung.

Aufgrund der historisch gewachsenen Struktur kamen an den Standorten zudem Zutrittskontrollkomponenten unterschiedlichster Hersteller zum Einsatz. Ergänzend wurden RFID-Technologien verwendet,

deren Verschlüsselung nicht mehr dem aktuellen Stand der Technik entsprach.

Besonders kritisch war die Situation in den sensiblen Bereichen der Rechenzentren: Die notwendige Zwei-Faktor-Authentifizierung ließ sich mit dem bestehenden System nicht umsetzen. Hinzu kam, dass auch die eingesetzte Zutrittskontrollsoftware veraltet war und nicht mehr weiterentwickelt wird – ein erheblicher Nachteil sowohl aus funktionaler Sicht als auch im Hinblick auf Dokumentations- und Auditfähigkeit.

Das Fazit der Prüfung fiel eindeutig aus: Das bestehende Zutrittskontrollsystem ist nicht KRITIS-konform und musste grundlegend erneuert werden. Teamlead Operational Technology Jörg Kaumanns bringt es auf den Punkt: „Wir haben ein recht altes Zutrittssystem betrieben, das über die Jahre gewachsen ist. Die KRITIS-Regularien fordern jedoch eine Umsetzung nach dem Stand der Technik und eine möglichst geringe Störanfälligkeit.“



Biometrische Handvenenerkennung ermöglicht sichere Zwei-Faktor-Authentifizierung in Hochsicherheitszonen

Von der Analyse zur Lösung

Nach einer umfassenden Marktanalyse entschied sich das Unternehmen für PCS Systemtechnik als Partner. Ausschlaggebend war insbesondere das breite Produktportfolio, mit dem sich die meisten Anforderungen des Pharmaunternehmens abdecken ließen. Die Task Force definierte daraufhin eine standardisierte Hardwarebasis für die gesamte Zutrittskontrolle. Diese Standardisierung erleichtert unter anderem die Bevorratung von Ersatzgeräten. Überzeugt hat PCS zudem durch das Konzept, die Migration im laufenden Betrieb umzusetzen. So konnte eine schrittweise, möglichst störungsfreie Umstellung über einen längeren Zeitraum realisiert werden.

Ein zentraler Schritt war die Migration der eingesetzten RFID-Technologie. Während der Umstellungsphase nutzten die Mitarbeiter sogenannte Kombikarten, die sowohl das bestehende Legic-prime-Verfahren als auch das neue, verschlüsselte Mifare-Desfire-Format unterstützen. Dadurch konnten die Zutrittsleser sukzessive ausgetauscht werden, ohne den Zugang zu einzelnen Bereichen zu beeinträchtigen.

Für Hochsicherheitszonen wie die Rechenzentren implementierte Berlin-Chemie eine Zwei-Faktor-Authentifizierung auf Basis von RFID und biometrischer Handvenenerkennung. Der Zutrittsleser Intus PS zeichnet sich dabei durch hohe Fälschungssicherheit, Nutzerfreundlichkeit und datenschutzkonforme Verarbeitung aus.

Eine weitere Herausforderung stellte die Absicherung von Brandschutztüren dar. Diese dürfen baulich nicht verändert werden und eignen sich daher nicht für verkabelte Zutrittsleser. Hier kamen mechatronische Schließsysteme Intus Flex zum Einsatz, die direkt im Türgriff integriert sind. Eine Funkvernetzung sorgt dafür, dass Berechtigungen zentral gesteuert und sofort wirksam werden. Für Zufahrten mit größerem Abstand wurde die Infrastruktur durch Weitbereichsleser ergänzt.

Eine zentrale Rolle spielt zudem die neue Zutrittskontrollsoftware: Statt Einzelberechtigungen erfolgt die Verwaltung nun über ein strukturiertes Rollen- und Zonenkonzept. Das verbessert die Übersicht und reduziert Fehler. „Mit Hilfe der Schnittstellen konnten wir die Anbindung an unser Corporate CRM realisieren. Das Rollen- und Zonenkonzept vereinfacht zusätzlich die Administration der Zutrittsrechte erheblich“, so Projektleiter Jörg Kaumanns.

Ein weiterer Schwerpunkt lag auf der revisionssicheren Dokumentation des gesamten Systems. Sämtliche Komponenten wurden erfasst, getestet und dokumentiert. Moderne Protokollierungsmechanismen gewährleisten, dass Zutritte und Zutrittsversuche zuverlässig gespeichert werden.

Für den Fall eines Stromausfalls erfolgt eine gesicherte Zwischenspeicherung im Zutrittskontrollmanager mit zusätzlicher Notstromversorgung – ein Konzept, das sich bereits im Ernstfall bewährt hat.

Schrittweise Migration für den Neustart

Die Modernisierung erfolgte in mehreren Phasen. Zunächst wurde die neue Zutrittslösung im Rahmen eines Pilotprojekts getestet. Ein ausgewähltes Gebäude diente dabei als Testumgebung. Ein technikaffines Team evaluierte das System zwei Monate lang unter realen Bedingungen. Erst nach erfolgreicher Testphase begann der unternehmensweite Rollout.

Parallel zum Austausch der Zutrittshardware begann die Migration der Ausweise mit Hilfe von Kombikarten, die sowohl alte als auch neue Technologien unterstützen. Zusätzlich wurde neue Zutrittshardware genutzt, die Kombinationsleser für alte und neue Ausweise verwendet. Mit dieser doppelten Kombivariante lief der Wechsel auf die neue Technologie nahezu problemlos. Die Installationsarbeiten der Hardware selbst fanden bevorzugt in den produktionsfreien Wartungsfenstern der Berlin-Chemie statt. Die enge Abstimmung zwischen dem internen Projektteam und den Technikern von PCS erwies sich dabei als entscheidend. Die Techniker von PCS waren vor Ort und konnten durch ihr Know-how aktiv die Installationsbedingungen gestalten.

KRITIS-konform und zukunftssicher

Nach Einschätzung des Projektleiters Kaumanns sind mit diesem neuen Sicherheitskonzept die Anforderungen für eine resiliente Gebäudesicherheit im Sinne des KRITIS-Dachgesetzes sehr gut umgesetzt. Mit inzwischen 64 Zutrittskontrollmanagern, 180 Online-Zutrittslesern, drei Handvenenlesern, zehn mechatronischen Schließsystemen und fünf Weitbereichsle-



Die neue Zutrittssoftware vergibt Berechtigungen rollen- und zonenbasiert und gewährleistet damit die auditfähige Rechtevergabe

sern verfügt das Unternehmen über eine standardisierte und umfassend dokumentierte Infrastruktur. Neben der sicheren RFID-Technologie und der biometrischen Authentifizierung trägt auch die Entscheidung für eine On-Premises-Lösung zur Resilienz bei. Das System ist bewusst autark ausgelegt und nach außen abgeschottet. Besonders bewährt hat sich bereits die Notstromversorgung der Zutrittskontrollmanager: Bei einem länger andauernden Stromausfall in Berlin blieb das System betriebsfähig und konnte anschließend ohne Datenverlust wieder gestartet werden.

Mit dem erfolgreichen Go-Live des Projekts ist sichergestellt, dass alle Berliner Standorte modernisiert sind und sich die gesamte Zutrittsinfrastruktur zentral administrieren lässt. Ein jährlicher Hardware Check stellt sicher, dass Firmware, Gerätezustand und Verkabelung kontinuierlich überprüft und dokumentiert werden – ein zentraler Baustein für die langfristige Auditfähigkeit.

Das Sicherheitsökosystem wächst

Die Modernisierung der Zutrittskontrolle bildet die Grundlage für weitere Projekte. Geplant ist unter anderem die Nutzung der neuen RFID-Ausweise für Zeiterfassung und Follow-Me-Printing. Zudem soll das bislang papierbasierte Besuchermanagement durch eine digitale Lösung ersetzt werden. Künftig könnten beispielsweise externe Techniker temporäre Besucherausweise erhalten. Auch Sicherheitsunterweisungen sollen digital erfolgen und dokumentiert werden. So entsteht Schritt für Schritt ein integriertes Sicherheitsökosystem, das weit über die Zutrittskontrolle hinausgeht. **GIT**



Interdisziplinäre Risikoanalyse und Planung bilden die Grundlage einer KRITIS-konformen Zutrittsarchitektur



PCS Systemtechnik GmbH
www.pcs.com

Multi-RFID-Box mit Ausrüstung

SCHLIESSFACHLÖSUNGEN

Kontrollierter Zugriff

Sicherheitskritische Assets verwahren, ausgeben und vollständig dokumentieren

Wenn Schlüssel, Arbeitsmittel oder Ausrüstung nicht dort verfügbar sind, wo sie gebraucht werden, entstehen Verzögerungen, Sicherheitsrisiken und zusätzlicher Abstimmungsaufwand. Keba stellt eine Lösung zur strukturierten Verwaltung vor.

■ Besonders in Organisationen mit Schichtbetrieb, wechselnden Einsatzlagen oder hohen Schutzanforderungen reicht die reine Aufbewahrung von Schlüsseln und anderen sicherheitskritischen Assets nicht aus. Entscheidend ist ein Prozess, der Verfügbarkeit, Zugriffsschutz und Nachvollziehbarkeit miteinander verbindet.

Im Schlüssel- und Objektmanagement ermöglicht Keba die strukturierte Verwaltung von Schlüsseln, Zutrittsmedien, Dokumenten, Werkzeugen, Kommunikationsmitteln und weiteren sicherheitsrelevanten Arbeitsmitteln. Berechtigte Personen identifizieren sich zum Beispiel über Ausweis, Chip, PIN oder ein anderes freigegebenes

Verfahren. Anschließend öffnet sich nur das Fach oder Depot, für das eine Berechtigung besteht. Jede Bewegung wird mit Person, Zeitpunkt und Objekt verknüpft. So bleibt jederzeit nachvollziehbar, welcher Schlüssel oder Gegenstand verfügbar ist, entnommen oder zurückgegeben wurde.

Von Waffe bis Notrufgerät

Auch für Waffen, Munition, Personennotrufgeräte und persönliche Einsatzausrüstung gelten ähnliche Anforderungen. Sie müssen geschützt verwahrt werden, im Einsatzfall aber schnell bereitstehen. Keba kombiniert dafür Depot- und Fachsysteme mit digitalen Berechtigungen, Identifikation und automatischer Dokumentation. Verantwortliche erhalten eine aktuelle Übersicht über Entnahmen, Rückgaben und Abweichungen. Je nach Prozess können zusätzliche Sicherheitsstufen wie Rollenmodelle, Zeitfenster oder Freigaben integriert werden.

Für Anwendungen, bei denen mehrere Gegenstände gemeinsam bereitgestellt und dennoch einzeln überwacht werden sollen, kommt die Multi-RFID-Box zum Einsatz. In einem Fach können mehrere mit Transponder ausgestattete Objekte sicher verwahrt und permanent auf Anwesenheit geprüft werden. So lassen sich beispielsweise Waffe, Funkgerät oder weitere Ausrüstung zentral

Schlüssel im überwachten Fach

Speedgate SG Expression

Moving by Design



Fachanlage im sicherheitsrelevanten Umfeld

bereitstellen, ohne die Einzelzuordnung zu verlieren.

Mobile Endgeräte oder Personennotrufgeräte können während der Aufbewahrung zugleich geladen werden. Die Ausrüstung bleibt damit nicht nur sicher verwahrt, sondern auch einsatzbereit.

Zentrale Steuerung

Die zentrale Steuerung erfolgt über die Kemas-Plattform. Sie verwaltet Personen, Rollen, Berechtigungen, Objekte und Anlagen und bildet Übergabeprozesse transparent ab. Über Schnittstellen können vorhandene Systeme eingebunden werden, damit Stammdaten und Berechtigungen nicht mehrfach gepflegt werden müssen.

Das Grundprinzip bleibt in allen Anwendungen gleich: Nur Berechtigte erhalten Zugriff, jede Übergabe wird dokumentiert und der tatsächliche Bestand bleibt sichtbar.

Wie diese Lösungen in der Praxis funktionieren, zeigt Keba auf der Security Essen vom 22. bis 25. September 2026 in Halle 6, Stand E36. Besucherinnen und Besucher können sich vorab ein Freiticket sichern und direkt einen Gesprächstermin vereinbaren. **GIT**

Security Essen: Halle 6, Stand E36



Keba Handover Automation GmbH
www.keba.com/security

PCS und Peply.ai starten Partnerschaft

PCS Systemtechnik kooperiert künftig mit Peply.ai, Agentic-AI-Plattform für Workforce Management im filialisierten Einzelhandel. Die Partnerschaft verbindet die cloudbasierte HR-Plattform von PEPLY.ai mit moderner Zeiterfassungshardware und zentralem SaaS-Betrieb durch PCS zu einer durchgängigen Lösung: von der zuverlässigen Zeitbuchung bis zur KI-gestützten Personalplanung. Für Unternehmen mit vielen Standorten ist eine reibungslose Verzahnung von Workforce Management und stationärer Zeiterfassung entscheidend. Zeitbuchungen müssen zuverlässig in Planung und weitere HR-Prozesse einfließen. Gleichzeitig steigt mit der

Zahl der Standorte der Aufwand für Einrichtung, Updates, Wartung und Betrieb der eingesetzten Terminals. Peply.ai bündelt Personalplanung, Zeiterfassung, Mitarbeiterkommunikation, Recruiting sowie weitere HR-Prozesse in einer cloudbasierten All-in-One-Plattform.

www.pcs.com

ZP Europe 2026: Halle 4.2, Stand L.55



MANAGED SECURITY

Bevorzugte Ziele

Wie KMU ihre IT-Sicherheit sofort verbessern können

80 Prozent aller gemeldeten Ransomware-Angriffe 2025 trafen kleine und mittlere Unternehmen. Auch, weil sie oft eine leichte Beute sind. Wie KMU ihre IT-Sicherheit direkt verbessern können, zeigen elf Tipps von Kimberly Stocker, Geschäftsführerin von Albakom, einem Unternehmen der Nobix Group.

Etwa 94 Prozent aller kleinen und mittelständischen Unternehmen waren 2024/2025 einem Cyberangriff ausgesetzt. Und die Angriffe steigen weiter, durchschnittlich gibt es 1.223 Attacken pro Woche auf deutsche Unternehmen. Und das unabhängig von Branche oder Unternehmensgröße. Die Frage ist also weniger, ob man angegriffen wird, sondern, ob die Abwehr standhält oder wie schnell eine Reaktion erfolgen kann.

Oft ist es nicht das große Geld, das die Angreifer anlockt, sondern die Daten von Kunden als Erpressungspotenzial. Es ist also fahrlässig zu glauben, dass man kein attraktives Ziel sei, weil das eigene Unternehmen nur wenige Mitarbeiter hat. Es ist eher umgekehrt: Hacker vermuten bei mittelständischen Firmen, dass die IT-Sicherheitsmaßnahmen nicht zeitgemäß sind und sich leichter umgehen lassen. Sie sind also bevorzugte Ziele.

Zögern steigert das Risiko

Wenn Sie sich unsicher sind, ob die aktuellen Maßnahmen und eingesetzten Tools

ausreichen, sollten Verantwortliche nicht zögern, Security-Audits selbst vorzunehmen oder über Dienstleister zu beauftragen und eine ganzheitliche Lösung auszuarbeiten. Es geht dabei nicht um blinden Aktionismus, sondern um ein planvolles Vorgehen.

IT-Sicherheit hat dabei mehrere Aspekte und betrifft nicht nur die Technik. Neben IT-technischen und physischen Schutzmaßnahmen müssen Unternehmen auch organisatorische und personelle Sicherheitsaspekte berücksichtigen. Mit folgenden elf Tipps, kann die IT-Sicherheit bereits erheblich verbessert werden.

1. Schwachstellen finden

Angreifer suchen nach Schwachstellen wie ungepatchte Sicherheitslücken. Daher ist es sinnvoll, seine Systeme auf Schwachstellen hin zu überprüfen. Dabei helfen spezielle Best-Practice-Tools, etwa von Enginsight und Palo Alto, die diese Schwachstellen kennen. Mit ihnen lassen sich Pseudo-Angriffe und Pen-Tests durchführen. Zusätzlich sinnvoll sind regelmäßige Netzwerk-Scans, mit

denen sich Schwachstellen der eingesetzten Geräte finden und sichtbar machen lassen.

2. Alle Netzwerk-Geräte erfassen

Bei Netzwerk denkt man an Notebooks, Server und Switches. Dazu zählen aber auch Türschließ-, Beleuchtungs- sowie Alarmsysteme, Telefonanlagen oder Kühlschränke mit Internet-Verbindung, also alle Geräte, die mit dem Internet kommunizieren und darüber schlussendlich auch angegriffen werden können. Diese sollten lückenlos erfasst und mit neuester Firmware und Updates aktuell gehalten werden.

3. Security nicht überdimensionieren

Die IT-Security-Landschaft sollte schlank und effektiv sein. „Viel hilft viel“ ist der falsche Ansatz, weil er Leistung und unnötiges Geld kostet, mehr Verwaltungsaufwand erfordert und die IT aufbläht. Es ist daher sinnvoll, eine genaue Aufstellung zu machen, welche Tools im Einsatz sind und welche Funktionalitäten doppelt vorhanden sind. Darauf basierend lässt sich einfach

entscheiden, welche Tools welche Aufgaben übernehmen sollen.

4. DNS-Schutzschirm aufspannen

Ein DNS-Server übersetzt Domain-Namen in eine IP-Adresse. Üblicherweise findet die Übersetzung ausnahmslos für alle Domainnamen statt, unabhängig davon, ob sich dahinter eine Hackerwebseite verbirgt oder ein seriöser Anbieter. Spezielle DNS-Server verweigern jedoch die Auflösung von Domainnamen zu IP-Adressen, die bekanntermaßen einem böswilligen Akteur zuzuschreiben sind. Mit solchen speziellen Servern schützen sich Unternehmen beispielsweise davor, auf Phishing-Mails hereinzufallen.

5. Backups schützen

Ransomware-Angreifer versuchen, alle Daten eines Unternehmens zu verschlüsseln und anschließend Geld zu erpressen. Zu den Daten im Visier der Hacker zählen auch Backups. Diese müssen gesondert gesichert, physisch getrennt und nicht überschreibbar sein. Hierbei helfen spezielle Tools wie Dell Data Protection oder auch Veeam-Backup-Lösungen. Zusätzlich sollten Unternehmen regelmäßig testen, ob ihre Backups intakt sind und sich zurückspielen lassen.

6. Multifaktor-Authentifizierung konsequent durchsetzen

Neben einem Login mit Passwort sollten Unternehmen konsequent überall dort eine Zweifaktor-Authentifizierung einrichten, wo es möglich ist. Denn dann reichen gestohlene Login-Passwortdaten allein nicht mehr aus, um Zugriff zu erhalten. Die gute Nachricht: Beim Einsatz von Hardware-Token oder Passwortsafe-Anwendungen ist der zweite Faktor kaum noch mit Komforteinbußen verbunden. Alternativ lassen sich auch Passkeys einsetzen.

7. Erbeutete Zugangsdaten automatisiert beobachten und auswerten

Im Darknet werden Listen mit Login-Zugängen gehandelt, die bei früheren IT-Angriffen erbeutet wurden. Es ist daher wichtig, Tools wie Passwortsafe-Anwendungen einzusetzen, die Zugangsdaten automatisch gegen bekannte Einbrüche testen und auf Schwachpunkte hinweisen.

8. Beschränken, wer ins Netzwerk darf

Es gibt technische Möglichkeiten, mit denen sich einfach begrenzen lässt, wer sich von außerhalb ins eigene Netzwerk einloggen oder interne Dienste von außerhalb nutzen darf. Sinnvoll ist hierfür eine Network-Access-Control-Lösung (NAC). Sie stellt sicher, dass nur autorisierte Nutzende und

Endgeräte Zugang zum Unternehmensnetzwerk erhalten. Grundsätzlich sollte die Authentifizierung und Autorisierung auf dem sicheren 802.1X-Standard beruhen und auch eng angebundene Dienstleister mit einbeziehen.

9. Netzwerk auf den Ernstfall vorbereiten

Damit ein erfolgreicher Angriff in einem Netzwerk- oder Computersystem nicht das gesamte Netzwerk lahmlegt, ist es sinnvoll, dieses zu segmentieren und mittels Zero-Trust-Technologie zu schützen. Spezielle Recovery-Systeme helfen zudem, nach einem Einbruch möglichst schnell wieder arbeitsfähig zu sein.

10. Regelmäßige Zertifizierungen und Trainings durchführen

Einige der häufigsten Einfallstore für Hacker-Angriffe sind Mitarbeiter, die einen Angriff als solchen nicht erkennen und sich fehlerhaft verhalten. Um das zu verhindern, sollten Verantwortliche regelmäßige Trainings und sich wiederholende Zertifizierungen durchführen, um für die notwendige Aufmerksamkeit zu sorgen.

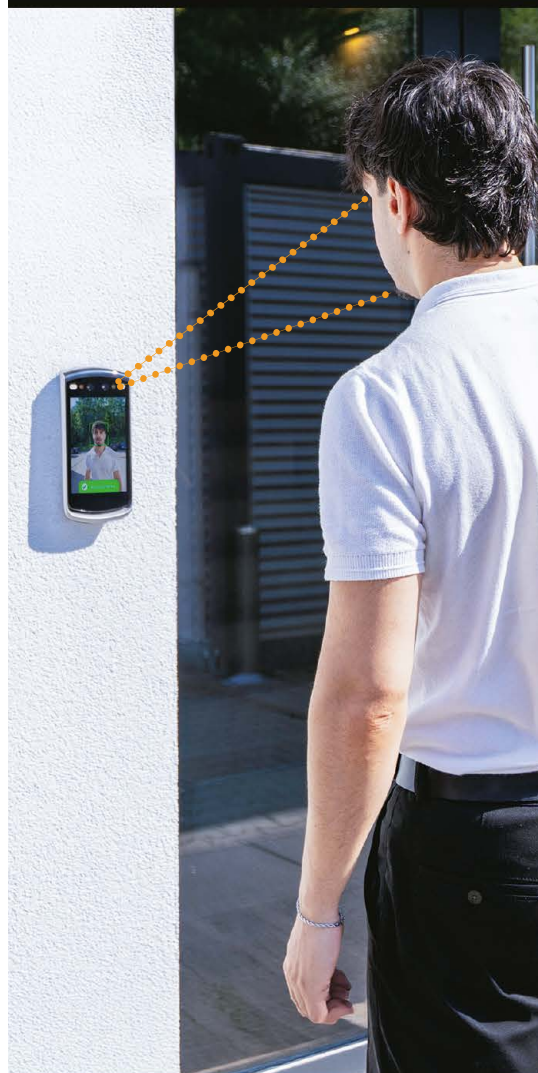
11. Software updaten und regelmäßig kontrollieren

Regelmäßig werden Sicherheitslücken entdeckt, die im Betriebssystem von Rechnern, in Treibern oder Anwendungen versteckt sein können. Das Durchführen von Updates sollte daher geübte Praxis und möglichst automatisiert erfolgen, um den Zeitraum zwischen Entdeckung und Behebung möglichst kurz zu halten. Gängige App-Stores können hierbei unterstützen, da sie Anwendungen mit einer automatischen Update-Funktion versehen. Außerdem sollten Unternehmen sicherstellen, dass Anwender nur geprüfte Applikationen aus vorgegebenen Quellen installieren können.

Ausgewogene Sicherheitsstrategie

Entscheidend für eine maximale IT-Sicherheit ist eine ausgewogene Gesamtstrategie, die auf einem umfassenden Audit des eigenen Unternehmens basieren sollte. Nach der Security-Analyse lassen sich mit einem erfahrenen IT-Dienstleister gezielt die Punkte angehen, die den größten Handlungsbedarf haben. Damit können Unternehmen kurzfristig die größten Angriffsflächen wirkungsvoll reduzieren. **GIT**

Zutritt per Gesichts- erkennung iDFace Max



✓ DSGVO-konform und
100 % sicher

✓ Integrierter SIP-Client
als Türsprechstelle

✓ Hands-free: Zutritt
ohne Karte, ohne PIN

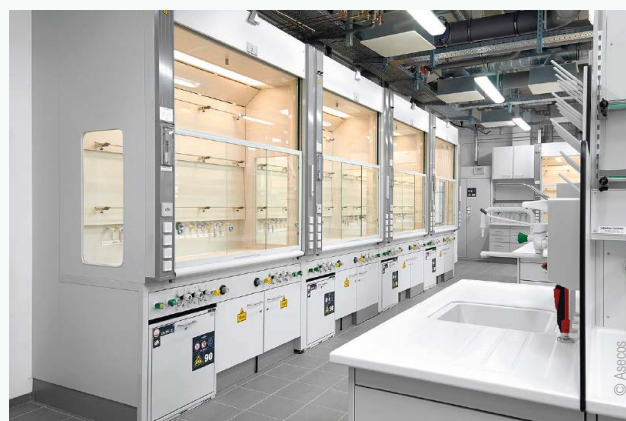


Nobix Group
www.nobix-group.de



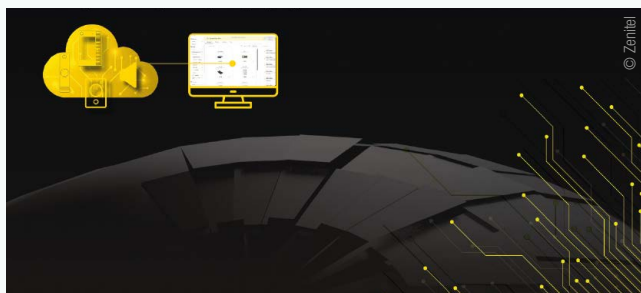
Secunet und Cloudflare bringen starke Cyberresilienz in die Cloud

Secunet und Cloudflare haben ihre neue Partnerschaft bekannt gegeben. Innerhalb dieser entwickeln sie Lösungen, die den Bedarf europäischer Unternehmen und Behörden an digitaler Souveränität adressieren. Mit diesen Lösungen laufen Cloud-Dienste der Kunden schnell, stabil, ausfallsicher und widerstandsfähig gegenüber Cyberangriffen. Der Ansatz steht im Einklang mit der Doppelstrategie des Bundesamts für Sicherheit in der Informationstechnik (BSI), relevante Technologie von US-Anbietern unter strengen Sicherheits- und Kontrollkriterien zugänglich zu machen und dabei Organisationen dabei zu unterstützen, ihre Souveränitätsanforderungen zu erfüllen. Die Lösung sieht außerdem vor, den Kunden entsprechend ihren jeweiligen Anwendungsfällen und Anforderungen Werkzeuge an die Hand zu geben, mit denen sie die C3A-Souveränitätskriterien des BSI erfüllen können. www.secunet.com



Sicherheits-Assistenz-System als Nachrüstlösung

Das weiterentwickelte Sicherheits-Assistenz-System (SAS) der Asecos GmbH ist erstmals auch als Nachrüstkit für bereits vorhandene Sicherheitsschränke erhältlich. Die kompakte Lösung überwacht kontinuierlich die technische Entlüftung der Schränke. Zudem wurde die Elektronik vollständig überarbeitet. Sicherheitsschränke sollten aus Gründen des Explosions- und Arbeitsschutzes technisch entlüftet werden – meist über eine feste Abluftanlage ins Freie. Dabei wird die Schrankentlüftung häufig in den vorgeschriebenen Laborraumluftwechsel einbezogen, da ein Teil des erforderlichen Raumluftwechsels über die Entlüftung der Sicherheitsschränke erfolgt. Das SAS überwacht die Entlüftung permanent: Es erfasst kontinuierlich den Differenzdruck im Abluftsystem, erkennt kritische Betriebszustände frühzeitig und alarmiert, sobald der erforderliche Mindest-Abluftvolumenstrom unterschritten wird. So erhöht es die Sicherheit im Arbeitsalltag. www.asecos.com



Zenitel stärkt Unified Critical Communications

Zenitel erweitert die Leistungsfähigkeit von Zenitel Connect Pro durch cloudbasierte Transparenz, proaktive Wartung und zentrales Lifecycle-Management für Onshore-Anwendungen. Die Zenitel Cloud Remote Monitoring & Management (RMM) – eine cloudbasierte Erweiterung von Zenitel Connect Pro, ist darauf ausgelegt, die Überwachung, Wartung und das Lifecycle-Management von Zenitels Kommunikationssystemen in standortübergreifenden Onshore-Umgebungen zu vereinfachen. Da Unternehmen zunehmend auf vernetzte Kommunikationsinfrastrukturen angewiesen sind, um Sicherheit und operative Kontinuität sicherzustellen, gewinnt die Fähigkeit zur Fernüberwachung und -wartung dieser Systeme immer mehr an Bedeutung. Durch die Erweiterung von Zenitel Connect Pro um cloudbasierte Remote-Monitoring- und Managementfunktionen ermöglicht Zenitel Cloud RMM Unternehmen, ihre Betriebssicherheit zu steigern und gleichzeitig Wartungskosten sowie Ausfallzeiten zu reduzieren. www.zenitel.com

Führende interne IT-Dienstleister wachsen trotz Konjunkturkrise

Das von Lünendonk & Hossenfelder zum fünften Mal in Folge veröffentlichte Ranking bietet einen Überblick über die größten internen IT-Dienstleister in Deutschland. Dazu zählen Unternehmen, die mehr als 90 Prozent ihrer Umsätze mit IT-Dienstleistungen innerhalb einer Organisation erwirtschaften und rechtlich selbstständige Unternehmen sind. Interne IT-Dienstleister setzen auch im Jahr 2025 ihr Wachstum fort und steigerten ihre Umsätze im Durchschnitt um 9,0 Prozent. Zu den zentralen Investitionsfeldern zählen die Modernisierung der IT-Landschaften, der Ausbau der Cybersecurity, die Prozessautomatisierung, die Entwicklung neuer digitaler Services sowie die KI-Transformation. Steigende Anforderungen aus den Fachbereichen und immer kürzere Technologiekzyklen dürfen das Wachstum der captiven IT-Dienstleister auch in den kommenden Jahren vorantreiben. www.luenendonk.de



Bequem auf dem Sofa durch die e-Ausgabe der GIT SICHERHEIT blättern: Registrieren Sie sich auf www.git-sicherheit.de/newsletter



Seminare & Tagungen

Sicherheit, Brandschutz, Ex-Schutz, Gefahrstoffe

DAS BESONDERE HIGHLIGHT

Essener Brandschutztage

27. Tagung mit fachbegleitender Ausstellung
03. - 04.11.26 in Essen

Prüfungen von Ex-Anlagen – Pflichten, Inhalte, Befähigung

03. - 04.11.26 in Regensburg

Sicherer Betrieb von Anlagen – Betreiberverantwortung und Anlagendokumentation

03. - 04.11.26 in Essen

Gefahrstoffbeauftragter

03. - 04.11.26 in Bad Oeynhausen

Weiterbildung im Explosionsschutz für befähigte Personen

05.11.26 in Essen

Prüfung von Brandschutztüren und Fachkraft für Feststellanlagen gemäß DIN 14677

10. - 11.11.26 in Essen

Weiterbildung von Brandschutzbeauftragten

mit Begehung der VELTINS-Arena auf Schalke

12. - 13.11.26 in Essen

Betreiberpflichten im Brandschutz

12. - 13.11.26 in Essen

Lagerung von Gefahrstoffen

19. - 20.11.26 in Bad Oeynhausen

Ausbildung zum Brandschutz-Manager

23. - 25.11.26 in Essen

Grundkenntnisse Gefahrstoffrecht:

Vom Sicherheitsdatenblatt zur Betriebsanweisung

24. - 25.11.26 in Essen

Explosionsschutz – Einführung und Übersicht

24. - 25.11.26 in Regensburg

Ausbildung zum Brandschutzbeauftragten

30.11. - 09.12.26 in Essen

18. - 27.01.27 in Essen

Ausbildung zum Explosionsschutzbeauftragten

01. - 04.12.26 in Essen

19. - 22.01.27 in Essen

NEU

Die neue Brandklasse L nach ISO 3941:2026 und Lithium-Ionen-Batterien im Betrieb

10. - 11.12.26 in Essen

Gefahrstoffe – Sicheres Arbeiten in Laboratorien (TRGS-526)

26. - 27.01.27 in Essen

Fachkunde zur Freigabe von Feuer- und Schweißarbeiten

01. - 02.02.27 in Essen

Neue Gefahrstoffverordnung 2024 kompakt

22.02.27 in Essen



IHRE ANSPRECHPARTNER:

Fachbereich Chemie – Brandschutz – Verfahrenstechnik

Dipl.-Ing. Kai Brommann

Fachbereichsleiter

Telefon: +49 (0)201 1803-251

Dipl.-Ing. Frank Adamczyk

Stellv. Fachbereichsleiter

Telefon: +49 (0)201 1803-373

E-Mail: fb5@hdt.de

www.gefahrstoffe.eu

Intelligenter, transparenter, schneller

**Digitale und vernetzte Prüfprozesse
im Brandschutz**

DT Connect von Detectortesters und Smartryx von Datolution zeigen, wie digitale Prüfprozesse den Brandschutz verändern. Global Marcomms Manager Stephen Beadle und Head of Customer Experience Oliver Dörle (beide von Detectortesters) und Aljona Ijoschina, Geschäftsführerin bei Datolution, erläutern im Gespräch mit GIT SICHERHEIT, wie vernetzte Prüftechnik, Cloud-Plattformen und intelligente Datenintegration Prüfungen beschleunigen, Transparenz schaffen und rechtssichere Nachweise ermöglichen.

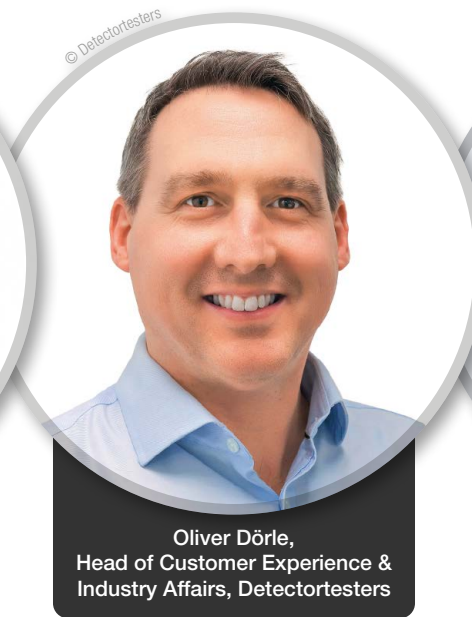
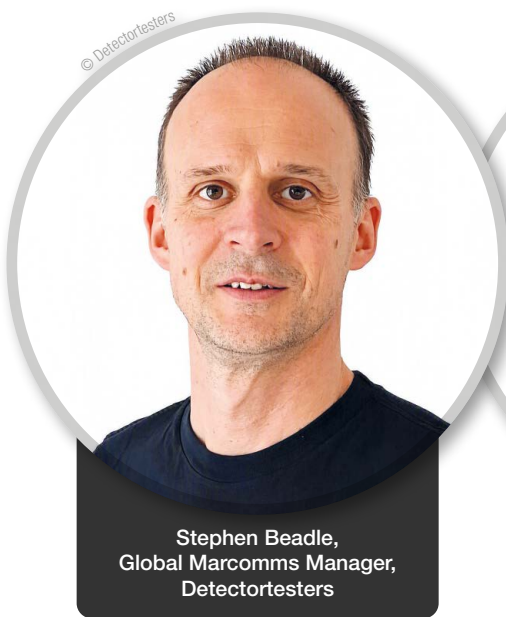
■ GIT SICHERHEIT: Herr Beadle, als wir uns das letzte Mal unterhielten, hatte Detectortesters gerade seine erste digitale Lösung, DT Connect, auf den Markt gebracht. Wie hat sich das weiterentwickelt?

Stephen Beadle: DT Connect markierte den Beginn unseres Portfolios vernetzter Prüfgeräte und ermöglichte es Brandschutztechnikern, von einer Lösung zu profitieren, die funktionale Rauch- und Wärmeproofungen mit einem automatischen digitalen Prüfnachweis kombinierte. Seit der Markteinführung hat die Lösung ihren Wert für den globalen Brandschutzmarkt unter Beweis gestellt: Bislang haben Anwender mehr als 500.000 Brandmelder geprüft und dabei Prüfberichte für über 15.000 Standorte in 50 Ländern erstellt.

Können Sie uns noch einmal erläutern, welchen Zweck DT Connect erfüllt und wie es sich in die traditionellen Prüfgeräte einfügt, für die Sie bekannt sind?

Stephen Beadle: Wir haben DT Connect eingeführt, um dem wachsenden Bedarf gerecht zu werden, nachweisen zu können, dass Funktionsprüfungen von Brandmeldern tatsächlich stattgefunden haben. Die zentrale technische Herausforderung bestand darin, eine zuverlässige Methode zu entwickeln, um die Auslösung des Melders am Ort der

XTR2 testet sowohl Rauch- als auch Wärmemelder, erfasst das Ergebnis jedes Tests und überträgt es an die DT Connect-App



Prüfung unabhängig zu bestätigen – also live und direkt vor Ort zu bestätigen, dass der Melder ordnungsgemäß funktioniert und bei Einleitung von Rauch oder Wärme ausgelöst hat.

Um dies zu bewältigen, wurde DT Connect mit dem XTR2 kombiniert. XTR2 ist unser fortschrittlichstes Funktionstest-Prüfgerät, das die schnelle Prüfung auf Rauch und Wärme mit einem einzigen Gerät ermöglicht. Im Testbecher befinden sich 21 optische Sensoren, die die vom Melder erzeugten optischen Alarmanzeigen erkennen, sobald dieser in den Alarmzu-

stand wechselt, und das Ergebnis über Bluetooth an die DT Connect-App übermitteln. Die Software zeichnet dieses Prüfergebnis automatisch zusammen mit Datum, Uhrzeit und Standort auf, um den endgültigen Prüfnachweis für jeden Melder vor Ort zu liefern.

Aufgrund der Nachfrage von Anwendern unserer herkömmlichen Prüfgeräte konnten wir DT Connect inzwischen auch für Nutzer von Produkten aus unserer Solo-Reihe einführen.

Herr Dörle, Daten und Compliance sind große Themen in der Branche. Wie unterstützen Sie Brandschutzfachleute dabei, Herausforderungen in diesen Bereichen zu meistern?

Oliver Dörle: Die Herausforderung besteht darin, dass Compliance oft mit mehr Papierkram verbunden ist. Techniker würden ihre Zeit lieber damit verbringen, sicherzustellen, dass Brandschutzsysteme ordnungsgemäß funktionieren, als Berichte auszufüllen. Mit XTR2 und DT Connect haben

wir Prüfung und Berichterstellung in einem einzigen Arbeitsablauf vereint. Die erfassten Prüfdaten werden zur Erstellung professioneller Compliance-Berichte verwendet, die Fachfirmen an ihre Kunden weitergeben können und die einen sofortigen Nachweis über die durchgeführten Arbeiten liefern – ganz ohne manuelle Dateneingabe.

Das Ergebnis ist einfach: Brandschutztechniker verbringen weniger Zeit mit Verwaltungsaufgaben und mehr Zeit mit dem Brandschutz, während Gebäudeeigentümer klare, überprüfbare Nachweise darüber erhalten, dass die Melder-Prüfungen stattgefunden haben. Der Techniker führt die Prüfung wie gewohnt durch; die Berichterstellung erfolgt automatisch im Hintergrund.

Warum sind diese Themen Ihrer Meinung nach so wichtig geworden? Was treibt den Fokus auf die Einhaltung von Vorschriften an?

Oliver Dörle: Ein Grund dafür ist das gestiegene öffentliche Bewusstsein nach schweren Brandkatastrophen, darunter auch die Grenfell-Katastrophe in Großbritannien. Wenn solche Ereignisse eintreten, richtet sich die Aufmerksamkeit darauf, ob Brandschutzsysteme ordnungsgemäß gewartet wurden und ob es Belege dafür gibt. Gleichzeitig sind sich Gebäudeeigentümer und Verantwortliche ihrer Pflichten zunehmend bewusst geworden. Auch wenn Prüfungen und Wartungsarbeiten oft an spezialisierte Auftragnehmer delegiert werden, liegt die Verantwortung letztendlich beim Gebäudeeigentümer.



Auch die Technologie hat die Diskussion verändert. Fortschritte bei Cloud-Plattformen, vernetzten Geräten und der digitalen Datenerfassung bedeuten, dass es nun weitaus einfacher ist, Compliance-Daten zu erfassen und zu verwalten. Nimmt man all diese Faktoren zusammen, wird schnell klar, warum Compliance zu einem so wichtigen Branchenthema geworden ist.

Sie erwähnen, dass es viele Unternehmen gibt, die Tools zur Unterstützung der Compliance anbieten. Was hat zur Zusammenarbeit mit Datolution geführt?

Stephen Beadle: Viele größere Fachfirmen nutzen bereits eigene oder fremde Compliance-Plattformen. Das bedeutet, dass zwar viele Nutzer direkt mit DT Connect arbeiten, andere jedoch eine Integration der Prüfdaten in umfassendere Compliance- und Anlagenmanagementsysteme benötigen.

Wir haben diesem Bedarf durch die Entwicklung eines Software Development Kits (SDK) Rechnung getragen, das es anderen Anbietern von Softwarelösungen ermöglicht, eine Anbindung an die XTR2-Prüfdaten herzustellen und die erfassten Daten anschließend in ihren eigenen Plattformen zu nutzen. Dadurch können die während der Funktionsprüfung erstellten Ergebnisse mit anderen Daten kombiniert werden, die während des Vor-Ort-Besuchs erfasst wurden. Dies hilft Fachfirmen dabei, umfassendere Berichte zu erstellen, auf die von einer einzigen Plattform aus zugegriffen werden kann. Datolution ist eines der Unternehmen, mit denen wir in diesem Bereich zusammenarbeiten, neben weiteren Partnern in Großbritannien.

Frau Ijoschina, „Datolution“ scheint eine Kombination aus den Begriffen „Daten“ und „Revolution“ zu sein. Könnten Sie uns das dahinterstehende Konzept bitte einmal vorstellen?

Aljona Ijoschina: Datolution ist in der Tat eine bewusste Verschmelzung aus Daten, Revolution und dem englischen Wort Solution. Als Teil der Schraner-Group sind wir in der Brandmeldebranche zuhause. Hier entstehen tagtäglich wichtige Systemdaten. Überraschenderweise werden diese Daten bis heute nur zu einem Bruchteil ausgewertet und genutzt.

Unsere „Revolution“ besteht also darin, komplexe Daten sicherheitstechnischer Anlagen intelligent nutzbar zu machen. Kurz gesagt, wir machen aus reinen Anlagendaten echte Lösungen und sparen unseren Kunden dadurch Zeit, Nerven sowie Aufwand. Da der Schutz dieser sensiblen Daten für uns absolute Priorität hat, betrei-

ben wir seit April 2022 ein Informationssicherheits-Managementsystem (ISMS), welches Anfang 2023 nach ISO/IEC 27001 erstmalig zertifiziert und Anfang 2026 rezertifiziert wurde.

Das zentrale Tool ist Ihre Smartryx-App, die einerseits für Feuerwehren verfügbar ist – und andererseits auch in Form der hier relevanten Wartungs-App. Wie funktioniert sie und welche Funktionen bietet sie?

Aljona Ijoschina: Richtig, mit unserem Smartryx-System digitalisieren wir Brandmeldeanlagen – und das konsequent herstellerneutral. Die Funktionsweise ist schnell erklärt: Zuerst wird die Anlagenprogrammierung in unsere SmartSecure-Cloud hochgeladen, wodurch ein virtuelles, statisches Abbild der Anlage entsteht. Um sie kommunikationsfähig zu machen, ist ein Gateway dazwischengeschaltet. Wer die Anlage 24/7 überwachen möchte, installiert ein festes Gateway. Für reine Wartungszwecke reicht meist ein mobiles Gerät. Das Gateway überträgt dann alle Live-Meldungen wie Alarmer oder Störungen sicher auf unseren Server. Über anwendungsspezifische Apps können diese Informationen dann ortsunabhängig für das Meldungs-

Störungs- oder das Wartungsmanagement genutzt werden.

Besonders bei der Wartung spielt das System seine Stärken aus: Bevor es zum Kunden geht, wird in der Cloud mit wenigen Klicks ein normkonformer Prüfplan generiert. Der Techniker öffnet diesen in seiner Smartryx-Maintenance App und sieht auf einen Blick, was zu tun ist. Da die App über das mobile Gateway live mit der Anlage verbunden ist, ermöglichen wir eine echte 1-Mann-Wartung. Der Techniker sieht sofort, ob er einen Melder mit Prüfgas ausgelöst hat. Das lästige Nachfragen per Funk bei einem Kollegen an der Zentrale entfällt, denn Smartryx hakt den Melder automatisch als erfolgreich geprüft ab. Ist der Einsatz beendet, reicht ein Klick auf „Abschließen“. In genau diesem Moment generiert das System ein lückenloses und normgerechtes PDF-Protokoll – inklusive aller Bemerkungen, Fotos und digitaler Unterschriften. Der Techniker kann diesen Bericht sofort an den Betreiber mailen.

Kurz gesagt: Wir reduzieren den Personalaufwand, setzen der fehleranfälligen Zettelwirtschaft ein Ende und machen den gesamten Prozess schnell, transparent und vor allem rechtssicher.

Heutige Brandmelder und Brandmeldezentralen sind datengesteuert, vernetzt und können per Fernzugriff gewartet werden. Welche besonderen Merkmale und neuen Möglichkeiten bieten Ihre Lösung und Ihre Zusammenarbeit?

Oliver Dörle: Bei der Markteinführung war es unser Ziel, die Prüfung von Brandmeldern zu digitalisieren und zuverlässige Prüfberichte zu erstellen. Unsere Zusammenarbeit mit Datolution stellt die nächste Etappe auf diesem Weg dar, indem sie die Prüfdaten der Brandmelder mit Informationen aus anderen Bereichen des Brandschutzsystems verknüpft.

Ein gutes Beispiel ist der Fall, wenn ein Techniker einen Brandmelder testet. Wenn der Melder korrekt anspricht, ist dieses Ereignis an der Brandmeldezentrale zu erkennen. Wenn jedoch ein Melder getestet wird und aufgrund eines Defekts nicht anspricht, zeigt die Zentrale nicht unbedingt an, dass der Melder getestet wurde und defekt ist. Durch die Kombination von Daten aus XTR2 mit Informationen aus der Brandmeldezentrale erhalten Techniker ein viel klareres Bild. Sie können nicht nur sehen, welche Melder erfolgreich ausgelöst haben, sondern auch, welche Melder getestet wurden und einer weiteren Prüfung bedürfen. Dies liefert einen besseren Nachweis für die Sys-



temleistung und die durchgeführten Wartungsmaßnahmen.

Aljona Ijoschina: Der große Mehrwert liegt in der nahtlosen Integration der Technologien beider Unternehmen in einer einzigen Anwendung. So wird die Bestätigung einer erfolgreichen Melderprüfung nun intelligent synchronisiert. Die Smartryx-Maintenance App verarbeitet sowohl das Signal aus der Brandmeldeanlage als auch die Bestätigung des Prüfgeräts XTR2. Indem wir diese zwei zuvor getrennten Prozesse zu einem smarten Arbeitsschritt vereinen, erzielen wir eine enorme Zeitersparnis für den Techniker.

Ein weiterer entscheidender Vorteil ist die direkte Bedienbarkeit des XTR2. So hat man über unsere App nicht nur die Betriebszustände im Blick, sondern kann zudem während der Wartung intuitiv den Betriebsmodus umschalten.

Schauen wir uns das einmal etwas genauer an: Wie sieht die Integration von Detectortestern in die Lösungen von Datolution konkret aus und welche wesentlichen Vorteile ergeben sich daraus für Techniker und Betreiber?

Aljona Ijoschina: Im Kern sorgt die Digitalisierung des gesamten Wartungsprozesses für maximale Transparenz und einen beschleunigten Informationsfluss zwischen allen Beteiligten. Daraus ergeben sich entscheidende Mehrwerte. Für den Betreiber bedeutet es in erster Linie volle Transparenz, da die Wartungsergebnisse sofort nachvollziehbar sind, was das Vertrauen in die Arbeit des Errichters enorm stärkt. Dem Techniker bringt das Ganze eine hohe Prozesssicherheit für den Techniker, denn wenn die Rückmeldung des XTR2 nahtlos mit den Smartryx-Meldungen übereinstimmt, hat er schon direkt vor Ort sofortige Gewissheit über seine Arbeit. Und am Ende profitieren alle von rechtssicheren Nachweisen, weil der gesamte Wartungsverlauf durch die digitale Dokumentation lückenlos belegt werden kann – ganz gleich, ob gegenüber Auditoren oder Sachverständigen.

Der Brandschutz wird zunehmend Teil integrierter Gebäudekonzepte, bei denen der Fokus nicht ausschließlich auf Sicherheitsfunktionen liegt. Wie sehen Sie diese Entwicklung?

Oliver Dörle: Ich halte dies für eine der wichtigsten Entwicklungen, die unsere Branche prägen. Gebäude werden zu immer stärker vernetzten Umgebungen, und Kunden erwarten, dass verschiedene Technologien und Systeme nahtlos zusammenarbeiten.



Die Partnerschaft zwischen Detectortestern (DT) und Datolution wurde auf der FeuerTrutz in Nürnberg bekannt gegeben. V.l.n.r.: Gareth Dibden, Senior Customer Success Manager (DT), Markus Koschade, Business Development Manager (DT), Aljona Ijoschina, Mitgeschäftsführerin (Datolution), Stephen Beadle, Global Marcomms Manager (DT)

Kein einzelnes Unternehmen kann in jedem Aspekt des Gebäudemanagements Experte sein. Bei Detectortestern liegt unsere Expertise in der Prüfung von Brandmeldern, aber das ist nur ein Teil eines viel umfassenderen Ökosystems.

Aljona Ijoschina: Wir sehen diese Entwicklung als absolut notwendig an. Brandmeldeanlagen waren lange autarke Systeme, deren wertvolle Daten im Gebäude verborgen blieben. Die Integration in ganzheitliche Gebäudeplattformen ändert das grundlegend.

Für uns bestätigt dieser Trend unseren eigenen Ansatz: Wir müssen Brandmeldedaten aus der Isolation befreien. Eine moderne Brandmeldeanlage ist im Grunde ein hochverfügbares, normiertes Sensornetzwerk, das das gesamte Gebäude durchzieht. Wenn wir diese Daten über Cloud-Technologien und offene Schnittstellen in übergeordnete Plattformen integrieren, stiften sie einen enormen Mehrwert – weit über die reine Gefahrenmeldung hinaus. Die Kernfunktion der Lebensrettung bleibt dabei unangetastet, aber die Systemdaten helfen plötzlich

dabei, das Facility Management zu optimieren oder prädiktive Instandhaltung zu ermöglichen.

In diesem Ökosystem sehen wir uns als die Spinne im Netz, die die Brücke zwischen streng normierter Sicherheitstechnik und modernen Plattformen schlägt. Dafür setzen wir gezielt auf intelligente Cloud-to-Cloud Verbindungen und starke Partnerschaften, wie etwa unsere Kooperation mit Detectortestern. **GIT**



Datolution
www.datolution.de

Detectortestern
www.detectortestern.com

Jürgen Hövelmann
Geschäftsführer von EPS

SICHERMACHER

„Innovation ist unser Motor“

GIT SICHERHEIT im Gespräch mit Jürgen Hövelmann von EPS

Auf der Feuertrutz 2026 sprach Dr. Timo Gimbel von GIT SICHERHEIT mit Jürgen Hövelmann, Geschäftsführer von EPS, über den Fachkräftemangel, die Zukunft funkbasierter Brandwarnanlagen und das Zusammenspiel von KI, Video- und Brandschutztechnik sowie über die gemeinsam mit Ajax entwickelte EN54-Brandwarnanlage.

— GIT SICHERHEIT: Herr Hövelmann, zum Einstieg für alle, die EPS noch nicht kennen: Stellen Sie sich und Ihr Unternehmen doch bitte mal kurz vor.

Jürgen Hövelmann: Gerne. Ich bin seit 45 Jahren in der Sicherheitsbranche tätig und habe die EPS vor 35 Jahren übernommen. Wir beschäftigen uns schwerpunktmäßig mit Brandschutz und Sicherheitstechnik. Als Familienunternehmen arbeiten wir mit viel Herzblut – meine Frau, mein Sohn und meine Tochter sind ebenfalls im Unternehmen aktiv. Insgesamt sind wir rund 40 Mitarbeiter und verstehen uns als Partner unserer Kunden.

Welche Themen beschäftigen Errichter und Planer aktuell besonders?

Jürgen Hövelmann: Es wird viel über Entbürokratisierung und Vereinfachung gesprochen. Gleichzeitig dürfen wir nicht vergessen, dass Brandschutz ohne Normen nicht funktio-

niert. Normen sind kein Hindernis, sondern die Grundlage unserer Arbeit. Gerade die EN-54-Normen schaffen Sicherheit und Verlässlichkeit. Was wir vereinfachen können, ist die Anwendung. Errichter wünschen sich heute Lösungen, die sich schnell installieren lassen und möglichst viele Einsatzbereiche abdecken – vom Einfamilienhaus über Schulen und Kindergärten bis hin zu gewerblichen Objekten. Genau dort setzen wir an.

Auf der Feuertrutz wurde Ihr System als „Produkt des Jahres 2026“ ausgezeichnet. Wodurch hebt es sich von anderen Lösungen ab?

Jürgen Hövelmann: Gemeinsam mit Ajax haben wir eine vollständig funkbasierte Brandwarnanlage entwickelt. Sie verbindet Brandwarntechnik, Einbruchmeldetechnik und Videotechnik in einem System und lässt sich zusätzlich komfortabel per App bedienen. Ein entscheidender Vorteil ist die Alarmverifikation. Im Ernstfall reicht es nicht aus

zu wissen, dass ein Alarm ausgelöst wurde. Der Betreiber muss möglichst schnell beurteilen können, ob es sich um einen Fehlalarm oder um einen tatsächlichen Brand handelt. Durch die Einbindung von Kameras erhält er unmittelbar Bilder der Situation und kann entsprechend reagieren.

Welche Funktionen bietet die App?

Jürgen Hövelmann: Die App spiegelt praktisch das Bedienfeld der Anlage auf das Smartphone. Betreiber können jederzeit den Systemstatus kontrollieren, Geräte überwachen, Livebilder abrufen oder bei Bedarf sogar eine Evakuierung auslösen. Dadurch bleibt das gesamte System jederzeit transparent und einfach bedienbar.

Welche Vorteile ergeben sich daraus für Errichter?

Jürgen Hövelmann: Der größte Vorteil liegt im vollständig funkbasierten Aufbau. Angesichts des Fachkräftemangels und steigender Arbeitskosten wird die Installationszeit immer wichtiger. Eine Funklösung lässt sich deutlich schneller nachrüsten als ein kabelgebundenes System. Häufig wird noch angenommen, ein Kabel sei grundsätzlich sicherer. Das entspricht jedoch nicht den geltenden Normen. Mit der EN 54-25 existiert eine eigene Norm für Funkübertragung-

gen, die deren Gleichwertigkeit bestätigt. Die Jury dürfte insbesondere die schnelle Installation, die einfache Inbetriebnahme, die Kombination von Brand- und Einbruchmeldetechnik sowie die integrierte Alarmverifikation überzeugt haben.

Gerade bei Bestandsgebäuden spart Funktechnik ja erheblichen Installationsaufwand...

Jürgen Hövelmann: Ganz genau. Kabelrassen nachzurüsten verursacht erhebliche Kosten. Viele verbinden Funk außerdem mit den Erfahrungen aus privaten WLAN-Netzen und befürchten Reichweitenprobleme. Deshalb verfügen unsere Systeme über zertifizierte Funk-Repeater, mit denen sich auch größere Gebäude zuverlässig abdecken lassen. Das gesamte System ist nach EN 54 geprüft und zertifiziert.

Ajax kommt aus der Ukraine – ein spannender Hintergrund.

Jürgen Hövelmann: Absolut. Wir haben intensiv mit den Entwicklern zusammengearbeitet, sind gemeinsam zu Kunden gefahren, haben Feedback direkt ins Produkt einfließen lassen. Die Entwicklung startete im Dezember 2023, im September 2025 hatten wir die ersten Geräte. Heute sind weltweit über 26.000 Systeme im Einsatz, in Deutschland knapp 1.000. Das zeigt: Wenn Innovation auf Innovation trifft, geht es auch in Europa schnell.

EPS vertreibt neben Ajax auch weitere Marken. Welche Rolle spielt diese Herstellerunabhängigkeit?

Jürgen Hövelmann: Wir verstehen uns seit vielen Jahren als herstellerunabhängiger Distributor. Deshalb wählen

wir für unsere Kunden jeweils die beste Lösung aus. Zu unserem Portfolio gehören unter anderem Dahua im Bereich Videotechnik, Jablotron sowie Fire Angel für Rauchwarnmelder. Dadurch können wir neutral beraten und individuelle Lösungen anbieten. Ajax ist dabei ein besonders innovativer Partner, mit dem wir gemeinsam die neue Brandwarnanlage entwickelt haben.

Wie entstand die Entwicklungspartnerschaft mit Ajax?

Jürgen Hövelmann: Das Produkt ist im Grunde ein europäisches Gemeinschaftsprojekt. Gemeinsam mit unseren Kunden haben wir Anforderungen gesammelt und dieses Feedback direkt an die Entwickler von Ajax weitergegeben. Innerhalb von anderthalb Jahren wurde daraus ein marktreifes Produkt. Mit der Entwicklung haben wir Ende 2023 begonnen, im September 2025 standen die ersten Systeme zur Verfügung. Inzwischen sind weltweit mehr als 26.000 Anlagen installiert, knapp 1.000 davon in Deutschland.

Was empfehlen Sie Errichtern, die sich mit dem System beschäftigen möchten?

Jürgen Hövelmann: Wir bieten bundesweit Schulungen an verschiedenen Standorten an. Uns geht es nicht nur darum, ein Produkt zu verkaufen, sondern unsere Partner umfassend zu qualifizieren. Ich empfehle jedem Errichter, sich das System unvoreingenommen anzusehen und selbst zu testen. Gerade in Schulen, Kindergärten, Feuerwehrhäusern oder Apotheken werden schnelle und wirtschaftliche Nachrüstlösungen benötigt. Dort spielt das System seine Stärken aus.

Wie hoch ist der Schulungsaufwand?

Jürgen Hövelmann: Unsere Zielgruppe sind qualifizierte Sicherheits- und Brandschutzeroberhalter. Für diese reicht in der Regel eine ein- bis zweitägige Produktschulung aus, um das System sicher installieren und in Betrieb nehmen zu können.

Abschließend ein Blick in die Zukunft: Wohin entwickelt sich die Sicherheitstechnik insgesamt nach Ihrer Wahrnehmung?

Jürgen Hövelmann: Künstliche Intelligenz wird die Branche nachhaltig verändern. Kameras werden intelligenter, Bildinformationen stehen nahezu in Echtzeit zur Verfügung und die einzelnen Gewerke wachsen immer stärker zusammen. Ich bin überzeugt, dass Alarmtechnik, Brandschutz und Videotechnik künftig zu integrierten Sicherheitssystemen verschmelzen werden. Genau diesen Weg haben wir mit unserer neuen Brandwarnanlage bereits eingeschlagen. **GIT**



SicherMacher
Der GIT-Talk mit den Marktführern



Jetzt ansehen:
das vollständige
Interview in unserem
Video-Podcast



EPS Vertriebs GmbH
www.eps-vertrieb.de



Brandmelderzentralen Serie BC800 - Der neue Maßstab im Brandschutz

- ✓ Intuitive Benutzerführung mit 10" Farb-Touch-Bildschirm
- ✓ Vernetzung von bis zu 127 Zentralen möglich
- ✓ Modularer Aufbau mit bis zu 20 Loops pro Zentrale

LST



**Besuchen Sie uns
am Stand 7D30!**

LITHIUM-IONEN-AKKUS

Tausend Grad und mehr

Lithium-Ionen-Akkus: wachsende Herausforderung für den Brandschutz

Lithium-Ionen-Akkus sind aus modernen Anwendungen nicht mehr wegzudenken. Ob in Handys, E-Bikes, Einweg-E-Zigaretten, Elektrowerkzeugen oder größeren Geräten wie E-Gabelstaplern – die leistungsstarken Energiespeicher treiben die Elektrifizierung in privaten Haushalten ebenso wie in Industrie und Logistik voran. Mit ihrer steigenden Verbreitung wächst jedoch auch das brandschutztechnische Risiko. „Entscheidend ist der sachgerechte Umgang“, sagt Mirco Sachse, Geschäftsführer von Infiprotec, einem Unternehmen, das sich auf moderne und nachhaltige Brandschutzlösungen spezialisiert hat.

■ Zurückführen lässt sich die Brandgefahr bei Lithium-Ionen-Akkus auf das sogenannte „thermische Durchgehen“. Dabei kommt es infolge eines Defekts oder einer Fehlbeanspruchung zu einer unkontrollierten Kettenreaktion im Inneren der Batterie. Temperaturen von über 1.000 °C sind möglich, wodurch sich Brände schnell ausbreiten können. Zu den häufigsten Auslösern zählen Überladung, mechanische Beschädigungen, Kurzschlüsse sowie die Verwendung ungeeigneter Ladegeräte.

„Für Gebäude und gewerbliche Nutzungen ergeben sich daraus spezifische Gefährdungslagen. Akkus werden häufig in Innenräumen geladen oder gelagert, etwa in Wohnungen, Werkstätten oder Lagerbereichen. Kommt es hier zu einem Brand, breitet sich dieser aufgrund der hohen Energiedichte schnell aus und kann zu erheblichen Sachschäden sowie Gefährdungen für Personen führen“, erläutert Sachse und ergänzt: „In Industrie und Logistik verschärft sich das Risiko zusätzlich durch größere Batteriesysteme, etwa in E-Gabelstaplern oder stationären Energiespeichern. Hier können Brände nicht nur Produktionsausfälle verursachen, sondern auch die Betriebssicherheit massiv beeinträchtigen.“

Brandschutzmaßnahmen: Prävention im Fokus

Um das Risiko von Bränden zu minimieren, lässt sich eine Kombination aus organisatorischen, baulichen und technischen Maßnahmen empfehlen. Zentrale Bedeutung hat die fachgerechte Nutzung und Wartung der Akkus. Beschädigte oder gealterte Batterien sollten umgehend außer Betrieb genommen werden.

Ebenso gilt es ausschließlich zertifiziertes Ladeequipment zu verwenden – um Überlastungen zu vermeiden – und Akkus nicht unbeaufsichtigt über Nacht oder in Fluchtwegen zu laden. Für gewerbliche Anwendungen und die Lagerung sind definierte Bereiche sinnvoll, die sich nicht in der Nähe von brennbaren Materialien befinden und brandschutztechnisch abgesichert sind, etwa durch feuerbeständige Abtrennungen oder automatische Löschsysteme.

„Da bei diesen Bränden enorme Hitze entsteht, gilt es zur Eindämmung Löschmittel mit einem hohen Kühleffekt einzusetzen – größere Mengen Wasser sind dazu in der Lage. Sprinkleranlagen reagieren beispielsweise schnell und können viel Wasser im Brandbereich abgeben. Sie eignen sich für eine Tiefgarage oder auch Industriehallen, Lager und Produktionsstätten“, berichtet der Brandschutzexperte und ergänzt: „Allerdings gibt es bisher keine perfekte Brandschutzlösung, denn Lithium-Ionen-Akkus selbst können nicht gelöscht werden. In der Regel werden die Akkus an eine sichere Stelle gebracht, um sie dort ausbrennen zu lassen.“

Um Feuer und Rauch möglichst frühzeitig zu detektieren, lassen sich deshalb Brandmeldeanlagen empfehlen. Sie können Alarmierungseinrichtungen und Löschsysteme aktivieren, Feuerschutztüren schließen, Rauch- und Wärmeabzüge starten und falls gewünscht die Feuerwehr anfordern. Ein häufig unterschätztes Thema ist auch die Entsorgung: Lithium-Ionen-Akkus dürfen keinesfalls im Hausmüll entsorgt werden, sondern müssen bei Rücknahmestellen im Handel oder Wertstoffhöfen abgegeben werden. **GIT**

Mirco Sachse,
Geschäftsführer
Infiprotec GmbH



Infiprotec GmbH
www.infiprotec.com



Brandschutzinnovationen für mehr Sicherheit

Auf der Messe Security Essen 2026 präsentiert die Wagner Deutschland GmbH innovative Lösungen für den anlagentechnischen Brandschutz. Im Mittelpunkt des Messeauftritts steht die neueste Generation der bewährten Titanus Produktfamilie: der Ansaugrauchmelder Titanus Rex. Dessen innovatives Detektormodul ermöglicht die besonders frühzeitige und zuverlässige Erkennung von Brandereignissen. Darüber hinaus zeigt die Tochtergesellschaft der Wagner Group GmbH das umfassende Portfolio des Unternehmens für den vorbeugenden Brandschutz. Das Spektrum reicht von der Branderkennung über aktive Brandvermeidung und Brandbekämpfung bis hin zu intelligentem Gefahrenmanagement und digitalen Services. „Mit Titanus Rex haben wir bei Wagner unsere bewährte Ansaugrauchmelder-Technologie konsequent weiterentwickelt und bieten unseren Kunden eine Lösung, die höchste Sensitivität mit maximaler Täuschungsalarmsicherheit verbindet“, sagt Markus Kock, Geschäftsführer der Wagner Deutschland GmbH.

www.wagnergroup.com

Security Essen: Halle 7, Stand 7A13

InnoTrans: Wagner zeigt Brandschutz für Schienenfahrzeuge

Wagner Rail präsentiert auf der InnoTrans 2026 in Berlin innovative Lösungen für den Brandschutz in Schienenfahrzeugen. Im Fokus des Messeauftritts stehen neue Lösungen für die Branddetektion, Brandbekämpfung und die Energieversorgung der Brandschutzsysteme, die speziell auf die Anforderungen moderner Schienenfahrzeuge ausgelegt sind. Ein besonderes Highlight ist der Fachvortrag von Dr. Markus Müller, Geschäftsführer der Wagner Rail GmbH, am 23. September 2026 auf der EventStage in Halle 2.2. Mit dem FirExting Water Mist Compact erweitert Wagner sein Portfolio um ein kompaktes Wassernebelssystem zur Brandbekämpfung in Fahrgasträumen, Schlafabteilen, Bordküchen oder Sanitärräumen. Die Lösung vereint Wasser und Stickstoff erstmals in einem einzigen Behälter und ermöglicht dadurch eine einfache, platzsparende Installation bei gleichzeitig hoher Wirksamkeit.

www.wagnergroup.com

InnoTrans 2026: Halle 2.2, Stand 250



XTR2

IMMER NOCH ZWEI PRÜFGERÄTE MIT SICH HERUMTRAGEN?

Es geht einfacher. Rauch- und Wärmeprüfung mit nur einem Prüfgerät.



▶ Sehen Sie selbst, wie XTR2 funktioniert



BRANDMELDETECHNIK

Brandmeldeanlagen mobil überwachen

Labor Strauss überarbeitet App für den Fernzugriff

Labor Strauss hat seine App für den mobilen Zugriff auf Brandmeldeanlagen neu entwickelt. Newreact übermittelt Ereignisse und Diagnosedaten an berechtigte Nutzer und soll den Fernzugriff auf angeschlossene Anlagen beschleunigen.

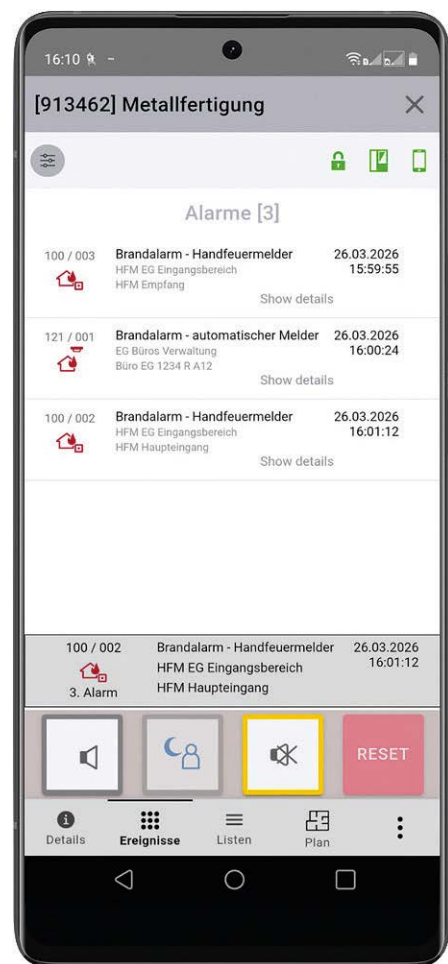
■ Brandmelderzentralen übermitteln kontinuierlich aktuelle Ereignisse der Anlagen, etwa über Rauchererkennung, Hitzeentwicklung oder Gaskonzentration. Newreact leitet diese Informationen per Push-Nachricht an zuvor festgelegte Empfänger weiter. Dazu können Eigentümer, Brandschutzbeauftragte, Servicetechniker und Feuerwehren gehören. Dies ermöglicht eine schnelle Lageeinschätzung schon vor dem Erreichen des Gefahrenorts.

Bei unkritischen Ereignissen spart die App Zeit, da die sofortige Anfahrt oder der Gang zur Brandmelderzentrale entfällt. Werden beispielsweise Störungen erkannt, können Wartungen oder Kontrollen vor einem möglichen Ausfall oder Fehlalarm eingeleitet werden. Der mobile Zugriff unterstützt Servicetechniker durch detaillierte Diagnosedaten, was die Instandhaltung der Brandmeldeanlagen wirtschaftlicher und zuverlässiger macht.

Fernzugriff für Betrieb und Instandhaltung

Das Grundprinzip von Newreact bleibt erhalten: Die App unterstützt die Anzeige anstehender Ereignisse, die Anlagenüberwachung sowie, abhängig von Berechtigung und Konfiguration, die Bedienung einzelner Anlagenteile. Nach Angaben des Unternehmens nutzt die Mehrzahl der Labor Strauss-Kunden das System nicht nur zur temporären Unterstützung bei der Anlagenwartung, der Anzeige anstehender Ereignisse oder der Bedienung von Anlagenteilen. Vielmehr ist es permanent mit den Servicestellen oder der Feuerwehr verbunden und wird zur Anlagenüberwachung genutzt.

„Unabhängig vom Anwendungszweck bleibt die wichtigste Funktion von Newreact nach wie vor, die Situation vor Ort zu überblicken und anstehende Ereignisse schnell zu übertragen“, sagt Andreas Schumacher, Produktmanager bei Labor Strauss. Die

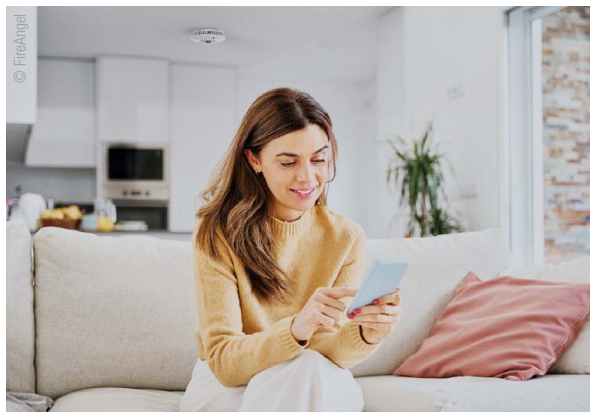


Die App Newreact übermittelt Ereignisse und Diagnosedaten angeschlossener Brandmeldeanlagen an mobile Endgeräte

neu entwickelte Anwendung ist für mobile Endgeräte vorgesehen; für den Fernzugriff müssen die jeweiligen Brandmelderzentralen mit dem Newreact-Server verbunden sein. **GIT**



Labor Strauss Gruppe
www.laborstrauss.com



Moderner Brandschutz von FireAngel auf der FeuerTrutz

FireAngel zeigte auf der FeuerTrutz 2026 in Nürnberg, dass moderner Brandschutz weit über den klassischen Rauchmelder hinausgeht. Auf seinem Messestand präsentierte das Unternehmen gemeinsam mit seinem langjährigen Vertriebspartner EPS sein Portfolio für den deutschen Markt mit mehreren Neuheiten. Im Mittelpunkt des Messeauftritts stand die Vorstellung eines neuen Rauchwarnmelders der Kategorie C für den deutschen Markt. Die Produktneuheit richtet sich gezielt an Messgesellschaften, Facility-Manager und die Wohnungswirtschaft, die Rauchmelder effizient und normenkonform betreiben müssen. Der besondere Vorteil: Über eine Funkanbindung an ein zentrales Gateway lassen sich Gerätestatus, Batteriepegel und mögliche Störungen per Ferninspektion auslesen – der aufwendige Gang in jede einzelne Wohnung entfällt. <https://fireangel.de.com>

Highlight auf der FeuerTrutz 2026:
Der barrierefreie Türschließer TS 7000
von Geze vereint hohen Bedien-
komfort mit innovativem Design



FeuerTrutz: Geze zeigte Lösungen für den vorbeugenden Brandschutz

Geze zeigte auf der internationalen Fachmesse FeuerTrutz in Nürnberg, wie sich im Sinne von „Connecting expertise – building solutions“ Brandschutzanforderungen mit intelligenter Tür-, Fenster- und Sicherheitstechnik zukunftsicher umsetzen lassen. Im Fokus standen innovative Produkte, die Brandschutzanforderungen mit Barrierefreiheit und Begehungskomfort vereinen. Vor dem geplanten Marktstart im Herbst präsentierte das Unternehmen den neuen Türschließer TS 7000 als Highlight des Messeauftritts: Die Lösung vereint zukunftsweisendes Design mit hohem Bedienkomfort und innovativen Funktionen für mehr Barrierefreiheit. Ausgestattet mit der Easyflow-Technologie funktioniert der TS 7000 auch in sicherheitskritischen Montagesituationen wie in Schleusen oder in Fluchtwegen zuverlässig und ohne Nachjustierung, unabhängig von Temperatur oder Jahreszeit.

www.geze.de

Wirtschaftliche Brandschutzlösungen von Inotec

Wie lassen sich Brandschutz und Wirtschaftlichkeit miteinander verbinden? Inotec Sicherheitstechnik zeigte auf der Brandschutzfachmesse FeuerTrutz praxistaugliche Antworten. Richtungsvariable Sicherheitsbeleuchtung steigert nicht nur den Personenschutz, sondern kann gleichzeitig die Gesamtbaukosten deutlich reduzieren. Dynamische Fluchtweglenkungssysteme bieten eine wirtschaftliche Möglichkeit, bauliche Anforderungen zu kompensieren, die im Neubau oder im Bestand nur mit hohem Aufwand umsetzbar wären. Wie sich Sicherheit und Wirtschaftlichkeit miteinander verbinden lassen, zeigte Inotec auf der FeuerTrutz live. Das dezentrale Notlichtsystem CLS Fusion ermöglicht in Verbindung mit der dynamischen TFT-Rettungszeichenleuchte FL 2820-TFT den einfachen Aufbau richtungsvariabler Sicherheitsbeleuchtungssysteme – ohne zusätzliche Verkabelung und mit weitgehendem Verzicht auf kostenintensiven Funktionserhalt.

www.inotec-licht.de



© Inotec Sicherheitstechnik GmbH

Großhandel für professionelle Sicherheitstechnik

EPS

Weil jede Sekunde zählt.

AJAX **JABLONTRON** **Alhuda** **FireAngel**
UR FOG **Milesight** und viele weitere Marken ...

☎ 02507 98750-0

✉ info@eps-vertrieb.de

🌐 www.eps-vertrieb.de

**security
essen 26**
the number one

HALLE 7
Stand 7F21
Kostenlose
Freikarten:





JUBILÄEN

50 Jahre Wagner

Vom Ingenieurbüro zur internationalen Unternehmensgruppe

Seit inzwischen 50 Jahren entwickelt Wagner Lösungen, die Menschen schützen, Sachwerte bewahren und die Betriebssicherheit in sensiblen Umgebungen gewährleisten. Aus einem Ingenieurbüro ist ein international tätiger Technologieführer im anlagentechnischen Brandschutz geworden. Heute ist das Unternehmen in 15 Ländern vertreten und beschäftigt weltweit mehr als 800 Mitarbeiter.

Die Geschichte des Unternehmens beginnt im Jahr 1976 mit der Gründung des Ingenieurbüros von Dipl.-Ing. Werner Wagner. Seine Vision war es von Anfang an, technische Herausforderungen nicht mit Standardlösungen zu beantworten, sondern neue Wege zu beschreiten. Diese Haltung prägt das Unternehmen bis heute. Was als spezialisierter Anbieter von Sicherheits- und Meldetechnik begann, entwickelte sich schrittweise zu einem Innovationsunternehmen für anlagentechnischen Brandschutz.

Die Gründungsmotivation war dabei eng mit einem ingenieurgetriebenen Anspruch verbunden: Risiken verstehen, Ursachen analysieren und Lösungen entwickeln, die nicht nur reagieren, sondern Gefahren möglichst früh erkennen oder sogar verhindern. Dieser Gedanke führte das Unternehmen früh zu einem Paradigmenwechsel im Brandschutz. Statt ausschließlich auf Löschtechnik zu setzen, rückte die Frage in den Mittelpunkt, wie Brände bereits in

ihrer Entstehungsphase erkannt oder unter definierten Bedingungen sogar ganz vermieden werden können.

Neben Gründer Werner Wagner übernimmt auch sein Sohn, Dipl.-Ing. Torsten Wagner, Verantwortung in der Geschäftsführung des Familienunternehmens. Auch die dritte Generation der Unternehmerfamilie bringt sich bereits in das Unternehmen ein. Diese generationenübergreifende Kontinuität ermöglicht langfristiges strategisches Denken, nachhaltige Investitionen und eine Unternehmenskultur, die Innovation mit Verantwortung verbindet.

Herausforderungen als Treiber für Innovation

Die vergangenen fünf Jahrzehnte waren von tiefgreifenden Veränderungen geprägt. Die Digitalisierung von Geschäftsprozessen, die zunehmende Automatisierung von Logistik- und Produktionsanlagen sowie steigende Anforderungen an Verfügbarkeit und Aus-

fallsicherheit haben auch den Brandschutz grundlegend verändert.

Besonders deutlich zeigt sich dies in hochautomatisierten und sicherheitskritischen Umgebungen, in denen Verfügbarkeit und Betriebskontinuität heute zentrale Anforderungen sind. In solchen Umgebungen können selbst kleinste Brandereignisse erhebliche wirtschaftliche Schäden oder den Verlust unwiederbringlicher Kulturgüter verursachen. Gleichzeitig wachsen die Anforderungen an Nachhaltigkeit, Energieeffizienz und Betriebskontinuität. Für Wagner bedeutet dies, bestehende Technologien kontinuierlich weiterzuentwickeln und neue Lösungen für immer komplexere Anwendungsfelder zu schaffen.

Hinzu kamen und kommen regulatorische Veränderungen und steigende internationale Anforderungen. Als global agierendes Unternehmen bringt Wagner technische Innovationen mit unterschiedlichen Normen, Zertifizierungen und Mark-

◀ Leidenschaft für den Brandschutz:
Drei Generationen der Gründerfamilie: v. l. n. r.:
Dipl.-Ing. Torsten Wagner, ((Platz lassen,
Name muss erfragt werden)), Werner Wagner

terfordernissen – regional und international – in Einklang. Die Fähigkeit, Herausforderungen dieser Art als Entwicklungschancen zu nutzen, wurde zu einem wesentlichen Erfolgsfaktor.

Meilensteine einer Innovationsgeschichte

Bereits in den 1980er-Jahren beschäftigte es sich intensiv mit hochsensibler Branddetektion. Auf der Sicherheitsmesse Security Essen stellte das Unternehmen bereits 1986 – also genau vor 40 Jahren – seinen ersten Ansaugrauchmelder Titanus vor. Diese Technologie entwickelte sich in den folgenden Jahrzehnten zu einem wichtigen Baustein moderner Brandfrüherkennung.

Ein weiterer bedeutender Schritt erfolgte in den 1990er-Jahren mit der Einführung von Stickstoff als natürlichem Löschmittel. Kurz darauf präsentierte Wagner die ersten Oxyreduct-Systeme zur aktiven Brandvermeidung durch Sauerstoffreduzierung. Die Grundidee: Brände gar nicht erst entstehen zu lassen. Dies wird möglich, indem die Sauerstoffkonzentration im geschützten Raum permanent auf einem Niveau gehalten wird, in dem Brände nicht entstehen bzw. sich nicht entwickeln können. Mit dieser Technologie etablierte das Unternehmen ein Konzept, das heute weltweit in automatisierten Lager- und Logistikbereichen eingesetzt wird – vom Kunstdepot bis zum Tiefkühlager.

Parallel dazu begann die internationale Expansion der Unternehmensgruppe. Tochtergesellschaften in Europa, Nordamerika



Das Sauerstoffreduzierungssystem Oxyreduct schützt ein Hochregallager

und Asien-Pazifik ermöglichten es, die eigenen Technologien weltweit verfügbar zu machen und lokale Kundenanforderungen direkt zu berücksichtigen.

Die wichtigsten Produktlinien

Das heutige Portfolio basiert auf einem ganzheitlichen Ansatz des anlagentechnischen Brandschutzes. Dazu gehören insbesondere Systeme zur Brandfrüherkennung, zur Brandvermeidung und zur Brandbekämpfung. Neben den Ansaugrauchmeldern und Sauerstoffreduzierungssystemen sind dies Löschsysteme, Gefahrenmanagementlösungen sowie umfassende Service- und Instandhaltungsleistungen.

Besonders deutlich wird die technologische Breite des Unternehmens in den vielfältigen Anwendungsbereichen. Die Lösungen des Unternehmens schützen heute Rechenzentren und IT-Infrastrukturen,

automatisierte Logistik- und Hochregallager, industrielle Produktionsanlagen, Tiefkühlhäuser sowie kulturell wertvolle Einrichtungen wie Museen, Archive und Bibliotheken oder Konzerthäuser. Hinzu kommen Spezialanwendungen etwa im Bereich Schienenverkehr. Allen Einsatzfeldern gemeinsam ist die Anforderung, Betriebsunterbrechungen zu vermeiden, kritische Prozesse abzusichern und gleichzeitig Menschen, Sachwerte und unverzichtbare Daten nachhaltig zu schützen.

Charakteristisch ist dabei die konsequente Ausrichtung auf individuelle Kundenanforderungen. Von der Risikoanalyse über Planung und Installation bis hin zum laufenden Betrieb entsteht ein integriertes Schutzkonzept aus einer Hand.

Zukunft gestalten, Sicherheit leben

Aus Sicht von Wagner wird die Zukunft des Brandschutzes stärker denn je von Prävention geprägt sein. Die Kombination aus hochsensibler Detektion, intelligenter Datenanalyse und aktiver Brandvermeidung eröffnet neue Möglichkeiten, Gefahren frühzeitig zu erkennen und Betriebsunterbrechungen zu vermeiden. Gleichzeitig werden Nachhaltigkeit, Automatisierung und Digitalisierung die Entwicklung neuer Lösungen beschleunigen. **GIT**

Security Essen: Halle 7, Stand 7 A13



Der Ansaugrauchmelder Titanus Rex ist VdS-zertifiziert und vereint höchste Sensitivität und Täuschungsalarmsicherheit mit smarten digitalen Lösungen

Lesen Sie auf der nächsten Seite das Interview mit Unternehmensgründer, Geschäftsführer und Gesellschafter Dipl.-Ing. Werner Wagner



Wagner Group GmbH
www.wagner-group.com



Unternehmensgründer, Geschäftsführer und Gesellschafter Dipl.-Ing. Werner Wagner

— GIT SICHERHEIT: Herr Wagner, als erstes einmal: Herzlichen Glückwunsch zum 50-jährigen Firmenjubiläum! Können Sie einmal kurz erzählen, wie es zur Gründung kam?

Werner Wagner: Vielen Dank für den Glückwunsch. Angefangen hat alles 1976 ganz bodenständig im Keller unseres Hauses. Direkt nach meinem Ingenieurstudium habe ich mich selbstständig gemacht, basierend auf meiner Leidenschaft für die Entwicklung elektronischer Sicherheitstechnik und dem Gedanken, mit innovativen Technologien Menschen und Werte besser zu schützen.

Schon damals hat mich der Pioniergeist angetrieben, bestehende Lösungen weiterzudenken und neue Anwendungsfelder zu erschließen. Aus diesen Anfängen entstand Schritt für Schritt das Unternehmen Wagner, das sich später konsequent auf innovative Brandschutz- und Brandvermeidungslösungen spezialisiert hat. Was als kleines Ingenieurbüro begann, ist heute eine international tätige Unternehmensgruppe mit mehr als 800 Mitarbeitern. Für mich ist das der beste Beweis dafür, dass große Entwicklungen oft mit einer mutigen Idee und sehr bescheidenen Anfängen starten.

Hätten Sie damals gedacht, dass das Unternehmen eine solche Zukunft haben wird? Was waren im Rückblick die wichtigsten Entscheidungen und Entwicklungen, die den nachhaltigen Erfolg von Wagner begründet haben?

Werner Wagner: Als wir gestartet sind, standen für uns vor allem die Begeisterung für Technik und der Wille, Herausforderungen zu lösen, im Vordergrund. Dass daraus einmal eine international erfolgreiche Unternehmensgruppe entstehen würde, hatten wir damals nicht im Blick.

Rückblickend waren vor allem der Mut zu neuen Wegen, unsere Innovationskraft und die Menschen bei Wagner entscheidend. Ein wichtiger Meilenstein war Anfang der 1980er-Jahre unser erster Großauftrag für Sicherungsanlagen für das Zwischenlager Gorleben. Als kleine Firma mit nur 20 Mitarbeitenden haben wir einen Auftrag mit einem Volumen von 3 Millionen DM erhalten.

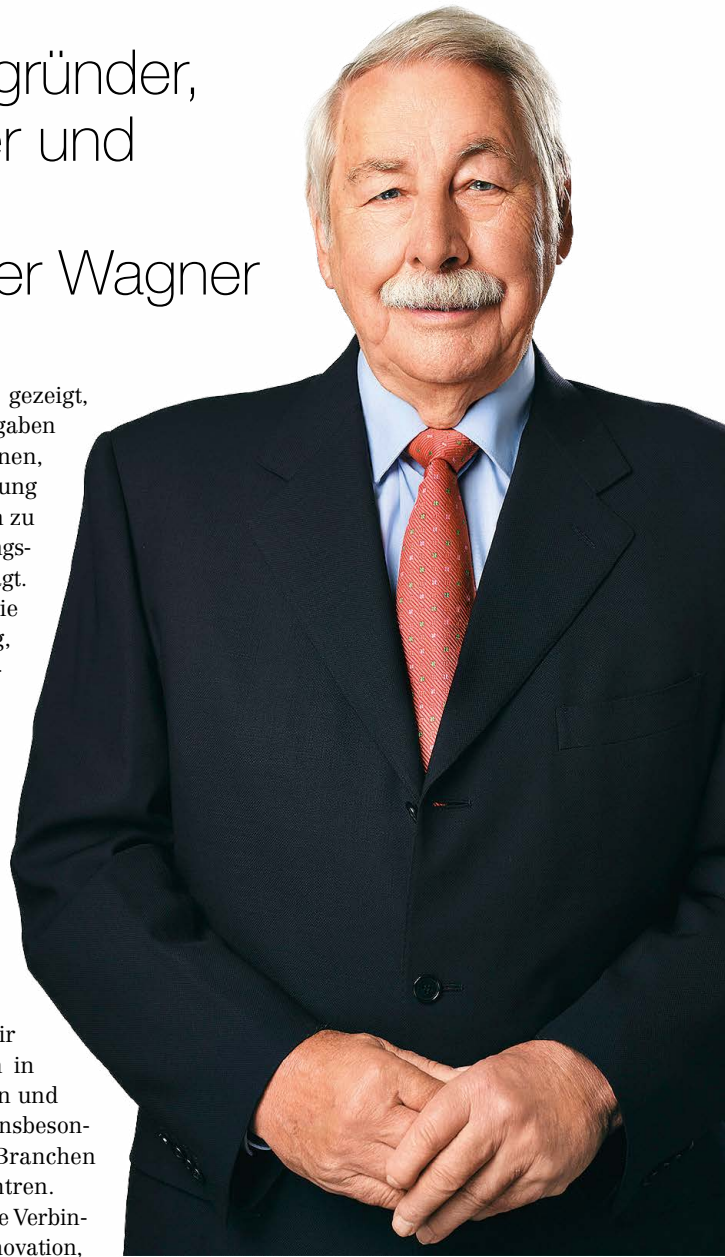
Dieses Projekt hat uns gezeigt, dass wir auch komplexe Aufgaben erfolgreich bewältigen können, und es hat unsere Entwicklung vom kleinen Entwicklerteam zu einem leistungsfähigen Lösungsanbieter entscheidend geprägt.

Ebenso wichtig war die strategische Entscheidung, uns auf innovative Brandschutz- und Brandvermeidungslösungen zu konzentrieren und diese kontinuierlich weiterzuentwickeln wie beispielsweise die Idee, Stickstoff zur aktiven Brandvermeidung einzusetzen. Auf diesem Ansatz aufbauend haben wir die Internationalisierung konsequent vorangetrieben. Heute sind wir mit eigenen Gesellschaften in wichtigen Märkten vertreten und begleiten Kunden weltweit, insbesondere in wachstumsstarken Branchen wie Logistik und Rechenzentren.

Aus meiner Sicht bildet die Verbindung aus technologischer Innovation, unternehmerischem Mut und internationaler Ausrichtung die Grundlage für den nachhaltigen Erfolg von Wagner.

Die Welt des Brandschutzes wurde durch Ihr Unternehmen mitgeprägt und ist heute eine durchaus andere als noch vor fünfzig Jahren. Vor dem Horizont Ihrer Erfahrung: Wo geht die Brandschutzreise in den nächsten Jahrzehnten nach Ihrer Einschätzung noch hin?

Werner Wagner: In den vergangenen 50 Jahren hat sich der Brandschutz von einer überwiegend reaktiven Disziplin zu einem zunehmend präventiven Ansatz entwickelt. Genau dieser Trend wird sich meines Erachtens weiter verstärken. Das Ziel wird künftig immer stärker sein, Brände gar nicht erst entstehen zu lassen, anstatt sie erst nach ihrer Entstehung zu bekämpfen. Aus ökonomischen, aber auch aus ökologischen Gründen. Denn Brandschutz ist Umweltschutz.



Gleichzeitig werden die Anforderungen weiter wachsen. Digitalisierung, Automatisierung, leistungsstarke Rechenzentren oder moderne Logistikzentren bringen neue Risiken mit sich, die intelligente und hochspezialisierte Schutzkonzepte erforderlich machen. Technologien wie künstliche Intelligenz, vernetzte Sensorsysteme und datenbasierte Analysen werden dabei eine immer größere Rolle spielen.

Trotz aller technischen Fortschritte bleibt aber eines unverändert: Brandschutz dient dem Schutz von Menschen, Werten und kritischer Infrastruktur. Deshalb bin ich überzeugt, dass innovative Brandvermeidung und frühestmögliche Branderkennung die Zukunft prägen werden. Für Wagner wird es auch weiterhin darum gehen, mit technologischer Kompetenz und Pioniergeist Lösungen zu entwickeln, die unseren internationalen Kunden ein Höchstmaß an Sicherheit bieten. **GIT**



Siemens stellt nächste Generation von Brandmeldern vor

Siemens Smart Infrastructure bringt seinen neuen Brandmelder Sintesio Nova auf den deutschen Markt. Das Portfolio überführt den klassischen Brandschutz in einen proaktiven, intelligenten und zukunftsfähigen Ansatz – und schafft damit eine wichtige technologische Grundlage auf dem Weg zu autonomen Gebäuden. Die neue Lösung erhöht die Betriebssicherheit, verbessert die Effizienz von Service- und Wartungsteams und erleichtert es, Systeme zu modernisieren. Gleichzeitig ermöglicht die Cloud-Konnektivität datenbasierte digitale Services. Aufgrund ihrer fortschrittlichen Technologie erfüllen die Systeme auch die Anforderungen verschiedener Branchen. In Krankenhäusern, in denen sowohl Patientensicherheit als auch ein effizienter Betrieb entscheidend sind, sorgen die neuen Siemens-Brandmelder durch kontinuierliche, autonome Detektion für mehr Zuverlässigkeit. Die integrierte Smoke Entry Supervision (SES)-Technologie überwacht die Raucheintrittsöffnung in Echtzeit und stellt die permanente Meldefähigkeit sicher, sodass Betreiber unmittelbar eingreifen können, bevor sich kritische Situationen entwickeln. www.siemens.com

Miele Safety AirPro für die Atemschutz-Aufbereitung

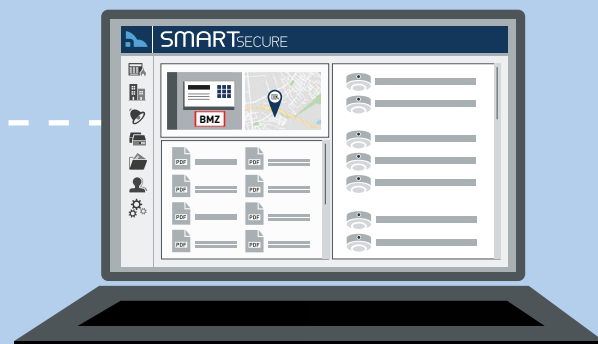
Miele Professional präsentierte sich wieder auf der Interschutz in Hannover. Von leistungsstarken Waschmaschinen über spezialisierte Trocknungslösungen bis hin zu digitalen Services bietet das Unternehmen alles aus einer Hand – für mehr Sicherheit, Hygiene und Transparenz im Einsatzalltag von Feuerwehren. Die bewährte Systemlösung umfasst besonders große, vernetzbare Waschmaschinen mit Beladefähigkeiten von 27 und 35 Kilogramm. Zudem sprüht die neue Technologie PowerGuard Pro Imprägniermittel präzise auf die Außenseiten der Bekleidung. Zum Portfolio gehören auch Spezialspüler für die Reinigung und Trocknung von Atemschutzmaterialien und Lungenautomaten. Im Fokus standen dabei die Lösungen mit der Safety AirPro-Technologie, die durch eine integrierte Druckluftversorgung das Eindringen von Feuchtigkeit und Prozesschemikalien während der maschinellen Aufbereitung von PSA verhindert und so die Sicherheit der Einsatzkräfte erhöht. www.miele.de



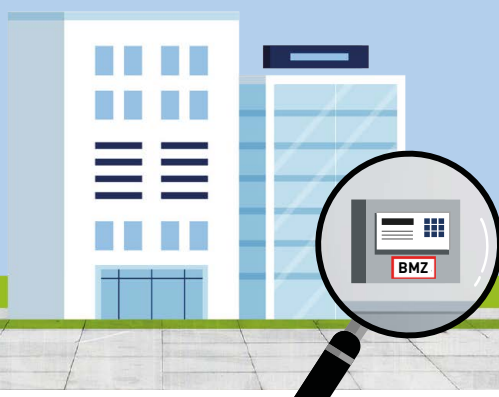
WIR DIGITALISIEREN BRANDMELDEANLAGEN



HERSTELLERUNABHÄNGIG



mit



AUTONOME GEBÄUDE

IoT-vernetzt in die Zukunft

Wie sich Brandschutz im Zeitalter
autonomer Gebäude verändert

Digitale Lösungen haben in der Brandmeldetechnik längst Einzug gehalten. Ein Prinzip ist dennoch seit Jahrzehnten weitgehend unverändert geblieben: Die Systeme lösen nur anlassbezogen aus. Dem stellt Siemens nun mit IoT-vernetzten Geräten einen neuen Ansatz entgegen: Cloudbasiert nutzen diese nicht nur neue Detektions- und Selbstüberwachungstechnologien. Sie übernehmen auch zentrale Aufgaben in autonomen Gebäuden.

■ Herkömmliche Brandmeldesysteme arbeiten überwiegend ereignisbasiert. Das heißt, sie reagieren auf definierte Schwellenwerte zwar möglichst früh, erkennen sie aber naturgemäß doch erst in einem fortgeschrittenen Stadium. Mit einer Neuentwicklung ändert Siemens diesen Ansatz nun grundlegend: Die neuen Brandmelder Sinteso Nova erfassen kontinuierlich, analysieren und interpretieren Daten. Im Ergebnis ermöglichen solche kontinuierlichen, datenbasierten Systeme damit eine neue Qualität der Brandsicherheit. Darüber hinaus ebnen sie den Weg zu zukunftsfähigen Gebäuden, die sich zunehmend selbst überwachen und organisieren. Denn sogenannte autonome Gebäude reagieren nicht nur auf Ereignisse, sondern bewerten aktiv Zustände und optimieren sie. Brandschutz wird damit zu einem integralen Bestandteil eines intelligenten, selbstlernenden Gebäudebetriebs.

Schnelle und präzise Branderkennung durch intelligente Sensorik

Ein zentrales Merkmal von Sinteso Nova ist die Fähigkeit zur sehr schnellen Detektion bei gleichzeitig höchster Täuschungsalarmsicherheit. Die Basis dafür bietet die ASApplus-(Advanced Signal Analysis)-Technologie, welche optische Multiwellenlängen-Sensorik mit dualer thermischer Detektion kombi-

niert. Für die neue Brandmelder-Generation hat Siemens dieses bewährte Verfahren nun nochmals auf ein neues technisches Niveau gehoben: Bis zu zehn Sensoren im Brandmelder analysieren kontinuierlich unterschiedliche Signalquellen und setzen diese in Beziehung zueinander. Dadurch wird nicht nur erkannt, ob Rauch vorhanden ist, sondern auch, ob es sich tatsächlich um ein Brandereignis handelt.

Diese differenzierte Analyse führt zu einer deutlich verbesserten Reaktionsgeschwindigkeit bei gleichzeitig reduzierten Fehlalarmen. Die Brandmelder Sinteso Nova leisten hier einen wesentlichen Beitrag zur Erhöhung der Betriebssicherheit. So lassen sich unnötige Evakuierungsmaßnahmen und Betriebsunterbrechungen vermeiden. Besonders in kritischen Bereichen wie Krankenhäusern oder Rechenzentren ist diese Kombination aus Geschwindigkeit und Präzision entscheidend, da jede Verzögerung oder Fehlinterpretation erhebliche

Folgen haben kann. Von der Leistungsfähigkeit dieser Technologie ist Siemens so überzeugt, dass das Unternehmen eine Vergütungsgarantie anbietet, die im Falle eines Fehlalarms die Kosten eines Feuerwehreinsatzes bis 2.000 Euro übernimmt.

Permanente Meldefähigkeit durch Raucheintrittsüberwachung (SES)

Ein herausragendes Merkmal der neuen Generation von Brandmeldern ist zudem die integrierte Raucheintrittsüberwachung (Smoke Entry Supervision, SES). Diese Technologie überwacht kontinuierlich die Raucheintrittsöffnungen der Melder und stellt sicher, dass Rauch jederzeit ungehindert detektiert werden kann. Damit ist eine permanente Meldefähigkeit in Echtzeit sichergestellt, sodass Betreiber frühzeitig reagieren können, bevor sich kritische Situationen entwickeln.

Der besondere Nutzen zeigt sich vor allem im laufenden Betrieb: Diese kontinuierliche Überwachung ergänzt die intelligenten Detektionsalgorithmen der Melder und geht deutlich über klassische Wartungsansätze hinaus, da sie nicht erst bei Inspektionen greift, sondern dauerhaft aktiv ist. Dadurch wird ein häufig unterschätztes Risiko adressiert, nämlich die schleichende Beeinträchtigung von Meldern durch Verschmutzung oder mechanische Einflüsse. In stark frequentierten oder anspruchsvollen



Carsten Meißner
Senior Consultant
Safety Lifecycle
Portfolio, Siemens
Smart Infrastructure,
Deutschland

vollen Umgebungen sorgt SES dafür, dass die Detektionsqualität langfristig stabil bleibt, wodurch ein wesentlicher Beitrag zur Zuverlässigkeit und Verfügbarkeit des gesamten Systems geleistet wird.

IoT-Vernetzung als Grundlage für autonome, nachhaltige Gebäude

Sinteso Nova ist von Grund auf als IoT-fähiges System konzipiert und kann nahtlos in cloudbasierte Plattformen integriert werden. Diese Vernetzung ermöglicht eine Vielzahl neuer Funktionen, die über die klassische Branddetektion hinausgehen. Zu den wichtigsten Aspekten zählen die Echtzeitüberwachung aller Systemzustände, Ferndiagnosen und digitale Servicezugriffe, vorausschauende Wartung auf Basis von Zustandsdaten bzw. digitale Reports und die Integration in die offene Plattform Building X und weitere zukünftige, digitale Anwendungen.

Als Teil des Siemens Xcelerator Portfolios sind die neuen Melder mit cloudbasierten Anwendungen kompatibel wie etwa mit den Building X Fire Connect Apps. Darüber hinaus können die von den Meldern erfassten Temperaturdaten übertragen und genutzt werden: Mit der Building X Environmental and Air Quality Application FIRE lassen sich zusätzliche Potenziale zur Steigerung der Energieeffizienz und Nachhaltigkeit eines Gebäudes erschließen.

Die Grundlage dafür bilden die umfangreichen Informationen, die die Melder über ihre zehn Sensoren erfassen. Damit stehen in einem Brandmelder so viele Sensorinformationen wie nie zuvor zur Verfügung. Die daraus resultierende Datentiefe schafft eine einzigartige Basis, um sicherheitsrelevante Ereignisse frühzeitig zu erkennen und gleichzeitig den Zustand eines Gebäudes ganzheitlich zu verstehen.

Der kontinuierliche Datenfluss liefert neben klassischen Brandschutzinformationen auch Erkenntnisse zur Temperaturentwicklung, Luftzusammensetzung und weiteren Umgebungsparametern. Durch die intelligente Analyse dieser Daten können Veränderungen der Umgebungsbedingungen und potenzielle Anomalien frühzeitig erkannt werden. Dies schafft Transparenz über Betriebszustände und unterstützt dabei, Optimierungspotenziale für Brandschutz, Gebäudebetrieb, Raumklima und Energieeffizienz gezielt zu erschließen.

Damit entwickelt sich der Brandschutz zu einem aktiven Bestandteil der Gebäudeintelligenz und unterstützt die Vision voll-

ständig autonomer Gebäude: ein System, das sich selbst optimiert, Fehler frühzeitig erkennt, Maßnahmen einleitet und nur dann menschliches Eingreifen erfordert, wenn es wirklich notwendig ist. Künstliche Intelligenz ist dabei kein Selbstzweck, sondern ein Werkzeug, um Gebäude wirtschaftlicher, komfortabler und resilienter zu betreiben.

Anwendungsvielfalt, Nachhaltigkeit und Skalierbarkeit

Die Sinteso Nova Brandmelder sind so konzipiert, dass sie in unterschiedlichsten Anwendungen eingesetzt werden können wie zum Beispiel in Krankenhäusern, Rechenzentren, Universitäten, Hotels sowie an Industrie- und Logistikstandorten. Allen diesen Umgebungen ist gemeinsam, dass sie hohe Anforderungen an Verfügbarkeit, Sicherheit und Effizienz stellen.

Rechenzentren zum Beispiel sehen sich aufgrund der hohen Energiedichte und der Notwendigkeit eines unterbrechungsfreien Betriebs mit besonderen Anforderungen an den Brandschutz konfrontiert. Risiken wie Überhitzung und elektrische Fehlfunktionen müssen frühzeitig erkannt werden. Die Brandmelder Sinteso Nova unterstützen Betreiber nicht nur dabei, kritische IT- und Elektroinfrastrukturen verfügbarer zu machen, sondern geben auch tiefere Einblicke in den Zustand der Systeme. Cloudbasierte Überwachung und vorausschauende Wartung ermöglichen es, schnell und proaktiv zu reagieren. So lassen sich Störungen minimieren, während die sensiblen Anlagen gleichzeitig effizient geschützt werden.

In anderen Branchen finden sich häufig mehrere, räumlich verteilte Gebäude mit unterschiedlichen Nutzungsbereichen. Hier ist ein zentralisiertes und zuverlässiges Brandschutzmanagement essenziell, um Sicherheitsstandards sicherzustellen, ohne den laufenden Betrieb oder das Gästelerlebnis zu beeinträchtigen. Die Skalierbarkeit der Systeme ermöglicht es hier, sowohl einzelne Gebäude als auch komplexe, verteilte Liegenschaften zentral zu überwachen und zu steuern.



In Rechenzentren zum Beispiel unterstützen IoT-vernetzte Brandmelder Betreiber nicht nur dabei, kritische Infrastrukturen verfügbarer zu machen, sondern erlauben auch tiefere Einblicke in den Zustand der Systeme



Siemens stellt die nächste Generation der Brandmelder Sinteso Nova vor, die fortschrittliche Detektion mit Cloud-Konnektivität und IoT-Funktionen verbindet

Die Möglichkeit zur schrittweisen Modernisierung bestehender Anlagen sorgt zudem dafür, dass Investitionen geschützt werden und Systeme ohne vollständigen Austausch der Infrastruktur auf den neuesten Stand gebracht werden können. Dabei bleiben bestehende Brandmeldezentralen kompatibel, sodass es nicht erforderlich ist, Anlagen vollständig auszutauschen. Dank einer Plug-and-Play-Integration einschließlich der automatischen Übernahme bestehender Konfigurationen lassen sich Installationsaufwand sowie Risiken deutlich reduzieren.

Die Nachhaltigkeit des Systems wird durch das Siemens EcoTech Label bestätigt. Dies umfasst energieeffiziente Elektronik, optimierte Materialien und ein ressourcenschonendes Design mit verbesserter CO₂-Bilanz.

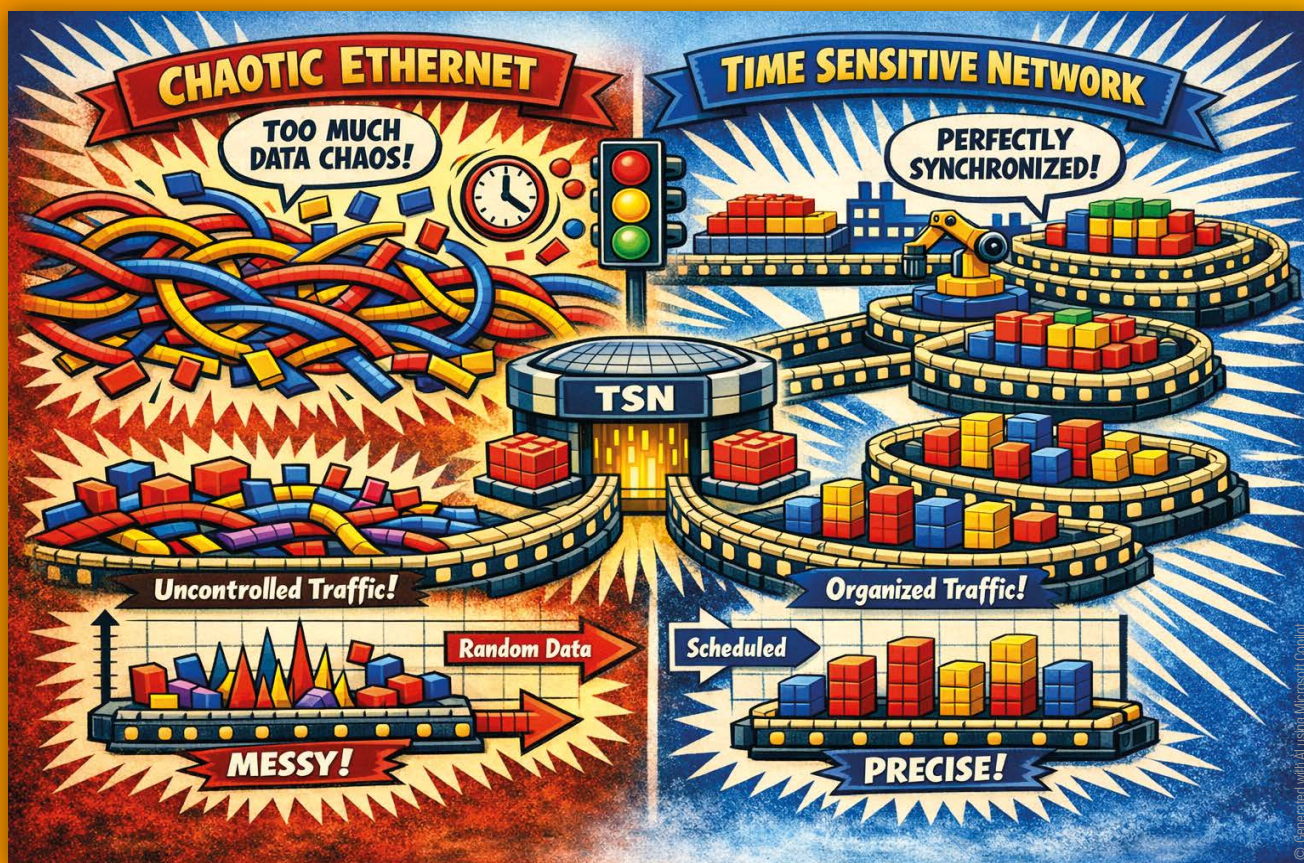
Vision intelligenter, sicherer und effizienter Gebäude

Mit Sinteso Nova setzt Siemens die eigene Tradition im Brandschutz konsequent fort und entwickelt sie in Richtung digitaler, intelligenter Systeme weiter. Die Verbindung aus schneller und präziser Detektion, kontinuierlicher Selbstüberwachung durch SES und umfassender IoT-Vernetzung schafft eine neue Qualität der Sicherheit. Gleichzeitig bildet die Integration von Cybersicherheit die Grundlage für einen zuverlässigen Betrieb in hochvernetzten Umgebungen. Brandschutz wird dadurch zu einem zentralen Baustein autonomer Gebäude, die sich selbst überwachen und optimieren können. Somit steht Sinteso Nova nicht nur für eine neue Produktgeneration, sondern für einen grundlegenden Paradigmenwechsel, der die Vision intelligenter, sicherer und effizienter Gebäude Realität werden lässt. **GIT**



Siemens AG

siemens.de/sinteso-nova



Digitalisierung und IT/OT-Integration stellen neue Anforderungen an die industrielle Kommunikation in Maschinen und Anlagen: Neben Funktionaler Sicherheit und Cybersecurity rücken große – parallel zu übertragende – Datenmengen sowie steigende Erwartungen an Betriebssicherheit und Verfügbarkeit in den Fokus. Hier setzt Time Sensitive Networking (TSN) an: Deterministische Kommunikation in Ethernet-basierten-Netzwerken liefert die Grundlage für sichere und zuverlässige Automatisierungslösungen.

Die Artikel-Serie in Kooperation von VDMA Elektrische Automation und GIT SICHERHEIT gibt eine Einführung in die Technologie, beleuchtet verschiedene Anwendungsszenarien und zeigt anhand von drei Industrial-Ethernet-Ökosystemen, worauf es bei Auswahl und Einsatz von TSN zu achten gilt.

VDMA-Ansprechpartner Birgit Sellmaier betreut im Fachverband Elektrische Automation Technik- und Technologiethematen wie Steuerungstechnik und Funktionale Sicherheit in der Anwendung im Maschinenbau.

MASCHINEN- UND ANLAGENSICHERHEIT

Time-Sensitive Networking – TSN in der Anwendung

Skalierbare und präzise Produktionsnetze mit PROFINET und TSN

Klassisches Ethernet stößt in der Industrie bis heute an Grenzen, wenn zeitkritische Steuerungsaufgaben gefragt sind. Time Sensitive Networking (TSN) bietet hierfür eine funktionale Erweiterung des Ethernet-Standards und ermöglicht eine deterministische, hochpräzise Kommunikation auf Basis kostengünstiger Standardhardware. In Kombination mit Profinet lassen sich Echtzeitsteuerung, IT-Kommunikation und Investitionsschutz zusammenführen – ohne Spezialtechnik oder komplexe Konfiguration. Der Beitrag zeigt, wie Profinet TSN nutzt, welche Vorteile sich daraus ergeben und wie sich skalierbare Produktionskonzepte, beispielsweise in der Batteriezellenfertigung, praxisgerecht umsetzen lassen.

Das größte Manko heutiger Ethernet-Produkte ist die fehlende Eignung für extrem zeitkritische Steuerungsaufgaben wie Motion-Control. Diese notwendige Funktionalität hat Profinet selbst entwickelt und die heutige Lösung Profinet IRT in zahlreichen Maschinen und Anlagen zum Einsatz gebracht.

Solche Eigenentwicklungen haben einen Nachteil: Sie machen einen Vorteil des Ethernet-Standards zunichte – nämlich die breite und kostengünstige Verfügbarkeit von Hardware. Aus dem Alltag kennen wir das: Jeder Smart-TV, jeder Router und jede Heimautomatisierung verfügt über eine Ethernet-Schnittstelle – ohne Mehrkosten. In der Industrie verhindert bislang die fehlende Funktionalität für zeitkritische Kommunikation eine vergleichbare Entwicklung.

Time Sensitive Networking (TSN) ist eine Weiterentwicklung des Ethernet-Standards. Das bedeutet: In Zukunft wird jede Ethernet-Schnittstelle ohne Mehrkosten das leisten können, wofür heute noch Spezialhardware notwendig ist. Dabei ist es entscheidend, dass bestehende Geräte und Anwendungen weiterhin uneingeschränkt genutzt werden können. Das ist der Vorteil für den Kunden aus der Kombination von Profinet mit TSN.

Anforderungen an industrielle Kommunikation mit Profinet

Eine wesentliche Eigenschaft von Profinet ist, dass dasselbe Netzwerk gleichzeitig für zeitkritische Steuerungsaufgaben und für den direkten Zugriff auf Geräte – etwa über Webseiten oder Softwaretools – genutzt werden kann, ohne dass sich beides gegenseitig beeinträchtigt. Dabei ist keine spezielle Netzwerkkonfiguration notwendig, was den Betrieb von Maschinen und Anlagen vereinfacht. Auch Redundanzlösungen für höhere Ausfallsicherheit lassen sich integrieren. Diese Eigenschaft lässt sich mit „Plug & Produce“ beschreiben: Ein Profinet Netzwerk soll sich so einfach handhaben lassen wie ein gewöhnliches Ethernet-Netzwerk.

Diese Eigenschaften sollen auch mit der Integration der TSN-Funktionalität vollständig erhalten bleiben. Anwender möchten von den Vorteilen der neuen Technologie profitieren – etwa höhere Übertragungsgeschwindigkeiten, geringere Verzögerungen und die Nutzung handelsüblicher Netzwerkkomponenten – ohne dass sich dabei die gewohnte Bedienung oder die Arbeit in den Programmierwerkzeugen ändert.

Eine weitere zentrale Anforderung ist der Schutz bestehender Investitionen – in Geräte ebenso wie in das aufgebaute Know-how. Die TSN-Funktionalität wurde so integriert, dass neue Möglichkeiten wie höhere Übertragungskapazität und der Betrieb größerer Anlagen schrittweise und



Xaver Schmidt,
Vorstandsvorsitzender
PNO/PI

Marcel Albert,
Senior Key Expert
bei Siemens

Gunnar Lessmann,
Master Specialist Profinet and
TSN bei Phoenix Contact

in Kombination mit vorhandenen Geräten erschlossen werden können – für einen reibungslosen Übergang ohne Brüche. Daher nutzt Profinet die TSN-Funktionalität so, dass die gewohnte Handhabung vollständig erhalten bleibt und bestehende Geräte uneingeschränkt verwendet werden können.

Nutzung von TSN-Funktionalität zur Erweiterung von Profinet

Profinet nutzt die Möglichkeiten moderner Ethernet-Technologien, um zukünftige Anforderungen industrieller Kommunikationsnetze zu unterstützen. Ein zentraler Vorteil von TSN ist die präzise Zeitsynchronisation: Alle Geräte im Netzwerk senden ihre Daten hochgenau aufeinander abgestimmt – das erhöht die Zuverlässigkeit und Effizienz der Kommunikation.

Die Weiterleitung von Datenpaketen im Netzwerk funktioniert wie bei klassischem Ethernet – ohne komplizierte Konfiguration. Das Netzwerk findet den richtigen Weg selbstständig.

Damit zeitkritische Steuerbefehle nicht durch andere Netzwerkkommunikation verzögert werden, sorgt eine in TSN spe-

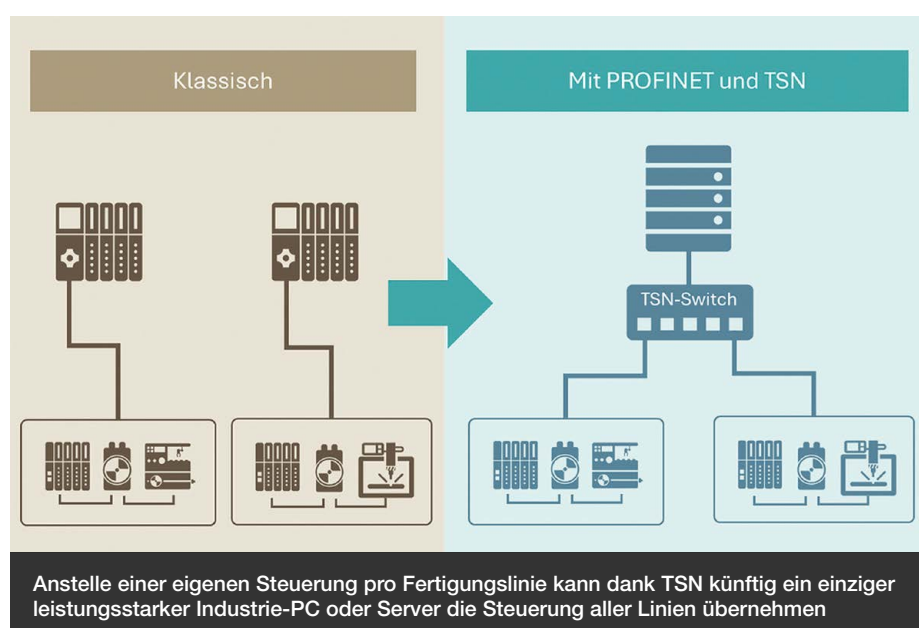
zifizierte Funktionalitäten dafür, dass weniger dringende Datenpakete bei Bedarf kurz unterbrochen werden. Das geschieht automatisch und erfordert keine manuelle Konfiguration. Zusätzlich werden im Netzwerk feste Kapazitäten für die Profinet-Kommunikation reserviert – eine Überlastung ist damit ausgeschlossen.

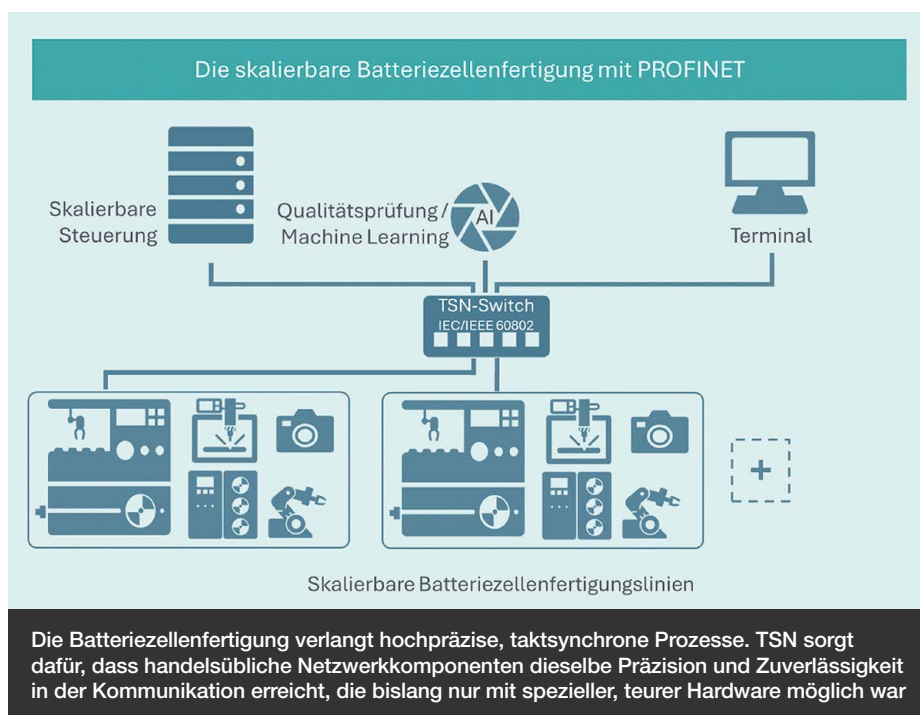
Durch diese Maßnahmen können vorhandene Profinet-Geräte mit TSN-fähigen Netzwerkkomponenten kombiniert werden – ohne Änderungen an der gewohnten Handhabung und ohne Abstriche beim Investitionsschutz und der Sicherheit.

Die Profinet Security Konzepte „Secure Cell“, „Secure Access“ und „Secure Real-time“ bleiben erhalten und bieten weiterhin alle notwendigen Schutzmechanismen für den industriellen Einsatz.

Dadurch können Anwender die zusätzlichen TSN-Funktionen nutzen, ohne auf bestehende Sicherheitsmechanismen verzichten zu müssen.

Bitte umblättern ►





Anwendungsbeispiel: Skalierbare Batteriezellenfertigung mit Profinet und TSN

Die bisherigen Abschnitte haben gezeigt, welche technologischen Möglichkeiten die Kombination von Profinet und TSN eröffnen. Ein besonders anschauliches Beispiel dafür, wie diese Möglichkeiten in der industriellen Praxis wirksam werden, liefert die Batteriezellenfertigung – ein Wachstumsmarkt, der

hohe Anforderungen an Präzision, Skalierbarkeit und Qualitätssicherung stellt.

Eine typische Batteriezellenfertigungslinie ist ein hochpräziser, takt synchrone Prozess. Kernschritte wie das Wickeln der Elektrodenfolien oder das Fügen der Zellkomponenten erfordern eine exakte Bewegungssteuerung. Profinet übernimmt dabei sowohl die präzise Antriebssteuerung als auch die Kommunikation mit Sensoren und weiteren Geräten entlang der Linie. Die gesamte Linie wird von einer einzigen Steuerung koordiniert.

Dieses Modell funktioniert zuverlässig – solange eine einzige Fertigungslinie betrieben wird. Sobald jedoch der Produktionsausstoß gesteigert werden soll, stößt der klassische Ansatz an seine Grenzen.

Der naheliegende Weg zur Kapazitätserweiterung ist das parallele Aufstellen weiterer Fertigungslinien. Jede zusätzliche Linie bringt jedoch auch eine eigene Steuerung mit sich, die eingerichtet, gewartet und in die übergeordnete Produktionssteuerung integriert werden muss. Mit wachsender Linienanzahl steigt damit nicht nur der Hardwareaufwand, sondern auch die Komplexität der Koordination zwischen den Linien.

Eine Lösung bietet der Einsatz von PROFINET mit TSN. Anstelle einer eigenen Steuerung pro Fertigungslinie übernimmt künftig ein einziger leistungsstarker Industrie-PC oder Server die Steuerung aller Linien gemeinsam. Das gleiche Steuerungsprogramm wird dabei parallel für jede Fertigungslinie ausgeführt, ohne dass für jede Linie eigene Hardware beschafft oder eine separate Einrichtung vorgenommen werden müsste.

Möglich wird das durch TSN: Die Technologie sorgt dafür, dass handelsübliche Netzwerkkomponenten dieselbe Präzision und Zuverlässigkeit in der Kommunikation erreichen, die bislang nur mit spezieller Hardware möglich war.

Das Ergebnis: Eine zentrale, leistungsstarke Steuerung kann über ein Netzwerk mit TSN-Funktionalität mehrere Batteriezellenfertigungslinien gleichzeitig und mit der erforderlichen Präzision betreiben – ohne Abstriche bei der Steuerungsqualität.

Neben der Steuerung der Fertigungsprozesse eröffnet ein Netzwerk mit TSN-Funktionalität auch die nahtlose Integration ergänzender Technologien. So lässt sich beispielsweise eine kamerabasierte Qualitätsprüfung mit KI-gestützter Auswertung direkt in das Netzwerk einbinden. Über das Netzwerk mit TSN-Funktionalität, das alle Fertigungslinien miteinander verbindet, wird das Kamerasystem als weiterer Teilnehmer angeschlossen – ohne Eingriffe in die bestehende Steuerung und ohne Beeinträchtigung der zeitkritischen Kommunikation.

Die Bildauswertung bewertet kontinuierlich die Qualität der produzierten und gewickelten Batteriezellen, erkennt Abweichungen frühzeitig und liefert Rückmeldungen, die in den Fertigungsprozess zurückfließen. Über die Zeit lernt das System, Fehlerursachen zu identifizieren und Prozessparameter gezielt zu optimieren. Das Ergebnis ist eine schrittweise Steigerung des Durchsatzes bei gleichzeitiger Reduzierung der Ausschussquote – ein messbarer Mehrwert, der sich direkt auf die Wirtschaftlichkeit der Produktion auswirkt. **GIT**

Echtzeit einfach erklärt

Echtzeit bedeutet nicht „besonders schnell“ – sondern vorhersagbar und deterministisch. Eine Steuerung arbeitet in Echtzeit, wenn garantiert ist, dass eine Reaktion auf ein Ereignis innerhalb einer definierten, maximalen Zeitspanne erfolgt – jedes Mal, ohne Ausnahme.

Der schlechteste Fall zählt. In der Automatisierungstechnik ist nicht der Durchschnitt entscheidend, sondern die sogenannte Worst-Case-Latenz: Auch im ungünstigsten Moment muss die Kommunikation innerhalb des erlaubten Zeitfensters ankommen.

Standard-Ethernet allein reicht nicht. Klassisches Ethernet arbeitet nach dem Prinzip „best effort“ – jeder bekommt, was gerade verfügbar ist, aber niemand bekommt eine Garantie. Für industrielle Steuerungsaufgaben ist das nicht akzeptabel.



Siemens AG
www.siemens.com
Phoenix Contact
www.phoenixcontact.com

Werma: Standorterweiterung in Rietheim-Weilheim

Bei der Erweiterung des Werma-Stammsitzes in Rietheim-Weilheim wurde ein weiterer bedeutender Meilenstein erreicht: Die neue Verbindungsbrücke zwischen dem bestehenden Firmengebäude und dem derzeit entstehenden Neubau für Produktion und Logistik wurde erfolgreich montiert. Mit dem Einhub der rund 21 Tonnen schweren Stahlkonstruktion wachsen Bestand und Neubau erstmals funktional zusammen.

Die Brücke wird künftig einen wettergeschützten Übergang für Mitarbeiter schaffen und die internen Abläufe zwischen Produktion, Logistik und den bestehenden Unternehmensbereichen weiter verbessern. „Diese Brücke verbindet nicht nur zwei Gebäude



Millimetergenaue Präzisionsarbeit: Die neue Verbindungsbrücke zwischen Bestand und Neubau wurde am Werma-Stammsitz in Rietheim-Weilheim erfolgreich eingehoben. Mit dem rund 21 Tonnen schweren Bauwerk wachsen beide Gebäude erstmals funktional zusammen

miteinander. Sie steht symbolisch für den Brückenschlag zwischen unserer erfolgreichen Unternehmensgeschichte und unserer Zukunft“, sagt Matthias Marquardt, Geschäftsführender Gesellschafter bei Werma Signaltechnik. „Sie verbindet Bewährtes mit Neuem und macht deutlich, dass wir langfristig an unseren Standort in Rietheim-Weilheim glauben.“

Größtes Neubauprojekt der Unternehmensgeschichte

Die Brückenmontage ist Teil des aktuell größten Bauprojekts in der Geschichte von Werma. Mit

dem Spatenstich im Juli 2025 hatte das Unternehmen den offiziellen Startschuss für die Erweiterung seines Werksgeländes im Industriegebiet Dillgarten Ost gegeben.

Das neue Gebäude entsteht gegenüber dem bestehenden Werksgelände zwischen dem heutigen Standort und der Bahnlinie Stuttgart–Singen. Insgesamt sind drei Bauabschnitte vorgesehen, derzeit entstehen im ersten Abschnitt auf rund 5.700 m² Grundfläche zusätzliche Kapazitäten für Produktion und Logistik. Die Fertigstellung ist für Anfang 2027 geplant. Mit dem Neubau schafft das Unternehmen die Voraussetzungen für weiteres Wachstum weit über das Jahr 2030 hinaus. Gleichzeitig soll die neue Infrastruktur maximale Flexibilität für zukünftige Technologien, Prozesse und Anforderungen bieten.

Anspruchsvolle Präzisionsarbeit

Der Einhub der rund 21 Tonnen schweren Verbindungsbrücke stellte alle Beteiligten vor eine besondere Herausforderung. Bei teils schwierigen Wetterbedingungen mit Regen und starken Windböen musste das Bauwerk mit einem Spielraum von nur vier Zentimetern millimetergenau zwischen Bestandsgebäude und Neubau positioniert werden. Die Planung verantwortet das Architekturbüro Schmelzle+Partner, für die Montage der Brücke zeichnete Haller Industriebau verantwortlich.

„Die Brücke ist eines der prägendsten Elemente des gesamten Projekts. Mit ihrer Funktion verbindet sie Bestand und Neubau, architektonisch steht sie zugleich für die konsequente Weiterentwicklung des Standorts“, erklärt Peter Gärtner, Partner bei Schmelzle+Partner mbB Architekten BDA. „Besonders die hohe Präzision bei Planung und Montage macht diesen Bauabschnitt zu einem außergewöhnlichen Meilenstein.“ www.werma.com

Neuer Schmersal Webshop: schneller, einfacher, komplett responsiv

Die K.A. Schmersal GmbH & Co. KG hat ihren neuen Webshop erfolgreich live geschaltet. Mit moderner Technologie und einer deutlich verbesserten Benutzerführung bietet die Plattform Kunden weltweit ein komfortableres und effizientes Einkaufserlebnis rund um Produkte, Bestelldaten und Services. Das Gesamtportfolio umfasst rund 15.000 Produkte aus den Bereichen Sicherheits-, Steuerungs- und Automatisierungstechnik. Ein Schwerpunkt des Relaunchs lag auf der weiteren Verbesserung der Nutzerfreundlichkeit. Der gesamte Bestellprozess wurde übersichtlicher und intuitiver gestaltet. Bestehende Freigabeprozesse für die Registrierung von Geschäftskunden bleiben erhalten, laufen nun jedoch effizienter ab. Ein weiterer Vorteil für Bestandskunden: Vorhandene Zugangsdaten behalten ihre Gültigkeit, sodass ein nahtloser Übergang zum neuen System gewährleistet ist.

www.schmersal.com

GIT SICHERHEIT

Sicher Macher

Der GIT-Talk mit den Marktführern



Kontakt:

Miryam.Reubold@Wiley.com

WILEY

CRA-Readiness für Maschinen und Anlagen

Cyberresilienz in der Automatisierung: Von Security by Design bis Secure by Default



Mit dem Cyber Resilience Act werden verbindliche Cybersicherheitsanforderungen für Produkte mit digitalen Elementen schon bald zur Pflicht. Bereits heute verändern die neuen Vorgaben Prozesse und Verantwortlichkeiten, etwa bei der Meldung und Veröffentlichung von Schwachstellen. Moderne Securitykonzepte und umfassende Schutzmaßnahmen schaffen dabei die Grundlage für eine zukunftssichere Umsetzung der Anforderungen.

■ Mit dem Cyber Resilience Act (CRA) – offiziell Verordnung (EU) 2024/2847 – beabsichtigt die Europäische Union langfristig die Stärkung der Resilienz vernetzter industrieller Systeme und eine Harmonisierung der Sicherheitsanforderungen im EU-Binnenmarkt. Der CRA gilt für alle Produkte, die digitale Elemente enthalten oder die Verarbeitung und Kommunikation von Daten ermöglichen – sowohl in Form von Hardware als auch von Software. Damit gilt der CRA in der Praxis für alle industriellen und vernetzbaren Automatisierungskomponenten – und somit auch für Produkte, die auf den Verdrahtungs- und Automatisierungstechnologien ASi-3 und ASi-5 sowie auf deren sicherheitszertifizierten Ausprägungen ASi Safety at Work und ASi-5 Safety basieren.

In Kraft getreten ist der CRA bereits am 11. Dezember 2025. Ab dem 11. Dezember 2027 wird er verpflichtend anzuwenden sein, wobei Meldepflichten bereits seit dem 11. September 2026 gelten. An Aktualität mangelt es dem CRA also nicht, ebenso wenig wie an der Relevanz für Betreiber, Integratoren und in besonderem Maße für Hersteller von Produkten mit digitalen Elementen, die Daten speichern, verarbeiten oder übertragen, mit Netzwerkschnittstellen ausgestattet sind und die Software

ausführen oder in eine solche eingebettet sind. Alle Merkmale, die auf das Produktportfolio von Bihl+Wiedemann zutreffen, weshalb das Unternehmen hinsichtlich der CRA-Konformität seiner Automatisierungslösungen alle Register zieht.

CRA: Verordnung (noch) ohne normative Basis

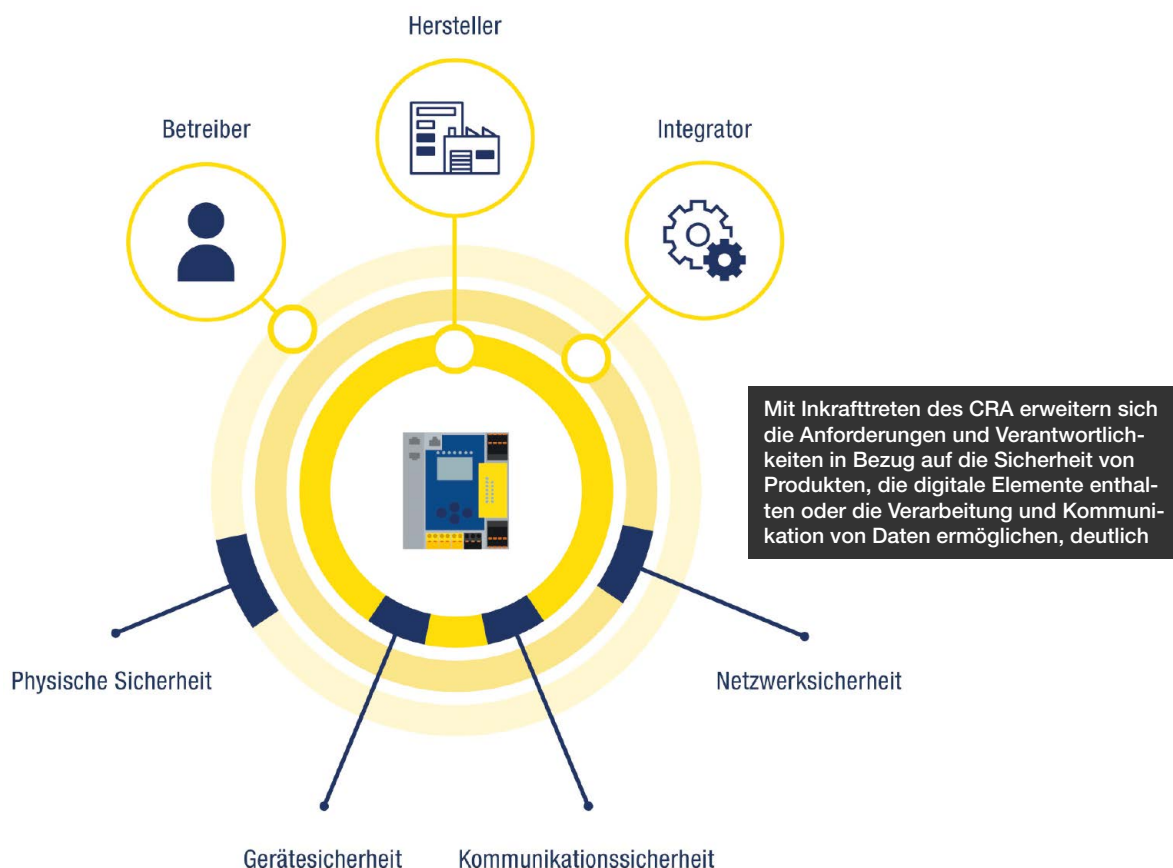
Da es sich beim CRA um eine Verordnung handelt, nicht aber um eine harmonisierte Norm, hat die Europäische Union am 3. Februar 2025 einen Normungsauftrag an die europäischen Standardisierungsorganisationen gestellt. Um Sicherheitsarchitekturen im Sinne des CRA realisieren zu können, orientiert sich Bihl+Wiedemann, wie auch viele andere Automatisierungshersteller, an den geltenden Sicherheitsnormen IEC 62443-4-1: Anforderungen an die sichere Softwareentwicklung – inklusive Threat Modeling, sowie IEC 62443-4-2: Technische Security-Anforderungen für Komponenten, die zum Beispiel Themen wie Schutz vor Denial of Service (DoS, Beeinträchtigung der Verfügbarkeit), Authentifizierung und Logging (Protokollieren von Sicherheitsereignissen) betrifft. Es ist davon auszugehen, dass eine Weiterentwicklung dieser Normen für den CRA harmonisiert, das heißt als Stand der Technik gemäß CRA akzeptiert wird.

„Defence in Depth“ durch „Security by Design“

„Security by Design“ zielt darauf ab, Produkte mit digitalen Elementen zu entwickeln, die frei von Schwachstellen und robust gegen Cyberangriffe sind. Die Sicherheit der Hard- und Software wird also bereits im Entwicklungsprozess – beim Design der Produkte – berücksichtigt und in deren kompletten Lebenszyklus integriert. Cybersicherheit wird hierbei durch eine Kombination mehrerer technischer und organisatorischer Schutzebenen erreicht. Diese „Defence in Depth“ gewährleistet auch bei Versagen einzelner Maßnahmen ein hohes Schutzniveau gegen Angriffe durch mögliche Einfallstore in externen und internen Netzwerken. Dementsprechend folgen die neuesten Produkte von Bihl+Wiedemann als Hersteller einem solchen mehrschichtigen Sicherheitskonzept.

AS-Interface: cybersichere Architektur und Kommunikation

Technologiebedingt bieten ASi-3 und ASi-5 von Haus aus eine cybersichere Architektur, denn beide gewährleisten durch besondere Kommunikationsmethoden – spezielle sin2-Pulse bei ASi-3, ein angepasstes, digitales Mehrträger-Modulationsverfahren OFDM (Orthogonal Frequency Division Multiplexing)



mit dynamischer Frequenzzuweisung bei ASI-5 – sowie durch eine physische Entkopplung zwischen TCP/IP und der Feldebene eine besonders abhörsichere Kommunikation mit minimaler Angriffsfläche. Damit sind ASI-3 und ASI-5 Netzwerke und Geräte weit aus abhörsicherer als vorhandene Ethernet-Protokolle, bei denen die Datenübertragung grundsätzlich durch handelsübliche Komponenten mitgelesen werden kann.

Neben der Datenübertragung und dem kommunikativen Bruch ist die verschlüsselte Kommunikation ein weiteres Security-Merkmal dieser ASI-5 Gateways. Hierbei erhalten TCP/IP-Geräte individuelle SSL-Zertifikate. Bei der Kommunikation über IT-Schnittstellen wie OPC UA und REST-API werden AES-256 bzw. TLS eingesetzt. Für die Feldbuskommunikation werden ebenfalls entsprechende Sicherheitsmechanismen berücksichtigt, soweit und sobald sie verfügbar sind. Und auch der Datenaustausch in Safe Link zur einfachen, flexiblen und sicheren Verbindung verschiedener Anlagenteile kann über ein DTLS-basiertes Verfahren (Datagram Transport Layer Security) verschlüsselt werden. Damit lassen sich die Geräte von Bihl+Wiedemann nahtlos in bestehende IT-Security-Konzepte integrieren. Und auch die Kommunikation der PC-Konfigurations- und Diagnose-Software

Asimon360 mit den ASI Gateways geschieht künftig über einen sicheren Kanal.

CRA-konforme Updates von Geräten: zertifikatsbasiert verschlüsselt und TÜV-geprüft

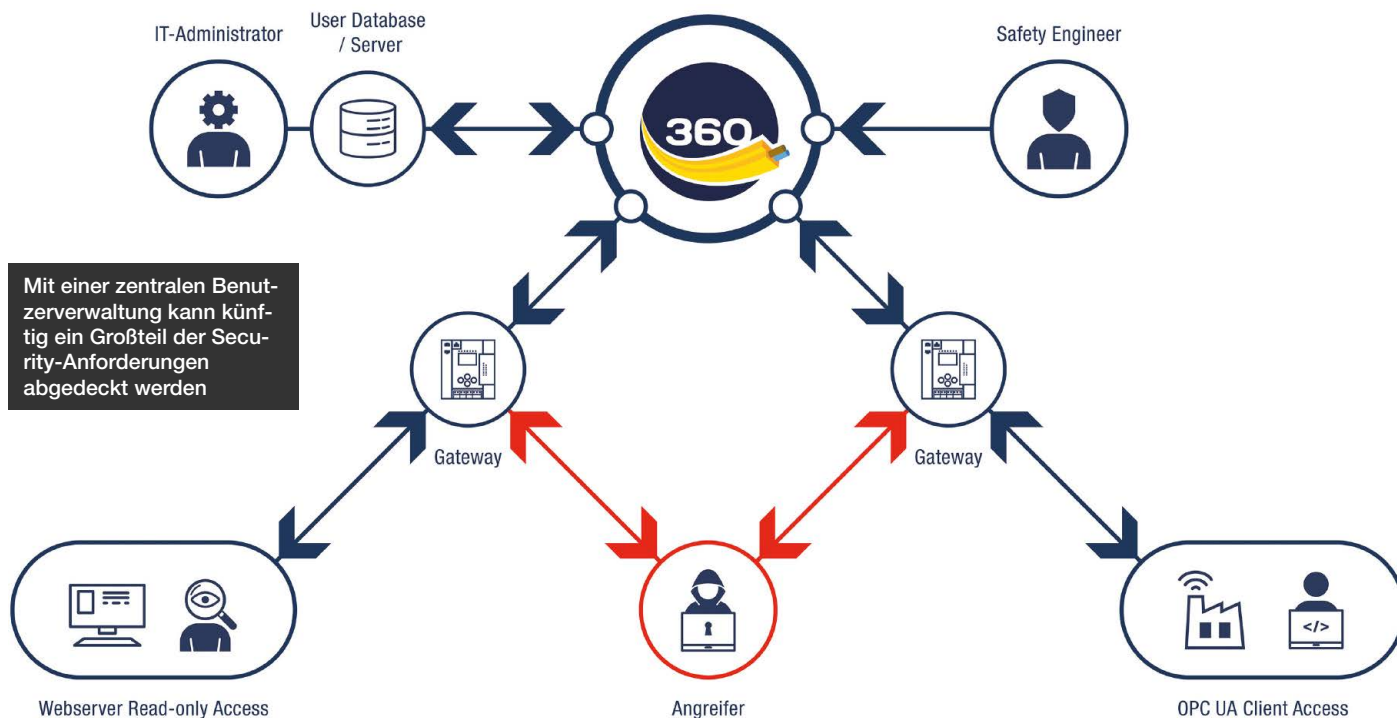
Ein weiteres Cybersecurity-Merkmal aller modernen Ethernet/ASI Gateways und Sicherheitssteuerungen sowie der Module der neuesten ASI Technologie ist ihre Updatefähigkeit, denn dadurch können aktuelle und zukünftige Sicherheitslücken, die Angreifern Zugang verschaffen können, schnell und effektiv geschlossen werden. Geräte, die bereits heute in Maschinen und Anlagen eingesetzt werden, können etwa beim Inkrafttreten neuer regulatorischer Anforderungen – in diesem Fall dem Cyber Resilience Act – durch Firmware-Updates immer auf den aktuellen Sicherheitsstand gebracht und, dank signierter Firmware, so auch noch lange nach der Erstinbetriebnahme an zukünftige Sicherheitsanforderungen angepasst werden. Die Updates sind durch eine zertifikatsbasierte Ende-zu-Ende-Verschlüsselung zwischen dem Update-Server und dem zu aktualisierenden Gerät geschützt und erfüllen die Integritätsanforderungen gemäß ZVEI. Das TÜV-geprüfte Verfahren ist auch für Firmware bei Safety-Produkten zugelassen.

Benutzerverwaltung als CRA-konformes Security-Tool

Insbesondere in seinen komplexeren, parametrierbaren Geräten – also Gateways und Safety Gateways – sieht Bihl+Wiedemann eine zentrale Benutzerverwaltung vor, die im Rahmen der CRA-Anforderungen entwickelt wird, künftig einen Großteil der Security-Anforderungen abdeckt und gleichzeitig die Grundlage für die folgenden zentralen Cybersecurity-Mechanismen bildet:

- Authentisierung: Geräte stellen sicher, dass sich ein Benutzer am Display, Webserver oder über die PC-Software anmelden muss,
- Autorisierung: Rollenlogik, die definiert, welche Funktionen ein Benutzer ausführen darf,
- Integrität der Kommunikation zwischen PC-Software und Gerät,
- kontrollierter Zugriff über Webserver, OPC UA und REST-API,
- Vertraulichkeit sensibler Parameter.

IT- und Automatisierungsverantwortliche können dann über die PC-Software Asimon360 von Bihl+Wiedemann Benutzerkonten mit individuellen Zugangsdaten und Rollen anlegen. Diese Benutzer- und Authentifikationsdaten werden in eine Datenbank geschrieben, die auf einem konfigurierten Server läuft. Im Rahmen der



sicheren Erstinbetriebnahme eines (Safety) Gateways werden die Benutzerinformationen im Gerät gespeichert, können aber dann, wenn es zu Änderungen im Rahmen der Benutzerverwaltung kommt, entsprechend aktualisiert werden.

Die zentrale Benutzerverwaltung ist somit ein komfortables Tool für die individuelle Vergabe von Zugriffsrechten. Ob sie als organisatorische Maßnahme vom Integrator oder Betreiber aber auch benötigt wird oder ob die CRA-Anforderungen auf andere Art und Weise gelöst werden können, hängt vom Sicherheitskonzept der Anlage ab – das entweder Zugriffssteuerung und Nachvollziehbarkeit verlangt oder eben nicht. In bestimmten Fällen können auch das Verschießen des Schaltschranks gegen unbefugten Zugriff, ein Security-Siegel über dem Chipkarten-Slot eines ASI Gerätes mit Chipkarte oder die geschützte Verlegung der Ethernetkabel ausreichend sein. In den meisten modernen Anlagen wird jedoch eine rollenbasierte Benutzerverwaltung zum zentralen Bestandteil der Sicherheitsstrategie gehören, um unbefugte Änderungen zu verhindern und Systemzugriffe transparent zu dokumentieren.

„Secure by Default“: sicher mit Beginn der Anwendungspflicht verfügbar

Mit Beginn der Anwendungspflicht des CRA am 11. Dezember 2027 dürfen Produkte mit digitalen Elementen in der EU nur dann CE-gekennzeichnet und vertrieben werden, wenn sie die CRA-Anforderungen erfüllen. Für Bihl+Wiedemann bedeu-

tet dies unter anderem, dass spätestens zu diesem Zeitpunkt alle Geräte – in der Regel Gateways – „secure by default“ ausgeliefert werden müssen, sie also das Werk im sicheren Grundzustand verlassen. Dabei steht dem Erstbenutzer dann gemäß Least Privilege Prinzip nur noch eine für die sichere Inbetriebnahme über die PC-Software Asimon360 notwendige minimale Kommunikationsschnittstelle zur Verfügung. Alle anderen Schnittstellen und Protokolle sind zur Minimierung möglicher Angriffsflächen standardmäßig deaktiviert. Der Inbetriebnahmeverantwortliche authentifiziert dabei zunächst das Gateway und stellt so sicher, dass eine Verbindung zum richtigen Gerät aufgebaut wird. Die benötigten Dienste und Schnittstellen werden zuvor in der Software-Suite konfiguriert. Im Rahmen der sicheren Inbetriebnahme werden diese Einstellungen inklusive Benutzerverwaltung anschließend in das Gerät übertragen. Dadurch lassen sich benötigte Funktionen komfortabel konfigurieren und gleichzeitig kontrolliert und nachvollziehbar aktivieren.

Der Integrator oder der Anwender wird jedoch auch in der Lage sein, in seiner Verantwortung den Security-by-Default-Modus zu deaktivieren, sofern dies auf Basis der Risikobeurteilung der Anlage und des jeweiligen Sicherheitskonzepts zulässig ist. Wie im heutigen Auslieferungszustand ist dann die Benutzerverwaltung deaktiviert. Ports und Dienste sind offen und das Gerät kann dann auch ohne Asimon360 betrieben werden.

CRA im Kontext von Altanlagen und Ersatzteilen

Mit der Einführung des CRA hat die EU gleichzeitig einen Bestandsschutz für Anlagen beschlossen, die bis zur vollständigen Anwendungspflicht bereits in Betrieb sind. So besteht für Anlagenbetreiber keine rechtliche Verpflichtung, vorhandene Bestandsanlagen CRA-konform zu machen. Ebenso wenig muss der Betreiber beim Austausch eines Altgerätes ein neues, CRA-fähiges Ersatzgerät einbauen – ein älteres Originalteil, das vielleicht noch im Ersatzteillaager verfügbar ist, darf verwendet werden. Konsequenterweise ist es damit Herstellern gestattet, auch nach dem 11. Dezember 2027 Originalkomponenten ohne CRA-Konformität als Ersatzteil bereitzustellen. Alle benötigten Geräte werden auch künftig bei Bihl+Wiedemann erhältlich sein. Allerdings empfiehlt das Unternehmen die Verwendung von CRA-konformen Ersatzteilen für den Austausch von defekten Geräten in Bestandsmaschinen. Da funktional und integrationstechnisch identische Geräte ausgetauscht werden, sind keine Änderungen an der Maschine erforderlich und die Konfiguration wird deutlich erleichtert. a

Autor
Thomas Rönitzsch
Leiter Unternehmenskommunikation

Bihl+Wiedemann GmbH
www.bihl-wiedemann.de

Sicherheitsrelais PSRcompact von Phoenix Contact

Mit dem Sicherheitsrelais PSRcompact baut Phoenix Contact sein Portfolio an Sicherheitsschaltgeräten weiter aus. Die Produktfamilie stellt in einem platzsparenden Gehäuse bis zu fünf Freigabestrompfade zur Verfügung. Damit eignen sich die Geräte für die Verwendung in modernen Konzepten des Maschinen- und Anlagenbaus. Die Geräte PSRcompact sind kompatibel zu allen relevanten Sensortypen wie beispielsweise Not-Halt, Schutztüren und Lichtgitter. Ein besonderes Feature ist der erweiterte Einsatztemperaturbereich von bis zu 60 °C, der die Komponenten auch für die Nutzung in rauen Umgebungen auszeichnet. Durch die Push-in-Anschlussstechnik lassen sich die Produkte einfach und effizient installieren. Für die Inbetriebnahme der Sicherheitsrelais ist keine zusätzliche Software erforderlich. Die Module sind ohne weiteren Aufwand sofort einsatzbereit. Über den Digital Twin 4 Industry Code kann der Anwender konkrete Produktinformationen komfortabel und schnell abrufen. www.phoenixcontact.com



Munk Günstzburger Steigtechnik startet Partnerschaft mit Gromet

Die Munk Günstzburger Steigtechnik und der italienische Arbeitsbühnenspezialist Gromet haben eine exklusive Entwicklungs- und Vertriebspartnerschaft vereinbart. Gemeinsam bringen sie neue FlexxLift-Arbeitsbühnen auf den deutschen und österreichischen Markt – vom mobilen Push-around bis zur elektrischen Mast- und Scherenbühne. Die Munk Günstzburger Steigtechnik und Gromet haben eine exklusive Kooperation geschlossen. Auf dieser Basis entstehen neue Arbeitsbühnen unter der Produktmarke FlexxLift. Munk vertreibt sie künftig im deutschen und österreichischen Markt. Das Sortiment reicht von manuell verfahrenbaren Push-around-Bühnen bis zu elektrischen Mast- und Scherenbühnen. Alle Produkte gelten als sichere Alternative zur Leiter und erfüllen die Anforderungen der Technischen Regeln für Betriebssicherheit (TRBS). www.munk-group.de



Gemeinsam in die Höhe: Ferdinand Munk (Munk Group, links) und Massimo Grossele (Gromet) erweitern die FlexxLift-Produktreihe – von Push-around- bis zu Mast- und Scherenbühnen

Keba übernimmt Transtechnik

Die international tätige Keba Gruppe mit Hauptsitz in Linz, Österreich, übernimmt Transtechnik SAS, einen etablierten französischen Spezialisten für Automatisierungs- und Mechatroniklösungen, und baut damit ihre Präsenz im französischen Markt weiter aus. Transtechnik mit Sitz nahe Dijon ist ein etablierter französischer Spezialist für kundenspezifische Automatisierungslösungen. Das 1987 gegründete Unternehmen begleitet industrielle Kunden über den gesamten Projektverlauf: von der Beratung und Planung über die Auswahl, Auslegung und Integration geeigneter Komponenten bis hin zur Inbetriebnahme. So verbindet Transtechnik fundiertes Produkt-Know-how mit hoher Applikationskompetenz und entwickelt passgenaue Lösungen für industrielle Anforderungen. Mit langjähriger Markterfahrung und ausgeprägter Kundennähe ist Transtechnik im französischen Automatisierungsmarkt fest etabliert. www.keba.com



Christoph Knogler, CEO Keba Gruppe

Softwarelizenzierung gehört zum Umsatzstrom

Wibu-Systems gibt die Integration von Instellix bekannt, einer zukunftsgerichteten Monetarisierungsplattform für abonnementbasierte, nutzungsorientierte, hybride und marktplatzgetriebene Geschäftsmodelle. Die gemeinsame Lösung wandelt die Softwarelizenzierung von einer unterstützenden Funktion in einen wesentlichen Bestandteil des Geschäftsbetriebs um. In diesem wirken die Verwaltung von Nutzungsrechten, das Tracking der Nutzung und die Finanzprozesse als ein durchgängiges System zusammen. Durch die Kombination der sicheren Lizenzierungs- und Schutztechnologien von CodeMeter mit den fortschrittlichen Monetarisierungsfunktionen von Instellix können Softwarehersteller den gesamten Lifecycle vom Vertragsabschluss bis zum Umsatz automatisieren. „Mit Instellix erweitern wir CodeMeter über Schutz und Lizenzierung hinaus zu einer vollständig integrierten Monetarisierungsumgebung“, so Stefan Bamberg, Director Sales and Key Account Management bei der Wibu-Systems AG. www.wibu.com



Stefan Bamberg, Director Sales and Key Account Management bei der Wibu-Systems AG

Bequem auf dem Sofa durch die e-Ausgabe der GIT SICHERHEIT blättern: Registrieren Sie sich auf www.git-sicherheit.de/newsletter

SICHERHEITSARCHITEKTUR

Alles Gute kommt von oben – Sicherheit auch

Normgerechte Kranmodernisierung bei internationalem Automobilzulieferer

Decken- und Brückenkrane sind bei dem Automobilzulieferer Marelli Mako Elektrik Sanayi ve Ticaret zentrale Elemente in Produktion und Intralogistik, mit hohen Anforderungen an funktionale Sicherheit und Verfügbarkeit. Eine normgerechte Modernisierung aktualisiert Schutzfunktionen und Steuerungsarchitektur, bei minimalem Eingriff in den Betrieb und ohne verlängerte Stillstandszeiten.

Im Gewerbepark der rund 100 Kilometer von Istanbul gelegenen Stadt Bursa stellt Marelli Mako Scheibenwischer, Heizungs- und Lüftermotoren, Zündspulen, Sicherungskästen sowie weitere Bauteile und Produktgruppen vorwiegend für die Automobilindustrie her. Spritzgießmaschinen sind zentrale Bestandteile einiger Fertigungslinien und vor jedem neuen Produktlauf stehen in unterschiedlichem Umfang Umrüstmaßnahmen an. Brückenkrane transportieren dann die von Werkern demontierten Gussformen ab und liefern die für eine neue Serie benötigten Werkzeuge und Vorrichtungen zu. Bei Marelli Mako verfahren Deckenkrane Lasten, wie beispielsweise Werkzeuge, mit hoher Geschwindigkeit und bringen diese punktgenau, sicher und just-in-time ans vorgegebene Ziel. Rüstwechsel sollen zügig erfolgen, Ausfälle sind nicht vorgesehen, Stillstand kostet Geld. Für das Bedienpersonal unter den transportierten Lasten darf zu keinem Zeitpunkt Gefahr für Leib und Leben ausgehen. Daher gelten für Decken- oder Brückenkrane besondere Sicherheitsvorkehrungen.

Sicherheitskonzept für Brückenkran-Retrofit

Im Zuge fälliger Retrofits standen bei Marelli Mako im Jahr 2024 neben der Optimierung von Produktivität und Zuverlässigkeit auch Sicherheitsaspekte auf der To-do-Liste. Zwanzig Brückenkrane mit einer Tragkraft von jeweils 16 und mehr Tonnen sind bei Marelli Mako 24/7 im Einsatz. Die Aufgabe: Mit modernen Automatisierungs- und Sicherheitskonzepten sollten sämtliche Krane für möglichst viele weitere Jahre fit gemacht werden. Damit die Brückenkrane im Werk auch aktuellen internationalen Normen entsprechen – hier insbesondere EN 13135-1 (Krane – Sicherheit – Konstruktive Anforderungen an Ausrüstungen) sowie EN ISO 13849-1 (Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen) – stand im ersten Schritt die Erstellung einer Risikoanalyse an. Das Ergebnis: Der Kranbetrieb ist sicher, jedoch in einigen Punkten nicht auf dem Stand der aktuellen Technik. So wurden zum Beispiel eine Reihe von Sicherheitsfunktionen, die

die Bewegungen der Krane begrenzen und stoppen, nicht von einer Sicherheitssteuerung überwacht. Auch entsprach die auf den Kranen installierte Sicherheitstechnik nicht mehr in jedem Punkt den aktuellen Anforderungen. In Eigenregie war das für den Automobilzulieferer nicht umsetzbar. Erschwerend kam hinzu, dass ein Sicherheitsupdate ohne das Absenken des kompletten Kranturms eigentlich nicht machbar wäre.

Da Pilz bereits seit 2022 Partner von Marelli Mako ist und in sämtlichen Fragen rund um Safety & Security hohes Ansehen genießt, holten sich die Entscheider Rat bei den Experten für die sichere Automation. Der Ansatz von Pilz, dass die anstehenden Modernisierungsmaßnahmen auch ohne Absenkung des Krans umsetzbar sind – bei sorgfältiger Planung parallel zum laufenden Betrieb – überzeugte die verantwortlichen Projektpartner bei Marelli Mako. Pilz erhielt den Auftrag: Zum Leistungspaket zählte neben der konzeptionellen Beratung zu den infrage kommenden Systemen der Ersatz

Weitere Informationen



Mit Retrofit
Kosten sparen



Automatisierungs-
system PSS 4000



Good to know:
Maschinenverordnung



Automatisierungssystem PSS 4000 von Pilz: Modular, flexibel und bei aller Komplexität übersichtlich. Im Schaltschrank aneinandergereiht sind E/A-Module mit genau jenen Funktionen, die gebraucht werden

und die Erneuerung der Sicherheitstechnik inklusive Engineering-Dienstleistungen.

Deckenkrane: Automatisierungs- lösung nach Maß

Kern der von Marelli Mako präferierten Automatisierungs- und Sicherheitslösung ist das industrierprobte Automatisierungssystem PSS 4000 von Pilz. Die Steuerung im System lässt sich über diverse E/A-Module anpassen, so dass Anwendern eine exakt auf ihre jeweilige Anforderung zugeschnittene Lösung zur Verfügung steht. PSS 4000 stellt so ein zukunftsfähiges System dar – inklusive einfacher Programmierung auf Basis der Pilz-Softwareplattform PAS4000 sowie webbasierter, intuitiver Diagnose und Visualisierung auf Grundlage der Visualisierungssoftware PASvisu.

Aufbauend auf diesem Konzept wurde Sicherheitstechnik wie zum Beispiel Endschalter, Not-Aus-Taster, Antriebe sowie der Schaltschrank ausgetauscht. Gleichzeitig integrierten die Pilz-Experten Serienantriebe im Deckenkran, die künftig die Bewegungen des Kranfahrwerks, des Katzantriebs und des Hubwerks steuern und sichere Abschaltvorgänge gewährleisten. Um Lasten in Echtzeit überwachen sowie Fehler schnell und einfach diagnostizieren zu können, wurde zusätzlich zur Visualisierungssoftware das Pilz-Bedienterminal Pilz Human Machine Interfaces (PMI) integriert.

Erwartungsgemäß stellte das Projekt an unterschiedlicher Stelle hohe Anforderungen. Weil das Kransystem insgesamt

neun Spritzgießmaschinen bedient und die Anlage nicht länger als unbedingt erforderlich stillstehen sollte, musste die Planung sorgfältig und unter Einhaltung enger Zeitfenster abgestimmt werden. Tatsächlich gelang es Pilz, auf ein zeitaufwändiges und teures Absenken des Kranturms zu verzichten: Der Automatisierungsexperte führte den gesamten Montageprozess erfolgreich in großer Höhe und bei nur begrenzt zur Verfügung stehenden Raum zwischen Kran und Decke durch.

Überwachung in Echtzeit für mehr Sicherheit

Die neue Automatisierungslösung einschließlich der installierten Sicherheitstechnik von Pilz erlaubt eine Überwachung des Kranbetriebs in Echtzeit. Ein Überlastkontrollsystem, die sichere Drehzahlüberwachung des Hakenantriebs, sichere Abschaltarchitektur, Sicherheitsverbindungsarchitektur gemäß EN ISO 13849-1 sowie ein Diagnosedisplay für einfache Fehlersuche und Wartung sind Leistungsmerkmale, die es zuvor nicht gab. Auch das Not-Halt-System wurde optimiert: Die Not-Halt-Taster PITestop wurden EN ISO 13850-konform in das Kransystem integriert, Bediener können die Anlage im Gefahrenfall sofort in einen sicheren Zustand versetzen. Diese Funktion erhöht sowohl die Sicherheit von Menschen im Umfeld der Anlage als auch die Zuverlässigkeit des Gesamtsystems. „Im Zuge des Projektes ist bei unseren Mitarbeitern das

Bewusstsein für Maschinensicherheit und die Bedeutung von Sicherheitsfunktionen gewachsen. Zudem garantiert die Integration moderner Technologien in unseren Anlagen allen Beteiligten ein hohes Maß an Sicherheit“, erklärt Muhammet Ali İçin, OHS (Occupational Health and Safety) Spezialist bei Marelli Mako.

Krane mit einheitlicher, international konformer Sicherheitsarchitektur

Die Vorteile für Marelli Mako beziehungsweise das Bedienpersonal liegen auf der Hand: Die modernisierten Krane garantieren einen sicheren Betrieb und verringertes Unfallrisiko. Eine schnelle und einfache Fehlerdiagnose reduziert Ausfallzeiten und erhöht die Produktivität des Gesamtsystems. Die mit dem modernen Automatisierungs- und Sicherheitssystem von Pilz ausgestatteten Krane verfügen über eine einheitliche, international konforme Sicherheitsarchitektur zur Abdeckung der identifizierten Gefahren. Die Einhaltung gesetzlicher und normativer Anforderungen (z. B. EN ISO 13849-1 und EN 13135-1) ist dokumentiert. **GIT**

Autor
Tansu Kundakçılar
Engineering Service Manager



Pilz GmbH & Co. KG
www.pilz.com

SCHUTZHANDSCHUHE

Die 11,5-Milliarden-Euro-Frage

Warum PSA nicht automatisch vor Kontamination schützt

In der Lebensmittelverarbeitung gilt Persönliche Schutzausrüstung (PSA) vielerorts als unverzichtbare Barriere gegen Risiken und Verunreinigungen. Doch was, wenn genau diese Schutzmaßnahme selbst zur Kontaminationsquelle werden kann? Philipp Heinemann, Country Manager DACH bei Showa, hinterfragt etablierte Annahmen und beleuchtet, welche Rolle PSA tatsächlich für Produktsicherheit und Hygiene spielt.



In Backumgebungen muss die Handschuhauswahl Lebensmittelsicherheit mit Griffigkeit, Komfort und manueller Kontrolle verbinden



Bei heißen und öligen Tätigkeiten in der Lebensmittelzubereitung müssen Handschuhe auf die jeweiligen Gefahren und Prozessbedingungen abgestimmt sein

■ Persönliche Schutzausrüstung ist ein Eckpfeiler der Lebensmittelsicherheit. Handschuhe, Schürzen und Schutzkleidung kommen täglich zum Einsatz, um sowohl die Mitarbeiter vor Verletzungen zu schützen als auch eine Kontamination von Lebensmitteln zu verhindern. Eine Analyse der Europäischen Kommission schätzt, dass vermeidbare Schäden im Zusammenhang mit unsicheren Konsumgütern EU-weit jährlich rund 11,5 Milliarden Euro kosten. Diese Zahl bezieht sich zwar nicht speziell auf Lebensmittel, verdeutlicht jedoch das Ausmaß vermeidbarer Risiken, die entstehen können, wenn Schutzmaßnahmen nicht wie vorgesehen funktionieren.

In der Lebensmittelverarbeitung bildet die PSA die direkte Schnittstelle zwischen Mensch und Produkt. Wenn sie gut funktioniert, verringert sie das Risiko. Wenn dies nicht der Fall ist, kann sie neue Kontaminationswege eröffnen. Für Lebensmittelher-

steller stellt sich nicht nur die Frage, ob PSA vorhanden ist, sondern ob sie unter realen Betriebsbedingungen tatsächlich eine Kontamination verhindert.

PSA als Maßnahme zur Lebensmittelsicherheit

Im Rahmen der europäischen Vorschriften zur Lebensmittelsicherheit spielt persönliche Schutzausrüstung (PSA) eine doppelte Rolle. Sie dient zum einen dem Schutz der Arbeitnehmer vor Gefahren wie Schnittverletzungen, Chemikalien und extremen Temperaturen und fungiert zum anderen als Barriere gegen biologische, chemische, physikalische und allergene Kontaminationen. Insbesondere Handschuhe gehören zu den am häufigsten eingesetzten Schutzmaßnahmen überall dort, wo Hände mit Lebensmitteln, Werkzeugen oder Oberflächen, die mit Lebensmitteln in Berührung kommen, in Kontakt kommen.

Was diese Vorschriften jedoch nicht definieren, ist, wie gut Schutzausrüstung funktioniert, sobald sie den tatsächlichen Arbeitsbedingungen ausgesetzt ist. Bei der Überprüfung der Einhaltung geht es darum, ob Kontrollmaßnahmen vorhanden sind, nicht darum, wie sich diese über lange Schichten, bei vielfältigen Aufgaben und in wechselnden Umgebungen bewähren. In manchen Fällen kann sogar das Gegenteil der Fall sein.

Wenn Handschuhe das Risiko erhöhen

Handschuhe werden oft eingesetzt, um den direkten Handkontakt mit Lebensmitteln zu reduzieren. Sind sie jedoch falsch ausgewählt oder werden sie unsachgemäß gehandhabt, können sie statt einer Barriere zu einer Kontaminationsquelle werden.

Ein häufiges Problem ist die Passform. Zu locker sitzende Handschuhe können die

Fingerfertigkeit beeinträchtigen und damit die Wahrscheinlichkeit erhöhen, dass Werkzeuge fallen gelassen werden, Verpackungen zerreißen oder unbeabsichtigter Kontakt mit Oberflächen außerhalb des Lebensmittelbereichs entsteht. Zu enge Handschuhe können Ermüdungserscheinungen verursachen, was eine konsequente Nutzung erschwert oder dazu führt, dass sie vorzeitig ausgezogen werden. In beiden Fällen steigt das Fehlerisiko.

Die Griffigkeit ist ein weiterer Faktor. In nassen oder öligen Verarbeitungsumgebungen kann eine unzureichende Griffigkeit die Handhabung beeinträchtigen, insbesondere beim Schneiden, Trimmen oder Umfüllen. Der Kontrollverlust erhöht nicht nur das Verletzungsrisiko, sondern auch die Wahrscheinlichkeit, dass Lebensmittel mit kontaminierten Oberflächen in Berührung kommen.

angemessenen Abständen gewechselt, bei Beschädigung ersetzt und zwischen verschiedenen Arbeitsschritten ausgezogen oder gewechselt werden. In hektischen Produktionsumgebungen, insbesondere dort, wo der Produktivitätsdruck hoch ist, können diese Vorgehensweisen leicht vernachlässigt werden.

Das sichere Ausziehen ist ein wichtiger Bestandteil dieses Managementprozesses. In Lebensmittelbereichen können Handschuhe zum Zeitpunkt des Ausziehens mit Blut, Fetten, Salzlake, Eiweißrückständen oder Reinigungschemikalien verschmutzt sein. Wenn Mitarbeiter beim Ausziehen die Handfläche oder die Fingerspitzen anfassen, können diese Rückstände auf die Haut, die Ärmel, Werkzeuge oder nahegelegene Oberflächen übertragen werden, bevor die Hände gewaschen werden. Kühlräume und Nassverarbeitungsbereiche können diese

nen Handschuhe Kontaminationen sogar effektiver verbreiten als bloße Hände, da sie sensorische Hinweise wie Feuchtigkeit oder Rückstände überdecken.

Dies ist besonders relevant in Umgebungen mit Allergenkontrolle. Wenn am selben Standort mit mehreren Allergenen umgegangen wird, können Handschuhe je nach Auswahl und Handhabung entweder Kreuzkontaminationen verhindern oder diese begünstigen. Eine unzureichende Unterscheidung zwischen den Arbeitsschritten oder mangelhafte Wechselverfahren können die Allergenkontrolle schnell untergraben.

Chemische Belastung und unbeabsichtigte Übertragung

Reinigung und Desinfektion bringen eine Reihe weiterer Risiken im Zusammenhang mit PSA mit sich. Bei der Reinigung und Desinfektion sind Handschuhe einer



Schnittschutzhandschuhe können Mitarbeitende schützen und gleichzeitig eine sichere, präzise Handhabung in der Lebensmittelverarbeitung unterstützen



Handschuhe beim direkten Umgang mit Lebensmitteln müssen Hygiene, Fingerfertigkeit und eine zuverlässige Arbeitsausführung unterstützen

Hinzu kommt die Frage der Haltbarkeit. Handschuhe, die wiederholter mechanischer Beanspruchung, Feuchtigkeit oder Chemikalien ausgesetzt sind, können im Laufe einer Schicht an Qualität einbüßen. Risse, Ausdünnungen oder der Verlust der Barrierewirkung sind nicht immer sofort sichtbar, untergraben jedoch sowohl den Schutz der Mitarbeiter als auch die Lebensmittelhygiene.

Verhaltensbedingtes Risiko und falsche Sicherheit

Das vielleicht bedeutendste Risiko im Zusammenhang mit PSA ist verhaltensbedingt. Das Tragen von Handschuhen kann ein falsches Sicherheitsgefühl vermitteln, wenn davon ausgegangen wird, dass das Kontaminationsrisiko allein durch das Vorhandensein einer Barriere gebannt ist.

In Wirklichkeit erfordern Handschuhe ein aktives Management. Sie müssen in

Aufgabe erschweren, da sie die Fingerfertigkeit beeinträchtigen und dazu führen, dass die Handschuhe an der Hand kleben bleiben. Eine klare Schulung zum Ausziehen von innen nach außen, gegebenenfalls unterstützt durch Handschuhe mit einer definierten Manschette oder einer Ausziehmarkierung, hilft dabei, die Technik auch bei häufigen Handschuhwechseln beizubehalten, und verringert das Risiko, dass Kontaminationen genau in dem Moment verbreitet werden, in dem die PSA ausgezogen wird.

Die unsachgemäße Verwendung von Handschuhen ist ein immer wiederkehrendes Thema bei Untersuchungen zur Lebensmittelsicherheit. Handschuhe werden zu lange getragen, zwischen verschiedenen Arbeitsschritten weiterverwendet oder ohne Wechsel sowohl für Lebensmittel als auch für nicht lebensmittelrelevante Oberflächen verwendet. In solchen Situationen kön-

Vielzahl von Chemikalien ausgesetzt, oft in erhöhten Konzentrationen. Sind die Handschuhmaterialien nicht mit den verwendeten Substanzen kompatibel, kann es im Laufe der Zeit zu einer Zersetzung kommen.

Dies hat zwei Konsequenzen. Erstens wird der Schutz der Mitarbeiter beeinträchtigt, wodurch das Risiko einer Hautexposition steigt. Zweitens können zersetzte Handschuhe chemische Rückstände zurück in Bereiche der Lebensmittelverarbeitung tragen, wenn sie wiederverwendet oder nicht ordnungsgemäß gewechselt werden. Auf diese Weise kann PSA, die eigentlich der Hygiene dienen soll, zu einer Quelle chemischer Kontamination werden.

Die Herausforderung wird in Betrieben noch größer, in denen dieselben Handschuhe für verschiedene Aufgaben eingesetzt werden sollen, von der Reinigung bis zur Produktion. Ohne klare, aufgabenspe-

zifische Auswahl- und Wechselprotokolle steigt das Risiko einer unbeabsichtigten Übertragung.

Risikobereiche und die Leistungsfähigkeit von PSA

Die Wirksamkeit von PSA hängt eng mit der Umgebung zusammen, in der sie eingesetzt wird. Nassbereiche, Kühlräume und Wartungsbereiche stellen jeweils unterschiedliche Anforderungen an Handschuhe und andere Schutzausrüstung.

In kalten Umgebungen kann eine verminderte Tastempfindung die Präzision beeinträchtigen und zu erhöhter Ermüdung führen. In feuchten Bereichen kann Feuchtigkeit die Griffbarkeit und den Tragekomfort beeinträchtigen. Bei Wartungsarbeiten belastet der Kontakt mit Ölen, Lösungsmitteln und scharfen Kanten die Materialien zusätzlich. PSA, die in einem Bereich angemessen funktioniert, kann in einem anderen ungeeignet sein.

Diese Variabilität wird bei Risikobewertungen oft unterschätzt. PSA wird häufig

auf einer allgemeinen Ebene festgelegt, ohne ausreichend zu berücksichtigen, wie sie sich in verschiedenen Bereichen, bei unterschiedlichen Aufgaben und bei unterschiedlichen Schichtmodellen bewährt.

PSA als kritischen Kontrollpunkt neu überdenken

Die Zahl von 11,5 Milliarden Euro macht deutlich, dass vermeidbare Schäden oft auf alltäglichen Entscheidungen beruhen und nicht auf außergewöhnlichen Versäumnissen. In der Lebensmittelverarbeitung gehört die PSA zu diesen alltäglichen Entscheidungen. Sie wird täglich unzählige Male ausgegeben, getragen und als Schutzmittel genutzt – oft ohne nähere Überprüfung, sobald die entsprechenden Kontrollkästchen abgehakt sind.

Doch Handschuhe und andere Schutzausrüstung befinden sich an einer kritischen Schnittstelle. Sie beeinflussen gleichzeitig das Verhalten der Mitarbeiter, die Aufgabenerfüllung und das Kontaminationsrisiko. Die Behandlung von PSA als passive Anforderung

statt als aktive Kontrollmaßnahme kann Lücken hinterlassen, die erst sichtbar werden, wenn etwas schiefgeht.

Für Lebensmittelhersteller besteht die Herausforderung nicht darin, mehr PSA einzusetzen, sondern sie intelligenter zu nutzen. Das bedeutet zu verstehen, wo Handschuhe Risiken verringern, wo sie Risiken verursachen und wie Auswahl, Schulung und Überwachung die Ergebnisse in der Produktion beeinflussen.

Wenn PSA auf die tatsächlichen Arbeitsbedingungen abgestimmt ist, unterstützt sie sowohl die Lebensmittelsicherheit als auch den Schutz der Mitarbeiter. Ist dies nicht der Fall, kann sie beides unbemerkt untergraben. **GIT**



Showa

www.showagroup.com

© Bilder-Showa

BG Bau: Branchenlösung für Walzasphalt stärkt den Gesundheitsschutz

Mit der Branchenlösung „Bitumen beim Heißeinbau von Walzasphalt“ stellen die Berufsgenossenschaft der Bauwirtschaft (BG Bau) und ihre Partner der Branche ein praxisnahes Präventionskonzept zur Verfügung. Anlass für die Aktualisierung ist der ab dem 1. Januar 2027 im Bereich Walzasphalt gültige Arbeitsplatzgrenzwert (AGW) für Dämpfe und Aerosole aus Bitumen. Die Branchenlösung zeigt Unternehmen, wie sie diesen Grenzwert einhalten und die Exposition ihrer Beschäftigten wirksam reduzieren können.

Die Branchenlösung „Bitumen beim Heißeinbau von Walzasphalt“ wurde vom Koordinierungsausschuss Bitumen im Walz- und Gussasphaltbau (KoA-Bit) erarbeitet. Ziel der gemeinsamen Initiative ist es, Unternehmen eine einheitliche und praxistaugliche Grundlage für die sichere Verarbeitung von Walzasphalt bereitzustellen.

„Ein wirksamer Gesundheitsschutz braucht Lösungen, die fachlich fundiert und in der Praxis erprobt und mit vertretbaren Mitteln umsetzbar sind. Deshalb haben die beteiligten Verbände und Sozialpartner sowie die BG Bau ihre Erfahrungen gebündelt und ein gemeinsames Maßnahmenkonzept entwickelt, das den Betrieben eine verlässliche Orientierung bietet“, sagt Marc Wählen, Vorsitzender des KoA-Bit.

Belastungen reduzieren mit den richtigen Schutzmaßnahmen

Beim Einbau von Walzasphalt entstehen aufgrund der hohen Verarbeitungstemperaturen Dämpfe und Aerosole aus Bitumen. Sie können insbesondere die Atemwege und Augen reizen. Um Beschäftigte vor Gesundheitsgefahren zu schützen, gilt für den Bereich Walzasphalt ab 1. Januar 2027 ein AGW von 1,5 Milligramm pro Kubikmeter für Dämpfe und Aerosole aus Bitumen. Die Branchenlösung für den Walzasphalteinbau unterstützt Unternehmen dabei, wirksame Präventionsmaßnahmen zur Einhaltung des AGW umzusetzen.

Im Vordergrund stehen die Substitution, also die Verwendung temperaturabgesenkter Asphalte und der Verzicht auf mineralölbasierte Trennmittel, sowie der Einsatz abgesaugter Asphaltstraßenfertiger als technische Maßnahme.

www.bgbau.de



© BG Bau / Joseph Vogele AG

Krause-Katalog „Sonderlösungen mit System“ erschienen

Der neue Katalog für Sonderlösungen von Krause zeigt, wie sich individuelle Steigetechnik wirtschaftlich, sicher und praxisgerecht umsetzen lässt. Im Mittelpunkt des Katalogs stehen Lösungen, die von einer konkreten Aufgabe oder Problemstellung ausgehen und nicht aus dem Standardsortiment bedient werden können. Ob stationäre Plattformtreppe, fahrbare Arbeitsbühne, Überstieg oder spezieller Zugang zu Fahrzeugen und Anlagen: Entscheidend ist, dass die Konstruktion zum Arbeitsprozess passt. Der Katalog macht deutlich, dass Krause Sonderlösungen nicht als Ausnahme, sondern als systematische Antwort auf typische Herausforderungen im Betriebsalltag zu verstehen sind. Gerade in Produktions- und Logistikbereichen zeigt sich dieser Bedarf besonders deutlich. Wenn Förderstrecken, Maschinenlinien oder technische Anlagen sichere Übergänge und definierte Zugänge erfordern, tragen passgenaue Lösungen dazu bei, Abläufe übersichtlicher und sicherer zu gestalten. www.krause-systems.de



BESUCHE UNS AUF
DER MESSE:
HALLE 1 / STAND H1.014

WEIL QUALITÄT MANCHMAL BESONDERS ZÄHLT.

Arbeitskleidung muss halten, was sie verspricht. In jeder Situation, ohne Ausnahmen. Deshalb setzen wir bei Blåkläder seit 1959 auf Komfort und Langlebigkeit in jedem Detail unserer Arbeitskleidung. Und geben eine lebenslange Garantie* auf unsere Nähte. Damit du dich auf das Wesentliche konzentrieren kannst: deine Arbeit.

Gewöhnen wir uns wieder daran, dass Dinge funktionieren! Wenn für dich Qualität zählt, besuche uns auf der Arbeitsschutz Aktuell.

Blåkläder. Weil Qualität zählt.

BLÅKLÄDER
WORKWEAR

BLAKLADER.COM

*Weitere Informationen und Bedingungen zur Nahtgarantie auf blaklader.de

KNIESCHUTZ

Stabil im Knien, beweglich im Einsatz

Knieschutz für Baustelle und Montage: reduziert Druckspitzen und verbessert den Tragekomfort

Bei zahlreichen Tätigkeiten im Handwerk, im Garten- und Landschaftsbau oder bei Montagearbeiten gehören kniende Arbeiten zum Alltag. Die dabei auftretenden Druckbelastungen auf Kniegelenke und umliegende Strukturen können zu akuten Beschwerden und langfristigen Verschleißerscheinungen führen. Mit dem Knieschoner „Ergo Pro“ stellt Nierhaus nun ein Produkt zur Verfügung, das auf eine gleichmäßige Druckverteilung und einen dauerhaft stabilen Sitz ausgelegt ist.

Ein Schwerpunkt der Entwicklung lag auf einer möglichst einfachen Handhabung. „Uns ging es darum, Schutz und Komfort zu vereinen, ohne aufwendige Nachstellungen im Arbeitsalltag“, erklärt Kerstin Stieghorst, Geschäftsführerin von Nierhaus. Ziel sei es zudem gewesen, Komfort und sicheren Halt auch bei längerer Tragedauer miteinander zu verbinden.

Breites Riemensystem für festen Halt

Kennzeichnend für den Ergo Pro ist ein etwa fünf Zentimeter breiter, elastischer und atmungsaktiver Textilgummiriemen. Dieser umschließt das Bein ober- und unterhalb des Knies und wird einmalig individuell angepasst. Anschließend lässt sich der Knieschoner über eine einrastende Schnalle schnell schließen. Das Nachziehen während des Arbeitstags soll dadurch weitgehend entfallen.

Gleichzeitig verteilt der breite Riemen den Anpressdruck auf eine größere Fläche, wodurch punktuelle Belastungen am Bein reduziert werden können. Dies trägt zu einem stabilen Sitz bei und unterstützt den Tragekomfort auch bei häufigen Bewegungen.

Ergonomische Konstruktion mit PU-Schaum

Für die Polsterung setzt der Hersteller auf PU-Schaum. Das Material wird aufgrund seiner dämpfenden und zugleich widerstandsfähigen Eigenschaften häufig in der persönlichen Schutzausrüstung eingesetzt. Die ergonomisch gestaltete Form des

Knieschoners schafft eine vergleichsweise große Auflagefläche, sodass sich beim Knien auftretende Kräfte besser verteilen können.

Ergänzt wird die Konstruktion durch eine gleitfähige Außenschale. Sie erleichtert Bewegungen auf unterschiedlichen Untergründen und kann insbesondere bei Tätigkeiten von Vorteil sein, bei denen die Arbeitsposition regelmäßig verändert werden muss. Der zum Schienbein hin angepasste Bereich sorgt zudem für eine körpernahe Passform, ohne die Bewegungsfreiheit einzuschränken.

Der rund fünf Zentimeter breite, elastische Textilgummiriemen des Ergo Pro sorgt für einen stabilen Sitz und verteilt den Anpressdruck großflächig

Für Innen- und Außeneinsätze ausgelegt

Der Ergo Pro ist für verschiedene Einsatzumgebungen konzipiert und kann auf Untergründen wie Beton, Estrich oder Erde verwendet werden. Typische Anwender finden sich unter anderem im Bodenlegerhandwerk, bei Installationsarbeiten sowie im Garten- und Landschaftsbau.

Knieschoner dienen grundsätzlich dazu, mechanische Einwirkungen auf die Knie zu reduzieren und Druckkräfte gleichmäßiger zu verteilen. Dadurch lassen sich Belastungsspitzen sowie mögliche Haut- und Gewebeerirritationen verringern. Aus arbeitsmedizinischer Sicht gilt eine gleichmäßige Druckverteilung als wichtiger Faktor zur Entlastung der Gelenkstrukturen bei regelmäßig knienden Tätigkeiten.

Insgesamt verfolgt der Ergo Pro das Ziel, durch die Kombination aus ergonomischer Polsterung, breitem Riemensystem und gleitfähiger Außenseite einen dauerhaft komfortablen und sicheren Knieschutz für den professionellen Einsatz bereitzustellen. **GIT**



Nierhaus GmbH

<https://nierhaus-knieschoner.de>

Produktneuheiten im Asecos Hauptkatalog



Die Asecos GmbH hat ihren Hauptkatalog „Sicheres Arbeiten mit Gefahrstoffen: Lagerung – Absaugung – Handling“ aktualisiert. Er enthält neben essenziellem Fachwissen auch Produktneuheiten, wie den Ion-Line Core Store Unterbauschrank. Der überarbeitete Hauptkatalog

präsentiert auf nun 500 Seiten das komplette Produktportfolio – von Sicherheits-schränken über Gefahrstoffarbeitsplätze und Zubehör bis hin zum Serviceangebot. Die Experten von Asecos vermitteln zudem praxisnahes Fachwissen mit Blick auf die neuesten Gesetze, Normen und Regelwerke. Zu den Produktneuheiten zählen unter anderem Erweiterungen der Ion-Line Sicherheitsschränke zum sicheren Lagern und Laden von Lithium-Akkus. Neue Fachbodentrenner ermöglichen eine übersichtliche Organisation in den Lagerebenen der Schränke der dritten Generation.

www.asecos.com

Weniger Schrauben, mehr Sicherheit: HYGHTS-Geländersysteme

Neuigkeiten vom Flachdach: Eine spezialisierte Montagefirma hat das HYGHTS-Geländersystem von Hymer-Steigtechnik erstmals installiert – und zeigt sich überzeugt. Der Aufbau ging spürbar schneller von der Hand. Begleitet wurde die Montage von einem Filmteam, das festhält, wie das ballastierte Dachgeländersystem unter realen Bedingungen funktioniert.



„Supereinfach und tatsächlich deutlich schneller in der Montage“, so das Fazit aus dem Montageteam. Der Praxisversuch macht sichtbar, was hinter dem Systemkonzept steckt: reduzierte Komplexität, hoher Vorfertigungsgrad und eine Montage, die ohne unnötige Arbeitsschritte auskommt. Für Christian Frei, Vertriebsleiter Steigtechnik bei Hymer-Leichtmetallbau, bestätigt das Feedback den Entwicklungsansatz: „Das HYGHTS-Geländersystem ist konsequent für den Einsatz auf dem Dach konzipiert. Intuitive Handhabung und ein cleveres Klippsystem sparen Zeit und entlasten die Monteure spürbar.“

www.hymer-steigtechnik.de

Offroad-System Premium erleichtert Materialtransport



Bordsteinkanten und Kopfsteinpflaster in der Innenstadt, matschige Wiesen und Holperpisten im Gelände: Diese Hindernisse können Einsatzkräfte jetzt auch mit vollbeladenen Rollcontainern problemlos überwinden und den Materialtransport selbst im unwegsamen Gelände sicherstellen. Möglich macht dies das neue Offroad-System Premium für Rollcontainer, das die Munk Rettungstechnik auf der Interschutz

2026 vorgestellt hat. Die Neuheit definiert die Einsatz-Logistik im Gelände neu, denn egal welcher Untergrund und welches Hindernis – das Offroad-System Premium ist schnell montiert und bleibt auch unter extremen Bedingungen einfach zu steuern. Mit dem Offroad-System Premium sei es gelungen, einen neuen Standard für die Logistik im Outdoor-Einsatz zu setzen. Denn die Rollcontainer seien nun so geländegängig wie nie zuvor, so Ferdinand Munk, Geschäftsführer und Inhaber der Munk Group mit Sitz in Günzburg und Leipheim.

www.munk-group.com



**SELBST
49 MINUSGRADE
KÖNNEN DICH
NICHT SCHRECKEN.**

TEMPEX® COLD Pro schützt dich zuverlässig im TK-Bereich, ist komfortabel ausgestattet, unfassbar bequem und leasingtauglich.



EN 17353
Typ B2



EN 342



PRO Label

HB Protective Wear
Phone +49 2639 8309-0
www.hb-online.com

be safe. we care.



EVENT

Arbeitsschutz Aktuell 2026

Wenn Sicherheit zur Chefsache wird



Vom 20. bis 22. Oktober 2026 wird die Landesmesse Stuttgart zum Treffpunkt der Arbeits- und Gesundheitsschutz-Branche. Mit neuen Themenwelten rund um KI und mentale Gesundheit, den erstmals angebotenen Safety Trails und der Live Experience Area Büro entwickelt sich der traditionsreiche Community-Treff konsequent weiter.

Wer im Arbeitsschutz Verantwortung trägt, geht ungern Risiken ein – schon gar nicht das Risiko, eine Entwicklung zu verpassen. Genau hier setzt die Arbeitsschutz Aktuell an, die seit 1972 im zweijährigen Turnus zu den festen Größen der Branche zählt. Rund 100 Aussteller und mehrere tausend Fachbesucher werden im Oktober in Halle 1 der Messe Stuttgart erwartet, wenn Veranstalter Hinte Expo & Conference das gesamte Spektrum von persönlicher Schutzausrüstung über Gefahrstoffmanagement bis hin zum technischen Arbeitsschutz zusammenführt. Fachmesse und Praxisprogramm sind dabei mit einem einzigen Ticket zugänglich und eng miteinander verzahnt.

Die Themen 2026: zwischen KI, Roboterarm und Resilienz

Was macht künstliche Intelligenz mit dem Arbeitsschutz? Wie arbeiten Mensch und

Roboter sicher Seite an Seite? Und was ist zu tun, wenn der Kopf nicht mehr mitmacht, obwohl der Helm sitzt? Das inhaltliche Gerüst bilden vier Leitthemen: Mensch & Maschine, Autonome Systeme & Fernarbeit, Resilienz & mentale Gesundheit sowie ESG & Nachhaltigkeit. Ergänzt werden sie um Praxisfelder wie smarte PSA, Wearables und Exoskelette, Sensorik und vernetzte Sicherheit sowie konkrete Lösungen für Baustelle, Halle und Lager. Roter Faden ist die Frage, wie sich gesetzliche Anforderungen, technische Lösungen und betriebliche Praxis sinnvoll verbinden lassen.

Neu: Safety Trails führen & Live Experience Area Büro

Insbesondere für Besucher mit knappem Zeitbudget, gibt es in diesem Jahr mit den sogenannten „Safety Trails“ erstmals einen fokussierten Rundgang. Vier thematische

Routen – Smart Safety, Next Generation, PSA & Workwear und High Risk – führen Besucher gezielt zu den passenden Ständen und Vorträgen. QR-Code auf dem Badge scannen, den Hallenplan aufs Smartphone laden und loslaufen: So lässt sich der Messebesuch auch dann strukturieren, wenn der Kalender kaum Spielraum lässt.

Dass Arbeitsschutz längst nicht mehr an der Werkshalle endet, macht die neue Live Experience Area Büro deutlich. Hier wird moderner Arbeitsschutz nicht nur präsentiert, sondern in realen Arbeitssituationen erlebbar – von Ergonomie und mentaler Gesundheit über New Work bis zum digitalen Alltagsschutz. Angesprochen sind alle, die Verantwortung für Menschen am Schreibtisch tragen: von der Geschäftsführung über Fachkräfte für Arbeitssicherheit bis zu BGM-, HR- und Organisationsverantwortlichen.

Zwei Bühnen, ein Ticket: das Fachprogramm

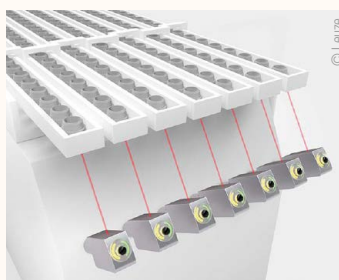
Das Konferenzprogramm verteilt sich auf zwei Formate. Auf der Expo Stage gibt es kompakte Impulse in 20-minütigen Slots – ideal für den schnellen Wissenstransfer zwischen zwei Standbesuchen. Wer tiefer einsteigen möchte, findet in der Praxis-konferenz kuratierte Themenblöcke der Medienpartner Konradin, Haufe und SZwei Verlag, die dank Silent-Stage-Technik mit Kopfhörern konzentriertes Zuhören mitten im Messegesehen ermöglicht. Vertiefendes Wissen zum sicheren Umgang mit Gefahrstoffen steuern die Themenpartner Asecos und Denios bei; für deren Seminare gibt es VDSI-Weiterbildungspunkte.

Treffpunkt mit Tradition

Seit über 50 Jahren treffen auf der Arbeitsschutz Aktuell Fachkräfte für Arbeitssicherheit auf Betriebsärztinnen und Betriebsärzte, HSE-Verantwortliche auf BGM- und HR-Profis. Zwischen den Ständen entstehen die Gespräche, für die im Arbeitsalltag sonst kaum Zeit bleibt. Mit einem Tagesticket für 60 Euro und einer Dreitageskarte für 90 Euro – jeweils inklusive Fachprogramm – bleibt die Hürde für einen Besuch niedrig. Auch die Redaktion der GIT SICHERHEIT wird wieder vor Ort sein, um Neuheiten aufzuspüren, mit den Marktführern zu sprechen und die Trends der Branche einzuordnen – vor, während und nach der Messe, im Heft wie online. Wer die Entwicklungen des Arbeitsschutzes aus erster Hand erleben will, sollte sich den Termin im Oktober also fest im Kalender vormerken. **GIT**



Hinte Expo & Conference GmbH
<https://arbeitsschutz-aktuell.hinte-messe.de>



Annex-1-konforme Lösung: Seitlich oder unterhalb des Produkts montierte ToF-Sensoren detektieren dieses zuverlässig, ohne den First-Air-Bereich zu unterbrechen – eine Sterilisation der Sensoren ist dann nicht erforderlich

Standards für Sensorik in steriler Umgebung

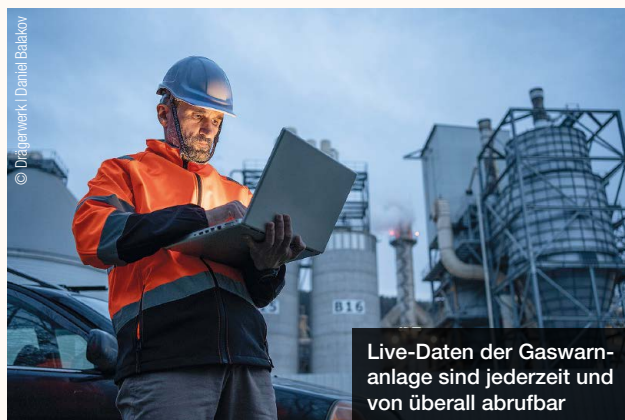
Sterile Arzneimittel und Medizinprodukte müssen kontaminationsfrei verpackt werden, die Anforderungen an die Sterilisation der Komponenten regelt die EU-GMP-Richtlinie, das teilt Leuze mit. Die Sterilisationspflicht betrifft mit dem aktualisierten Annex 1 seit Ende August 2024 nicht nur direkt und indirekt produktberührende Teile, sondern auch alle Komponenten, die als „First-Air-unterbrechend“ gelten – etwa Sensoren oder Reflektoren, die sich oberhalb der sterilen Komponenten befinden. Je nach Sensortyp ergeben sich unterschiedliche Herausforderungen und Chancen im Hinblick auf den Einsatz in der Pharmaproduktion und -verpackung. Die neuen Annex-1-Anforderungen machen eine durchdachte Auswahl und Integration der Sensorik unverzichtbar. Hygienegerechte, flexibel montierbare Edelstahl-Sensoren von Leuze unterstützen dabei, die Vorgaben sicher und effizient umzusetzen.

www.leuze.com

Neues Edge Device macht Dräger-Gaswarnanlagen IIoT-fähig

Das neue Edge Device von Dräger verwandelt bestehende Regard 3000, 3000 plus und 7000 Gaswarnanlagen in smarte IIoT-Systeme. Es verbindet die Anlagen mit der Cloud-basierten Softwarelösung Gas Detection Connect und ermöglicht so einen flexiblen Zugriff auf alle Geräte- und Messdaten. Anlagenbetreiber können von jedem internetfähigen Gerät ohne vorherige Installation Trendcharts sowie Ereignis- und Alarmlisten ihrer Gaswarnanlage abrufen. Die Software visualisiert durch die Integration des Edge Devices sowohl Live- als auch historische Daten von stationären Gaswarntansmittern und mobilen Ein- und Mehrgasmessgeräten. Die Daten werden nach aktuellen Sicherheitsstandards in die Cloud übertragen. Alternativ zur Cloud steht auch ein Zugriff über einen OPC-UA-Server zur Verfügung.

www.draeger.com



Live-Daten der Gaswarnanlage sind jederzeit und von überall abrufbar



FC Schalke 04 begrüßt Blåkläder als neuen Ärmelpartner

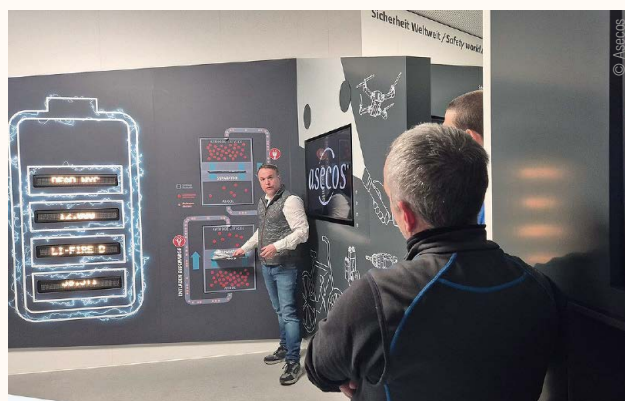
Zur Spielzeit 2026/2027 gewinnt der Bundesliga-Aufsteiger FC Schalke 04 mit Blåkläder einen international renommierten Workwear-Spezialisten als neuen Haupt- und Ärmelpartner. Der Name der schwedischen Marke bedeutet übersetzt „blaue Kleidung“ und schafft damit bereits sprachlich eine natürliche Verbindung zur königsblauen Identität des Vereins. Entscheidend ist jedoch vor allem die gemeinsame Haltung: anpacken, als Team funktionieren und verlässlich bleiben. Erfahrung im Sportumfeld bringt Blåkläder bereits mit, etwa als Sponsor der Handball-WM. Mit dem FC Schalke 04 schließt die Marke nun ihre erste Trikotpartnerschaft in Deutschland. Damit verbindet die Partnerschaft die Arbeitswelt, aus der Schalke historisch gewachsen ist, mit der Kompetenz eines Spezialisten für professionelle Arbeitskleidung und dem gemeinsamen Verständnis von Leistung, Teamgeist und Verlässlichkeit.

www.blaklader.com

Asecos online Expo „Lithium Special“ geht in die zweite Runde

Am 29. und 30. September lädt die Asecos GmbH, Experte für Gefahrstofflagerung und -handling, zur zweiten Sonderausgabe der Asecos online Expo ein. Im Mittelpunkt der digitalen Veranstaltungsreihe steht der sichere Umgang mit Lithium-Akkus. Der Einsatz von Lithium-Akkus nimmt in zahlreichen Branchen kontinuierlich zu. Bei ordnungsgemäßem Betrieb gelten sie als sicher, im Falle von Defekten bergen sie jedoch Brandrisiken. Entsprechend wachsen die Anforderungen an ihre sichere Lagerung und Handhabung. Die Asecos online Expo „Lithium Special“ greift diese Entwicklung auf und bietet Einblicke in aktuelle Erkenntnisse, neue Anforderungen sowie praxisnahe Lösungen. In exklusiven Vorträgen und interaktiven Präsentationen vermitteln Experten Fachwissen aus erster Hand – kompakt aufbereitet, praxisnah und für den direkten Einsatz im Betrieb.

www.asecos.com



GIT BusinessPartner

– kompetente Anbieter und Institutionen in Sachen Sicherheit.



ARBEITSSCHUTZ

MASCHINEN- &
ANLAGENSICHERHEIT

BRANDSCHUTZ

PHYSISCHE
SICHERHEITIT- & CYBER-
SECURITY

Generated with AI

Sicherheitsmanagement



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
Sicherheitsfachhändler.

Sicherheitsmanagement



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 Zutrittskontrollsysteme;
biometrische Verifikation; Wächterkontrollsysteme;
Verwahrung und Management von Schlüsseln und
Wertgegenständen

Sicherheitsmanagement



GU BKS SERVICE GmbH
Heidestr. 71 · 42549 Velbert
Tel. 0800/2051001
office@gu-bks.de · www.gu-bks.de

Service mit System



Sicherheitsmanagement



hensec – secure solutions
Luisenstr. 56, 76689 Karlsdorf-Neuthard
Tel.: +49(0)72519238750 · kontakt@hensec.com
360-Grad-Sicherheitslösungen für Industrie,
Wirtschaft und Behörden um physische Sicherheit
und Cybersecurity. **Drohnenabwehr**, Abhörschutz,
OT-Security, Informationssicherheit, KRITIS, OsInt,
Perimeterschutz. Prüfung, Entwicklung, Implemen-
tierung und Schulung.

Sicherheitsmanagement



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



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

SICHERHEITS MANAGEMENT

Sicherheitsmanagement



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 Privat-
anwendern spezialisiert.

Sicherheitsmanagement



ADI Global Germany GmbH
Neuer Zollhof 3 · 40221 Düsseldorf
Tel.: +49 (0)211 869 42089
www.adiglobal.de · sales.de@adiglobal.com
Ihre zentrale Anlaufstelle für Sicherheit, Brandschutz
und audiovisuelle Produkte. Unser Sortiment besteht
aus über 200 führender Marken und einem globalen
Lieferantennetzwerk sowie einem leistungsstarken
24/7 Onlineservice.

Sicherheitsmanagement

ASSA ABLOY

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



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



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-, Brand-
melde-, Sprachalarm- und Managementsysteme, professionelle
Audio- und Konferenzsysteme. In ausgewählten Ländern bietet
Bosch Lösungen und Dienstleistungen für Gebäudesicherheit,
Energieeffizienz und Gebäudeautomation an.

Sicherheitsmanagement

Signum Consulting GmbH
Marke **DISA**
Rungestraße 19 · 10179 Berlin
info@de.disa.com · martin.mehner@de.disa.com
<https://disa.com/de>



Signum Consulting GmbH / Marke DISA – Ihr Ansprechpartner für Pre-Employment-Screening und Geschäftspartnerprüfungen, prozessbegleitend von der Planung bis zur Umsetzung.

Gebäudesicherheit



DOM Sicherheitstechnik GmbH & Co. KG
Wesseling 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

PERIMETER SCHUTZ

Sicherheitsmanagement



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.

Gebäudesicherheit



SimonsVoss Technologies GmbH
Münchner Str. 16 · 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.

Sicherheitsmanagement



DISTRIBUTION MIT LÖSUNGSKOMPETENZ

Spezialisiert auf die weltweite Distribution von Komponenten namhafter Hersteller der Video- und Sicherheitstechnik.

Xortec GmbH
Frankfurt am Main (Hauptsitz) | Niederlassungen:
Berlin - Hamburg - München - Regensburg

xortec.de

Ihr Eintrag in der Rubrik



Schicken Sie einfach eine E-Mail
an miryam.reubold@wiley.com

Wir beraten Sie gerne!

VIDEO ÜBERWACHUNG

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 Privat-anwendern spezialisiert.

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



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



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



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



Uhlmann & Zacher GmbH
Gutenbergstraße 2-4 · 97297 Waldbüttelbrunn
Tel.: +49(0)931/40672-0 · Fax: +49(0)931/40672-99
contact.uz@assaabloy.com · www.uhlmannzacher.com
Elektronische Schließsysteme, modular aufgebaut und individuell erweiterbar.
Seit 2025 gehört das Unternehmen zur Assa Abloy-Firmengruppe.

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.

Videoüberwachung

i-PRO

i-PRO EMEA B.V.
Herikerbergweg 292 · 1101CT Amsterdam
Netherlands
<https://i-pro.com/eu/en>
Hochwertige CCTV-Lösungen (IP & analog), Video-Auto-
matisierung und KI, Technologien für hohe Ansprüche
(FacePro, Personen-Maskierung), Schutz vor Cyber-
Angriffen im Einklang mit DSGVO, VMS: Video Insight

Zeit + Zutritt


DoorBird
Technology meets Design.

Bird Home Automation GmbH
Uhlendstr. 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

FEIG

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 Zufahrts-
kontrolle, Geländeabsicherung, Bezahlssysteme u.v.m.

Videoüberwachung


**MOBILE
VIDEOSICHERHEIT**



LivEye GmbH
Europa-Allee 56b
54343 Föhren
liveye.com

Zeit + Zutritt

Connect people.
Create access.



CES
C.Ed. Schulte GmbH Zylinderschlossfabrik
Friedrichstraße 243 · D-42551 Velbert
Objektabteilung@ces.eu · www.ces.eu
Mechanische, mechatronische und elektronische
Schließsysteme, Zutrittskontrolle

Zeit + Zutritt


gantner
INSPIRED ACCESS

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

**ZEIT
ZUTRITT****Ihr Eintrag in der Rubrik**

BusinessPartner
Die Einkaufsrubrik für den direkten Kontakt

Schicken Sie einfach eine E-Mail
an miryam.reubold@wiley.com

Wir beraten Sie gerne!

Zeit + Zutritt


phg
Die richtige Verbindung

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

Zeit + Zutritt


AceProx
Identifikationssysteme GmbH

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, 125kHz LF/13,56MHz HF
sowie ATEX-Lesetechnik.

Zeit + Zutritt


**cichon+
cryptin** **STOLBERG**

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


primion

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, Perso-
naleinsatzplanung, grafisches Alarmmanagement, SAP-
Kommunikationslösungen, Ausweiserstellung, Biometrie

Zeit + Zutritt

ASSA ABLOY

ASSA ABLOY Entrance Systems GmbH
Lagerstr. 45 · 64807 Dieburg
Tel.: +49 6071 208 0 · Fax: +49 6071 208 111
sec.de@assaabloy.com · www.assaabloyentrance.de
Speedgates, Durchgangs- und Sicherheitsschleusen,
Drehkreuze, Schwenktüren, Sicherheits-Karussell-
türen und -Portale für die Sicherheits-Zutritts-
kontrolle und Personenvereinzelnung.

Zeit + Zutritt


**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

Zeit + Zutritt


salto
INSPIRED ACCESS

SALTO Systems GmbH
Schwelm 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.

Zeit + Zutritt


A Z S
SYSTEM AG

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 Schranken-
anlagen, OPC-Server

Zeit + Zutritt


dormakaba

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 ver-
netzte elektronische Zutrittslösungen, physische Zugangs- und
automatische Türsysteme, Türbänder, Beschläge, Türschließer,
Zeiterfassung inkl. ERP-Anbindungen, Hotelschließsysteme
und Hochsicherheitsschlösser.

Zeit + Zutritt


**TKH
SECURITY**

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

NOTRUF SERVICE LEITSTELLE

Notruf- und Service-Leitstelle

HWS

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, Alarmempfangs-
stelle DIN EN 50518, Alarmprovider, Mobile Einsatz-
und Interventionskräfte, Objekt- und Werkschutz



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.

Ihr Eintrag in der Rubrik

git BusinessPartner
Die Einkaufsrubrik für den direkten Kontakt

Schicken Sie einfach eine E-Mail
an miryam.reubold@wiley.com

Wir beraten Sie gerne!

BRAND SCHUTZ

Brandschutz

DENIOS

UMWELTSCHUTZ & SICHERHEIT

DENIOS SE
Dehmer Straße 54-66
32549 Bad Oeynhausen
Fachberatung: 0800 753-000-3
Gefahrstofflagerung, Brandschutzlager,
Brandschutz für Lithium-Akkus, Wärme- und Kälte-
kammern, Containment, Auffangwannen, Arbeits-
schutz, sicherheitsrelevante Betriebsausrüstung,
Gefahrstoff-Leckage-Warnsystem

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 Brandschutz-
lösungen. Branchenspezifisches Fachwissen mit hoch-
wertigen Brandschutzkomponenten vereint zu einem
sicheren und verlässlichen Brandschutz. Flankiert wird
dies mit Fachschulungen und einem umfangreichen,
lösungsorientierten Kundenservice.

Brandschutz

setec

Securitas Technology GmbH
SeTec Sicherheitstechnik
Hauptstr. 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
Schlüsseldepos, Feuerwehr, Schlüsselmanager,
Feuerwehrperipherie, Feststellanlagen, Störmeldezentralen

Brandschutz

WAGNER

DIE BESSERE LÖSUNG IM 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

ARBEITS SICHERHEIT

Arbeitssicherheit



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

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



Bequem auf dem Sofa durch die
e-Ausgabe der GIT SICHERHEIT
blättern: Registrieren Sie sich auf
www.git-sicherheit.de/newsletter



Arbeitssicherheit



KRAUSE-Werk GmbH & Co. KG
Am Kreuzweg 3 · D-36304 Alsfeld
Tel.: +49 (0) 6631 / 795 - 0
info@krause-systems.de
www.krause-systems.com

Tritte, Leitern, Steigtechnik, Podestleitern, Fahrgerüste

Gefahrstoffmanagement



SÄBU Morsbach GmbH
Zum Systembau 1 · 51597 Morsbach
Tel.: 02294 694-24 · Fax: 02294 694-38
safe@saebu.de · www.saebu.de
Gefahrstofflagerung, Gefahrstoffcontainer, Auffangwannen, Bodenschutzsysteme, Gasflaschenlagerung, Gasflaschencontainer, Gasflaschenbox, Kleingebinderegale
Unser Online-Shop: www.fladafi.de

Ihr Eintrag in der Rubrik



Schicken Sie einfach eine E-Mail
an miryam.reubold@wiley.com

Wir beraten Sie gerne!

Maschinen + Anlagen



IBF Solutions GmbH
Bahnhofstr. 8 · 6682 Völs - 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.

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- und Arbeitsschutz, Sicherheitsschranken, Chemikalien- und Umluftschränke, Druckgasflaschenschranken, Gefahrstoffarbeitsplätze, Absauganlagen, Raumluftreiniger uvm.

Gasesmesstechnik



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 Gasesmesstechnik

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
Sicherheitsschaltungen und Sicherheitssensoren, optoelektronische Sicherheitseinrichtungen wie Sicherheitslichtschranken sowie Sicherheitsrelaisbausteine, programmierbare Sicherheitssteuerungen und die Safety Services des Geschäftsbereichs tec.nicum

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

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

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.com · info@euchner.de
Automation, Mensch/Maschine, Sicherheit

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, Zuhalten, Module, Steuerungen, Mensch-Maschine-Schnittstelle, Positions- und Mikroschalter, Komponenten für die Aufzugsindustrie, u.v.m.

Jetzt

Newsletter abonnieren



Ihre
Nummer 1
seit mehr als
35 Jahren

inklusive
e-Ausgabe!



Nachrichten für
Entscheider und
Führungskräfte in
Sachen Sicherheit

DIE VIP LOUNGE



Hans-Peter Stuch

Gruppenleiter Drohnenabwehr im Fraunhofer FKIE

- Hans Peter Stuch; geb. 1956 in Bonn, verheiratet, 2 Kinder, Ingenieur der Nachrichtentechnik
- U. a. Entwicklungsingenieur für Mikroprozessorsysteme und Anwendungen im Bereich der Funkaufklärung
- Verbindungsingenieur des Rüstungsbereiches (BMVg und BWB [heute BAaINBw]) im Rahmen des Programms LAPAS bei der Firma E-Systems, Greenville, TX
- Forschung und Entwicklung zur Störung und Täuschung von modernen Funkkommunikationsverfahren einschl. C-RCIED (Verhindern der Funkauslösung von Sprengfallen)
- Forschung und Entwicklung im Kontext Drohnenabwehr
- Leiter der Drohnenabwehrprojekte AMBOS und IDAS-PRO (Co-Lead)
- Co-Lead des Projekts „Erkennen von hybriden Bedrohungen“
- Projektarbeit im Kontext Drohnenabwehr sowie Unterstützung bei Arbeiten zur Störung und Täuschung von Funkkommunikationsverfahren

Ihr Berufswunsch mit 20 war: Ingenieur zu werden – und mit 21 war ich einer.

Was hat Sie dazu bewogen, eine Aufgabe im Bereich Sicherheit zu übernehmen? Zunächst der Zufall, weil nahe meines Heimatortes Bonn eine Forschungseinrichtung Ingenieure der Nachrichtentechnik suchte. Über die Jahre kam das Bewusstsein dazu, mit dieser Arbeit zur Sicherung unserer Art zu leben beizutragen. Daneben trug ich 50 Jahre lang als aktives Mitglied in der Freiwilligen Feuerwehr Bonn zur lokalen physischen Sicherheit bei.

Welche sicherheitspolitische Entscheidung oder welches Projekt sollte Ihrer Meinung nach schon längst umgesetzt sein? Die Verschlinkung der Bürokratie im Bereich der Sicherheit Deutschlands. Hierbei stehen mit der Digitalisierung und der Künstlichen Intelligenz relevante Enabler zur Verfügung.

Die beste Erfindung im Bereich Sicherheit ist Ihrer Meinung nach: Hier gibt es aus meiner Sicht nicht die eine Erfindung, die aus den vielen Erfindungen im Bereich der Sicherheit heraussticht.

Ein Erfolg, den Sie kürzlich errungen haben, war: Das Thema „Drohnenabwehr“ in zahlreichen Vorträgen als in 2026 relevant zu verdeutlichen und den Zuhörern bzw. Zuschauern eine Einordnung „Drohne – worüber sprechen wir überhaupt“ zu geben.

Wer hat Ihrer Meinung nach eine Auszeichnung verdient? Alle Personen, die sich jeden Tag auf der Straße oder auch in militärischen Konflikten für unser aller Sicherheit großen persönlichen Gefahren aussetzen – und für die Home Office nicht möglich ist.

Wobei entspannen Sie? Beim Walken, Fahrradfahren und Spiel mit den Enkelkindern

Welchen Urlaubsort können Sie empfehlen? Agios Nikolaos auf Kreta

Welche Zeitschriften lesen Sie regelmäßig? Printmedien lese ich eher selten, aber digitale Angebote wie GIT SICHERHEIT, Hartpunkt, Polizei Verkehr&Technik sowie tagesaktuelle Nachrichtenportale.

Die GIT SICHERHEIT ist für mich wichtig, weil... ich hier aktuelle Informationen aus vielfältigen Bereichen der Sicherheit erhalte. Dieses trägt zum Überblick bei und ermöglicht Anknüpfungspunkte für weitergehende Recherchen zu finden.

Welches Buch haben Sie zuletzt gelesen? „Blackout“ von Marc Elsberg

Welche Musik hören Sie am liebsten? Rock- und Popmusik

Was motiviert Sie? Mit meinen Beiträgen im technisch-wissenschaftlichen Umfeld die Welt – im Kleinen wie vielleicht auch im Großen – etwas sicherer zu machen und so meinen Nachkommen den positiven Blick in die Zukunft zu stärken.

Worüber machen Sie sich Sorgen – und was stimmt Sie zuversichtlich? Im politischen Umfeld – und zwar in Deutschland, Europa und der Welt – scheint das Recht des Stärkeren Werte wie Demokratie, Menschen- und Völkerrecht sowie Toleranz zu verdrängen. Akteure, die zum eigenen Nutzen anderen Menschen Unheil antun, einfach, weil sie es können, machen mich besorgt. Zuversichtlich machen mich Fortschritte in der Wissenschaft und die zahlreichen – häufig bilateralen – Gespräche, in denen der Wille dominiert, diese Fortschritte zum Wohle der Menschheit zu nutzen.

Entwickelt für maximale Wirkung

HID liefert den ächenbündigen
Signo-Leser, auf den Sie
gewartet haben.



Jedes sichtbare Detail eines Gebäudes ist eine bewusste Designentscheidung. Zutrittskontrollleser bilden dabei keine Ausnahme. Der HID Signo Décor erfüllt daher die höchsten Anforderungen von Planern, Architekten und Designern. Der ächenbündige Signo-Leser, fügt sich harmonisch in die Architektur ein, während er im Inneren alles bietet, was Sie von Signo erwarten: höchste Sicherheitsstandards, Unterstützung für mobile Zutrittsberechtigungen und komfortables Remote-Management.

Erhältlich in Weiß oder Schwarz – passend für jede Umgebung.

Kommen Sie vorbei und erfahren Sie mehr an
unserem Stand auf der **Security Essen**.

Stand: 6E28 | Halle 6



Mehr erfahren >>
campaigns.hidglobal.com/signo



**Moderne Cloud-Plattform für
Ihre gesamte physische Sicherheit.**

Jede Tür. Jede Kamera.
Jederzeit im Blick.



Mehr erfahren unter brivo.com/de



A Brivo Solution