

GIT SICHERHEIT

Mit
TOP PLAYER
Interviews

MAGAZIN FÜR SAFETY UND SECURITY

TITELTHEMA Seite 20:

Vorbereitet auf den Ernstfall

Marco Skolik und Jörg Kastner über
Krisen- und Notfallmanagement bei Roche



Interflex:

Ganzheitliche Sicherheit
ohne aufwendige
Verkabelung

S. 47



Fire Protection Solutions:

Digitale Löschtechnik
für komplexe Logistik-
gebäude

S. 64



Asecos:

Sicheres Lagern und
Laden von Lithium-
Ionen-Akkus

S. 77

**GIT
SICHERHEIT
AWARD**
FINALISTS



JETZT ABSTIMMEN

WWW.SICHERHEIT-AWARD.DE



PRO-4-PRO

PRODUCTS FOR PROFESSIONALS

DIE LEAD-PLATTFORM

GIT-SICHERHEIT.de/de/produkte

NACHRICHTEN

INTERVIEWS

MARKTANALYSEN

PRAXISBERICHTE

PRODUKTE

WILEY



REAL-TIME ASSET MONITORING –

FÜR EINE SICHERE ZUKUNFT

Ob Gefahrstoffe, Elektrowerkzeuge oder Lithium-Ionen-Batterien – mit dem DENIOS Real-time Asset Monitoring wissen Sie jederzeit, ob sich Ihr Inventar außerhalb des Sicherheitsschranks befindet und wer es nutzt – rund um die Uhr und in Echtzeit.



denios.de/asset-monitoring

Resilienz zeigen – Sicherheit gestalten

Resilienz ist zu einem der zentralen Schlagworte unserer Zeit geworden. Zwischen geopolitischen Spannungen, zunehmender Digitalisierung und einer wachsenden Bedrohungslage für kritische Infrastrukturen zeigt sich: Sicherheit bedeutet heute mehr als Schutz – sie bedeutet Anpassungsfähigkeit. Wer morgen bestehen will, muss heute lernen, flexibel auf Unvorhersehbares zu reagieren.

Genau diesen Gedanken greift unser Titelthema „Gelebte Resilienz“ (ab Seite 20) auf. Es zeigt eindrucksvoll, wie Unternehmen und Organisationen ihre Sicherheitsstrategien nicht nur robuster, sondern zugleich agiler gestalten – und warum Resilienz längst zum entscheidenden Wettbewerbsfaktor geworden ist.

Ein weiterer Schwerpunkt dieser Ausgabe ist die Fortsetzung der Vorstellung unserer GIT SICHERHEIT AWARD-Finalisten (ab Seite 6). Nach der ersten Runde in der Juni-Ausgabe lernen Sie nun weitere innovative Lösungen und Produkte kennen, die die Branche mit frischen Ideen und praxisnahen Ansätzen voranbringen.

Wer den Markt im Blick behalten will, kommt außerdem an unseren PRO-4-PRO-Übersichten nicht vorbei: Wir stellen die Top-Player der Branche vor – ergänzt durch gekürzte Interviews aus unserem Video-Podcast „SicherMacher“ (ab Seite 28 und Seite 66).

Auch der Blick über den Tellerrand lohnt sich: Europas Rolle im globalen Technologiewettbewerb wird im Beitrag „Europas Moment der Quantensouveränität“ (ab Seite 58) analysiert. Die Frage, wie technologische Unabhängigkeit in Zukunft gesichert



werden kann, ist dabei nicht nur politisch, sondern auch wirtschaftlich von zentraler Bedeutung.

Mit dem zweiten Teil unserer Reihe „Time-Sensitive Networking – TSN in der Anwendung“ setzen wir zudem einen klaren Fokus auf industrielle Kommunikation. Gemeinsam mit dem VDMA Elektrische Automation zeigen wir im Beitrag „OPC UA und TSN – vernetzte Produktion mit deterministischer Kommunikation“, wie sich Echtzeitfähigkeit und Vernetzung in der Praxis erfolgreich verbinden lassen. **GIT**

Herzlichst,
Ihr

Dr. Timo Gimbel
für das Team GIT SICHERHEIT

Erratum

Trotz größter Sorgfalt lassen sich Fehler nicht immer vermeiden. Daher möchten wir an dieser Stelle eine Korrektur zur GIT SICHERHEIT 6/2026 vornehmen:

Im Titelhinweis zur Titelgeschichte über Denios und die „Vision Zero“ haben sich zwei Fehler eingeschlichen. Gesprächspartner war Tobias Dankert von ARU. Zudem lautet die korrekte Schreibweise „Gefahrstoffmanagement“.

Wir bedauern diese Versehen und die daraus entstandenen Missverständnisse sehr und bitten unsere betroffenen Kunden sowie unsere Leserinnen und Leser um Entschuldigung.



Speedgate SG Expression

Moving by Design





TITELTHEMA

Gelebte Resilienz

Krisen- und
Notfallmanagement bei
Roche in Penzberg

ab Seite 20



SicherMacher
Der GIT-Talk mit den Marktführern



Sehen Sie unsere
Interviews im
Video-Podcast

Bequem auf dem Sofa
durch die e-Ausgabe der
GIT SICHHERHEIT blättern:
Registrieren Sie sich hier



24 Markus Vollerthun



28 Dr. Jens Hartmann



34 Christian Linthaler



40 Alexander Biederer

3 Editorial

Dr. Timo Gimbel

GIT SICHHERHEIT AWARD

8 JETZT ABSTIMMEN

www.sicherheit-award.de

MANAGEMENT

PERIMETER, CLOUD UND KI

12 Neue Praxisfragen für Video und Zutritt

BHE-Fachkongress 2026 in Mainz:
Erkenntnisse aus Praxis, Recht und Technik

MESSEN

17 Sichere Kommunikation

Die PMRExpo 2026 lädt vom 24. bis zum
26. November 2026 nach Köln

SICHERHEITSTECHNIK

18 Technik am See

Ein Sommerfest mit Wissenstransfer
und Networking

TITELTHEMA

20 Gelebte Resilienz

Krisen- und Notfallmanagement
bei Roche in Penzberg

KÜNSTLICHE INTELLIGENZ

24 KI-gestütztes Recruiting im Sicherheitsgewerbe

Einblicke von der BVS SecTec 2026

KOMPLETTLÖSUNG

26 Sensible Prozesse

Präzision braucht zuverlässigen Schutz

SECURITY

INNENTITEL

48 Von Kellertür bis Haupteingang

Wie man die (Zutritts-) Kontrolle
zurückgewinnt

ZUTRITT

50 Automatisch verriegelt

Intuitive Sicherheit für Gebäudezugänge

SCHNELLAUFTORE

52 Hinein ins Waschparadies!

Schnellauftore für Autowaschanlage
in Füßen

SCHLIESSSYSTEME

54 Ständig in Bewegung

Schließtechnik bei der Messe Berlin

ZUTRITT

56 Kirchgang digital

Elektronisches Schließsystem für
katholisches Pfarrzentrum in Velbert

TOP PLAYER

28 TOP-PLAYER aus der Branche

Dr. Jens Hartmann, Advancis
Thore Peters, AG Neovo
Mathias Schmid, Assa Abloy
Rudolf Rohr, Barox
Thorsten Wallerius, Hikvision
Christian Linthaler, Dallmeier
Falk Herrmann, Funkwerk Security Solutions
Christian Sohn, Funkwerk Security Solutions
Heiko Viehweger, Hirsch Secure
Alexander Biederer, ID-ware
Aleksij Tokarev, Security Robotics
Sven Horstmann, Klüh Security
Axel Schmidt, Salto Systems



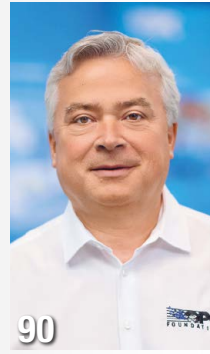
Alexandra Kovacs



Achim Löffler



Herbert Köbel



Peter Lutz

CYBER-SECURITY

QUANTENCOMPUTING

58 Europas Moment der Quantensouveränität

Von wissenschaftlicher Exzellenz zu strategischer Infrastruktur

IDENTITÄTSMANAGEMENT

61 Vertrauen dank Zero Trust

Mit integriertem Identitätsmanagement werden SuperApps sicher

BRANDSCHUTZ

FEUERWEHRBEKLEIDUNG

62 Flammenschutz im freien Gelände

PSA: Sicheres und bequemes Outfit für steigende Anforderungen an Einsatzkräfte

KI-VIDEO-LÖSUNGEN

63 Millionenschäden vorbeugen

Videotechnik und KI heben Brandschutz auf ein neues Level

SPRINKLERANLAGEN

64 Brandschutz, der mitdenkt

Smarte Sprinklerlösungen, die schneller reagieren, gezielter löschen und Werte effektiv schützen

TOP PLAYER

66 TOP-PLAYER aus der Branche

Günther Rossdeutscher, Asecos
Horst Rose, Denios
André Hartmann, Bihl+Wiedemann GmbH
Achim Giesselmann, Gloria
Alexandra Kovacs, Hoffmann Group
Tobias Zöllkau, Hoffmann Group
Simon Schurr, Telenot
Henning Grözin, Leuze-Gruppe
Tobias Vähjunker, Kirotec

SAFETY

INNENTITEL

78 Sicher lagern und laden

Welche Anforderungen Sicherheitsschränke für Lithium-Akkus erfüllen sollten

MATERIALIEN

82 Materialien für Jahrzehnte

Vor einem halben Jahrhundert wurde Gore-Tex Fabrics gegründet

SICHERHEITSSCHUHE

86 Sicherheit trifft Sneaker-Style

Jalas Flex verbindet S3S-Schutz mit leichter Bauweise und sportlichem Design

87 Sicherer Schritt trotz schmalem Fuß

ESD-Einlegesohlen verbessern Passform und Halt in Sicherheitsschuhen für schmale Füße

SCHNITTSCHUTZ

88 Eingebaute Notbremse

Sollbruchstellen in Schnittschutzhandschuhen reduzieren Einzugsrisiken bei rotierenden Maschinenteilen

MASCHINEN- UND ANLAGENSICHERHEIT

90 Time-Sensitive Networking – TSN in der Anwendung

OPC UA und TSN – vernetzte Produktion mit deterministischer Kommunikation

94 Vom blinden Fleck zur Datenquelle

Infrastrukturdiagnose mit Ethernet-APL

98 Cybersecurity wird Teil der Maschinenzulassung

CRA und Maschinenverordnung machen Cybersecurity zur Pflicht im gesamten Produktlebenszyklus.

INDEX

QUICK-FINDER

ORGANISATIONEN, INSTITUTIONEN
UND UNTERNEHMEN IM HEFT

A bus	29
Advancis	28
AFAG	7
AG Neovo	30
Asecos	66, 77
Assa Abloy Entrance Systems	3
Assa Abloy	31, 43, 54
Atlas Schuhfabrik	U4
Aug. Winkhaus	50
Automatic Systems	43
Axis	46
B aak	87
Barox	25, 32
BHE e.V.	12, 39, 57
Bihl & Wiedemann	68
BVSW e.V.	6, 24, 97
C hubb	46
D allmeier	34, 41
Denios	U2, 67, 76
Dom Sicherheitstechnik	11
E jendals	86
Elaflex Hiby	52
F unkwerk	36
G eorg Schlegel	95, 97, 98
Gloria	69
GU BKS	6, 35
H B Protective Wear	62
Hekatron	75
HID	29
Hikvision	33
Hilscher	96
Hirsch Secure	38
HWR Berlin	6
Hoffmann Group	70
I D-ware	40, 53
Interflex	47
K. A. Schmersal	93
KGS	11
Klüh	7, 44
Kobil	61
Koelnmesse	17
Kötter	7, 63
L euze	73
Lünendonk	19
M ersen	9
Mewa	85
Moxa	9
N ürnbergMesse	41
P epperl+Fuchs	94
Priorit	74
R oche Diagnostics	20
Rohde & Schwarz	7
S alto Systems	45, 46
Satel	11
Schöffel Pro	76
Schraner Group	65
Security Robotics	42
SuperQ	58
T elenot	26, 72
U vex	88
V DMA e.V.	90, 97
Vinci Energies	64
VSW e.V.	19
W. L. Gore	82
Wagner Group	75
Wilka	56
X ortec	18
Z VEI e.V.	6, 19

NEWS

ZVEI: Daniel Hager übernimmt Verbandsspitze

Der ZVEI bekommt eine neue Verbandsspitze: Daniel Hager ist vom Vorstand für drei Jahre zum ZVEI-Präsidenten gewählt worden. „Die Digital- und Elektroindustrie ist eine der tragenden wirtschaftlichen Säulen unseres Landes“, betonte Daniel Hager unmittelbar nach seiner Wahl. In seiner Eröffnungsrede zum eSummit erklärte er, die hohe Bedeutung dieser Branche für technologischen Fortschritt und gesellschaftlichen Wohlstand in Deutschland im politischen Dialog noch stärker verankern zu wollen.



**ZVEI-Präsident
Daniel Hager**

Als Vizepräsidenten neu gewählt worden sind: Dr. Peter Körte (Siemens), Dr. Frank Meyer (Bosch), Dr. Peter Weckesser (Schneider Electric). Dem engeren Vorstand gehören an: Dr. Markus Bergholz (Kostal), Christian O. Erbe (Erbe Elektromedizin), Philip W. Harting (Harting), Tim Holt (Siemens Energy), Ulrich Leidecker (Phoenix Contact), Philipp Steinberger (Wöhner), Andreas Urschitz (Infineon).

www.zvei.org



Joachim Herrmann, Bayerischer Staatsminister des Innern, und BVSW Geschäftsführerin Caroline Eder auf der SicherheitsExpo

SicherheitsExpo: Gemeinsamer Messeauftritt von BVSW und BDSW

Der Bayerische Verband für Sicherheit in der Wirtschaft (BVSW) und der Bundesverband der Sicherheitswirtschaft (BDSW) präsentierten sich gemeinsam auf der SicherheitsExpo im MOC München. Auf ihrem Messestand empfingen die Verbände Fachbesucher, standen für Gespräche zur Verfügung und boten einen Ort für geschäftliche Meetings. Ein Hauptanliegen beider Verbände ist es, Unternehmen und Behörden auf die sicherheitsrelevanten Herausforderungen unserer Zeit aufmerksam zu machen. Neben klassischen Bedrohungsszenarien rücken dabei zunehmend hybride Bedrohungslagen und der Schutz kritischer Infrastrukturen in den Vordergrund. BVSW und BDSW begleiten ihre Mitglieder durch Schulungsangebote, Informationen über neue Technologien sowie den direkten Dialog auf zahlreichen Fachveranstaltungen. Qualifikation und Weiterbildung für die Sicherheitsbranche bilden einen weiteren Schwerpunkt des BVSW.

www.bvsw.de

Marcel Philipp übernimmt Leitung Projekt bei der GU BKS Service GmbH

Die GU BKS Service GmbH freut sich, Marcel Philipp als neuen Leiter Projekt im Unternehmen begrüßen zu dürfen. Marcel Philipp hat mehr als zehn Jahre Erfahrung in der Sicherheits- und Gebäudetechnik. In dieser Zeit hat er sich vom Servicetechniker über die Inbetriebnahme komplexer Sicherheitssysteme bis hin zur Leitung anspruchsvoller Projekte und Standorte entwickelt. Sein fachlicher Schwerpunkt liegt insbesondere auf sicherheitskritischen Anwendungen sowie Projekten im Umfeld kritischer Infrastrukturen (KRITIS) und regulatorischer Anforderungen wie NIS2. Zuletzt verantwortete er im Bereich AES/NSL den Betrieb sicherheitsrelevanter Leitstellenstrukturen sowie die technische Abteilung eines Standorts. In seiner neuen Funktion als Leiter Projekt bei der GU BKS Service GmbH ist Marcel Philipp für die strategische und operative Steuerung des Projektgeschäfts verantwortlich.



**Marcel Philipp,
Leiter Projekte GU
BKS Service GmbH**

www.g-u.com

3. SiMa-Praxistag „Security meets students“ an der HWR Berlin

Beim SiMa-Praxistag an der Hochschule für Wirtschaft und Recht (HWR) Berlin tauschten sich rund 150 Studenten, Alumni sowie Vertreter aus Unternehmen und Behörden zur Sicherheitswirtschaft aus. Der 3. SiMa-Praxistag fand unter dem Motto „Security meets students“ am Fachbereich Polizei und Sicherheitsmanagement der HWR Berlin statt. Prof. Dr. Harald Olschok, Honorarprofessor und Initiator des Praxisformats, begrüßte die Anwesenden und moderierte durch die Veranstaltung. Er erinnerte an das 20-jährige Jubiläum des Bachelorstudiengangs Sicherheitsmanagement und hob hervor, dass seit 2006 fast 1000 Studenten erfolgreich auf ihrem Weg in die Branche begleitet wurden. Prof. Dr. Olschok unterstrich die aktuellen sicherheitspolitischen Herausforderungen, insbesondere im Bereich der kritischen Infrastruktur und verwies auf die Bedeutung neuer gesetzlicher Grundlagen wie das KRITIS-Dachgesetz.



www.hwr-berlin.de



Für professionelle Sicherheitsdienstleistungen sind die Erfahrung und das Engagement des Teams entscheidend

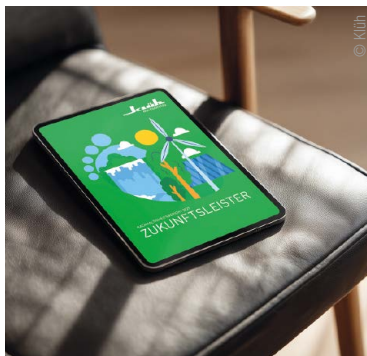
Zwei Standorte von Kötter Security feiern 65. Jubiläum

Zwei Standorte der Kötter Security Gruppe haben Grund zu feiern: Die Niederlassung in Stuttgart beging ihr 65. Jubiläum am 1. Mai, die Niederlassung in Frankfurt feierte am 12. Juni. Während in den 1960er-Jahren Stuttgart seine Rolle als industrielles Herz Süddeutschlands weiter festigte und Frankfurt seinen Weg zum internationalen Finanzzentrum beschritt, sah die Arbeit in der Sicherheitsdienstleistung noch ganz anders aus als heute: Streifengänge, Werkstore und analoge Dokumentation prägten den Alltag. 65 Jahre später ist sie technikgestützt, vernetzt und ohne Cybersecurity undenkbar. Als die Standorte 1961 gegründet wurden, befand sich Deutschland im Aufbruch: Wirtschaftswachstum und Industrialisierung sorgten für steigenden Bedarf an Schutz und Sicherheit. In Stuttgart standen vor allem große Werksgelände im Fokus, während in Frankfurt Banken, Unternehmen und Infrastruktur zunehmend abgesichert werden mussten.

www.koetter.de

Klüh setzt nachhaltige Entwicklung mit digitaler Kompetenz fort

Die Klüh-Gruppe hat im Geschäftsjahr 2025 mit einem Umsatz von 1,108 Mrd. Euro ihr Wachstum fortgesetzt und damit ein Plus von 3,6 % gegenüber dem Vorjahr erzielt. Das Ergebnis spiegelt die stabile Entwicklung der Geschäftsbereiche im In- und Ausland in einem anspruchsvollen Marktumfeld wider. Mit Blick auf die Umsatzverteilung zeigten sich erneut die Dienstleistungsbereiche Cleaning (35,0 %), Security (21,3 %), Catering (18,0 %) und Clinic Service (16,3 %) als tragende Säulen, gefolgt von Personal Service (6,1 %) sowie integrierten Serviceleistungen (3,3 %). Das Auslandsgeschäft trug mit einem Umsatz von 340,7 Mio. Euro einen stabilen Anteil von 30,7 % zum Gesamtumsatz bei. „Unser Anspruch ist es, Dienstleistungen konsequent weiterzuentwickeln und dabei Digitalisierung, Nachhaltigkeit und Servicequalität miteinander zu verbinden“, so Frank Theobald, CEO der Klüh-Unternehmensgruppe.



www.klueh.de

SicherheitsExpo Alpe Adria

Am 14. und 15. Oktober 2026 feiert die SicherheitsExpo Alpe Adria in der Messe Klagenfurt ihre Premiere. Mit diesem Schritt bringt die SicherheitsExpo ihr bewährtes Konzept nach Österreich und eröffnet in der Alpen-Adria-Region eine exklusive Plattform für die Präsentation innovativer Sicherheitslösungen, den fachlichen Austausch und den Aufbau wertvoller Branchenkontakte. Die SicherheitsExpo, die sich seit über 20 Jahren in München als führende Fachmesse für Sicherheitstechnik in Süddeutschland etabliert hat, wird im Oktober 2026 ihr bewährtes Messekonzept erstmals auch in Klagenfurt präsentieren. Fachlicher Partner der neuen SicherheitsExpo ist der VSÖ – Verband der Sicherheitsunternehmen Österreichs. Er gestaltet das Fachforum auf der Messe inhaltlich und stellt sicher, dass österreichische Branchenforderungen optimal berücksichtigt werden. Dabei stehen sowohl fachliche Tiefe als auch der wirtschaftliche Nutzen von Investitionen gleichermaßen im Fokus. www.afag.de



Die Sicherheitsscanner von Rohde & Schwarz sind nun auch im Einsatz am neuen Terminal 3 des Frankfurter Flughafens

Rohde & Schwarz liefert Sicherheitsscanner für das neue Terminal 3

Der Flughafen Frankfurt hat das hochmoderne Terminal 3 eröffnet, das mit drei Flugsteigen jährlich bis zu 19 Millionen Passagiere abfertigen soll. Im Zuge der Inbetriebnahme werden auch neue Sicherheitskontrollspuren mit Millimeterwellenscannern von Rohde & Schwarz ausgestattet. Die Entscheidung für die Modelle QPS201 und QPS Walk2000 verspricht nicht nur eine spürbare Beschleunigung des Passagierflusses, sondern auch höchste Sicherheit und Komfort. Der neue Großflughafen-Abschnitt stellt eine der modernsten Infrastrukturen Europas dar. Neben einer klaren Wegeführung, digitalen Services und optimierten öffentlichen Anbindungen legt der Betreiber Fraport den Schwerpunkt auf die Effizienz der Sicherheitskontrollen. Dazu wurde Rohde & Schwarz beauftragt, 17 seiner QPS201 Sicherheitsscanner und zwei QPS Walk2000 in den Kontrollspuren einzusetzen.

www.rohde-schwarz.com

JETZT ABSTIMMEN

www.sicherheit-award.de

dort auch ausführliche Infos zu den Produkten

Auf geht's in die nächste Runde – und zwar gleich in doppelter Hinsicht. Wie in unserer letzten Ausgabe der GIT SICHERHEIT geht es auch diesmal wieder um innovative Produkte und Lösungen, die das nächste Jahr sicherheitstechnisch prägen werden. Wir haben Einreichungen und Anmeldungen von Anbietern bewertet: Wie innovativ ist eine Lösung, wie bedeutend kann sie für welchen Markt und welche Zielgruppe sein? Finden Sie auf den folgenden Seiten die neuen Kategorien und die Shortlist für den GIT SICHERHEIT AWARD.

Wer sind Ihre Favoriten?

Treffen Sie jetzt online je eine Auswahl in jeder Kategorie:

- A – Maschinen- & Anlagensicherheit
- B – Arbeitsschutz & Ex-Schutz
- C – Video-Sicherheit & Video-Management
- D – Zutritt & Einbruchschutz
- E – Sicherheitsmanagement, Gebäudesicherheit & Perimeterschutz
- F – Brandschutz

Um für eine faire Abstimmung zu sorgen, ist es nicht gestattet, für das eigene Unternehmen zu stimmen. Daher sehen die Regeln vor, dass ausschließlich online und unter Angabe eines Firmennamens gevotet werden kann. Privatpersonen sind nicht stimmberechtigt. Weitere Informationen (siehe auch QR-Code rechts) auf www.sicherheit-award.de

Leserpreis gewinnen

Unter allen gültigen Stimmabgebenden verlosen wir drei hochwertige Ledlenser Taschenlampen P7R Work UV.



**Leser
Preis**

**GIT
SICHERHEIT
AWARD
FINALISTEN**



Kategorie A: Maschinen- & Anlagensicherheit

Bihl+Wiedemann	ASI-5 Safety Leiterplattenmodul
E. Dold & Söhne	Innovatives Funk-Sicherheitssystem RE 6900
Euchner	Transpondercodiertes Schlüsselsystem CKS2
K. A. Schmersal	SFB Port Extender für flexible Sicherheitsarchitekturen
Mersen	ProGrid Solutions – Sicherungslasttrennschalter für die Energiewende
Moxa Europe	NPort 6000-G2 Serie – Sichere Serial Device Server
Murr	MVK Fusion CIP Safety – 3-in-1 Hybrid-Feldbusmodul
Phoenix Contact	Multifunktionales Sicherheitsrelais PSR-UNI
Sick AG	Sicherheitssteuerung Flexi Net – für stationäre und mobile Maschinen

Shortlist Highlights**Kategorie A: Maschinen- & Anlagensicherheit****Mersen: ProGrid Solutions – Sicherungslasttrennschalter für die Energiewende**

Der Sicherungslasttrennschalter ProGrid von Mersen ist eine robuste Schalt- und Schutzlösung für Energie-, Industrie- und Infrastrukturanwendungen. Er ermöglicht das sichere Schalten und Trennen von Stromkreisen und schützt zuverlässig vor Überlast und Kurzschluss. Ein patentierter Mechanismus gibt die NH-Sicherungsmesser parallel von beiden Seiten frei und sorgt für eine effektive Lichtbogenunterbrechung bei gleichzeitiger Einhaltung von IP20-Kontaktschutz. Eine anschließende Drehbewegung erleichtert den Sicherungswechsel und erhöht die Betriebssicherheit bei reduziertem Platzbedarf. Das modulare System reicht von Standard- bis zu Smart-Varianten mit integrierter Sensorik zur Messung von Energieflüssen sowie zur Überwachung von Transformatorzustand, Umgebung und Schaltschrankzugang. ProGrid lässt sich jederzeit ohne bauliche Änderungen nachrüsten. Kompaktes Design und Echtzeitüberwachung unterstützen effizientes Energiemanagement und erhöhen die Anlagenverfügbarkeit.

**Mehr Infos****Kategorie A: Maschinen- & Anlagensicherheit****Moxa Europe: NPort 6000-G2 Serie – Sichere Serial Device Serve**

Die Moxa NPort 6000 G2 Serie ermöglicht die sichere Einbindung serieller Geräte wie SPS, Zähler oder Controller in moderne Ethernet-basierte OT-Netzwerke. Sie verbindet RS 232/422/485 Schnittstellen mit IP-Infrastrukturen und reduziert Risiken durch ungeschützte Kommunikation und fehlende Transparenz. Als erster Serial Device Server mit IEC 62443 4 2 Security Level 2 Zertifizierung bietet sie ein hohes Sicherheitsniveau. Funktionen wie zentrale Authentifizierung, Remote Syslog und webbasiertes Traffic Monitoring unterstützen Security-Policies und erleichtern die Diagnose. Durch Retrofit statt Austausch können bestehende Anlagen weiter genutzt werden. Die Lösung stärkt damit Defense in Depth direkt auf Feldebene und erhöht Sicherheit sowie Verfügbarkeit industrieller Anwendungen.

**Mehr Infos**

© Moxa Inc.



Jetzt abstimmen
vom 1. Juni bis
1. September 2026 auf
www.sicherheit-award.de

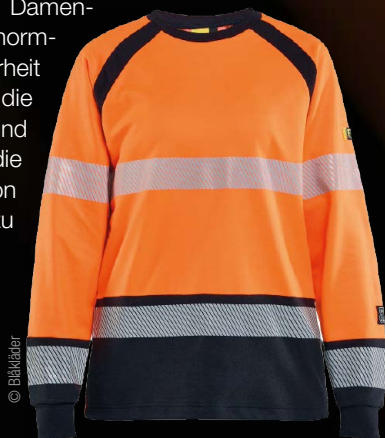


Kategorie B: Arbeitsschutz & Ex-Schutz

Ansell Healthcare	Acetonbeständige Handschuhe TouchNTuff 93-800
Atlas Schuhfabrik	Max Series – Sicherheitsschuhe für extreme Einsatzbedingungen
Blåkläder	Multinorm-Langarmshirts 3436/3437
Denios	Real-time Asset Monitoring für Sicherheitsschranke
Dupont	Chemikalienschutz mit Fokus auf Tragekomfort
Ejendals	Schutzhandschuh Tegera Uniform 9078
Fristads	Multinorm Green – Schutzkleidung mit transparenter Umweltbilanz
HB Protective Wear	Softshelljacke HB-ArcFlash Pro 4kA und 7kA
Krause-Werk	Stabilo Stufen-Stehleiter 135 XL
Munk Group	Modulare Montageplattform

Shortlist Highlights**Kategorie B: Arbeitsschutz & Ex-Schutz****Blåkläder: Multinorm-Langarmshirts 3436/3437**

Mit den Multinorm-Langarmshirts 3436 (Herren) und 3437 (Damen) adressiert Blåkläder die zentrale Herausforderung mangelnder Trägerakzeptanz bei Schutzkleidung. Die Shirts bestehen aus leichtem Piqué-Strick und bieten einen an Freizeitbekleidung orientierten Tragekomfort bei gleichzeitig umfassendem Schutz für anspruchsvolle Einsatzbereiche. – Die Materialien sind inhärent flammhemmend und antistatisch, wodurch die Schutzwirkung dauerhaft erhalten bleibt. Zertifizierungen nach EN ISO 11612, EN 61482-2, EN 1149-5 sowie EN ISO 20471 gewährleisten den Einsatz bei thermischen Gefahren, Lichtbogenrisiken und Sichtbarkeitsanforderungen. Ein speziell entwickelter Damen-Schnitt stellt im Multinorm-Segment eine Besonderheit dar. Insgesamt verbindet die Lösung Schutz, Komfort und Passform mit dem Ziel, die konsequente Nutzung von PSA im Arbeitsalltag zu erhöhen.

**Mehr Infos**

© Blåkläder

Kategorie C: Video-Sicherheit & Video-Management

Ajax Systems	Serie Superior NVR H2D – KI-gesteuerte Netzwerkvideorekorder
Axis Communications	Q6411-LE Bispectral PTZ Camera
Dallmeier Electronic	Multifocal-Sensorkamera Panomera V8
Hanwha Vision	PTZ-Kameras für raue Umgebungen
LiveEye	Digitales Planungstool für temporäre Sicherheitskonzepte
Security Robotics	Sicherheitsplattform ACUDA
Spectro AI	Spectro AI: DockWatch Trailer

Kategorie D: Zutritt & Einbruchschutz

Ajax Systems	Superior MotionCam G3 (PhOD) Jeweller – Kabelloser PIR-Bewegungsmelder
ASL-Ademco	Klinkenwächter ABAX
Aug. Winkhaus	Elektronisches Schließsystem BlueEvo
DOM Sicherheitstechnik	Online Mesh zur Vernetzung digitaler Schlösser
Dormakaba	Automatische Schiebetür ST PRO Green RC3
Hirsch	Zutrittssystem Microsesame
Ksenia	Conexa ist die IP-Touchscreen-Tastatur
MP-Bos	Digitaler Ausweis BOS-ID
Portier Global	Schließenanlagen-Software Portier Vision 5
Satel	Be Wave Hybrid – Sicherheits- und Gebäudeautomationssystem
Schmeissner	Kapazitive Durchbruchsicherung
Telenot Electronic	hiline1 – Übertragungseinrichtung
Tell Software	Nachrüstmodul OPEN.ioting Smart Gate Opener

Kategorie F: Brandschutz

Ajax Systems	EN54 Fire Hub Jeweller – Funk-Brandwarnzentrale
Axis	D6310 Air Quality Sensor für sicherheitsrelevante Innenbereiche
Dehn	Geprüfte E30-Lösung für Überspannungsschutz im Brandfall
Gekartel	VdS 6024-zertifiziertes Brandschutztablet
Hanwha Vision Europe	Bi-Spektrum-Kameras für Brandfrüherkennung
Inotec	Sicherheitsleitsystem GMS zur Evakuierung
Johnson Controls	SafeLinc-Cloud-Weboberfläche und mobile App
Securiton	SecuriGas – Ansaugrauchmelder-System mit hochsensibler Gassensorik
Munk Group	Modulare Montageplattform

Kategorie D: Zutritt & Einbruchschutz

DOM Sicherheitstechnik: Online Mesh zur Vernetzung digitaler Schlösser

Dom Online Mesh von Dom Sicherheitstechnik ist der Ethernet-Einstiegspunkt für ein skalierbares Thread-Mesh-Netzwerk in Zutrittslösungen. Es verbindet vorhandene Zutritts-IT mit einem Funknetzwerk und ermöglicht die Kommunikation zu digitalen Schließkomponenten über Bluetooth LE. Ein Gateway bindet mehrere Online-Repeater an, die die Reichweite bis zur Tür erweitern. Funktionen wie Fernsteuerung, Live-Ereignisse und Echtzeit-Batteriestatus sind so auch in komplexen Gebäuden bei geringem Verkabelungsaufwand verfügbar. Pro Repeater lassen sich bis zu 16 Komponenten integrieren, insgesamt bis zu 512 Geräte über einen IP-Anschluss. Das selbstheilende Mesh sorgt für hohe Verfügbarkeit, da Geräte bei Ausfällen alternative Funkwege nutzen. Monitoring und kontrollierte Geräteaufnahme erhöhen Transparenz und reduzieren Serviceaufwand. Geeignet für Bestandsgebäude, Kliniken, Schulen und Campus.



**Mehr
Infos**

Kategorie E: Sicherheitsmanagement

Advancis	AIM – Advanced Identity Management
Ajax Systems	Superior Hub G3 Jeweller – Kabellose Hub-Zentrale mit Fotoverifizierung
Ambient System	ICO Emergency – Notrufsprechstelle für kritische Situationen
Axis	D2122-VE Radar und Axis D2123-VE Radar
Chubb	Connected Services – Vernetzte Sicherheitsdienstleistung
Hirsch	Lumor Faseroptik-Intrusionsdetektion
Hiscout	GSS – Geheim- und Sabotageschutzmodul der HiScout GRC Suite
ID-ware	Softwarebasierte Management-Plattform PIAM-Suite
IVMS	Lynx – Gefahrenmanagement-System
KGS Fire & Security	Fusion – Sicherheitsplattform
Octave	Coda Spatial – 3D-Sicherheits- und Perimeter-Überwachung
Quanergy Solutions	Q-Shield – LiDAR-Sensor für Intrusion Detection
Security Robotics	Autonome mobile Sicherheitsroboter (AMSR)

Kategorie D: Zutritt & Einbruchschutz

SATEL: Be Wave Hybrid – Sicherheits- und Gebäudeautomationssystem

Be Wave vereint Einbruchschutz nach Grade 2, Gebäudeautomation und visuelle Alarmverifizierung in einer integrierten Plattform. Das System unterstützt drahtlose, hybride und kabelgebundene Installationen und arbeitet ohne Cloud-Abhängigkeit, sodass Daten lokal beim Betreiber bleiben. Die Satel-Funktechnologie ABAX 2 ermöglicht Reichweiten bis 2.000 m, lange Batterielaufzeiten und sichere Kommunikation per AES 128. Vier Funkkanäle im 868 MHz-Band sorgen für stabile Verbindungen auch bei Störungen. Je nach Zentrale sind GSM, LAN und WLAN integriert. Funktionen wie Fernsteuerung, Push-Benachrichtigungen und visuelle Alarmverifizierung per Livebild oder Snapshot stehen in der App bereit. Die Bedienung bleibt auch ohne Internet lokal möglich. Erweiterbare Automationsfunktionen und flexible Skalierung machen Be Wave zu einer Lösung für vernetzte Sicherheits- und Smart-Building-Anwendungen.



**Mehr
Infos**

Kategorie E: Sicherheitsmanagement, Gebäudesicherheit & Perimeterschutz

KGS Fire & Security: Fusion – Sicherheitsplattform

Fusion von Aritech ist eine integrierte Sicherheitsplattform für Einbruch, Zutritt und Video, die lokale Installationen mit Cloud-Funktionen verbindet. Die modulare Architektur ermöglicht den Einsatz vom Einzelstandort bis zu internationalen Infrastrukturen und unterstützt eine schrittweise Erweiterung ohne Systemwechsel. Zentrale Verwaltung, Remote-Konfiguration und eine durchgängige Plattformlogik erhöhen Transparenz und Effizienz in Betrieb und Wartung. Serviceunternehmen profitieren von Fernzugriff und Diagnose, während Anwender konsistente Sicherheits- und Betriebsdaten erhalten. Durch die Integration mehrerer Gewerke reduziert Fusion die Systemkomplexität, verkürzt Reaktionszeiten und unterstützt ein proaktives Sicherheitsmanagement. Skalierbarkeit und modulare Erweiterung bieten Investitionsschutz und Flexibilität für wachsende Anforderungen.

**Mehr
Infos**

Fusion
Unified Intelligence

- Seamless integration
- Multi-site incident management
- Cloud-based & on-premise

Neue Praxisfragen für Video und Zutritt

BHE-Fachkongress 2026 in Mainz: Erkenntnisse aus Praxis, Recht und Technik

Unser Bericht vom BHE-Fachkongress 2026 in Mainz: Mit KI in der Videosicherheit, Cloud-Modelle, CRA/NIS2, Videoaufschaltung auf Leitstellen, Perimeterschutz, Biometrie und Besuchermanagement.

■ Beim BHE-Fachkongress „Videosicherheit/Zutrittssteuerung“ am 21. und 22. April 2026 im Atrium Hotel Mainz rückten zwei Fragen in den Mittelpunkt: Wie lässt sich physische Sicherheit in Zeiten von KI, Cloud und wachsender regulatorischer Dichte belastbar planen – und wie funktioniert das Zusammenspiel von Perimeter, Video, Zutritt und Leitstelle im Betrieb wirklich? Das Programm verband Praxisberichte, technische Entwicklungen und juristische Einordnung – von rechtskonformer Videoüberwachung über den Cyber Resilience Act bis zu Biometrie-Anwendungen und der Organisation von Videoaufschaltungen.

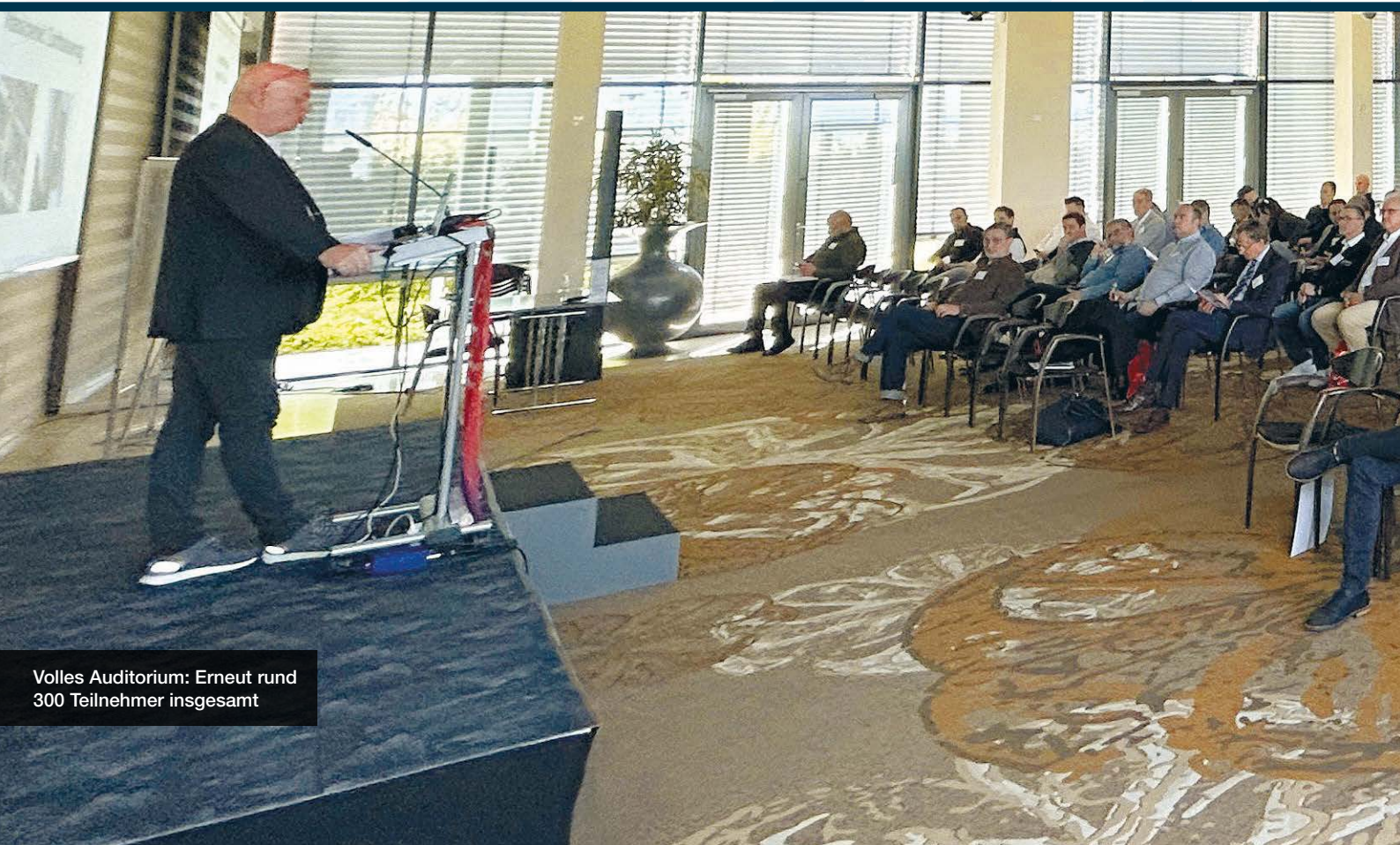
Der Kongress war dabei in zwei Stränge gegliedert: Block A mit Schwerpunkt Videosicherheit und Perimeter, Block B mit Schwerpunkt Zutrittssteuerung. In beiden Tracks zeigte sich ein gemeinsamer Nenner: Technik allein entscheidet selten, ob Sicherheitskonzepte wirken – entscheidend sind Datenqualität, Zuständigkeiten, Schnittstellen, rechtliche Grundlagen und ein Betrieb, der Fehlalarme und „Eventlast“ beherrscht.

Um thematische Linien klarer sichtbar zu machen und Querverbindungen zwischen Technik, Betrieb und Regulierung herauszuarbeiten, folgt unser Beitrag in der Folge einer inhaltlichen Dramaturgie und nicht

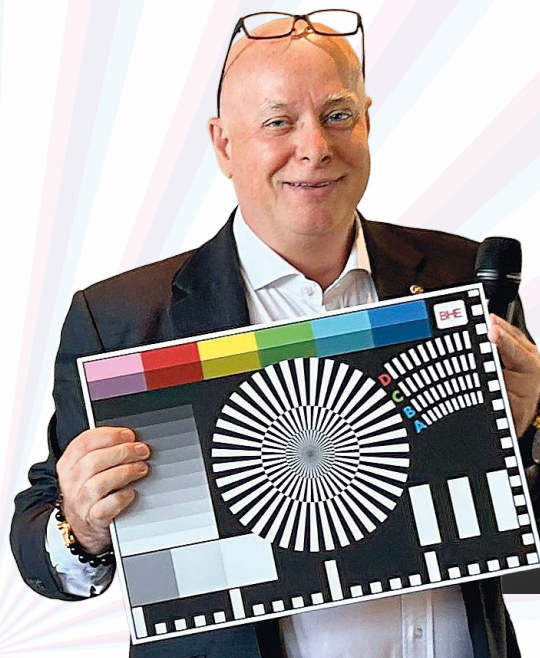
strikt der zeitlichen Abfolge der Vorträge an den beiden Kongresstagen.

Rechtsrahmen und Realität: Videosicherheit zwischen DSGVO, KI und Cloud

So machte in seinem Vortrag zu Beginn des zweiten Tages mit Dennis Haerberlein von EnBW der Verantwortliche eines Betreibers ein Praxisdilemma sichtbar: Private Betreiber dürfen den öffentlichen Raum nicht „ohne weiteres“ überwachen. Videoüberwachung endet in der Regel an der Grundstücksgrenze. Damit wird eine Vorfelderkennung außerhalb des Hausrechts-



Volles Auditorium: Erneut rund 300 Teilnehmer insgesamt



Von MDORII zu OODPCVS:
Michael Meissner
mit dem neuen
Testbild für Video-
sicherheit

Technischer Fortschritt
versus Datenschutz:
Dr. Ulrich Dieckert über neue
rechtliche Herausforderungen



bereichs schnell zur rechtlichen und organisatorischen Herausforderung – obwohl der Bedarf je nach Lage existiert.

In seinem Solarpark-Beispiel setzte Dennis Haebler auf einen Ansatz mit vollständiger Anonymisierung („keine Wiederherstellung möglich“) und Abstimmung mit dem Landesdatenschutz. Der Vortrag blieb bewusst nüchtern: In der Praxis traten Einschränkungen auf – etwa die fehlende Möglichkeit, Personen oder Kennzeichen nachträglich im Klarbild zu prüfen, sowie Grenzen bei der Leitstellen-Auflösung von Situationen. Das Pilotprojekt wurde am Ende nicht weiterverfolgt, weil die Nachteile die Vorteile überwogen.

Den juristischen Unterbau genau dazu lieferte Dr. Ulrich Dieckert bereits tags zuvor. Er ordnete KI-basierte Videoauswertung zunächst datenschutzrechtlich ein: Für private/gewerbliche Anwendungen wird regelmäßig Art. 6 Abs. 1 lit. f DSGVO („berechtigtes Interesse“) relevant, während biometrische Daten nach Art. 9 DSGVO grundsätzlich einem Verarbeitungsverbot unterliegen – mit wenigen, eng auszulegenden Ausnahmen. Besonders wichtig: Eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO ist bei KI-gestützter Videoüberwachung häufig erforderlich – verantwortlich indes bleibt der Betreiber.

Konkrete Fallbeispiele schärften den Blick für rote Linien: „Professional People Counting“, das über KI biometrische Merkmale vieler Personen verarbeitet, wurde als datenschutzwidrig eingeordnet, wenn keine tragfähige Rechtsgrundlage vorliegt. Auch bei präventiven Verhaltensanalysen gilt: Sobald biometrische Merkmale ausgewertet werden, kippt die Zulässigkeit schnell. Zudem erinnerte Dr. Ulrich Dieckert an Fälle, in denen Behörden hohe Bußgelder verhängten, wenn Einwilligungen wegen Machtungleichgewichten nicht freiwillig sein konnten.

Bitte umblättern ▶





Vorstand und Panel der BHE/GIT-Podiumsdiskussion: Mirko Dohse (3. v.l.) Monic Wölker (4. v.l.), Michael Meissner (5. v.l.) und Benedict Mähn (6. v.l.) – hier mit GIT-Moderator Steffen Ebert und BHE-Vorstandsvorsitzender Axel Schmidt

Perimeterschutz und Datenfusion: Vom Einzelalarm zur qualifizierten Meldung

Sicherheit ist nicht nur Technik, so viel war denn auch durch die vorgenannten Beiträge klar. Doch bilden technische Systeme die notwendige Basis. In diesem Sinne führte – schon zu Beginn des Kongresses – John Rosenbusch (Senstar GmbH) im Themenblock Videosicherheit die Perimeter-Debatte zusammen. Seine Folien verknüpften Normen- und Gesetzesbezüge – etwa CER/KRITIS-Dachgesetz (seit Januar 2026 mit Pflichten zur Risikoanalyse) sowie die Normenfamilien DIN CLC/TS 50661-x und DIN VDE V 0826-20 – mit dem praktischen Trend zu Mehrfachdetektion und Sensorfusion. Die Quintessenz: Nicht ein System macht Sicherheit aus, sondern das Zusammenspiel mehrerer Schichten.

In Szenario-Vergleichen wurde sichtbar, warum Kombinationen attraktiv sind: Reine Videosysteme liefern Abschreckung und Verifikation, detektieren aber teils erst „im Gelände“ und sind anfällig für unerwünschte Auslösungen und Datenschutzkonflikte. Zaun-Detektion kann dagegen direkt an der Perimeter-Grenze mit präziser Lokalisierung arbeiten, sieht aber nur die Zaunlinie. Aus der Perspektive knapper Leitstellenressourcen ist das Ziel klar: weniger Fehlinterpretationen, weniger Falschalarmrate, bessere Priorisierung.

KI in der Videosicherheit: Von Mustererkennung zu Systemarchitektur – mit Grenzen

Die KI-Session von Hardo Naumann und Luka Johnsen setzte bei den Grundlagen an: Mustererkennung hängt von Perspektiven ab – und neuronale Netze arbeiten in sehr hohen Dimensionalitäten („KI ist nicht hochintelligent, sondern hochdimensional“). Darauf aufbauend ordneten die Referenten Video Content Analyse (VCA) als zentrale

KI-Technik der Videosicherheit ein und skizzierten eine Systemlandschaft aus Computer Vision, Regelwerken, Statistik und multimodalen Ansätzen.

Die BHE-Hilfestellung zur KI in der Videosicherheitstechnik ergänzt den Blick um Realismus: Erwartungshaltungen sind häufig zu hoch – nicht zuletzt durch Marketingversprechen und popkulturelle Bilder. Das Papier unterscheidet konsequent zwischen einfacher Bewegungserkennung, ML-basierter Analytik und KI-gestützten Verfahren, diskutiert False Positives und fehlende Kontextbewertung und betont: Qualität entsteht aus Daten, Parametrierung, Organisation und klaren Reaktionszeiten – nicht aus dem Algorithmus allein.

Von MDORII zu OODPCVS: Neue Anwendungsregeln für Videosicherheitssysteme gemäß IEC 626764:2025

Michael Meissner, Vorsitzender des BHE-Fachausschusses Video, stellte die neuen Anwendungsregeln für Videosicherheitssysteme gemäß IEC 626764:2025 vor und ordnete deren Auswirkungen auf Planung, Bewertung und Betrieb moderner VSS ein. Kern der Überarbeitung ist eine grundlegend neue Systematik der Pixeldichten als Qualitätskriterium: An die Stelle früherer, teils missverständlich genutzter Begriffe treten klar definierte Wahrnehmungs- und Bewertungsstufen, die von Überblick und Umreißen über Verfolgen und Wahrnehmen bis hin zu Feststellen, Ermessen und Begutachten reichen und jeweils eindeutig mit erforderlichen Pixeldichten verknüpft sind.

Aus MDORII bzw. DORI (Monitor, Detect, Observe, Recognize, Identify, Inspect) wird somit OODPCVS (Overview, Outline, Discern, Perceive, Characterize, Validate, Scrutinize). Wie man sich das künftig merken kann? Meissner liefert die Eselsbrücke gleich mit:

„Our Operators Deserve Perfectly Clear Video Surveillance“.

Meissner machte deutlich, dass diese Differenzierung nicht nur die Kameraplanung präzisiert, sondern unmittelbar Einfluss auf Sicherheits- und Sicherungskonzepte sowie auf den operativen Betrieb von Videosicherheitssystemen hat. Anhand von Anwendungstabellen zeigte er, wie unterschiedliche Nutzungsszenarien – von Einzelhandel, Industrie und Logistik bis hin zu sicherheitskritischen Infrastrukturen – empfohlenen Sicherungsgraden zugeordnet werden können.

Für KRITIS-Bereiche sieht die Norm dabei höhere Anforderungen vor, insbesondere im Hinblick auf Angriffsrelevanz, Reaktionszeiten und Systemverfügbarkeit. Ergänzend verwies Meissner auf die begleitenden Hilfsmittel des BHE: Die Checkliste zur DIN EN 626764 wurde überarbeitet, Schulungs und Seminarangebote angepasst und Planungs sowie Projektierungswerkzeuge auf die neuen Pixeldichten ausgerichtet. Die internationale Norm IEC 626764:2025 ist seit Herbst 2025 veröffentlicht; die deutsche Fassung der DIN EN 626764 befindet sich derzeit in der finalen Übersetzung und redaktionellen Abstimmung und wird voraussichtlich im Laufe des Jahres 2026 verfügbar sein.

Zutritts- und Besuchermanagement: KRITIS-Prozesse, die im Alltag bestehen müssen

Einleitend in den Themenblock Zutrittssteuerung zeigte Werner Störmer, wie Besuchermanagement und Zufahrtssteuerung Sicherheitslücken der Zutrittssteuerung adressieren können: verlorene oder weitergegebene Ausweise, unverschlüsselte RFID-Technologie, Social-Engineering-Muster („falsche Handwerker“) oder auch Risiken durch Dienstleister mit Zugang zu sensiblen Bereichen. Seine Folien führten über QR-/



Einblicke in Perimeter-schutz-Pilotversuch: Dennis Haeblerlein von EnBW



Live-Hacking mit Yannis Knoll und Michael Topal: Offene Fenster und Blaumann als Türöffner

RFID-Besucherausweise, Kioskterminals, Mehrsprachigkeit und Sicherheitsunterweisungen bis zur Sanktionslistenprüfung und zur Zufahrtssteuerung per Kennzeichenerkennung.

Im Zutrittsblock verbanden dann am Folgetag Axel Schmidt und Stephan Kiese von Salto Systems aus Wuppertal den KRITIS-Kontext mit einem Praxisbericht aus dem Umfeld eines Versorgers der Kritischen Infrastruktur. Ein zentrales Schutzzonenkonzept, unterschiedliche Zutrittszonen und Systemintegration (Alarm, Video, Brand) bildeten die Basis. Beim Besuchermanagement standen digitale Voranmeldung, automatische Benachrichtigung, zeitlich begrenzte Ausweise und Bewegungsprotokolle im Mittelpunkt – mit automatisierter Löschung als Datenschutzbaustein.

Die Learnings zielten auf die alltäglichen Reibungspunkte: technische Komplexität, Zielkonflikte zwischen Nutzerfreundlichkeit, Sicherheit und Datenschutz sowie der hohe Koordinationsbedarf zwischen Gewerken – bis hin zur „Tür“ als Projekt, in dem Fluchtweg- und Brandschutz, Barrierefreiheit, Sonderwünsche und Schnittstellen zusammenlaufen. Der Satz „Koordination ist der Schlüssel“ war hier weniger Schlagwort als Zusammenfassung gelebter Praxis.

Biometrie in der Anwendung: Handvenen als Baustein für Mehrfaktor-Strategien

Mit Blick auf NIS2- und KRITIS-Anforderungen argumentierte Dr. Alexander Lenhardt (iCognize GmbH), dass Einzelfaktoren („Haben“, „Wissen“, „Sein“) allein häufig nicht genügen. Biometrie kann Anwenderfreundlichkeit mit Sicherheitszielen verbinden – aber nicht ohne Systemdesign. Seine Folien unterschieden Betriebsmodi und Speicherorte (Template-in-Database, Template-on-Card, Split-Template) und verwiesen auf zentrale Kennzahlen wie FAR, FRR und EER.

Am Beispiel Flughafen BER (FBB) blieb der Vortrag stark an Prozesskennzahlen orientiert: 55 Zutrittspunkte, „Template-on-Card“, über 7.000 Durchtritte pro Tag (mit Spitzenwerten an einzelnen Übergängen) und ein ROI, der in Wochen statt in Jahren gemessen wurde. Gleichzeitig wurde deutlich, dass Umgebungslicht, Erfassungsqualität und Betriebsbedingungen den Erfolg prägen – Biometrie ist damit eher ein sorgfältig zu planender Bestandteil als ein austauschbares Feature.

Cloud, Cybersecurity und CRA: Regulatorik trifft Architekturentscheidungen

Die Frage nach Cloud- und Hybridmodellen griff zuvor Andreas Flemming auf. Sein Blick richtete sich auf Markttrends („Software as a Service“), Datenschutz und Cybersicherheit sowie auf technische Umsetzungen in hybriden Kontinua zwischen On-Prem, Managed Appliances und Direct-to-Cloud-Geräten. Besonders konkret wurde der Katalog an Nachweisen und Zertifizierungen, die Anbieter in Ausschreibungen zunehmend beantworten müssen – von ISO/IEC 27001 und 27017 über SOC 2 Type II bis zu UL 2900-2-3 Level 3.

Tags darauf, jedoch parallel und passend dazu legte Harald Ratz die Cyber-Resilience-Perspektive auf Hardware und Software in der physischen Sicherheit. Der CRA gilt als EU-Gesetz für Produkte mit digitalen Elementen, mit Fokus auf „Security by Design“ und Anforderungen an Hersteller, Händler/Distributoren und Importeure. Zu berichten gab es über Pflichten wie Risikobewertung, Supportzeiträume, Schwachstellenmanagement inklusive SBOM sowie konkrete Meldezeiträume (24/72 Stunden und Abschlussbericht). Zudem werden Händlerpflichten ab dem 11. September 2026 betont und ein Ausblick auf eine CE-Kennzeichnung, die künftig auch Cyber-Sicherheit signalisiert.

„Live Hacking“: Cyberangriffe als Bestandteil physischer Sicherheitsrisiken

Als bewusster Kontrapunkt setzte das Programm den Vortrag „Live-Hacking – Was hat ein Hackerangriff mit physischer Sicherheit (Videosicherheit, Zutrittssteuerung etc.) zu tun“ von Michael Topal und Yannis Knoll von der ProSec GmbH. Zum Besten gegeben wurden Einblicke in IT-Sicherheit 2026, Angriffsziele und -szenarien, Live-Demonstrationen sowie Schutzmaßnahmen – ohne Folienmaterial, aber als programmatisches Signal: Video- und Zutrittsysteme müssen als digitale Produkte mit Angriffspunkten verstanden werden. Und die Schwachstelle Mensch kann nach wie vor noch allzu oft überlistet werden – Stichworte „offene Fenster“ oder der „Blaumann als Türöffner“.

Videoaufschaltung in der Leitstelle: Nutzen entsteht erst im Betrieb

Der Impulsvortrag zum Thema Einbruchprävention drehte sich schließlich um die Frage, ob Videoaufschaltung auf Notruf- und Serviceleitstellen (NSL) Kriminalität tatsächlich verhindern kann. Mirko Dohse von FSO Fernwirk-Sicherheitssysteme Oldenburg skizzierte die Entwicklung der alarmgesteuerten Aufschaltung seit Ende der 1990er Jahre, die mit IP-Netzen deutlich an Fahrt aufgenommen hat – und zugleich neue Last erzeugt: Je nach Objekt und Bedingungen seien hunderte oder tausende Auslösungen pro Monat keine Seltenheit. Damit steigt der Aufwand der Klassifizierung durch Operatoren: Meldungsfluten können Wachstum begrenzen.

Wichtig war die Differenzierung: Videoaufschaltung ist kein Allheilmittel. Dennoch gibt es dokumentierte Fälle, in denen Taten früh erkannt und durch Maßnahmen wie Intervention, Audioansprache oder weitere Abwehrmittel unterbrochen wurden. Gleichzeitig bleibt die Haftungsfrage offen,



Schutzziel muss definiert werden, die Kommunikation stimmen: Podiumsdiskussion mit Mirko Dohse, Benedict Mähn, Michael Meissner und Monic Wölker (v. l. n. r.)

wenn KI bei der Klassifizierung unterstützt und Fehler mit Schäden an Leib und Leben einhergehen könnten.

Die BHE-Unterlagen rahmen diese Praxisbeobachtung mit einem klaren Funktions- und Prozessbild: Videoaufschaltung soll Prävention, Intervention und Aufklärung verbinden – aber nur, wenn Livebilder, Alarmbilder, Metadaten, Audio/Intercom, Fernwirken sowie zuverlässige Übertragungs- und Health-Check-Mechanismen geplant und betrieben werden. Auch die Kompatibilität zwischen Objekttechnik und Leitstelle bleibt ein limitierender Faktor, weil Leitstellen nicht beliebig viele Systeme effizient bedienen können.

Fehlalarm, Falschalarm, Eventlast: Warum Qualität mehr ist als Sensorik

Ein präziser Begriff hilft im Alltag: Das BHE-Papier trennt „Fehlalarm“ (ein Alarm, der ausbleibt) von „Falschalarm“ (Alarm ohne Ereignis). Gerade im Außenbereich sind Falschmeldungen durch Wetter, Vegetation, Tiere und Betriebsabläufe kaum vollständig zu vermeiden. Der Text der Fachleute vom BHE betont deshalb Planung, Wartung und Alarmverifikation – häufig über Video – sowie technische Kombinationen unterschiedlicher Wirkprinzipien, um Falschalarmquote und Alarmwahrscheinlichkeit in ein sinnvolles Verhältnis zu bringen.

Genau hier setzte Monic Wölker von MW Lighthouse an – mit dem Blick aus Leitstellen- und Betriebspraxis. Ihre Kernaussage: Der Engpass ist oft nicht die Technik, sondern Kommunikation und Betriebslogik. Falschalarme senken Aufmerksamkeit – und Grenzfälle leiden zuerst. Sie plädierte für eine definierte Stabilisierungsphase (kurze Feedbackzyklen), klare Owner-Rollen zur Nachjustierung, Ereignisklassen mit Reaktionslogik und wenige, datenbasierte KPIs wie Eventrate, Anteil relevanter Ereignisse und Top-Ursachen. Und vor allem rät sie zur Kommunikation zwischen

Errichter und NSL, um für größtmöglichen Erfolg und für Sicherheit für den Betreiber zu sorgen.

Das wirtschaftliche Argument blieb dabei messbar: Schon eine moderate Eventlast kann die Marge in Betriebsmodellen spürbar angreifen. Monic Wölker zeigte Plausibilitätsrechnungen und warnte vor „Ausnahmezustand als Dauerbetrieb“, wenn Zuständigkeiten und Nachsteuerung fehlen.

Podiumsdiskussion: Einbruchprävention als Schnittstellen- und Organisationsfrage

Die abschließende BHE/GIT-Podiumsdiskussion bündelte schließlich die Leitmotive des Kongresses: Einbruchprävention in Industrie, Handel und KRITIS gelingt nur, wenn Perimeter, Video, Zutritt und Live-Aufschaltung in die NSL als Prozesskette verstanden werden. Moderiert wurde die Runde von Steffen Ebert von GIT SICHERHEIT. Auf dem Podium stand mit den Fachleuten Monic Wölker, Mirko Dohse, Michael Meissner und Benedict Mähn geballte Expertise dem Auditorium auf alle Fragen Rede und Antwort.

Anregungen aus dem Teilnehmerkreis gaben der Diskussion klare Leitfragen: Wie verändert sich Einbruchkriminalität – und wo liegen aktuelle Schwachstellen? Was braucht es für gute Planung, damit Schnittstellen nicht erst im Betrieb „auffallen“? Wo entstehen die häufigsten Fehlerquellen – technisch oder organisatorisch – und wie kann KI-basierte Videoanalyse helfen, ohne neue Risiken zu schaffen? Markant war eine These aus der Runde: Technik sei in vielen Projekten weiter als die Zusammenarbeit dahinter; ohne belastbare Errichter-NSL-Schnittstelle bleibe Videosicherheit im Ernstfall laut Monic Wölker zu oft „Deko mit Aufzeichnung“.

Einen operativen Rahmen lieferte Michael Meissner mit einer Planungslogik: Professionelle Technik (inklusive Videoanalyse und Audio), enge Verknüpfung mit Zutritt und Einbruchmeldetechnik, gege-

benenfalls Perimeterdetektion sowie die 24/7-Aufschaltung auf eine NSL – ergänzt um Abstimmung zwischen Betreiber, Planer, Errichter und Leitstelle. Damit wurde aus einer Technologie-Debatte eine Organisationsfrage: Wer definiert Schutzziele, wer übernimmt Ownership für Nachjustierung, und wie wird Qualität im Regelbetrieb gemessen?

Fazit: Was aus Mainz mitgenommen werden kann

Der BHE-Fachkongress 2026 zeigte ein konsistentes Bild: Moderne Videosicherheit und Zutrittssteuerung wachsen technisch zusammen, werden aber zugleich stärker von Recht, Betrieb, Organisationsfragen und Cyber-Risiken geprägt. Wer Systeme plant, muss Datenschutz (DSFA), CRA-Pflichten, Schnittstellenfähigkeit und Leitstellenprozesse früh mitdenken. Wer Systeme betreibt, braucht Zuständigkeiten, Messgrößen und eine Routine zur Nachsteuerung. Und wer KI einsetzen will, kommt nicht um die Frage herum, welche Entscheidungen automatisiert werden dürfen – und welche Verantwortung beim Menschen bleiben muss.

Wer Technik auch live erleben wollte, konnte dies übrigens ebenfalls vor Ort tun: Eine begleitende Ausstellung mit Anbietern wie AG Neovo, Aritech, Axis, ebenso wie Barox, Dom, Eizo, EPS, Hirsch, Salto oder Slat und Telenot bot Systeme zum Anfassen und Ausprobieren.

Der BHE-Kongress Videosicherheit und Zutrittssteuerung findet alle zwei Jahre statt – und bleibt ein echter Tipp für alle, die rund um diese Themen Verantwortung tragen **GIT**



**BHE Bundesverband
Sicherheitstechnik e.V.**
www.bhe.de



MESSEN

Sichere Kommunikation

Die PMRExpo 2026 lädt vom 24. bis zum 26. November 2026 nach Köln

Die PMRExpo 2026 ist die europäische Leitmesse für sichere einsatz- und geschäftskritische Kommunikation. Veranstalter ist die Koelnmesse, ideeller Träger ist der PMeV – Netzwerk Sichere Kommunikation. Vorgestellt werden hier sichere Kommunikationslösungen für Behörden, Organisationen mit Sicherheitsaufgaben, Kritische Infrastrukturen und die Industrie.

■ Im Mittelpunkt der diesjährigen PMRExpo steht die missionskritische Kommunikation der nächsten Generation. Es geht um vernetzte Kommunikationen, Leitstellen und Datensysteme für BOS, KRITIS-Betreiber, Industrie und weitere Wirtschaftssektoren. Ergänzend zum professionellen Mobilfunk gewinnen Themen wie 5G, Künstliche Intelligenz, Satellitenkommunikation, Cyberresilienz und die zivilmilitärische Zusammenarbeit weiter an Bedeutung.

Konferenz: Resilient vernetzt

Der PMRExpo Summit bietet ein hochkarätiges Konferenzprogramm unter dem

Leitthema „Resilient vernetzt. Herausforderungen und Lösungen in der kritischen Kommunikation der nächsten Generation“. Experten diskutieren aktuelle Entwicklungen, technologische Trends und Zukunftsperspektiven der Branche. Zusätzliche Impulse setzen Formate wie der 5G-Hub for Private Networks, ein eigener 5G-Thementag in der Connecting Area, die Startup Area sowie der Hackathon at PMRExpo in Zusammenarbeit mit Corevas.

2026 feiert die PMRExpo zudem ihr 25-jähriges Bestehen. Seit einem Vierteljahrhundert begleitet sie die Entwicklung sicherer Kommunikationslösungen – von klassischen Funktechnologien über private

5G-Netze bis hin zu modernen digitalen Plattformen. Als Denkfabrik und Innovationstreiber prägt sie den fachlichen Austausch und setzt kontinuierlich Akzente für neue Technologien und Anwendungen.

Die PMRExpo 2026 findet vom 24. bis 26. November 2026 in Köln statt und verspricht ein besonders starkes Messejahr mit hoher internationaler Beteiligung und wegweisenden Impulsen für die Zukunft sicherer Kommunikation. **GIT**



PMRExpo

www.pmrexpo.com



SICHERHEITSTECHNIK

Technik am See

Ein Sommerfest mit Wissenstransfer und Networking

Rund 150 Gäste aus der Sicherheitsbranche erlebten beim Xortec Sommerfest in Blankenfelde-Mahlow, was es bedeutet, wenn ein Value-Added-Distributor nicht nur Produkte, sondern echtes Fachwissen liefert. Acht Hersteller, eine Keynote zu KRITIS und Cybersicherheit sowie ein Kamera-Shootout in der Abenddämmerung boten das richtige Umfeld für Wissenstransfer, Austausch und Networking.

■ Xortec ist ein auf Sicherheitstechnik spezialisierter B2B-Distributor mit regionalen Standorten in Frankfurt am Main, Hamburg, Berlin, Regensburg und München. Das Portfolio umfasst Videoüberwachung, Einbruch- und Brandwarntechnik, Zutrittskontrolle, Netzwerktechnik und Kamerasystemen. Der Distributor verfolgt einen konsequent beratungsorientierten Ansatz als Partner der Sicherheitserrichter – mit technischem Pre-Sales-Support und gezielter Wissens-

vermittlung auf Augenhöhe. Das Motto „Mehr als Distribution“ versteht das Unternehmen als gelebte Kultur. Zum Herstellernetzwerk zählen Ajax-Systems, Barox, Hanwha Vision, Hikvision, IQ Sight, Mirasys, Motorola Solutions, Octave und viele weitere.

Acht Hersteller, ein Nachmittag voller Praxis

Thoralf Brandt (Regionalleiter Nord) und Michael Schaller (Geschäftsführer Xortec) eröffneten das Event. Im Mittelpunkt standen acht Hersteller-Kurzvorträge à 15 Minuten: Sebastian Hanne (Ajax Systems), Diana Henn (Barox), Maurice Schuster (Hanwha Vision), Sebastian Dittmann (Hikvision), Ronny Voigt & Jens Gässner (IQ Sight), Udo Schneider (Mirasys), Alexander Birr (Motorola Solutions) und Frank Müller (Octave).

Einen Höhepunkt setzte Carsten Pinnow mit seiner Keynote zu KRITIS und Cybersicherheit: aktuelle Angriffsvektoren, die Verknüpfung physischer und digitaler Sicherheit, die Rolle des Distributors als Kompetenzvermittler – praxisnah, ohne abstrakte Bedrohungsszenarien. Die



Resonanz war eindeutig: die Keynote zählte für viele zum wertvollsten Programmpunkt des Abends.

Kamera-Shootout

Ein besonderes Highlight war der Kamera-Shootout ab 21:30 Uhr in der einsetzenden Dämmerung. Hanwha Vision, Hikvision, IQSight und Motorola Solutions traten unter realen Outdoor-Bedingungen gegeneinander an – KI-Analyse, Bildschärfe, Farbwiedergabe, Rauschverhalten und Thermaldarstellung bei Low-Light, live und ohne Laborsetting. Barox lieferte mit spezialisierten



PoE-managed-Switches die Netzwerkinfrastruktur, Mirasys stellte als VMS-Plattform die Vergleichsgrundlage bereit. „Live zu sehen, wie sich die Kameras unter identischen Bedingungen schlagen, ist etwas völlig anderes als ein Datenblatt“ – so das Fazit eines Teilnehmers, das viele teilten.

Partner für Sicherheitstechnik

Xortec positioniert sich als Value-Added-Distributor mit überregionaler Reichweite und tiefem technischen Know-how. Als Partner führender Hersteller der Sicherheitsbranche verbindet das Unternehmen Produktkompetenz mit praxisnaher Beratung – und schafft damit Mehrwert für Errichter und Fachplaner im täglichen Projektgeschäft. Wer Live-Vergleiche, Fach-

Auf dem diesjährigen Sommerfest von Xortec wurde nicht nur die neuesten Produkte rund um Sicherheit präsentiert, sondern in verschiedenen Vorträgen auch wichtiges Fachwissen vermittelt – und bis in die Nacht hinein genetzt

vorträge und den direkten Austausch mit Herstellern in diesem Format erleben möchte, findet Informationen zu kommenden Veranstaltungen unter <https://xortec.de/Unternehmen/Veranstaltungskalender>. **GIT**



Xortec GmbH
www.xortec.de



© Bilder: Xortec

ZVEI zum TÜV Baurechtsreport

Der aktuelle TÜV Baurechtsreport dokumentiert zahlreiche Mängel an sicherheitstechnischen Anlagen in Gebäuden. Dabei zeigt sich erneut: Defizite im Betrieb und in der Instandhaltung sowie unklare Zuständigkeiten in der organisatorischen Verantwortung der Betreiber sind die häufigsten Problemsachen.

Dirk Dingfelder, Vorsitzender des ZVEI-Fachverbands Sicherheit, sieht einen dringenden Nachholbedarf bei der Instandhaltung von Sicherheitstechnik: „Die beste Technik verliert an Zuverlässigkeit, wenn sie nicht gepflegt wird. Im Markt begegnen uns immer wieder Anlagen, die nur nachlässig oder gar nicht gewartet werden. Im Unterschied zur TÜV-Plakette am Auto, bei der jeder auf einen Blick erkennen kann, ob sie abgelaufen ist, fällt das bei sicherheitstechnischen Anlagen zunächst nicht auf.“

Die vertiefende Analyse zum Beispiel für Brandmeldeanlagen und Rauch- und Wär-

meabzugsanlagen zeige, dass die eingesetzte Technik selten die Fehlerquelle ist. Die öffentliche Wahrnehmung sei jedoch eine andere, denn der Betreiber der Anlage werde im Report nicht sichtbar – das Typenschild des Herstellers hingegen schon. „Es gilt, die Betreiber deutlich stärker in die Pflicht zu nehmen“, so Dirk Dingfelder weiter.

Die Analyse der Ergebnisse des Baurechtsreports zeigt: Technische Defekte an sicherheitstechnischen Komponenten spielen lediglich eine untergeordnete Rolle. Moderne sicherheitstechnische Anlagen sind in der Regel zuverlässig ausgelegt. Sie verfügen über automatische Prüf- und Überwachungsfunktionen, mit denen sich Abweichungen frühzeitig erkennen. Diese lassen sich mit vergleichsweise geringem Aufwand beheben.

Der Schwerpunkt der Beanstandungen liegt vielmehr in organisatorischen und betrieblichen Mängeln. Dazu zählen unzu-

reichend gepflegte oder nicht aktualisierte technische Dokumentationen, unregelmäßige oder fachlich nicht ausreichende Wartungs- und Instandhaltungsmaßnahmen sowie Defizite bereits in der Planungs- und Errichtungsphase. Häufig sind Unterlagen nicht ausreichend dokumentiert, weichen vom tatsächlichen Anlagenzustand ab oder berücksichtigen spätere bauliche und technische Änderungen nicht.

Hinzu kommt, dass Wartungs- und Inspektionsarbeiten vielfach nicht den bau- und anlagentechnischen Mindestanforderungen entsprechen. „Sicherheitstechnische Anlagen können ihre Schutzwirkung nur dann entfalten, wenn sie fachgerecht betrieben, regelmäßig instandgehalten und vollständig dokumentiert werden“, betont Dirk Dingfelder. Unabhängig vom technischen Ausstattungsniveau liege die Verantwortung dafür in erster Linie bei den Gebäude- und Anlagenbetreibern.

www.zvei.org

Lünendonk: Schwache Konjunktur ist spürbar

Nach drei wachstumsstarken Jahren kehrt die Marktentwicklung für Facility-Service in Deutschland wieder auf das Niveau der Jahre 2011 bis 2019 zurück, lauten erste Ergebnisse der neuen Lünendonk-Studie „Facility Service in Deutschland“. Die 25 größten Anbieter steigerten ihren Umsatz im abgelaufenen Geschäftsjahr um durchschnittlich 6,3 Prozent. Die Prognosen bleiben mit erwarteten jährlichen Wachstumsraten von 6,6 bis 7,0 Prozent bis 2030 moderat. Gründe hierfür sind die angespannte Konjunktur, die damit verbundene Investitionszurückhaltung bei Sonderprojekten sowie ein steigender Preisdruck in Vergabeverfahren. Neue Wachstumsimpulse erwarten die Dienstleister aus der verschärften Regulatorik für kritische Infrastrukturen und dem damit verbundenen Bedarf an professionellen und auf Resilienz zielenden Facility-Services.

www.luenendonk.de

VSW-Positionspapier zum KRITIS-Dachgesetz eingereicht

Der VSW-Bundesverband hat eine Stellungnahme zum Entwurf der Rechtsverordnung zur Bestimmung kritischer Anlagen beim BMI eingereicht. Vor allem die Ergänzung um den Sektor Weltraum, die Orientierung an einer einheitlichen Methodik, die grundsätzliche Kohärenz mit bestehenden Regelwerken im Bereich der IT-Sicherheit sind hier positiv hervorzuheben. Jedoch sollten vor dem Hintergrund der derzeitigen Bedrohungslage Anwendungsbereiche und auch einzelne Schwellenwerte nachgeschärft werden.

www.vsw.de

Die Einsatzkräfte meisterten die Bekämpfung mehrerer künstlich erzeugter Brände sowie die Rettung von Personen, um die Abläufe und Schnittstellen im Ernstfall aufeinander abzustimmen

TITEL STORY

Gelebte Resilienz

Das Gesetz richtet sich als Teil einer ...
Krisen- und Notfallmanagement bei Roche in Penzberg

— GIT SICHERHEIT: Herr Skolik, Herr Kastner, der Deutsche Bundestag hat kürzlich das Kritis-Dachgesetz beschlossen. Dass es kommt, ist – es handelt sich ja um die Umsetzung einer EU-Richtlinie – schon lange klar. Vermutlich erfüllen Sie bei Roche schon längst alle darin enthaltenen Forderungen?

Marco Skolik: Natürlich beschäftigt sich Roche bereits seit längerer Zeit intensiv mit der Umsetzung der zugrunde liegenden EU-Richtlinie. Das Themenfeld ist allerdings insgesamt sehr komplex. Zum einen geht es um die Anforderungen an kritische Infrastrukturen, zum anderen sind wir als Standort auch ein sogenannter Störfallbetrieb.

Jörg Kastner: Zum jetzigen Zeitpunkt ist noch nicht abschließend geklärt, ob der Standort Penzberg tatsächlich unter die neuen Regelungen des Kritis-Dachgesetzes fällt. Die relevanten Schwellenwerte werden erst zu einem späteren Zeitpunkt per Rechtsverordnung festgelegt. Sollte das Gesetz für uns Anwendung finden, werden wir die entsprechenden Vorgaben selbstverständlich erfüllen. Wir gehen allerdings davon aus, dass die wesentlichen Auswirkungen für uns vor allem im Bereich zusätzlicher Dokumentations- und Meldepflichten liegen werden. In den übrigen Themenfeldern sind wir bereits sehr gut aufgestellt. Krisen- und Notfallmanagement existieren bei uns nicht nur auf dem Papier, sondern werden aktiv gelebt.

Roche in Penzberg zählt zu den bedeutendsten Biotechnologiestandorten Europas. Er setzt auf enge Abstimmung mit Polizei, Feuerwehr und Rettungsdiensten, regelmäßige Großübungen und klare Schnittstellen. Ziel ist eine robuste Gefahrenabwehr, die interne Strukturen und externe Behörden konsequent verzahnt und so die Versorgungssicherheit für Patientinnen und Patienten weltweit stärkt. GIT SICHERHEIT sprach mit Marco Skolik, Leiter Unternehmenssicherheit, und Jörg Kastner, Leiter Krisen- und Notfallmanagement am Standort Penzberg.

Neuordnung der Sicherheitsarchitektur in Deutschland ja primär an Betreiber kritischer Infrastrukturen – allerdings führt es auch zu mehr Verantwortung für die Behörden und Organisationen mit Sicherheitsaufgaben (BOS). Wie ist es Ihrer Ansicht nach um die Vernetzung zwischen BOS und Unternehmen heute bestellt?

Marco Skolik: Aus meiner Sicht besteht an vielen Stellen bereits ein guter Kontakt. Gleichzeitig gibt es noch Potenzial, die Zusammenarbeit weiter zu stärken und Prozesse zu verbessern. Es gibt zwar viele Betriebe – dazu zählt auch unser Standort in Penzberg –, die sich über Jahre hinweg ein sehr enges und vertrauensvolles Ver-

Organisationen aufgebaut haben. Diese Vernetzung ist jedoch längst nicht überall gegeben, obwohl sie für eine funktionierende Gefahrenabwehr und Krisenbewältigung absolut erfolgskritisch ist. Ich wünsche mir daher ausdrücklich, dass auch die Behörden selbst stärker umdenken und proaktiv auf Unternehmen der kritischen Infrastruktur sowie auf Störfallbetriebe zugehen.

Jörg Kastner: Wichtig ist aus meiner Sicht zudem, dass Betriebe der kritischen Infrastruktur bei der Vorbereitung auf Schadensereignisse auch dann berücksichtigt werden, wenn diese nicht dem klassischen oder gewohnten Einsatzbild entsprechen. Unternehmen bringen eigenes Potenzial,

besondere Gefahrenlagen und spezifische Rahmenbedingungen mit, die in die Planung zwingend einfließen müssen. Das gilt insbesondere für übergeordnete Handlungskonzeptionen für Einsatzszenarien, etwa die Handlungskonzeption für lebensbedrohliche Einsatzlagen in Bayern.

Lassen Sie uns das einmal anhand der Standorte von Roche, für die Sie verantwortlich sind, ein wenig durchdeklinieren. Zunächst einmal zur Einordnung: Roche in Penzberg ist ja selbst praktisch eine Stadt für sich – und gleichzeitig ein erheblicher Teil von Penzberg?

Marco Skolik: Roche in Penzberg ist eines der größten Biotechnologiezentren in Europa und innovatives Kompetenzzentrum für Life Science im Großraum München. Der Standort ist mit 7.900 Mitarbeitenden der größte Arbeitgeber im bayerischen Oberland und einer der wichtigsten Wirtschaftsfaktoren der Region. Das Werk, das 590.000 Quadratmeter umfasst, ist eine weltweit wichtige Zentrale für die Erforschung, Entwicklung und Produktion von biopharmazeutischen Wirkstoffen, diagnostischen Tests und Reagenzien, Analyse-Systemen sowie molekularem Tumorphilung und Gentherapie.

Sie dürften ja Polizei, Feuerwehr, Rettungsdienste etc. weitgehend persönlich und strukturell gut kennen?

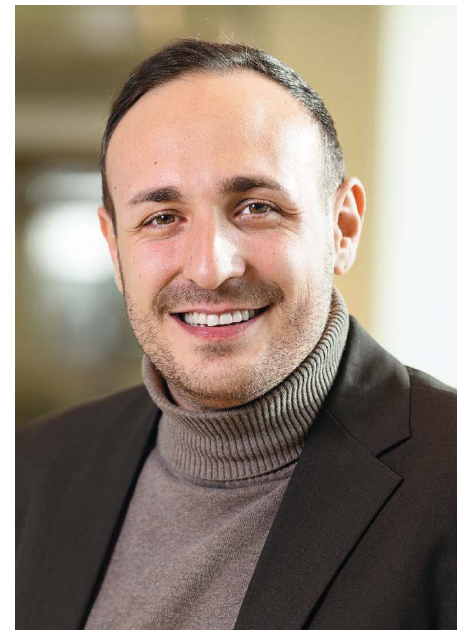
Marco Skolik: Ja, das ist tatsächlich so. Insbesondere mit der Polizei, den umliegenden Feuerwehren sowie dem Rettungsdienst besteht ein sehr guter und regelmäßiger Austausch. Einsatzszenarien werden gemeinsam im Vorfeld geplant und auch praktisch erprobt.



Jörg Kastner, Leiter Krisen- und Notfallmanagement bei Roche in Penzberg

Darüber hinaus gibt es in Teilen bereits abgestimmte Prozesse im Tagesgeschäft. Dazu zählt beispielsweise die enge Zusammenarbeit zwischen unserem Werkschutz und der Polizei, etwa bei der Anzeigerstattung, die in vielen Fällen ohne ein erneutes persönliches Vorsprechen bei der zuständigen Dienststelle direkt beim Werkschutz erfolgen kann. Auch die Zusammenarbeit zwischen unserer Werkfeuerwehr und der Freiwilligen Feuerwehr Penzberg bei Einsätzen im und um das Werk ist fest etabliert.

Jörg Kastner: Darüber hinaus pflegen wir auch mit der unteren Katastrophenschutzbehörde am Landratsamt Weilheim-Schongau einen sehr guten und regelmäßigen Austausch. Sämtliche Roche betreffenden



Marco Skolik, Leiter Unternehmenssicherheit bei Roche in Penzberg

Themen werden hier offen, konstruktiv und partnerschaftlich besprochen.

Nun veranstalten Sie, wie es in großen Unternehmen vielfach gemacht wird, Übungen zur Zusammenarbeit. Von wem geht dabei eigentlich die Initiative aus?

Jörg Kastner: Grundsätzlich sehen wir uns selbst in der Verantwortung, die für unseren Standort relevanten Szenarien proaktiv mit den externen Einsatzkräften abzustimmen und regelmäßig zu üben. Als Unternehmen sind wir durch unsere Tätigkeit ein sogenannter Störfallbetrieb. Daraus ergibt sich für uns die klare Verpflichtung, den Vorgaben der Störfallverordnung nachzukommen und sowohl die Bevölkerung als auch die Umwelt jederzeit bestmöglich vor Beeinträchtigungen zu schützen.

Marco Skolik: Das gilt in gleicher Weise für unsere Mitarbeitenden und unsere Sachwerte. Wir haben eine ausgeprägte Fürsorgepflicht und einen hohen Anspruch an die Sicherheit unserer Kolleginnen und Kollegen. Hinzu kommt die Verpflichtung durch die Regierung von Oberbayern, regelmäßig Übungen gemeinsam mit externen Einsatzkräften durchzuführen. Vor diesem Hintergrund haben wir uns im vergangenen Jahr bewusst dazu entschieden, künftig jährlich eine Großübung am Standort Penzberg umzusetzen. Diese Übungen finden im Wechsel mit internen Kräften und gemeinsam mit externen Einheiten statt. Darüber hinaus verstehen wir uns nicht nur als Übungsbeteiligte, sondern auch als aktiver Partner in der Gefahrenabwehr.

Bitte umblättern ▶



Mit von Schauspielern dargestellten Patientinnen und Patienten wurde das Zusammenspiel zwischen internen und externen Rettungskräften trainiert

Wer sind die Teilnehmer und wie sieht im Groben der Ablauf der Übung aus?

Marco Skolik: Grundsätzlich binden wir bei all unseren Großübungen mit externen Kräften stets die umliegenden Feuerwehren, die Rettungsdienste sowie die Polizei ein. Abhängig vom jeweiligen Szenario setzen wir jedoch unterschiedliche Schwerpunkte, was sich entsprechend auch im Kräfteansatz widerspiegelt. Bei der letzten Großübung haben wir erstmals den Hauptfokus auf den Werkschutz und die Polizei gelegt. Hintergrund war eine polizeiliche Einsatzlage – gewissermaßen die Königsdisziplin unter den Gefahrenlagen.

Das Übungsszenario deckte dabei die gesamte Einsatzkette ab: von der Absetzung des Notrufs über die polizeiliche Abarbeitung mit Unterstützung durch den Werkschutz – insbesondere durch Ortskenntnis, Drohnentechnik und die Lenkung von Betroffenen – bis hin zur Sichtung und Versorgung von „Verletzten“ durch die Rettungsdienste sowie der Bekämpfung mehrerer künstlich erzeugter Brände durch die Werkfeuerwehr. Entsprechend anspruchsvoll und umfangreich war die Übung angelegt.

Jörg Kastner: Die Grundlage für einen Einsatzerfolg wird häufig bereits in der ersten Phase gelegt. Deshalb haben wir versucht, das Szenario möglichst realitätsnah aufzubauen. Ausgangspunkt war ein zunächst mehr oder weniger alltäglicher Werkschutzeinsatz, wobei bereits die erste Lagemeldung ein kritischer Punkt war. Die Werkschutz-Einsatzzentrale hat daraufhin die internen Kräfte über die Gefährdungslage informiert und gleichzeitig die Meldung an die Polizei-Einsatzzentrale sowie an die Integrierte Leitstelle abgesetzt.

Nachdem die Polizei die Lage bereinigt hatte, haben interne und externe Einsatzkräfte gemeinsam die schauspielenden Patientinnen und Patienten versorgt und abtransportiert sowie die künstlich erzeugten Brände gelöscht.

Der Einsatz von Drohnen spielte eine besondere Rolle...?

Marco Skolik: Ja, der Einsatz der Drohne war in diesem Szenario absolut erfolgskritisch. Bereits rund sechs Minuten nach Einsatzbeginn befand sie sich in der Luft und lieferte eine Live-Lageübersicht über das gesamte Geschehen. Diese Echtzeitinformationen ermöglichten eine schnelle Eingrenzung des Gefahrenbereichs und eine gezielte Lenkung der Polizeikräfte. Dadurch konnten Entscheidungen deutlich schneller und fundierter getroffen werden, was maß-



Im Rahmen einer Großübung im Herbst 2025 in Penzberg übernahm der Roche Werkschutz zentrale Koordinierungsaufgaben

geblich zu einer zügigen und erfolgreichen Einsatzbewältigung beigetragen hat.

Was haben beide Seiten von dieser Übung mitgenommen – und welche Schlussfolgerungen ziehen Sie für Ihre eigene Sicherheitskonzeption?

Marco Skolik: Beide Seiten haben vor allem eines mitgenommen: Sicherheit entsteht durch Übung, Vertrauen und klare Schnittstellen. Die Übung hat gezeigt, wo Abläufe bereits sehr gut funktionieren und wo wir gemeinsam noch nachschärfen müssen. Für unsere Sicherheitskonzeption bedeutet das, dass wir den eingeschlagenen Weg konsequent weitergehen – mit regelmäßigen Übungen, enger Vernetzung und einem klaren Fokus auf praxisnahe Vorbereitung statt rein formaler Konzepte.

Jörg Kastner: Neben einigen wichtigen Detailerkennnissen war insbesondere das Thema der psychosozialen Notfallversorgung ein zentrales Ergebnis der Übung. In unserem Werk halten sich täglich mehrere Tausend Menschen auf, die bei einer Großschadenslage in unterschiedlicher Weise betroffen sein können. Vor diesem Hintergrund haben wir das Thema im Nachgang gemeinsam mit unseren internen Ressourcen sowie mit der Arbeitsgemeinschaft Psychosoziale Notfallversorgung des Landkreises neu geplant und weiterentwickelt.

Sie haben aber auch Vorstellungen davon, was die Anforderungen an die Behörden betrifft, wenn es um die Zusammenarbeit bei besonderen Einsatzlagen geht? Insbesondere betonen Sie ja die Verbindung nicht nur von Security und Safety, sondern auch das Zusammenspiel von internen und externen Kräften als zur Definition des Allgefahrenansatzes gehörig?

Marco Skolik: Ja, diese Erwartungen haben wir. Aus unserer Sicht müssen Behörden Security- und Safety-Aspekte konsequent zusammendenken und interne Unternehmensstrukturen als festen Bestandteil des Allgefahrenansatzes begreifen. Werkfeuerwehren, Werkschutz oder Werkrettungsdienste sind im Ereignisfall keine Randakteure, sondern integraler Teil der Gefahrenabwehr. Eine frühzeitige Einbindung, klare Zuständigkeiten und gelebte Zusammenarbeit auf Augenhöhe sind dafür entscheidend.

Jörg Kastner: Aus unserer Sicht ist es wichtig, dass die betriebliche Gefahrenabwehr auf allen Ebenen als Partner auf Augenhöhe anerkannt wird. Gerade bei besonderen Einsatzlagen kann ein wirksames Krisen- und Notfallmanagement nur dann funktionieren, wenn interne und externe Akteure frühzeitig und strukturiert zusammenarbeiten.

Herr Skolik, Herr Kastner, wir hatten es eingangs schon angerissen: Die normativen Neuordnungen finden nicht im luftleeren Raum, sondern im Zeichen geopolitischer Veränderungen statt. Insbesondere Deutschland ist rein geografisch ein logistisches Zentrum für militärische Bewegung, ggf. von Flüchtenden, etc. Der „Operationsplan Deutschland“ etwa wird nicht nur militärisch und staatlich, sondern auch als gesamtgesellschaftliche Aufgabe angesehen. Könnten Sie einmal skizzieren, wie Sie hier als Unternehmen eingebunden sind?

Marco Skolik: Aktiv eingebunden sind wir derzeit noch nicht. Gleichzeitig haben wir als Unternehmen ein großes Eigeninteresse daran, auf sämtliche denkbare Szenarien vorbereitet zu sein – auch vor dem Hintergrund der aktuellen geopolitischen Entwicklungen. Entsprechend analysieren wir fortlaufend die Lage und überprüfen sowie schärfen unsere internen Prozesse. Aktuell erarbeiten wir eine übergeordnete Strategie, um perspektivisch auch aktiv auf Akteure wie die Bundeswehr zuzugehen. Ziel ist es, die Verzahnung mit dem Operationsplan Deutschland strukturiert voranzubringen und eine funktionierende, belastbare Schnittstelle zwischen unternehmerischer Vorsorge und gesamtgesellschaftlicher Resilienz zu schaffen. **GIT**



Roche Diagnostics GmbH
www.roche.de

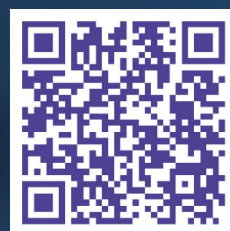


Expertenforum Reisesicherheit

Tübingen · 28.–29. September 2026

Reale Erfahrungen. Relevante Themen. Wertvolle Gespräche.

Programm ansehen & anmelden →



KÜNSTLICHE INTELLIGENZ

KI-gestütztes Recruiting im Sicherheitsgewerbe

Einblicke von der BVSW SecTec 2026

Stark schwankende Personalbedarfe sind Alltag bei Sicherheitsdienstleistern und machen die Recruiting-Prozesse zur Herausforderung. Auf der BVSW SecTec 2026 erklärte Markus Vollerthun, Geschäftsführer des Veranstaltungsdiensts Paul Mayr (VD Mayr), wie künstliche Intelligenz hier unterstützen kann.



■ Ob Sportveranstaltungen, kulturelle Events oder Messen – der Münchner Sicherheitsdienstleister VD Mayr ist auf die Betreuung von Veranstaltungen spezialisiert. Ergänzend gehört der klassische Objektschutz zum Portfolio. Insbesondere im Eventbereich schwankt der Personalbedarf stark und das „High-Volume-Recruiting“ ist mit einem erheblichen organisatorischen Aufwand verbunden.

Wie das aussehen kann, lässt sich am Beispiel eines Fußballspiels verdeutli-

chen: Hierfür benötigen die Sicherheitskräfte zwei Qualifikationen, nämlich die Unterrichtung nach §34a GewO sowie die QuaSOD-Schulung des DFB. Diese Anforderungen hat die VD Mayr früher immer in persönlichen Gruppenterminen vermittelt, zu denen die Bewerber eingeladen wurden. Neben der eigentlichen Durchführung bedeuteten Terminorganisation, Vor- und Nachbereitung sowie der Umgang mit Absagen und Rückfragen einen erheblichen Zeitaufwand für die Personalabteilung.

KI-Einsatz steigert Effizienz im Recruiting

Zu Beginn des Jahres 2025 hatte sich das Unternehmen ambitionierte Wachstumsziele gesetzt, ohne dabei die Verwaltungskosten steigern zu wollen. „Im Zuge der Überlegung, wie wir das erreichen können, bin ich eher zufällig bei einer Recherche darauf gestoßen, dass KI auch im Recruiting unterstützen kann“, sagt Markus Vollerthun, Geschäftsführer der VD Mayr. „Ab diesem Zeitpunkt haben wir das Thema konsequent weiterverfolgt, bis wir eine passende Lösung gefunden hatten.“

Nach der Analyse von mehreren Anbietern entschied sich das Unternehmen für eine Lösung von Paul's Job. Sie kann den gesamten Onboarding-Prozess abbilden, von der Bewerbung über die Terminvereinbarung bis hin zur Vertragserstellung.

Die Auswirkungen auf die Effizienz sind überzeugend: Während früher für die Einstellung von 50 Leuten rund 40 Arbeitsstunden anfielen, ist dieser Prozess heute in 15 Minuten zu bewältigen. Die KI übernimmt einen Großteil der administrativen Aufgaben, prüft formale Voraussetzungen, koordiniert Termine und beantwortet grundlegende Fragen von Bewerbern. Insbesondere standardisierte Informationsprozesse, wie die eingangs genannte Erklärung von Qualifikationsanforderungen bei Fußballspielen, können automatisiert ablaufen.

Darüber hinaus wirkt sich der Einsatz von KI auf die Passgenauigkeit der Kandidaten aus. So sind im Empfangsbereich beispielsweise gute Deutschkenntnisse, Freundlichkeit und Kritikfähigkeit Vor-



Selbstverständlich werden die Bewerber vorab darüber informiert, dass sie mit einer KI sprechen



Markus Vollerthun, Geschäftsführer des Veranstaltungsdiensts Paul Mayr (VD Mayr)

aussetzung. Diese Fähigkeiten werden im Rahmen von telefonischen Erstgesprächen überprüft und diese Telefonate übernimmt jetzt die KI.

„Selbstverständlich werden die Bewerber vorab darüber informiert, dass sie mit einer KI sprechen“, erklärt Vollerthun. „Doch diese Lösung verbessert auch die sogenannte Candidate Experience und bietet damit Vorteile für alle: Gespräche können jederzeit stattfinden, was die Terminfindung vereinfacht und die Prozesse beschleunigt.“

Richtige Konfiguration entscheidend

Damit KI die Recruiting-Prozesse optimal unterstützen kann, ist eine Feinjustierung gemäß den individuellen Anforderungen des Anwenderunternehmens wichtig. Tonalität, Entscheidungslogiken und Bewertungskriterien müssen passen und vorab entsprechend festgelegt werden, denn KI ist vor allem ein Werkzeug, wie Vollerthun bestätigt.

Auch im laufenden Betrieb ist eine regelmäßige Feinjustierung erforderlich. Die KI-Lösung muss regelmäßig überprüft und angepasst werden, da sie auch unerwünschte Verhaltensweisen entwickeln können, wie etwa einen unpassenden Kommunikationsstil.

Einbindung der Personalabteilung verbessert Akzeptanz

Ein wesentlicher Erfolgsfaktor bei der Einführung der KI-Lösung war die frühzeitige Einbindung der Personalabteilung, die mit darüber entscheiden konnte, ob KI überhaupt zum Einsatz kommen sollte. Die Entscheidung fiel eindeutig aus, den das Recruiting-Team von VD Mayr hatte das Potenzial der Lösung erkannt.

Durch die Entlastung bei administrativen Tätigkeiten können sich die Mitarbeitenden jetzt stärker auf Bereiche fokussieren, die langfristig betrachtet auch in menschlicher Hand bleiben werden, näm-

lich der direkte Austausch mit Bewerbern und die individuelle Vertragsgestaltung.

KI-gestütztes Recruiting bietet im Sicherheitsgewerbe erhebliche Effizienzpotenziale, insbesondere bei stark schwankendem Personalbedarf. Der Erfolg ist dabei maßgeblich von der richtigen Implementierung und kontinuierlichen Steuerung abhängig. KI übernimmt vor allem Routineaufgaben, während sich die Mitarbeitenden auf Bereiche fokussieren können, die einen direkten Austausch erfordern.

BVSW SecTec ist ein jährlicher Fachkongress, auf dem technische Innovationen und ihre Einsatzmöglichkeiten in der Sicherheitsbranche präsentiert werden. **GIT**



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

Effizientes Netzwerkmanagement

Barox präsentiert seine neue Software xNMS

ADVERTORIAL

Mit der neuen Management-Software xNMS setzt barox Kommunikation neue Maßstäbe für Effizienz und Transparenz in Video- und Sicherheitsnetzwerken. Die zentrale Plattform vereinfacht die Konfiguration, Verwaltung und Wartung komplexer Infrastrukturen und begleitet den gesamten Lebenszyklus eines Netzwerks, von der Planung bis zum laufenden Betrieb.

xNMS von Barox erkennt bestehende Netzwerke automatisch, erstellt übersichtliche Listenansichten sowie grafische Topologien und sorgt damit für maximale Transparenz. Dies erleichtert die Administration und beschleunigt die Fehlersuche erheblich. Ein integrierter Diff-Checker überwacht Konfigurationsabweichungen in Echtzeit und macht unautorisierte oder versehentliche Änderungen sofort sichtbar.

Beschleunigte Inbetriebnahme

Bereits vor der Hardwarelieferung können Switches virtuell vorbereitet und validiert werden. Dadurch lassen sich Abhängigkeiten frühzei-



Die zentrale Plattform xNMS von Barox vereinfacht die Konfiguration, Verwaltung und Wartung komplexer Infrastrukturen

tig erkennen und Inbetriebnahmen deutlich beschleunigen. Das Ergebnis ist eine nahezu Plug & Play-Inbetriebnahme mit reduzierter Fehlerquote.

Künftige Updates erweitern xNMS zudem um Firmware- und Backup-Management, inklusive sicherer Rollback-Funktion. Die Software

ist als Free-Version mit Basisfunktionen sowie als Paid-Version mit erweitertem Funktionsumfang erhältlich.

barox
Switche für Video

Kontakt
barox
Kommunikation GmbH
www.barox.de



Umfangreiche Schaltfunktionen ermöglichen bei den Bedienteilen den Zugriff auf alle Komponenten der Gebäudeautomationstechnik

KOMPLETTLÖSUNG

Sensible Prozesse

Präzision braucht zuverlässigen Schutz

Medizintechnikhersteller Albomed setzt anlässlich des Ausbaus seines Standorts und dessen Sicherheitsinfrastruktur auf eine Lösung von Telenot, die Einbruchschutz, Brandschutz und Zutrittskontrolle intelligent miteinander verbindet.

Albomed ist Entwickler und Hersteller moderner viskoelastischer Medizinprodukte in Deutschland. Die Produkte kommen im medizinischen Alltag unter anderem in der Augenheilkunde (Ophthalmologie) und der Orthopädie zum Einsatz. In der Ophthalmologie stabilisieren sie während chirurgischer Eingriffe empfindliche Strukturen im Auge und schützen das Gewebe – etwa bei Operationen zur Behandlung des Grauen Stars. In der Orthopädie weist Hyaluronsäure ähnliche Eigenschaften wie die natürliche Gelenkflüssigkeit (Synovia) auf. Sie wirkt schmerzlindernd und fungiert im Gelenk als „Schmiermittel“, das die Gleitfähigkeit der Gelenkflächen verbessert. Dadurch kann sie die Beweglichkeit bei Arthrose positiv beeinflussen. Ein Markt mit großem Potenzial – und entsprechend dynamischer Entwicklung.

Neben dem Hauptsitz im fränkischen Schwarzenbruck bei Nürnberg hat Albomed in den vergangenen Jahren den Gründungsstandort im nordrhein-westfälischen Unna weiter auf- und ausgebaut. In zwei Bauabschnitten entstanden dort moderne Produktions- und Logistikhallen. Ein weiterer Ausbau ist schon geplant. Die

beiden bereits fertiggestellten Gebäude bieten auf jeweils rund 1.600 Quadratmetern Platz für etwa 35 Mitarbeitende aus den Bereichen Produktion, Logistik, Verpackung und Verwaltung.

Hygiene und Sicherheit

Die Produktionsprozesse bei Albomed stellen auch besondere Anforderungen an die Sicherheitsinfrastruktur eines Gebäudes. Eine Herausforderung: der Reinraum. Dort muss verhindert werden, dass kleinste Staub- oder Keimpartikel eindringen und in die sensiblen Prozesse gelangen. Daher ist exakt geregelt, wer den Bereich betreten darf – und zu welchem Zeitpunkt. Gleichzeitig sind Medizintechnikunternehmen mit ihren hochwertigen Anlagen und Geräten potenzielle Ziele für Einbruchversuche. Für Sven Reese, Geschäftsführer von Albomed, war daher klar, dass auch die Sicherheitslösung höchsten Ansprüchen genügen muss.

Beim Einbruch- und Brandschutz sowie bei der Zutrittskontrolle nutzt Albomed Technik von Telenot. Als Vollsortiments-Anbieter kann Telenot mit einem wichtigen Trumpf punkten: Alle Komponenten stammen aus einem System und sind

optimal aufeinander abgestimmt. „Es gibt keine Schnittstellen, die überbrückt werden müssen. Alles passt zusammen. Das ist eine wichtige Grundlage für das perfekte Zusammenspiel der einzelnen Bausteine und damit für die Zuverlässigkeit der gesamten Lösung“, erklärt Andreas Haas, Geschäftsführer von Schrödel und Haas Sicherheitstechnik. Das Unternehmen aus der Nähe des Albomed-Stammsitzes in Schwarzenbruck betreut den Medizintechnikhersteller bereits seit mehreren Jahren und hat dort wiederholt Sicherheitslösungen konzipiert und installiert.

Für das Projekt in Unna arbeitete das Unternehmen mit MAB Meldeanlagenbau aus Bissendorf zusammen. „Wir kennen uns seit vielen Jahren, sind beide autorisierte Telenot-Stützpunkte und zudem Teil der Integral Security Gruppe. Die Zusammenarbeit lief deshalb von Anfang an unkompliziert und reibungslos“, berichtet Christoph Siebert, Geschäftsführer von MAB.

Das Herz der Sicherheitslösung

Zentrale Komponente der Anlage ist die Gefahrenmelderzentrale Hiplex 8400 H – das Flaggschiff im Telenot-Portfolio. Dank



Optisch-akustische Signalgeber informieren im Außenbereich laut- und leuchtstark über drohende Gefahren



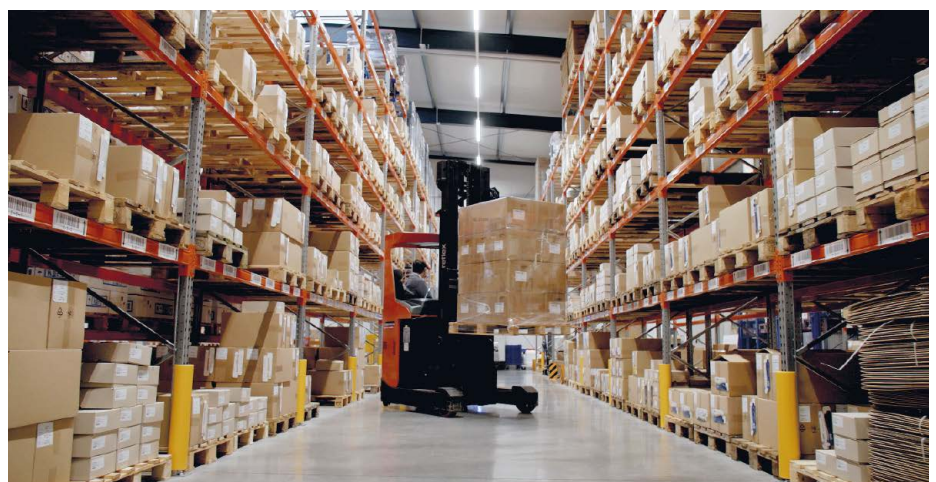
ihrer hohen Flexibilität und Erweiterbarkeit lassen sich mit ihr unterschiedlichste Sicherheitsfunktionen in einem System integrieren. Dazu gehört auch die Zutrittskontrolle, durch die klassische Schlüssel bei Albomed überflüssig geworden sind.

Mitarbeiter öffnen Türen mit individuellen RFID-Chips, die einfach an die Cryptlock-Leser gehalten werden. „Das System erkennt anhand des Chips automatisch, ob eine Person berechtigt ist, einen bestimmten Bereich zu betreten“, erklärt Haas. Sollte ein Chip verloren gehen, wird er einfach aus dem System entfernt. Dies kann der Betreiber über die Verwaltungssoftware sogar selbst vornehmen. Ein teures Auswechseln des gesamten Schließsystems ist nicht notwendig. Die zentrale Steuerung des Zutritts für Gebäudeteile wie Finanzbuchhaltung, Lager, Umkleidebereiche oder den Serverraum erfolgt über das Auswert- und Steuergerät Hilock 5500 von Telenot. Mit diesem lassen sich individuelle Zutrittsregeln für einzelne Türen, Räume oder Mitarbeiter definieren.

Eine Funktion der Hilock 5500 war für Albomed besonders wichtig: In bestimmten Bürobereichen sollten einmal entriegelte Türen für einen festgelegten Zeitraum geöffnet bleiben. „So müssen Mitarbeiter ihren Chip nicht jedes Mal erneut hervorholen“, erläutert Siebert. Erst wenn am Abend die Alarmanlage aktiviert wird, verriegeln sich die Türen wieder automatisch. In sensiblen Bereichen wie der Produktion hingegen muss der Zugang bei jedem Betreten erneut freigegeben werden.

Schutz für Reinräume

In dem Reinraumbereich erfüllt die Zutrittskontrolle zugleich auch eine wichtige Anforderung. Durch eine Schleusenfunktion lässt sich sicherstellen, dass eine Tür zum Reinraum erst geöffnet werden kann, wenn die Tür zur Außenumgebung vollständig geschlossen ist. „So verhindern wir zuverlässig, dass Staub oder Keime in die



Die Lagerhallen sind mit einer Zutrittskontrolle gegen unbefugtes Eindringen geschützt. Im Alarmfall erkennen Bewegungsmelder, wo sich Eindringlinge befinden

sensiblen Bereiche gelangen“, erklärt Haas. Entwickelt wurde diese Lösung gemeinsam mit dem Hersteller der Reinraumanlagen.

Intelligenter Schutz vor Einbruch

In beiden Hallen sorgen verschiedene Bewegungsmelder für zuverlässigen Einbruchschutz. „Je nach Einsatzort haben wir bewährte Comstar-Modelle oder Dual-Bewegungsmelder von Telenot eingesetzt, die mit Infrarot- und Mikrowellentechnik arbeiten“, erläutert Siebert. Zusätzlich überwachen Kontakte an den Rolltoren jeden Versuch, diese unerlaubt zu öffnen. Wird eine Bewegung erkannt, kann das Team von Albomed sofort sehen, in welchem Bereich des Gebäudes ein Alarm ausgelöst wurde. „Für uns ist es entscheidend zu wissen, ob sich jemand beispielsweise in der Produktion, im Lager oder nur im Verwaltungsbereich befindet“, sagt Geschäftsführer Reese.

Früherkennung bei Bränden

Auch der Brandschutz ist integraler Bestandteil der Sicherheitslösung. In den Gebäuden sind zahlreiche optische Rauchmelder installiert, die mithilfe einer Licht-

streuung in einer Rauchkammer zuverlässig Rauchpartikel erkennen. Überschreitet die gemessene Partikelkonzentration einen bestimmten Schwellenwert, löst das System automatisch Alarm aus. In besonders sensiblen Bereichen kommen zusätzlich Mehrsensormelder zum Einsatz. Diese kombinieren optische und thermische Sensorik und werten die erfassten Daten mithilfe intelligenter Algorithmen aus. Eine automatische Lernfunktion sorgt dafür, dass das System auch in anspruchsvollen Umgebungen zuverlässig arbeitet und Fehlalarme minimiert. **GIT**



Telenot Electronic GmbH
www.telenot.com

© Bilder: Telenot

TOP PLAYER

SICHERHEITSMANAGEMENT

Dr. Jens Hartmann

Vice President of Sales – Continental Europe,
Africa & Global Accounts, Advancis

Wie beurteilen Sie die aktuelle Marktentwicklung – und wie positioniert sich Advancis strategisch?

Jens Hartmann: Wenn wir auf die Makrolage schauen, dann läuft die deutsche Volkswirtschaft gerade nicht unbedingt rund. Aber in der Sicherheitsbranche sieht das anders aus. Wir haben Rückenwind durch Regulatorik wie KRITIS und NIS2. Investitionen werden heute nicht mehr nur technisch begründet, sondern über Risiko, Verfügbarkeit, Betriebsfähigkeit und Wirtschaftlichkeit. Und in unserer Nische – Gefahrenmanagement, Integration, Prozessabbildung – sehen wir ein nachhaltiges globales Wachstum von rund 15 Prozent pro Jahr. Das bestätigt uns darin, weiter zu investieren.

Wir haben uns vor zwei Jahren einen Minderheitsinvestor an Bord geholt, um unser internationales Wachstum zu beschleunigen. Gleichzeitig bekommen wir durch unsere globale Präsenz viele Impulse aus anderen Märkten. In den USA und Asien sehen wir zum Beispiel eine viel höhere Geschwindigkeit bei CloudTechnologien und KI. Der deutsche Markt ist konservativer, oft zurecht, aber wir nehmen diese Impulse kontrolliert in unsere Produktentwicklung auf. So stellen wir sicher, dass wir international konkurrenzfähig bleiben und gleichzeitig die Anforderungen des deutschen Marktes erfüllen.

Unsere Erfahrung aus über 2.800 realisierten Leitstellensystemen weltweit hilft uns, diese Anforderungen sehr praxisnah einzuordnen – über Branchen, Regionen und Projektgrößen hinweg.

Viele Betreiber kämpfen mit heterogenen Bestandsanlagen und steigenden regulatorischen Anforderungen. Wo sehen Sie die größten Herausforderungen – und wie unterstützt Advancis?

Jens Hartmann: Die Basistechnologien – Brand, Einbruch, Video, Zutritt – sind in der Fläche vorhanden und auf gutem Niveau. Aber über die Jahre entstehen Wildwuchs und Komplexität: mehrere Brandmeldeanlagen, mehrere Einbruchsysteme, unterschiedliche Hersteller, verschiedene Bedienplätze. Irgendwann stellt sich die Frage: Ist das noch handhabbar? Gleichzeitig rückt Sicherheit durch Regulatorik viel stärker in den Fokus der Unternehmen. Es geht nicht mehr um einen einzelnen Standort, sondern um Cluster, um ganze Unternehmenslandschaften. Die Anzahl der Systeme, die ich im Ereignisfall beherrschen muss, steigt massiv.

Der erste Schritt zur Lösung dieser Herausforderung ist Integration. Ich muss alles zentral sichtbar machen. Genau hier setzen unsere Softwarelösungen WinGuard und AIM an. Aber Integration allein reicht nicht. Unternehmen brauchen eine Abbildung ihrer Sicherheitsprozesse: Was passiert im Ereignisfall? Wer entscheidet? Wer handelt? Wer dokumentiert? Das ist Physical Security Governance – und genau dort liefern wir durch unsere geführten Workflows Mehrwert, der über reine technische Integration hinausgeht.

Wenn Integration und Prozessabbildung zusammenkommen, entsteht Transparenz, Qualität und Geschwindigkeit. Abläufe, Entscheidungen und Maßnahmen werden nachvollziehbar dokumentiert. Damit entsteht zugleich eine belastbare Grundlage für regulatorische Nachweise.

International sehen wir ähnliche Herausforderungen, nur anders gerahmt. In Südostasien spricht man von Smart Cities, im Mittleren Osten von Safe Cities. Aber am Ende geht es immer um hohen Schutzbedarf und hohe Integrationskomplexität. Unsere Produkte funktionieren global – die letzte Meile, also Ansprache, lokale Besonderheiten und Projektumsetzung, lösen wir durch



eigenes Personal in den Regionen gemeinsam mit unserem globalen Partnernetzwerk.

Welche technologischen Entwicklungen treiben Sie aktuell besonders voran – und welche Rolle spielen API-Architekturen, KI und Cybersecurity?

Jens Hartmann: Wir haben mit WinGuard ein starkes Standardprodukt, aber wir wollten mehr Flexibilität, mehr Geschwindigkeit und die Möglichkeit neuer Geschäftsmodelle für uns und unsere Partner. Deshalb haben wir unseren Software-Kern geöffnet und eine standardisierte API geschaffen – die Advancis Open Platform, kurz AOP. Damit können Entwicklungspartner, Systemintegratoren und sogar Endkunden WinGuard erweitern: eigene Schnittstellen bauen, eigene Applikationen entwickeln, individuelle Integrationen umsetzen. Wir haben heute 550 Schnittstellen, entwickeln selbst jedes Jahr 20 bis 30 neue – aber mit AOP können wir das Ökosystem vervielfachen.

Natürlich stellt sich die Frage nach der Sicherheit. Eine API schafft Möglichkeiten, aber auch Risiken. Deshalb ist sie technisch gemanagt, überwacht und eingebettet in unser Security-by-Design- und Security-by-Default-Konzept. Wir betreiben seit Jahren externe Penetrationstests und haben unsere Entwicklungsprozesse darauf ausgerichtet.

Der EU Cyber Resilience Act bestätigt genau diesen Weg.

Parallel treiben wir KI-Themen voran. Wir wollen Errichter bei der Projektkonfiguration unterstützen – schneller, qualitativ besser. Und wir wollen Operatoren in Leitstellen entlasten, gerade bei hohem Ereignisaufkommen. Aber KI darf keine Black Box sein. Sie muss nachvollziehbar und auditierbar bleiben. Wir müssen erklären können, warum ein KI-gestützter Vorschlag entsteht.

Ein weiteres großes Thema ist Cloud Native. Wir transformieren unser Portfolio, damit wir Plattformbetrieb für viele Kunden gleichzeitig ermöglichen. Das schafft Geschwindigkeit, Transparenz und neue Geschäftsmodelle wie Security-as-a-Service. Partner können sich auf Konfiguration, Prozesse und Integration konzentrieren, während Betrieb und Sicherheit der Plattform zur Verfügung gestellt wird.

Wenn Sie fünf Jahre nach vorne blicken – wie wird sich der Markt entwickeln, und welche Rolle wird Advancis spielen?

Jens Hartmann: In fünf Jahren wird KI in Leitstellen selbstverständlich sein. Prozesse werden KI-unterstützt ablaufen, aber nachvollziehbar und auditierbar. Die Komplexität der Systeme wird weiter steigen, und genau deshalb wird Integration kombiniert mit Prozesssteuerung noch wichtiger. Cloudbasierte Plattformen werden sich durchsetzen. Wir werden zentral betreiben, schneller ausrollen, schneller optimieren und neue Funktionen sofort verfügbar machen. Partner werden hybride Modelle nutzen – lokale Server für Schnittstellen, zentrale Plattform für Prozesse und Betrieb.

Geschäftsmodelle werden sich verändern. Nutzungsbasierte Modelle, Security-as-a-Service, flexible Plattformen – all das wird Realität. Geschlossene Systemwelten

geraten dabei zunehmend unter Druck; offene, sichere und skalierbare Plattformen werden zum Standard. Und wir werden uns als Anbieter positionieren, der Technologie, Prozesse, Sicherheit und Skalierbarkeit zusammenbringt. Ich sehe eine Branche, die sich stark weiterentwickelt, aber auch eine Branche, die positive Impulse setzt. KI, Cloud, Automatisierung – das sind keine Bedrohungen, sondern Chancen. Und wir wollen diese Chancen aktiv gestalten.



SicherMacher
Der GIT-Talk mit den Marktführern



Jetzt ansehen:
das vollständige
Interview in unserem
Video-Podcast



Advancis
<https://advancis.net>

Funk-Sicherheitssystem Comfion Pro von Abus

Abus bringt mit der Comfion Pro ein neues Funk-Sicherheitssystem auf den Markt, das Einbruchschutz, Videoüberwachung, Zutrittskontrolle und Smarthome-Funktionen in einer zentralen Lösung bündelt. Das System richtet sich an private Haushalte sowie kleine und mittlere Gewerbebetriebe und ist auf flexible Einsatzszenarien sowie eine einfache Nachrüstung ausgelegt. Mit der Comfion Pro setzt Abus auf die durchgängige Vernetzung bislang häufig getrennt betrachteter Sicherheitsbereiche. Alarmierung, Videoaufzeichnung und Zutrittssteuerung greifen ineinander und lassen sich zentral steuern. Die Nutzer können den Systemstatus jederzeit einsehen, Live-Bilder abrufen und individuelle Szenarien konfigurieren. Die Installation ist kabellos und eignet sich sowohl für Neubauten als auch für die Nachrüstung im Bestand.

www.abus.com



Die Abus Comfion Pro ist ein neues Funk-Sicherheitssystem, das Einbruchschutz, Videoüberwachung, Zutrittskontrolle und Smarthome-Funktionen in einer zentralen Lösung bündelt



HID Converged Credentials vereint physische und logische Identitäten

HID gibt die Einführung von HID Converged Credentials bekannt. Mit der neuen Lösung können Unternehmen ihre Standorte sichern sowie die Identitäten und Credentials der Mitarbeiter über eine einzige, einheitliche Plattform verwalten. HID Converged Credentials wurde entwickelt, um Sicherheitsteams einen einfachen Weg zur Modernisierung ihrer Identitätsarchitektur zu ebnen. Die Lösung konsolidiert physischen und logischen Zugriff in einem einzigen, phishing-resistenten Credential. Außerdem reduziert der ganzheitliche Ansatz die Komplexität, die entstehen kann, wenn Unternehmen Anwendungen mehrerer Anbieter nutzen. Auf diese Weise steigert HID Converged Credentials die Sicherheit von Unternehmen, ohne die bestehende Identitätsinfrastruktur zu beeinträchtigen.

<https://campaigns.hidglobal.com>

TOP PLAYER

MONITORE

Thore Peters

Senior Sales Manager AG Neovo



AG Neovo hat sein Portfolio zuletzt um neue Displayserien für Leitstellen, Videoüberwachung und sicherheitskritische Anwendungen erweitert. Welche Neuerungen sind dabei besonders relevant für moderne SecurityInfrastrukturen?

Thore Peters: Die Basis dieser Systeme bleibt zuverlässigste 24/7 Display-Technologie über Jahre. Darauf aufbauend ist es uns gelungen, eine neue innovative Monitorserie zu launchen. Die 2. Generation der QX-Serie mit 4 K/UHD Auflösung von 27“ bis 65“ beinhaltet neben NeoV-Schutz- & Filterglas, Metallgehäuse sowie Anti-burn-in nun auch eine Dimmbarkeit auf 1 % z. B. mit optionalem Dimmknopf oder Keypad. Des weiteren sind ein vierfach-HDMI Multiviewer zur gleichzeitigen Darstellung verschiedener Systeme sowie verfügbare Tempest- und MIL-Zertifizierungen für Marine, Militär und KRITIS implementiert.

Sie positionieren sich zunehmend als Spezialist für robuste Monitore in sicherheitskritischen Umgebungen wie Leitstellen, Verkehr oder Gesundheitswesen. Welche strategischen Schwerpunkte setzen Sie aktuell, um Ihre Rolle

in diesen anspruchsvollen Märkten weiter auszubauen?

Thore Peters: Die genannte Position möchten wir weiterhin durch unsere professionelle Marktbearbeitung mit Weitsicht ergänzen. Die Herausforderung für AG Neovo ist, das Bewusstsein bei Planern, Integratoren und Anwendern zu schärfen, dass die Bilddarstellung eines Sicherheitssystems inklusive Service und Wartung zur Aufgabe des Sicherheitsmarktes gehört. Um diese Bekanntheit zu steigern, wird es in 2026 einen weiteren Distributionskanal sowie weiterhin eine Hand-in-Hand-Partnerschaft mit marktführenden NDAA-konformen Herstellern anderer Systemkomponenten geben – z. B. auf der Security in Essen im September.

Welche Entwicklungen werden die nächsten Jahre aus Ihrer Sicht die Visualisierung in Sicherheitsanwendungen prägen? Welche Märkte – vertikal und regional – sind für Sie am vielversprechendsten?

Thore Peters: Künstliche, menschliche und systemische Intelligenzen werden Sicherheitslösungen in raschem Tempo

immer vielseitiger werden lassen. Sämtliche sicherheitsrelevanten Aufgaben werden visuell gleichzeitig darstell- bzw. abrufbar sein müssen, was eine thematische Auseinandersetzung mit Multiviewer-Displays und Videowallmanagement für alle Marktteilnehmer mit sich bringt. Nicht nur für die D/A/CH-Region gesprochen, werden Sicherheitsanforderungen weiter wachsen – auch außerhalb klassischer professioneller Vertikalmärkte wie Justiz, Öffentlichkeit, Einzelhandel, Verkehr, Logistik, Industrie, Medizin, Marine und Militär.



AG Neovo
www.agneovo.com

TOP PLAYER

ZUTRITTSKONTROLLE

Mathias Schmid

Leiter Business Development Zutrittskontrolle DACH,
Assa Abloy Sicherheitstechnik

Sie haben jüngst festgestellt, dass drahtlose Zutrittssysteme erstmals kabelgebundene Lösungen überholt haben und mobile Credentials stark wachsen. Welche technologischen und organisatorischen Faktoren treiben diesen Wandel – und wie verändert er die Anforderungen an moderne Sicherheitsinfrastrukturen?

Mathias Schmid: Die Entwicklung ist das Ergebnis mehrerer Trends, die sich in den vergangenen Jahren gegenseitig verstärkt haben. Auf technologischer Seite haben drahtlose Zutrittssysteme inzwischen einen Reifegrad erreicht, der sie für viele Anwendungen zur ersten Wahl macht. Gleichzeitig ermöglichen mobile Credentials eine deutlich einfachere und schnellere Verwaltung von Zutrittsrechten – vom Onboarding neuer Mitarbeitender bis zur temporären Vergabe von Berechtigungen für Dienstleister oder Besucher.

Hinzu kommen organisatorische Anforderungen: Unternehmen erwarten heute flexible Lösungen, die sich ohne aufwendige Verkabelung an veränderte Gebäudenutzungen anpassen lassen. Gerade in Bestandsgebäuden, bei Modernisierungen oder in hybriden Arbeitsumgebungen sind Skalierbarkeit und geringe Installationsaufwände wichtige Kriterien.

Moderne Sicherheitsinfrastrukturen müssen deshalb zunehmend digital, vernetzt und cyberresilient gedacht werden. Die klassische Tür wird zum intelligenten Bestandteil einer übergeordneten Sicherheits- und Gebäudearchitektur. Neben physischer Sicherheit gewinnen Themen wie Identitätsmanagement, mobile Nutzung, Compliance und die Integration in IT- und Gebäudemanagementsysteme an Bedeutung. Wer heute in seine Sicherheitssysteme investiert, fordert integrierte Lösungen ein,

die mit den Anforderungen der eigenen Organisation mitwachsen.

Mit Scala net, eCliq und der Integration von Aperio- sowie Uhlmann & Zacher Komponenten positionieren Sie sich als Anbieter durchgängiger digitaler Zutrittsplattformen. Welche Rolle spielt Interoperabilität künftig – insbesondere in Smart Building Umgebungen mit hohen Anforderungen an Rettungswegtechnik und Gebäudemanagement?

Mathias Schmid: Interoperabilität wird zum entscheidenden Faktor. In Smart Buildings müssen Zutrittskontrolle, Rettungswegtechnik und Gebäudemanagement zuverlässig und nahtlos zusammenspielen. Statt isolierter Insellösungen profitieren Betreiber von Plattformen, die unterschiedliche Technologien und Sicherheitsanforderungen komfortabel zusammenführen.

Deshalb gewinnen offene Schnittstellen weiter an Bedeutung, die elektromechanische, elektronische und drahtlose Komponenten miteinander verbinden. Dank innovativer Möglichkeiten zur Verwaltung über eine einzige Anwenderoberfläche erfüllen diese komplexen Smart-Building Lösungen gleichzeitig höchste Ansprüche an Verfügbarkeit, Sicherheit sowie regulatorische Konformität. Ziel ist eine durchgängige Sicherheitsinfrastruktur, die bestehende Investitionen schützt und gleichzeitig zukünftige Digitalisierungsanforderungen antizipiert.

Welche Entwicklungen werden in den nächsten Jahren aus Ihrer Sicht die Zutritts- und Gebäudesicherheitsbranche prägen? Welche Märkte – vertikal und regional – sind für Sie am vielversprechendsten?



Mathias Schmid: Die Branche wird in den kommenden Jahren von drei Entwicklungen geprägt: der weiteren Digitalisierung des Zutrittsmanagements, steigenden Anforderungen an die Cybersecurity und einer stärkeren Ausrichtung auf Nachhaltigkeit, die ein nicht zu unterschätzendes Investitionskriterium ist. Sicherheitslösungen werden noch viel stärker dazu beitragen müssen, Ressourcen zu sparen und bestehende Infrastrukturen möglichst wirtschaftlich zu modernisieren. Mobile Credentials, Cloud-Services und digitale Identitäten werden bei allen drei Strömungen weiter an Bedeutung gewinnen.

Besonders großes Wachstumspotenzial sehen wir in den Bereichen Gesundheitswesen, Bildung, kritische Infrastrukturen und Industrie. Regional bleibt die DACH-Region ein wichtiger Wachstumsmarkt, zugleich steigt europaweit die Nachfrage nach integrierten Sicherheitslösungen, die physische und digitale Sicherheit miteinander verbinden.



Assa Abloy Sicherheitstechnik GmbH
www.assaabloy.com

TOP PLAYER

VIDEONETZWERKLÖSUNGEN

Rudolf Rohr

Geschäftsführer, Barox

Zu den jüngsten Innovationen bei Barox gehört u. a. die Vertiefung von Switch-Diagnosefunktionen in Plattformen wie dem Gallagher Command Center. Wie verändern Sie mit der erweiterten Netzwerkdiagnose den Alltag von Sicherheitsbetreibern?

Rudolf Rohr: Die zunehmende Komplexität moderner Sicherheitsinfrastrukturen erfordert neue Ansätze im Netzwerkmanagement. Die Integration der Barox-Technologie in führende VMS-/PSIM-Systeme zeigt, wie sich der Betriebsalltag von Sicherheitsbetreibern deutlich effizienter gestalten lässt. Im Mittelpunkt steht die vollständige Transparenz über das Sicherheitsnetzwerk. Werden Switches und IP-Geräte nahtlos in eine zentrale Plattform eingebunden, lassen sich sämtliche Komponenten, von der Zutrittskontrolle bis zur Netzwerkinfrastruktur, direkt überwachen und steuern. So entfällt die sonst oft übliche Verteilung auf mehrere Einzelsysteme. Dadurch können Entscheidungen schneller und auf einer fundierten Datenbasis getroffen werden.

Ein besonderer Vorteil liegt in der schnelleren Fehlerdiagnose. Dank Funktionen wie der Visualisierung der Netzwerktopologie, der automatischen Geräteerkennung sowie integrierte Alarmmeldungen lassen sich Störungen frühzeitig erkennen und gezielt lokalisieren. Das verkürzt die Reaktionszeiten, reduziert Ausfälle und beschleunigt die Behebung von Problemen.

Hinzu kommt der direkte Remote-Zugriff auf Netzwerkkomponenten. Geräte oder einzelne Ports können zum Beispiel aus der Ferne neu gestartet werden, ohne dass ein Vor-Ort-Einsatz nötig ist. Dies senkt nicht nur Kosten, sondern steigert auch die Effizienz und die Arbeitssicherheit.

Durch kontinuierliches Monitoring und integrierte Sicherheitsfunktionen wird ein proaktiver Betrieb möglich. Probleme können erkannt werden, bevor sie den laufenden Betrieb beeinträchtigen, was die Verfügbarkeit und Resilienz der gesamten Infrastruktur nachhaltig verbessert.

Mit der neuen US-Tochter und verstärkten Aktivitäten in Nordamerika verfolgen Sie eine klare Wachstumsstrategie. Welche Besonderheiten des nordamerikanischen Marktes haben Ihre Entscheidung zur Expansion beeinflusst, und wie unterscheiden sich die Anforderungen dort von europäischen Sicherheitsinfrastrukturen?

Rudolf Rohr: Unsere Expansion nach Nordamerika wird vor allem durch die hohe Nachfrage nach skalierbaren und resilienten Sicherheitslösungen getragen. Gerade in den USA sehen wir ein sehr großes Interesse an unseren VMS- und PSIM-Integrationen, mit denen wir als technologischer Vorreiter gelten. Diese Nachfrage hängt eng mit den spezifischen Anforderungen des Marktes zusammen: Typisch sind große, geografisch verteilte Infrastrukturen, bei denen zentrale Steuerung, Remote-Diagnose und hohe Verfügbarkeit entscheidend sind.

Gleichzeitig sind Sicherheitsnetzwerke in den USA deutlich stärker IT-orientiert und meist von Beginn an fest in die gesamte IT-Architektur eingebunden. Das führt zu hohen Anforderungen an Integration, Cybersecurity und Transparenz, ein Umfeld, in dem unsere integrierten Monitoring- und Diagnoselösungen ihre Stärken besonders gut ausspielen können.

Welche technologischen Entwicklungen werden von Ihrer Warte aus im kommenden Jahr die Branche am stärksten prägen? Welche Märkte – vertikal und regional – sind für Sie am vielversprechendsten?

Rudolf Rohr: Aus technologischer Sicht beobachten wir, dass Netzwerke immer mehr zum kritischen Zentrum für alle Sicherheitsanwendungen werden. Dadurch gewinnen Themen wie Cybersecurity, effizientes Netzwerkmanagement und integrierte Diagnosefunktionen deutlich an Bedeutung.

Gleichzeitig sehen wir aber auch einen starken Trend hin zu plattformbasierten Lösungen. Kunden erwarten heute keine voneinander getrennten Einzelsysteme



mehr, sondern tief integrierte Ökosysteme, in denen Video, Zutrittskontrolle und Netzwerkmanagement nahtlos ineinandergreifen. Genau darin sehen wir großes Potenzial für unsere VMS- und PSIM-Integrationen, weil sie eine zentrale und effiziente Steuerung ermöglichen.

Mit Blick auf die Märkte erkennen wir das größte Wachstumspotenzial vor allem in kritischen Infrastrukturen, im Transportwesen sowie bei Behörden. Diese Bereiche stellen besonders hohe Anforderungen an Verfügbarkeit und Sicherheit. Wie bereits erwähnt, ist Nordamerika für uns ein sehr interessanter Markt. Gleichzeitig sehen wir auch in Europa weiterhin großes Potenzial, insbesondere durch steigende regulatorische Anforderungen im Bereich Cybersecurity sowie durch die fortlaufende Modernisierung bestehender Infrastrukturen.



Barox Kommunikation GmbH
www.barox.ch

TOP PLAYER

KI-VIDEO

Thorsten Wallerius

Key Account Team Leader DACH bei Hikvision

Herr Wallerius, wie beurteilen Sie die aktuelle wirtschaftliche Lage und welche Auswirkungen hat sie auf Ihre strategischen Entscheidungen?

Thorsten Wallerius: Die gesamtwirtschaftliche Lage ist derzeit sehr angespannt. Wir sehen ein verhaltenes Wachstum, dazu kommen globale Instabilitäten, insbesondere geopolitische Themen im Nahen Osten. Die Preise steigen überall, Lieferketten werden teurer, und vieles ist schwer kalkulierbar. Gleichzeitig fungieren genau diese Unsicherheiten oft als Katalysator für die Sicherheitsbranche. Investitionen in den Schutz von Werten und Infrastrukturen gewinnen an Priorität.

Für uns bedeutet das: Wir setzen strategisch auf Resilienz und Konformität. Durch die gesetzliche Verankerung von KRITIS steigen die Anforderungen in den Projekten. Das ist für uns positiv, weil wir dafür spezialisierte Produkte haben – etwa Thermalkameras oder zertifizierte Kameras, die höchste IT-Sicherheitsstandards erfüllen. In diesem Bereich sind wir sehr gut aufgestellt.

Welche Herausforderungen erleben Ihre Kunden und Partner aktuell – und wie reagieren Sie darauf?

Thorsten Wallerius: Unsere Partner kämpfen im Moment an drei Fronten. Erstens gibt es eine enorme budgetäre Planungsunsicherheit, die sich aus der wirtschaftlichen Lage ergibt. Zweitens haben wir einen akuten Fachkräftemangel. Viele Errichter und Integratoren fragen uns inzwischen direkt, ob wir technische Mitarbeiter kennen. Und drittens erleben wir einen Generationswechsel in vielen Betrieben, bei dem Knowhow gesichert werden muss. Gleichzeitig wird die Technik komplexer, muss aber intuitiver werden.

Für uns heißt das: Wir müssen weg vom reinen Produktverkauf und hin zur ganzheitlichen Projektbegleitung. Wir steigen möglichst früh in Projekte ein, unterstützen in der Planungsphase und bieten intensiven Wissenstransfer an. Mit einfachen Wartungsmodellen helfen wir, Personalressourcen optimal zu nutzen. So können wir die Herausforderungen unserer Partner ein Stück weit abfedern.

Wo sehen Sie aktuell die größten Wachstumsmärkte und Chancen – auch im Hinblick auf das neue KRITIS-Dachgesetz?

Thorsten Wallerius: Ein massiver Wachstumstreiber ist für uns die Transformation des Einzelhandels. Self-Scan-Kassen und „Tap and Go“-Märkte benötigen deutlich mehr Kameras und intelligenteren Analysen. Auch das Small- und Medium-Business-Segment wird wachsen, weil selbst kleinere Händler zunehmend professionelle Lösungen nachfragen.

Eine große Chance liegt außerdem in der KI-gestützten Prozessoptimierung. Wir betrachten das Videobild nicht mehr nur als Sicherheitstool, sondern als Datenquelle, mit der wir echten Mehrwert für Betriebsabläufe generieren können.

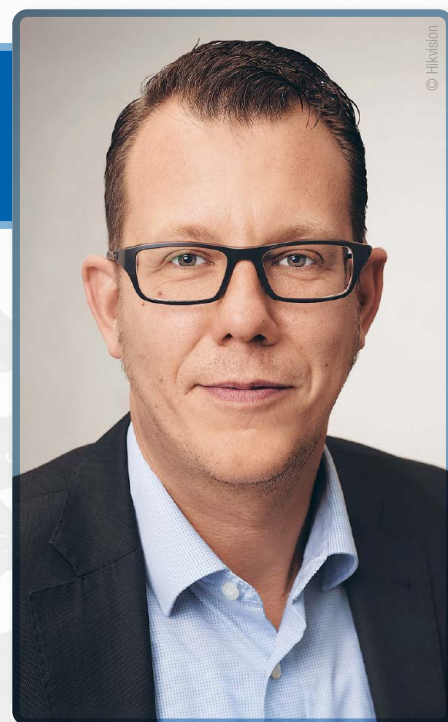
Beim Thema KRITIS rechne ich nicht damit, dass die Projekte sofort starten. Viele Unternehmen müssen zuerst ihre eigenen Daten schützen, Lieferketten prüfen und alternative Lieferanten finden. Erst wenn diese Kernthemen geklärt sind, kommt der Perimeter. Und genau dort sind wir stark: Perimeterschutz mit Thermalkameras ist eines unserer größten Themen.

Welche konkreten technologischen Entwicklungen und Produkte dürfen wir in naher Zukunft von Ihnen erwarten?

Thorsten Wallerius: Das größte Thema ist für uns ganz klar KI. Mit unserer eigenen KI revolutionieren wir die Auswertung. Man geht weg von stundenlangen Recherchen, weil man per Textprompt oder Sprache suchen kann und in Sekundenschnelle die relevanten Dateien oder Personen findet. Das spart ein immenses Zeitfenster.

Außerdem halten KI-unterstützte Chipsets Einzug in unsere Kameras. Sie ermöglichen eine deutlich größere Detektionsreichweite, auch unter extremen Lichtverhältnissen, und reduzieren Fehlalarme – ich will nicht sagen auf Null, aber nahezu gen Null. Das ist ein enorm wichtiger Schritt.

Und natürlich bleibt der Perimeterschutz ein zentrales Thema. Wir sind Hersteller eigener Thermalsensoren und bieten eine



sehr breite und tiefe Produktpalette an. Diese Lösungen werden in Zukunft noch stärker nachgefragt werden.

Wie wird sich der Markt in der DACH-Region in den nächsten fünf Jahren entwickeln?

Thorsten Wallerius: In fünf Jahren wird Sicherheitstechnik ein integraler Bestandteil des Alltags sein – nicht nur für Unternehmen, sondern auch für Privatleute. Der Markt für KI-basierte Sicherheitstechnik wird sich vervielfachen. Wir werden eine Verschmelzung von physischer Sicherheit, IoT und betrieblicher Intelligenz erleben.

Auch im privaten Bereich wird die Akzeptanz für vernetzte Alarm- und Videosysteme deutlich steigen. Mit KI-Unterstützung wird das Ganze intuitiver und stärker in den Alltag integriert. Insgesamt wird Videosicherheit Einzug in den Alltag halten – und das ist ein Trend, den wir sehr klar sehen.



SicherMacher
Der GIT-Talk mit den Marktführern



Jetzt ansehen:
das vollständige
Interview in unserem
Video-Podcast



Hikvision Deutschland GmbH
www.hikvision.com/de

TOP PLAYER

VIDEOSICHERHEIT

Christian Linthaler

CSO Dallmeier

Wie bewerten Sie die aktuelle Marktlage und welche Rolle spielt Sicherheit heute?

Christian Linthaler: Die wirtschaftliche Lage lässt sich derzeit vor allem mit einem Wort beschreiben: Ungewissheit. Geopolitische Spannungen, steigende Kosten und starke Preisschwankungen bei Komponenten wie Servertechnik oder Festplatten erschweren langfristige Kalkulationen erheblich. Gerade bei Projekten mit langen Vorlaufzeiten wird die Planung anspruchsvoller. Gleichzeitig beobachten viele Unternehmen eine gewisse Investitionszurückhaltung.

Dennoch gehört Sicherheit in vielen Branchen nicht zu den Ausgaben, die man beliebig verschieben kann. Besonders dort, wo Sicherheit Voraussetzung für den operativen Betrieb ist, bleibt die Nachfrage hoch. Unternehmen betrachten dabei verstärkt die gesamten Lebenszykluskosten einer Lösung.

Gleichzeitig gewinnen Themen wie Cybersecurity, vertrauenswürdige Lieferketten und europäische Entwicklung zunehmend an Bedeutung. „Made in Germany“ bedeutet dabei nicht nur langlebige Hardware, sondern auch transparente Entwicklungsprozesse und eine konsequente Absicherung gegen mögliche Sicherheitsrisiken.

Welche Herausforderungen beschäftigen die Kunden heute am meisten?

Christian Linthaler: Die Anforderungen an moderne Videosicherheitssysteme haben sich grundlegend verändert. Kunden erwarten längst nicht mehr nur klassische Videoüberwachung zur Dokumentation von Ereignissen. Moderne Systeme sollen analysieren, automatisiert alarmieren und gleichzeitig zur Optimierung betrieblicher Prozesse beitragen.

Videotechnik entwickelt sich zunehmend zu einem optischen Sensor, der wertvolle Daten für unterschiedlichste Unternehmensbereiche liefert. In der Logistik oder Industrie können beispielsweise Bewe-

gungs- und Prozessdaten ausgewertet werden, ohne dass dafür ständig Livebilder betrachtet werden müssen. Informationen über Kundenströme, Auslastungen oder Prozessabläufe können direkt in Analyse- und Business-Intelligence-Systeme einfließen.

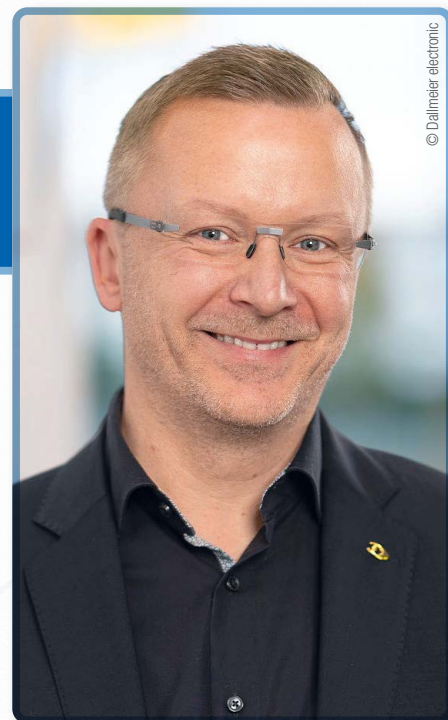
Parallel dazu steigen die Anforderungen an Datenschutz und Cybersicherheit. Unternehmen hinterfragen daher immer stärker, wo Produkte entwickelt werden, wer Zugriff auf Systeme hat und wie Sicherheitsstandards umgesetzt werden.

Eine weitere zentrale Herausforderung ist der Fachkräftemangel. Sicherheitslösungen dürfen deshalb keine zusätzliche Belastung darstellen, sondern müssen Mitarbeiter aktiv entlasten.

Welche Chancen ergeben sich aus neuen Regulierungen und gesetzlichen Vorgaben?

Christian Linthaler: Wir betrachten sie vor allem als Chance. Insbesondere die NIS-2-Richtlinie, der Cyber Resilience Act, der AI Act und das KRITIS-Dachgesetz spiegeln Anforderungen wider, die bei Dallmeier bereits seit Jahren Bestandteil der Produktentwicklung sind. Datenschutz, Cybersicherheit, Transparenz und vertrauenswürdige Technologie gehören zu unseren strategischen Grundprinzipien. Gerade europäische Hersteller können von dieser Entwicklung profitieren.

Besonders attraktive Wachstumsmärkte sind alle Bereiche, in denen Sicherheit unmittelbar für den Betrieb erforderlich ist: Flughäfen, Energieversorgung, Verkehrsinfrastruktur, Stadien sowie industrielle Großanlagen. Ein weiterer Wachstumstreiber ist die Digitalisierung von Sicherheitsprozessen. Video dient zunehmend nicht mehr nur der nachträglichen Dokumentation, sondern wird Teil operativer Entscheidungen und automatisierter Prozesse. Gleichzeitig wächst die Nachfrage nach vertrauenswürdiger Technologie. Kunden interessieren



© Dallmeier electronic

sich heute nicht nur dafür, wo ein Produkt gefertigt wird, sondern auch dafür, wo Forschung und Entwicklung stattfinden.

Welche technologischen Entwicklungen prägen die nächsten Jahre?

Christian Linthaler: Ein wesentlicher Trend besteht darin, immer mehr Intelligenz direkt auf die Kamera zu verlagern. Statt Bilder lediglich aufzuzeichnen, sollen Kameras eigenständig analysieren und relevante Informationen bereitstellen. Unsere Panorama V8 kann zum Beispiel mit einem Sichtfeld von 180 Grad Flächen von bis zu 10.000 Quadratmetern ohne Blindbereiche erfassen. Darüber hinaus gewinnen KI-gestützte Suchfunktionen an Bedeutung. Mit dem sogenannten Attributfinder können Personen anhand von Merkmalen wie Oberbekleidungsfarbe, Hosenfarbe oder Taschen identifiziert werden.

Auch im Perimeterschutz wird künstliche Intelligenz zunehmend leistungsfähiger. Moderne Systeme analysieren nicht nur Objekte, sondern auch Verhaltensmuster. Potenzielle Täter bewegen sich häufig nicht offen über ein Gelände, sondern kriechen, rollen sich ab oder tarnen sich. Solche Verhaltensweisen werden gezielt trainiert, damit die Systeme auch ungewöhnliche Eindringversuche erkennen.

Ein wichtiger Punkt dabei: Selbstlernende KI-Systeme vor Ort sind wenig prak-

tikabel. Entscheidend sind vielmehr hochwertige Trainingsdaten und kontinuierliche Verbesserungen der neuronalen Netze, die anschließend per Software-Update in die Produkte einfließen.

Daneben spielen Cloud-Lösungen eine immer größere Rolle. Dabei sollten die eigentlichen Videodaten weiterhin lokal gespeichert werden, während Verwaltung, Lizenzmanagement und bestimmte Dienste über sichere Cloud-Infrastrukturen bereitgestellt werden.

Wie sieht die Videosicherheit in fünf Jahren aus?

Christian Linthaler: Die Zukunft wird weniger von Einzelprodukten als von integrier-

ten Gesamtlösungen geprägt sein. Kameras, Aufzeichnungssysteme, Managementplattformen und KI-Anwendungen werden immer enger zusammenarbeiten. Gleichzeitig wird Vertrauen zu einem entscheidenden Wettbewerbsfaktor. Künstliche Intelligenz wird eine immer größere Rolle spielen. Allerdings nicht als Ersatz für Menschen, sondern als Assistenzsystem.

Die Leistungsfähigkeit der Hardware wird weiter steigen. Höhere Auflösungen, leistungsstärkere Prozessoren und komplexere Analysen direkt auf der Kamera werden zur Normalität werden. Gleichzeitig bleibt die Herausforderung bestehen, diese technischen Möglichkeiten wirtschaftlich sinnvoll und benutzerfreundlich einzusetzen.

Erfolgreich werden jene Unternehmen sein, die technologische Innovation mit Vertrauen, Qualität und langfristiger Wirtschaftlichkeit verbinden können.



SicherMacher
Der GIT-Talk mit den Marktführern



Jetzt ansehen: das vollständige Interview in unserem Video-Podcast



Dallmeier electronic GmbH & Co KG
www.dallmeier.com

GU BKS Service GmbH erhält ISO 27001-Zertifizierungsempfehlung

Die GU BKS Service GmbH hat das Audit zur ISO/IEC 27001 erfolgreich abgeschlossen und innerhalb des Stufe-2-Audits die Zertifizierungsempfehlung erhalten. Damit bestätigt das Unternehmen die erfolgreiche Einführung und Wirksamkeit eines umfassenden Informationssicherheits-Managementsystems (ISMS) und setzt ein deutliches Signal für höchste Standards in der Informationssicherheit. Die Zertifizierung ist das Ergebnis einer intensiven Vorbereitungsphase und eines mehrjährigen Audits, das den hohen Reifegrad der Sicherheitsprozesse sowie das konsequente Engagement des Unternehmens beim Schutz sensibler Daten eindrucksvoll bestätigt. Ein zentraler Erfolgsfaktor war die enge und wirkungsvolle Zusammenarbeit innerhalb der Unternehmensgruppe Gretsche-Unitas. Besonders hervorzuheben ist die konzernweite Initiative zur Stärkung der Informationssicherheit, die maßgeblich zum Projekterfolg beigetragen hat.

www.g-u.com



www.agneovo.com/de

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

TOP PLAYER

INTEGRIERTE SICHERHEIT

Dr. Falk Herrmann

Geschäftsführer, Funkwerk Security Solutions &
Vorstand Funkwerk-Gruppe

Wie schätzen Sie derzeit die wirtschaftliche Lage insgesamt und die Ihrer Branche insbesondere ein, und welche Rückschlüsse ziehen Sie daraus für Ihre strategischen Entscheidungen?

Dr. Falk Herrmann: Viele Branchen spüren derzeit Investitionszurückhaltung, Kostendruck und Unsicherheit. Sicherheitstechnik ist jedoch kein normaler Investitionsgütermarkt, weil sie in nahezu allen Branchen und der öffentlichen Hand benötigt wird – von Industrie und Bildung über Justiz, Verwaltung, Energieversorgung, Verkehr und Logistik bis hin zu Gesundheitswesen und kritischen Infrastrukturen. Diese breite Basis macht den Markt robust. Gleichzeitig erhöhen internationale Krisen und geopolitische Unsicherheiten die Sensibilität. Betreiber bewerten Risiken neu und fragen stärker nach der Widerstandsfähigkeit ihrer Standorte. Neue regulatorische Anforderungen – etwa im KRITIS-Umfeld – verstärken diesen Professionalisierungsdruck.

Der Markt verändert sich zudem strukturell: Statt einzelner Gewerke wie Video, Zutritt oder Brandmeldung stehen heute integrierte Sicherheitsarchitekturen im Fokus. Wenn jemand einen Serverraum betritt oder

einen Netzwerkschrank öffnet, ist das nicht nur ein physisches, sondern auch ein IT-Sicherheitsereignis. Für unsere Strategie heißt das: Wir investieren in Fähigkeiten – Menschen, Zertifizierungen, IT-Kompetenz, Softwareintegration, Servicefähigkeit und regionale Nähe. Zudem setzen wir auf offene, skalierbare Plattformen, die Investitionssicherheit bieten.

Herr Sohn, Sie erleben diese Veränderungen täglich im Projektgeschäft. Wie kommen sie operativ bei den Kunden an?

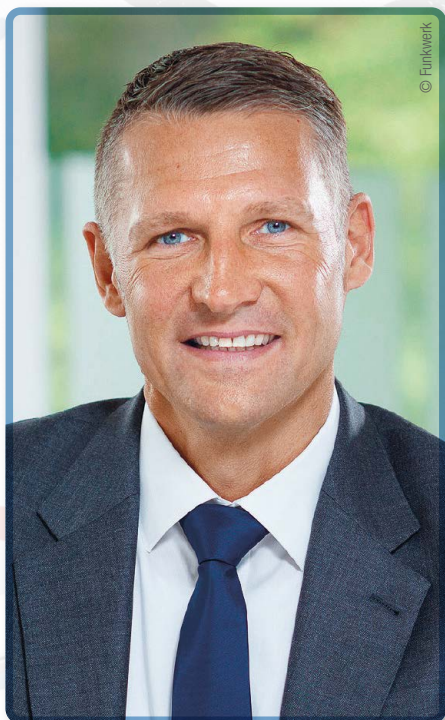
Christian Sohn: Im Projektgeschäft erleben wir diese Entwicklung sehr deutlich. Viele Gespräche beginnen mit einem konkreten Bedarf, doch schnell zeigt sich, dass die Aufgabe größer ist. Häufig existieren historisch gewachsene Systeme verschiedener Hersteller, die technisch funktionieren, aber schlecht integrierbar sind. Unsere Aufgabe ist es, daraus ein System zu machen, das im Alltag funktioniert – im Betrieb, im Störfall und im Ereignisfall. Das erfordert frühzeitige Beratung, Mitplanung, Verständnis für Schnittstellen und IT-Anforderungen sowie verlässlichen Service. Umsetzungskompetenz gewinnt massiv an Bedeutung.

Welches sind die drängendsten Herausforderungen Ihrer Kunden – und welche Anforderungen ergeben sich daraus für Sie als Partner?

Dr. Falk Herrmann: Zu den größten Herausforderungen unserer Kunden zählen eine komplexere Bedrohungslage, hochgradig vernetzte Systeme und fehlende personelle Tiefe. Sicherheitstechnik hängt heute an IT-Infrastrukturen, Softwareplattformen und Datenflüssen. Kunden erwarten daher Beratung, Konzeptionsfähigkeit, Integrationskompetenz und Verlässlichkeit im Betrieb.

Christian Sohn: Am Ende will niemand eine Technik-Show, sondern ein System, das verständlich ist, zuverlässig funktioniert und im Ereignisfall die richtigen Informationen liefert. In größeren Objekten kommen Brandmeldung, Einbruchmeldung, Zutritt, Video, Sprachalarmierung, Perimeterschutz, IT-Netze und Leitstellenprozesse zusammen. Der Nutzen entsteht erst im Zusammenspiel.

Dr. Falk Herrmann: Sicherheitstechnik ist heute Teil der digitalen Infrastruktur. Unsere Rolle verschiebt sich vom Errichter einzelner Systeme hin zum Integrator sicherheits-



Christian Sohn

Geschäftsführer, Funkwerk Security Solutions

kritischer Infrastruktur – mit langfristiger Verantwortung.

Wo sehen Sie derzeit die wichtigsten Wachstumsmärkte?

Dr. Falk Herrmann: Wachstum sehen wir dort, wo Sicherheit, Digitalisierung und Verfügbarkeit zusammenkommen: in kritischen Infrastrukturen, Energieversorgung, Verkehr, Industrie, Justiz und öffentlicher Hand. Dort geht es nicht nur um Objektschutz, sondern um Betriebsfähigkeit und Resilienz. Ein großes Feld ist die Modernisierung bestehender Anlagen. Viele Systeme funktionieren noch, erfüllen aber nicht mehr die heutigen Anforderungen an Vernetzung, Bedienbarkeit, Dokumentation, Cybersecurity und Integration. Kunden wollen selten alles neu machen, sondern bestehende Infrastrukturen weiterentwickeln und Investitionen schützen.

Christian Sohn: Bei Videotechnik etwa geht es nicht nur um Kameras, sondern um Auswertung, Zugriffsrechte, Netzarchitektur, Schnittstellen und Betrieb. Isolierte Lösungen funktionieren heute nicht mehr. Technologisch arbeiten wir intensiv an integrierten Lösungen und am Gefahrenmanagement.

In vielen Objekten laufen Brand- und Einbruchmeldungen, Zutrittsereignisse, Videobilder, technische Meldungen und Daten aus IT- und Gebäudesystemen zusammen. Die Frage lautet: Wie entsteht daraus ein übersichtliches Lagebild? Wie unterstützen wir den Bediener? Wie vermeiden wir Fehler? Unsere Erfahrung mit Lösungen wie ViPRO.gms ist hier zentral. Software ist das Werkzeug, um Technik, Prozesse und Menschen zu verbinden.

Künstliche Intelligenz gewinnt pragmatisch an Bedeutung – etwa bei der Priorisierung von Ereignissen, der Reduzierung von Falsch-Alarmen oder der Echtzeit-Übersetzung in vielsprachigen Umgebungen. Intelligenz entsteht zunehmend direkt in Kameras und Sensoren. Entscheidend bleibt die saubere Einbindung in die Gesamtarchitektur.

Abschließend: Wo sehen Sie Ihren Markt in den nächsten fünf Jahren?

Dr. Falk Herrmann: In fünf Jahren wird der Markt professioneller, integrierter und softwaregetriebener sein. Sicherheitstechnik wird strategisch wichtiger und als Teil von Resilienz verstanden. Die Trennung zwischen Sicherheitstechnik, Gebäudetechnik und IT verschwimmt weiter. Gleichzeitig steigen Anforderungen an Regulierung, Ver-

fügbareit, Cybersecurity und Betreiberverantwortung. Vertrauen wird entscheidend.

Christian Sohn: Wir brauchen mehr Standardisierung, aber auch Verständnis für individuelle Prozesse. Ein Flughafen funktioniert anders als eine JVA oder ein Krankenhaus. Gute Sicherheitstechnik muss diese Realität abbilden.

Dr. Falk Herrmann: Unsere Stärke liegt im Zusammenspiel von klassischer Sicherheitstechnik, IT-Kompetenz, Softwareintegration, Service und operativer Umsetzung. Wenn wir dadurch Komplexität reduzieren und Sicherheit, Verfügbarkeit und Handlungsfähigkeit erhöhen, leisten wir den Beitrag, den der Markt braucht.



SicherMacher
Der GIT-Talk mit den Marktführern



Jetzt ansehen:
das vollständige
Interview in unserem
Video-Podcast



Funkwerk Security Solutions GmbH
Funkwerk-Security.com

TOP PLAYER

ZUTRITTSKONTROLLE

Heiko Viehweger

Vertriebsleiter DACH, Hirsch Secure

Sie haben Ihr Portfolio zuletzt um neue Technologien wie das faseroptische Intrusionsdetektionssystem Lumor- und die Quanergy-LiDAR-Lösungen erweitert. Welche Vorteile bieten diese Systeme für moderne Perimeterschutzanwendungen im KRITIS-Umfeld?

Heiko Viehweger: Mit Lumor- und Quanergy-LiDAR-Systemen haben wir unser Portfolio um zwei technologisch komplementäre Systeme erweitert. Beide Technologien fügen sich strategisch in unseren Best-of-Breed-Ansatz ein: Lumor schließt die Lücke bei der Langstreckenüberwachung linearer Perimeter dort, wo Kamertechnik oder konventionelle PIR-Sensoren an ihre Grenzen stoßen kann. Quanergy Q-Track ergänzt klassische Videoüberwachung durch eine datenschutzkonforme, witterungsunabhängige 3D-Lagebilderfassung ohne Kamerabil-der. In Kombination mit unseren bewährten Lösungen zur Zaundetektion, Videoanalyse und den IR-Lichtschranken können wir KRITIS-Betreibern heute eine vollständig redundante, mehrschichtige Perimeterschutzlösung anbieten, die keine blinden Flecken hinterlässt.

Mit der Gründung von Hirsch Secure bündeln Sie Kompetenz in der Sicherheitstechnik unter einer gemeinsamen Marke. Welche strategischen Ziele verfolgen Sie mit dieser neuen Struktur?

Heiko Viehweger: Wir fassen mit Hirsch Secure die Kompetenz der Tochterunternehmen der Hirsch Group in den Bereichen Perimeterschutz, Zutrittskontrolle, Videoüberwachung und -analyse sowie Identitätsauthentifizierung zusammen – von der Grundstücksgrenze bis in den Kernbereich einer Liegenschaft.

Strategisch verfolgen wir ehrgeizige Ziele: Erstens schaffen wir eine spezialisierte, regional verankerte Organisation, die internationale Innovationskraft mit lokalem Markt- und Regulierungswissen verbindet. Zweitens positionieren wir uns konsequent als One-Stop-Shop für Integratoren und Errichter. Das Ergebnis: Eine schlagkräftige Einheit, die unseren Kunden ein modulares, durchgängig integriertes Sicherheitsportfolio aus einer Hand bietet.

Welche Entwicklungen werden aus Ihrer Sicht in den nächsten Jahren die Sicherheitsbranche prägen? Welche Märkte – vertikal und regional – sind für Sie am vielversprechendsten?

Heiko Viehweger: Drei Entwicklungen werden die Branche maßgeblich prägen: der zunehmende Einsatz von Multisensor-Systemen in der Ereigniserkennung, die wachsenden regulatorischen Anforderungen durch das KRITIS-Dachgesetz sowie die fortschreitende Konvergenz von physischer Sicherheit und Cybersicherheit.



Vertikal sehen wir das größte Potenzial bei kritischen Infrastrukturen – Energie, Bahn, Flughäfen, Rechenzentren und Militär – sowie im industriellen Umfeld. Regional liegt unser Schwerpunkt naturgemäß auf der DACH-Region, wo wir unsere Marktpresenz gezielt ausbauen. International profitieren wir von der globalen Aufstellung der Hirsch Group, die starke Referenzen und erprobte Technologien liefert, und ausgewählten Partnerschaften – eine solide Basis für weiteres Wachstum.



Hirsch Group
www.hirschsecure.com

Leverkusen | 20.10.2026

BHE-ERRICHTER-TAG

Für Inhaber, Geschäftsführer & Führungspersonal

Betriebswirtschaft. Klar. Umsetzbar.

KI sinnvoll nutzen

Fachkräfte gewinnen, binden und motivieren

Haftungsfallen vermeiden

Cyber-Risiken minimieren

Zertifizierungen sinnvoll wählen



Nutzen Sie die Veranstaltung zum Netzwerken und knüpfen Sie neue Kontakte.

**SICHERN SIE SICH JETZT IHREN PLATZ.
20.10.2026**



**KOSTENLOS FÜR
BHE-MITGLIEDER**

TOP PLAYER

PIAM

Alexander Biederer

Director Sales DACH bei ID-ware

Wie bewertet ID-ware die aktuelle Marktlage und welche Auswirkungen haben neue Regulierungen?

Alexander Biederer: Die wirtschaftliche Lage macht es derzeit niemandem leicht. Budgets werden genauer geprüft, Entscheidungen dauern länger und gerade in größeren Unternehmen müssen deutlich mehr Beteiligte eingebunden werden, bevor Investitionen freigegeben werden. Trotzdem verzeichnen wir im Bereich Physical Identity and Access Management ein solides Wachstum. Der Grund ist einfach: Sicherheit wird nicht mehr als optional angesehen.

Hinzu kommen regulatorische Anforderungen. Spätestens mit NIS2 und den weiteren Sicherheitsvorgaben wird das Thema nicht mehr nur operativ betrachtet, sondern zunehmend als Compliance- und Governance-Thema. Unsere Kunden kommen dabei aus nahezu allen Branchen. Entscheidend ist weniger das Geschäftsfeld als vielmehr die Größe und Komplexität einer Organisation. Ob bei Industrieunternehmen, Behörden, Universitäten oder Betreibern kritischer Infrastruktur – überall stellt sich die gleiche Grundfrage: Wie lässt sich physischer Zutritt sicher, nachvollziehbar und regelkonform organisieren?

Welche Herausforderungen begegnen den Kunden heute am häufigsten?

Alexander Biederer: Die größte Herausforderung sind historisch gewachsene Systemlandschaften. Viele Unternehmen arbeiten mit Lösungen, die über Jahre oder Jahrzehnte entstanden sind. Unterschiedliche Systeme existieren nebeneinander, viele Prozesse werden noch manuell durchgeführt und häufig fehlen durchgängige Nachweise.

Gerade bei Audits oder behördlichen Prüfungen wird das problematisch. Die zen-

trale Frage lautet dann: Kann ich lückenlos belegen, wer wann wo Zugang hatte? Und viele Unternehmen stellen fest, dass sie das nicht können.

Die Ursache liegt meist in der Fragmentierung. Es gibt zahlreiche Insellösungen, die nicht miteinander kommunizieren. Informationen liegen verteilt vor, Prozesse laufen manuell ab und die Transparenz fehlt.

Hinzu kommt, dass bestehende Systeme oft zehn, fünfzehn oder sogar zwanzig Jahre alt sind. Niemand möchte diese Investitionen einfach abschreiben. Deshalb suchen die Unternehmen keinen Anbieter, der alles ersetzt, sondern einen Partner, der vorhandene Systeme integriert und modernisiert. Wir betrachten deshalb zunächst, was bereits vorhanden ist, was sinnvoll weitergenutzt werden kann und an welchen Stellen die eigentlichen Probleme liegen. Unser Ziel ist es nicht, alles neu zu machen, sondern Bestehendes in eine moderne Gesamtarchitektur einzubinden.

Wie unterstützt ID-ware Unternehmen bei diesen Herausforderungen?

Alexander Biederer: Der Kern unserer Lösung ist eine zentrale Plattform für Physical Identity and Access Management (PIAM). Unsere PIAM-Suite bringt Credential Management, Access Management, Visitor und Contractor Management zusammen – automatisiert und nachvollziehbar. Der Kern ist dabei immer das Access Management – also wer darf wann wohin. Aber erst wenn ich auch weiß, welche Ausweise im Umlauf sind, wer gerade als Besucher im Haus ist, und wer überhaupt welche Identität hat, bekomme ich wirklich vollständige Kontrolle. Das ist der Unterschied zwischen einer Insellösung und einer echten Plattform.



Die zentrale Frage lautet immer: Wer darf wann wohin? Um diese Frage zuverlässig beantworten zu können, müssen Ausweise, Mitarbeiterdaten, Besucher- sowie Fremdfirmeninformationen und Zutrittsrechte gemeinsam betrachtet werden. Dadurch, dass sämtliche relevanten Informationen auf einer gemeinsamen Plattform zusammenlaufen. So steigt nicht nur die Transparenz, sondern auch der Automatisierungsgrad erheblich. Ein weiterer wichtiger Aspekt ist die Integrationsfähigkeit. Unsere Plattform verfügt über Schnittstellen zu gängigen HR-Systemen, bestehenden Zutrittskontrollsystemen und vielen weiteren Anwendungen.

Wir empfehlen selten einen radikalen Neustart. In den meisten Fällen ist es sinnvoller, zunächst das dringendste Problem zu lösen, schnelle Erfolge sichtbar zu machen und anschließend Schritt für Schritt weitere Prozesse zu integrieren. Auf diese Weise wächst auch das Vertrauen in die Plattform und in den gesamten Transformationsprozess.

Welche technologischen Entwicklungen stehen bei ID-ware derzeit im Mittelpunkt?

Alexander Biederer: Ein zentrales Zukunftsthema ist selbstverständlich künstliche Intelligenz. Wir beschäftigen uns intensiv

damit, an welchen Stellen KI tatsächlich einen praktischen Nutzen erzeugt. Ein vielversprechender Ansatz ist die Erkennung von Anomalien. Das System soll ungewöhnliche Muster selbstständig erkennen und auf Auffälligkeiten hinweisen, bevor Mitarbeiter diese manuell identifizieren müssen.

Ein Beispiel wäre ein Ausweisinhaber, der wiederholt versucht, einen Bereich zu betreten, für den er gar keine Berechtigung besitzt. Ebenso könnten ungewöhnliche Verhaltensmuster in anderen angebundenen Systemen erkannt werden. Die Plattform soll solche Auffälligkeiten proaktiv sichtbar machen und damit die Transparenz deutlich erhöhen.

Gleichzeitig sehen wir einen starken Trend in Richtung Software-as-a-Service. Viele Unternehmen möchten keine komplexen On-Premise-Infrastrukturen mehr betreiben. Sie wollen schneller starten, flexibler bleiben und ohne große IT-Projekte auf

aktuelle Softwareversionen zugreifen können. Besonders im Mittelstand beobachten wir hier eine deutlich steigende Nachfrage.

Wie sieht die Zukunft des Marktes aus?

Alexander Biederer: Wenn ich auf die nächsten fünf Jahre blicke, bin ich überzeugt, dass Physical Identity Management zu einem selbstverständlichen Bestandteil jeder professionellen Sicherheitsarchitektur werden wird. Unternehmen werden künftig nicht mehr akzeptieren, dass Sicherheitsvorfälle erst im Nachhinein erkannt werden. Systeme müssen intelligenter werden, Muster erkennen und Risiken frühzeitig sichtbar machen. Gleichzeitig werden regulatorische Anforderungen weiter zunehmen und immer mehr Branchen erfassen.

Ich glaube deshalb, dass künftig nicht das Unternehmen mit dem besten Einzelprodukt erfolgreich sein wird. Entscheidend

wird sein, wer seine Kunden durch diese Transformation begleiten kann. Es geht um Plattformen, Integration, Beratung und langfristige Partnerschaften. Genau darin sehen wir unseren Anspruch. Wir verfügen über die technologische Basis, das Know-how und die Kundenbeziehungen, um Unternehmen auf diesem Weg zu begleiten.



SicherMacher
Der GIT-Talk mit den Marktführern



Jetzt ansehen:
das vollständige
Interview in unserem
Video-Podcast



ID-Ware Deutschland GmbH
www.id-ware.com

Panomera S4 Skyview für weiträumige Überwachung des Luftraums

Die Panomera S4 Skyview von Dallmeier ist eine Kameralösung, die speziell für die hochauflösende Überwachung des Luftraums an Flughäfen entwickelt wurde. Die besondere Sensorausrichtung ermöglicht eine zuverlässige Erfassung von Bereichen weit oberhalb des Bodenniveaus und erweitert damit gezielt die Einsatzmöglichkeiten moderner Videosicherheitssysteme. Die Panomera S4 Skyview basiert auf der patentierten Multifocal-Sensortechnologie und bietet eine durchgängige Erfassung großer Bereiche bei gleichzeitig hoher Detailtiefe. Durch den großen vertikalen Erfassungswinkel nach oben kann der Luftraum an Flughäfen effizient überwacht werden. Damit eignet sich das System zur Erkennung und Beobachtung von Flugkörpern jeglicher Art. Beispielsweise können Flugzeuge, die sich im Landeanflug oder einer Warteschleife befinden, zuverlässig verfolgt werden. Auch größere Vogelschwärme oder unautorisierte Flugobjekte lassen sich frühzeitig erkennen und bewerten. www.dallmeier.com



Zaunbaumeisterschaft auf der Perimeter Protection

Die Zaunbaumeisterschaft presented by Perimeter Protection ist ein etablierter Branchenwettbewerb, der 2026 erstmals von der Perimeter Protection präsentiert und als Connected Event umgesetzt wurde. Profi-Zaunbauer, Nachwuchskräfte und Teams haben sich in Winsen (Luhe) in spannenden Wettkämpfen gemessen. Das Format vereint Handwerk, Eventcharakter sowie Networking und macht Perimeterschutz auf der Baustelle praxisnah erlebbar. Präzise Handgriffe, hohe Geschwindigkeit und echtes handwerkliches Können: Die Zaunbaumeisterschaft steht seit Jahren für Spitzenleistung im professionellen Zaunbau. 2026 hat der etablierte Branchenwettbewerb nun ein neues Kapitel aufgeschlagen. Erstmals wurde die Zaunbaumeisterschaft von der Perimeter Protection präsentiert und als offizielles Connected Event in das Umfeld der internationalen Fachmesse für Perimeterschutz eingebunden. www.nuernbergmesse.de

TOP PLAYER

SICHERHEITSROBOTIK

Aleksej Tokarev

CEO, Mitgründer und Inhaber von Security Robotics

Herr Tokarev, wie beurteilen Sie die aktuelle wirtschaftliche und sicherheitspolitische Lage – und welche Konsequenzen ergeben sich daraus für Security Robotics?

Aleksej Tokarev: Die Wirtschaftslage befindet sich in einem sehr starken Wandel. Es passiert unglaublich viel – politisch, technologisch, gesellschaftlich. Wir sehen anhand vieler Zahlen, etwa der BDSW-Statistiken, dass der Bedarf nach Sicherheit massiv steigt. Das entsteht nicht von alleine. Menschen spüren Unruhe, sie suchen sichere Orte, sie wollen sich absichern. Genau in diese Richtung bewegt sich die gesamte Wirtschaft.

Wir müssen heute viel stärker auf Sicherheit achten. Wir müssen Stammdaten und Strukturen schaffen, die Resilienz ermöglichen. Wir müssen in der Lage sein, uns abzusichern und rechtzeitig auf Vorfälle zu reagieren. Und genau dafür entwickeln wir unsere Systeme. Unsere Roboter sind seit fünf Jahren im Einsatz, bei jedem Wetter, Tag und Nacht. Für uns ist das Alltag, aber viele Menschen haben Roboter noch nie gesehen. Die Akzeptanz ist noch nicht überall da, aber sie wächst.

Die technologische Entwicklung beschleunigt sich enorm. KI, Automatisierung, vernetzte Systeme – das alles verändert die Sicherheitsbranche grundlegend. Wir sehen uns als Antwort auf diese Veränderungen. Wir wollen Technologie so einsetzen, dass sie Probleme lindert, Anforderungen erfüllt und die Gesellschaft unterstützt.

Welche Herausforderungen erleben Sie bei Kunden, Partnern und Lieferanten – und wie begegnen Sie diesen Anforderungen?

Aleksej Tokarev: Wir bewegen uns in einem Bereich neuer Technologien. Das ist nichts, was man seit Jahrzehnten von der Stange

kaufen kann. Diese Systeme entwickeln sich kontinuierlich weiter. Das bedeutet: Wir arbeiten mit Partnern in einem ständigen Verbesserungsprozess. Roboter verändern sich, Software verändert sich, Sensorik verändert sich – und das über Jahre hinweg.

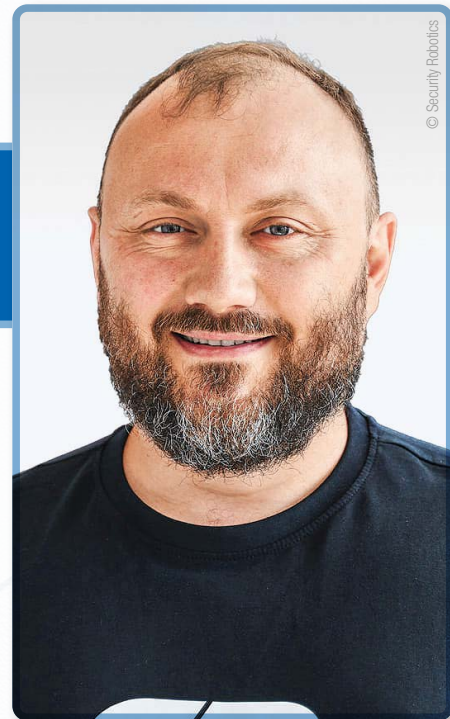
Auf Kundenseite kommen weitere Herausforderungen hinzu: Personalmangel, steigende gesetzliche Anforderungen, neue Regulatorik wie NIS2 oder das KRITIS-Dachgesetz. Wir merken sehr deutlich, dass die Nachfrage aus kritischen Infrastrukturen stark steigt. Wir haben mehrere Projekte, in denen unsere Systeme Wasserwerke, Energieanlagen oder andere kritische Bereiche unterstützen.

Wir bieten keine Einzelkomponenten an, sondern Komplettlösungen. Unsere Roboter führen Sicherheitsaufgaben und Inspektionen parallel durch. Sie messen thermisch, sie können mit Gassensoren ausgestattet werden, sie liefern Daten in Echtzeit. Alles läuft über unsere zentrale Softwareplattform Acuda, die wie eine Schwarmintelligenz funktioniert. Sie verbindet alle Systeme, analysiert Daten, erkennt Anomalien und leitet Informationen an Leitstellen weiter.

Wir arbeiten mit Leitstellenherstellern zusammen, wir erfüllen die Anforderungen von NIS2-Unternehmen, wir durchlaufen Zertifizierungen. Wir sind selbst kein NIS2-Unternehmen, aber wir müssen dieselben Standards erfüllen. Und wir sind sehr weit. Die Anforderungen sind hoch, aber sie sind notwendig – und sie machen unsere Technologie skalierbar.

Wo sehen Sie die größten Wachstumspotenziale – technologisch, geografisch und in Bezug auf neue Einsatzszenarien?

Aleksej Tokarev: Wir wollen deutsche Technologie in Deutschland entwickeln und dann weltweit etablieren. Wenn man eine Technologie in Deutschland durchsetzt, kann man



© Security Robotics

sie überall einsetzen. Die Vorschriften sind hier sehr streng, aber genau das ist ein Vorteil. Wenn wir diese Standards erfüllen, sind wir global einsatzfähig.

Wir sehen enormes Wachstum in kritischen Infrastrukturen, in großen Arealen, in Bereichen, in denen kontinuierliche Beweissicherung notwendig ist. Flughäfen sind ein gutes Beispiel: 24 Kilometer Zaunlinie kann kein Mensch dauerhaft überwachen. Das geht nur technisch – mit Robotern, Sensorik und KI. Personal muss für kritische Entscheidungen eingesetzt werden, Routine-tätigkeiten müssen Maschinen übernehmen.

Inspektion ist ein riesiges Thema. Wenn wir frühzeitig Vorfälle erkennen, sparen wir nicht nur Kosten, sondern verhindern Ausfälle mit enormen Folgeschäden. Unsere Roboter sind autonome mobile Plattformen, ausgestattet mit Sensoren, die Daten in Echtzeit liefern. Die eigentliche Revolution passiert unter der Haube: Physical AI. KI bekommt einen Körper. KI lernt anders, wenn sie in einem Roboter steckt. Sie kann Probleme lösen, die wir Menschen nicht einmal formulieren könnten.

Wir erweitern unsere Systeme ständig. Die Plattform bleibt, aber die Payloads – also die Sensoren – entwickeln sich weiter. Ein Roboter, der nur Personen erkennt oder ein Loch im Zaun meldet, wäre eine Verschwendung. Unsere Systeme können Facility-Management-Aufgaben überneh-

men, Wärmebrücken erkennen, Gebäudeschäden identifizieren, Netzstörungen feststellen. Wir sehen, wenn 5G schwächer wird, wir erkennen Störsender, wir analysieren Anomalien. Das alles ist essenziell für kritische Anlagen. Die Nachfrage wird überall steigen. Überall, wo man auf Google Maps mit dem Finger auf eine Fläche tippt, entsteht Bedarf. Große Areale, Industrie, Energie, Logistik, Flughäfen, Häfen, Rechenzentren – überall dort wird Robotik unverzichtbar.

Wie wird sich die Branche in den nächsten fünf Jahren entwickeln?

Aleksej Tokarev: In fünf Jahren stehen wir ganz woanders. Früher hätte ich gesagt,

fünf Jahre sind eine lange Zeit. Heute sage ich: Mit KI ist das ein Wimpernschlag. KI ist ein riesiger Beschleuniger. Für Ingenieure, für Entwickler, für alle, die damit arbeiten können, ist das ein enormer Vorteil. Wir werden sehr nah mit Robotern zusammenarbeiten – viel näher, als wir es uns heute vorstellen. KI wird Standard sein. Heute ist KI für viele noch fremd oder beängstigend. Aber KI ist ein Werkzeug. Und dieses Werkzeug muss richtig genutzt werden.

Natürlich wird es Menschen geben, die KI nicht ethisch einsetzen. Aber die guten Leute dürfen nicht aufgeben. Wir müssen KI nutzen, um Großes zu schaffen. Physical AI wird uns als Menschheit nach vorne bringen. Wir werden Aufgaben lösen, die heute unlösbar erscheinen.

Ich sehe eine Zukunft, in der Roboter und Menschen selbstverständlich zusammenarbeiten. Vielleicht stehen wir in fünf Jahren nicht auf dem Mars, aber wir werden technologisch dort sein, wo wir heute nicht einmal hinträumen.



SicherMacher

Der GIT-Talk mit den Marktführern



Jetzt ansehen:
das vollständige
Interview in unserem
Video-Podcast

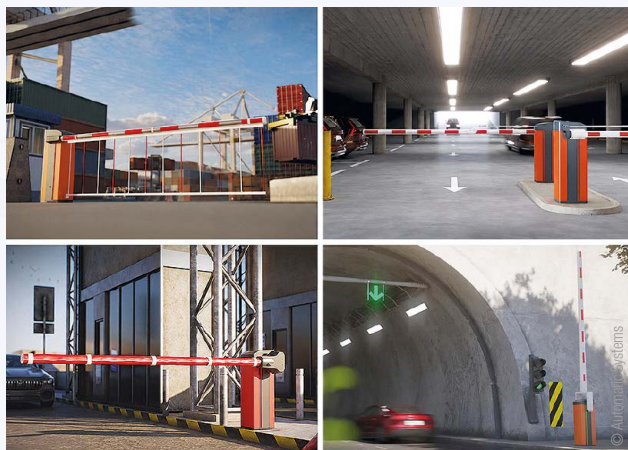


**Security Robotics –
Development & Solutions GmbH**
<https://security-robotics.de>

Schrankenserie AS1 von Automatic Systems

Automatic Systems bringt mit der Serie AS1 eine Schrankenlösung auf den Markt, die Geschwindigkeit, Robustheit und Vernetzung auf höchstem Niveau vereint. Mit intelligentem Design, weitreichenden Anpassungsoptionen und integrierter Steuerungsintelligenz definiert die AS1 die Anforderungen an Effizienz, Sicherheit und Betriebszuverlässigkeit im Bereich der Zufahrtskontrolle neu. Die Serie umfasst vier unterschiedliche Modelle, sodass für jeden Standort und jede spezifische Anforderung die passende Lösung zur Verfügung steht. Die Schranken sind mit einem leistungsstarken bürstenlosen Motor ausgestattet, der auf bis zu 10 Millionen Zyklen ausgelegt ist. Dies sorgt für minimale Wartungsintervalle und hohe Verfügbarkeit selbst unter anspruchsvollen Einsatzbedingungen. Öffnungszeiten ab 0,6 Sekunden beschleunigen den Durchfluss und tragen erheblich zur Reduzierung von Staus sowie zur Optimierung der Verkehrskapazitäten bei.

<https://de.automatic-systems.com>



Assa Abloy zeigte Zutrittslösungen auf der „The smarter E Europe“

Die Assa Abloy Sicherheitstechnik GmbH zeigte auf der „The smarter E Europe“ in München innovative Sicherheits- und Zutrittslösungen. Auf ihrem Messestand zeigten die Experten für Sicherheitslösungen rund um Türen und Türsysteme Lösungen für moderne Schließ- und Zutrittskonzepte – mit besonderem Fokus auf die NIS2- und KRITIS-Dachgesetz konformen Schließanlagenkomponenten der eCliq-Produktfamilie. Die Leitmesse für Energiewirtschaft und Energieversorgung gilt als zentrale Plattform für Zukunftsthemen rund um nachhaltige Energie, intelligente Infrastruktur und vernetzte Technologien. Gerade Betreiber kritischer Infrastrukturen, Energieversorger und Industrieunternehmen stehen dabei vor der Herausforderung, hohe Sicherheitsanforderungen mit flexiblen und effizienten Zutrittsprozessen zu verbinden. www.assaabloy.com/de



Das umfangreiche Produktportfolio von eCliq zählt zu den Schließanlagen systemen, die alle erforderlichen Kriterien und Voraussetzungen für NIS2- und KRITIS-Dachgesetz Konformität mitbringen

TOP PLAYER

SICHERHEITSDIENSTLEISTER

Sven Horstmann

Geschäftsführer Klüh Security

Klüh Security setzt zunehmend auf technologiegestützte Sicherheitslösungen – von digitalen Leitstellen über Echtzeit-Reporting bis hin zu Bodycams und Drohnenunterstützung. Welchen Mehrwert bieten sie Ihren Kunden in Kritis und allgemein in Objektschutzumgebungen?

Sven Horstmann: Die Fragen, die mir Kunden heute stellen, sind andere als noch vor fünf Jahren. Es geht nicht mehr nur darum, wer nachts das Gelände abläuft. Kunden wollen heute wissen, wer den Überblick behält, wenn gleichzeitig ein Alarm in der Notaufnahme eingeht, eine Tür im Rechenzentrum offensteht und die Kamera im Außenbereich etwas meldet. Das können klassische Bewachungsmodelle allein nicht mehr leisten.

Wir setzen deshalb auf eine intelligente Leitstelle, in der alle sicherheitsrelevanten Systeme zusammenlaufen: Brandmeldung, Videoüberwachung, Zutritt, Einbruchmeldung und Außengelände. Und das Ganze auf einer herstellerneutralen Plattform. Die Leitstelle ist rund um die Uhr besetzt und wird VdS-zertifiziert betrieben.

Der Unterschied zur klassischen Technik liegt im Konzept. Eine Anlage meldet einen Alarm. Eine besetzte Leitstelle bewertet ihn und handelt. Das macht den Unterschied zwischen Reaktion und echter Kontrolle. Hinzu kommen mobile Lösungen für den Objektschutz und die Überwachung temporärer Risikozonen: eigene Videoüberwachungseinheiten mit KI-gestützter Analyse, Drohnen mit Wärmebildkameras sowie Echtzeitreporting. Für Kritis-Betreiber kommt eine weitere Dimension hinzu. Wer einen Vorfall lückenlos dokumentiert, ist regulatorisch auf der sicheren Seite. Und genau das ist heute Pflicht.

Sie investieren stark in Qualifizierung, eigene Ausbildungsprogramme und

zertifizierte Qualitätsprozesse. Welche strategische Rolle spielen diese Maßnahmen für Ihre Positionierung im anspruchsvollen Kritis und Objektschutzmarkt?

Sven Horstmann: Wer Sicherheitsdienstleistungen in einem Krankenhaus, einem Rechenzentrum oder einer Energieanlage erbringt, braucht Personal, das mit diesen Umgebungen fachlich, rechtlich und unter Druck umgehen kann. Das ist der Ausgangspunkt unserer Qualifizierungsstrategie.

Wir haben eigene Ausbildungsprogramme entwickelt, die weit über die gesetzlichen Mindestanforderungen hinausgehen. Das zahlt sich aus: in niedrigerer Fluktuation, in höherer Qualität vor Ort und in der Fähigkeit, komplexe Mandate langfristig stabil zu betreuen.

Zertifizierte Prozesse sind dabei kein Selbstzweck. In regulierten Umgebungen sind sie die Grundlage für die Zulassung, das Vertrauen der Kunden und die Nachweispflichten, die NIS-2 und das Kritis-Dachgesetz heute einfordern. Für unsere Kunden bedeutet das Planungssicherheit. Für uns bildet es den Kern unserer Positionierung in einem Markt, in dem Personal der entscheidende Engpass bleibt.

Welche Entwicklungen werden aus Ihrer Sicht die nächsten Jahre der Sicherheitsdienstleistungsbranche prägen? Welche Märkte – vertikal und regional – sind für Sie am vielversprechendsten?

Sven Horstmann: In den nächsten Jahren werden drei Entwicklungen die Branche strukturell verändern. Erstens: Regulierung als Markttreiber. Durch NIS-2 und das Kritis-Dachgesetz sind Betreiber kritischer Infrastrukturen dazu verpflichtet, ihre Sicherheitskonzepte neu zu bewerten



und nachzuweisen. Dadurch entsteht eine Nachfrage nach Dienstleistern, die Schutz, Dokumentation und zertifizierte Prozesse bieten. Dieser Markt wächst.

Zweitens verändert Technologie das Berufsbild. KI-gestützte Analyse, automatisierte Alarmverarbeitung und vernetzte Systeme werden den Anteil rein manueller Tätigkeiten senken. Das bedeutet nicht weniger Personal, aber Personal mit anderen Qualifikationen. Wer heute nicht in Qualifizierung investiert, wird diesen Wandel nicht mitgehen können.

Drittens: Konsolidierung im Markt. Der Fachkräftemangel sowie steigende Anforderungen an Technologie und Zertifizierung werden kleinere Anbieter unter Druck setzen. Für integrierte Dienstleister mit eigener Infrastruktur ist das eine Chance.

Das größte Wachstumspotenzial sehen wir vertikal in den Bereichen Rechenzentren, Gesundheitswesen und Energieversorgung. Regional liegt unser Fokus auf dem deutschsprachigen Raum mit dem klaren Ziel, in den von uns besetzten Segmenten Marktführer zu sein.



Klüh Service Management GmbH
www.klueh.de

TOP PLAYER

ZUTRITT & ID-MANAGEMENT

Axel Schmidt

Geschäftsführer Salto Systems

Von Salto IDM bis zu cloudbasierten Plattformen: Ihre Lösungen adressieren zunehmend KRITIS-Anforderungen. Welche Funktionen werden für Betreiber kritischer Infrastrukturen unverzichtbar?

Axel Schmidt: Die regulatorischen Vorgaben aus z. B. NIS2 und KRITIS-Dachgesetz verschieben die Anforderungen von punktuellen Sicherheitsmaßnahmen hin zu ganzheitlichen, nachweisbaren Sicherheitsprozessen. Entscheidend sind dabei aus unserer Sicht drei Fähigkeiten: identitätsbasierte Steuerung, systemseitige Sicherheit und vollständige Transparenz. Mit unseren Lösungen erfüllen Anwender nicht nur die gesetzlichen Vorgaben, sondern erreichen darüber hinaus eine effizientere Gebäudewirtschaft als bspw. mit mechanischen Schließsystemen.

Mit der Einführung von Salto Wecosystem und der neuen globalen Struktur richtet sich Ihr Unternehmen strategisch neu aus. Welche Vorteile erwarten Sie für Innovation, Marktdurchdringung und die Zusammenarbeit Ihrer drei Kernmarken?

Axel Schmidt: Wir entwickeln uns von einer Gruppe einzelner Unternehmen hin zu einem integrierten Ökosystem. Ziel ist eine noch engere Verzahnung unserer Kompetenzen. Ein Beispiel dafür ist unsere Gesichtserkennungslösung XS4 Face, die

aus der Zusammenarbeit verschiedener Einheiten innerhalb des Unternehmens hervorgegangen ist und das Potenzial dieser vernetzten Innovationsstruktur zeigt.

Damit verändert sich zugleich unsere Positionierung in Richtung Lösungsanbieter. Statt einzelner Produkte rücken integrierte Systeme in den Mittelpunkt, die verschiedene Anwendungen, Technologien und Services miteinander verbinden. Für Kunden und Partner wird es damit einfacher, komplexe Anforderungen abzudecken und von einem ganzheitlichen Ansatz zu profitieren.

Welche Entwicklungen werden aus Ihrer Sicht die nächsten Jahre der Zutritts- und Identity-Managementbranche prägen? Welche Märkte – vertikal und regional – sind für Sie am vielversprechendsten?

Axel Schmidt: Anwender erwarten zunehmend Lösungen, die verschiedene Funktionen und Prozesse miteinander verbinden und sich nahtlos in bestehende IT- und Gebäudestrukturen einfügen. Auf diese Entwicklung haben wir durch unsere Plattformansätze und integrierten Lösungen reagiert. In diesem Zusammenhang wird eben auch Compliance zum Innovationstreiber, weil sie Investitionen in neue Technologien und digitale Prozesse beschleunigt. Dementsprechend sehen wir insbesondere bei KRITIS-Betreibern und KRITIS-nahen Anwendern eine sehr großes Potenzial.



Gleichzeitig eignen sich unsere Lösungen für ein breites Spektrum von vertikalen Märkten. Daher sind wir überall da aktiv, wo wir Endkunden unterstützen können, ihre Zutritts- und Identitätsprozesse effizient, sicher und flexibel zu gestalten.

Wir sehen außerdem in mobilen Technologien einen wesentlichen Treiber. Das Smartphone ist ein Funktions-Hub für Nutzer, der immer mehr Anwendungen einbezieht. Die Zutrittskontrolle gehört hier ebenfalls dazu, um nahtlose digitale Prozesse zu ermöglichen oder zu vervollständigen.



Salto Systems GmbH
<https://saltosystems.com/de-de>

Hochauflösende Wärmebildfunktion trifft auf 4 K-Bildsensor

Axis Communications bringt mit der Axis Q2802-E Bispectral Camera eine All-in-One-Netzwerkamera auf den Markt, die einen hochauflösenden Wärmebild- mit einem visuellen 4K-Sensor kombiniert. Die Bispektralkamera detektiert Objekte zunächst per Wärmebildanalyse und bestätigt die Detektion anschließend anhand des visuellen Bildes. Damit eignet sich die Kamera insbesondere für Anwendungsszenarien, in denen die zuverlässige Detektion und visuelle Verifizierung von Objekten für den Perimeterschutz in weitläufigen Außenbereichen entscheidend ist.

Die All-in-One-Bispektralkamera Q2802-E ist mit einem hochauflösenden VGA-Wärmebildsensor mit einer thermischen Empfindlichkeit von weniger als 20 Millikelvin (NETD kleiner als 20 mK @25 °C, F1.0) ausgestattet und bietet damit eine besonders niedrige Falschalarmrate. Die Wärmebildtechnologie kombiniert der Hersteller in diesem Gerät zudem mit einem präzisen 4K-Bildsensor und vier Objektivoptionen für breitere und schmalere Sichtfelder. Eine Bildfusionsfunktion vereint die thermischen und visuellen



Die Axis Q2802-E Bispectral Camera ist eine All-in-One-Netzwerkamera, die einen hochauflösenden Wärmebild- mit einem visuellen 4 K-Sensor kombiniert

Aufnahmen der Kamera dabei nahtlos in einem Videostream, indem sie die Daten aus beiden Quellen zu einem umfassenden Gesamtbild zusammenfügt. Das Ergebnis ist eine deutlich verbesserte Informationsdichte, die Sicherheitsverantwortlichen eine schnellere Bewertung der Situation und somit eine

gezieltere Reaktion auf potenzielle Vorfälle ermöglicht.

Unterstützt wird dies durch zusätzliche Funktionen, die das Situationsverständnis verbessern: So kann die vorinstallierte Analyse-Software Axis Object Analytics Objekte direkt im Bildausschnitt erfassen, erkennen, klassifizieren, verfolgen und zählen. In anspruchsvollen Anwendungsszenarien, in denen es auf einen noch umfassenderen Perimeterschutz ankommt, ermöglicht die separat erhältliche Analyse-Software Axis Perimeter Defender zudem eine zuverlässige Detektion von Personen und Fahrzeugen über große Distanzareale hinweg im Wärmebild-Stream.

Diese leistungsstarken, KI-gestützten Analysefunktionen kann die Kamera über eine integrierte Deep-Learning-Verarbeitungseinheit (DLPU) direkt auf dem Gerät („on the Edge“) ausführen. Die entsprechenden Daten werden lokal verarbeitet, was die Anforderungen hinsichtlich Datenübertragung, Bandbreite und Serverkapazitäten – und damit deren Kosten – deutlich reduziert.

www.axis.com



Salto XS4 Face mit German Innovation Award 2026 ausgezeichnet

Salto ist für seine Gesichtserkennungslösung XS4 Face mit dem German Innovation Award 2026 ausgezeichnet worden. Der renommierte Preis würdigt branchenübergreifend Produkte, Technologien und Dienstleistungen, die durch zukunftsweisende Ideen und einen besonderen Mehrwert für Nutzer überzeugen. Die Lösung ermöglicht einen sicheren, berührungslosen Zutritt ausschließlich über biometrische Gesichtserkennung. Mechanische Schlüsseln, Karten oder mobile Endgeräte werden überflüssig, wodurch sich Zutrittsprozesse deutlich vereinfachen und gleichzeitig sicherer gestalten lassen. Das Risiko verlorener oder gestohlener Zutrittsmedien entfällt vollständig. XS4 Face ist als skalierbare Lösung konzipiert und eignet sich für unterschiedlichste Anwendungen – von Bürogebäuden bis hin zu komplexen, vernetzten Infrastrukturen.

www.saltosystems.de

Sicherheitstechnik für Juweliere, Pfandleihhäuser und Goldankäufer

Die Chubb Deutschland GmbH bietet mit den intelligent vernetzten Connected Services einen ganzheitlichen Ansatz, der Sicherheitsprozesse zentralisiert, automatisiert und nachweisbar macht. Insbesondere Juweliere, Pfandhäuser und Edelmetallhändler agieren in einem sicherheitstechnisch hochsensiblen Umfeld. Connected Services basieren auf der intelligenten Vernetzung verschiedener Sicherheitssysteme – darunter Einbruch- und Überfallmeldetechnik, Videoüberwachung, Zutrittskontrolle sowie Brandmeldeanlagen. Alle Systeme laufen zentral in der zertifizierten Chubb Notruf- und Serviceleitstelle in Dresden zusammen. Dort verifizieren geschulte VdS-zertifizierte Disponenten eingehende Meldungen in Echtzeit und leiten anhand definierter Interventionspläne unmittelbar passende Maßnahmen ein. Die Kombination aus Technologie und menschlicher Bewertung ermöglicht schnelle, maßgeschneiderte und revisionssichere Reaktionen.

www.chubbfs.com/de-de



GIT **SICHERHEIT**

INNENTITEL – SECURITY



interflex 
UPGRADES YOUR WORK

Die größte Sicherheitslücke in vielen Unternehmen ist das System, das man nicht hinterfragt. Wer den Sprung zur ganzheitlichen Zutrittskontrolle aus Sorge vor baulichem Chaos scheut, riskiert heute mehr denn je. Die Kombination aus smarter Plattform-Logik und kabellosen Schließkomponenten bietet einen Weg aus dem Dilemma. Ein Beitrag von Robert Karolus, Product Manager Devices bei Interflex Datensysteme.

INNENTITEL

Von Kellertür bis Haupteingang

Wie man die (Zutritts-) Kontrolle zurückgewinnt

Das Bild in vielen deutschen Unternehmen ist paradox: Am Haupteingang glänzt modernste Sicherheitstechnik mit vernetzten Drehkreuzen und Kameras. Doch nur wenige Meter weiter, in den Nebenfluren regiert die Vergangenheit. Hier klappern mechanische Schlüsselbünde oder veraltete elektronische Schließanlagen. In der Verwaltung der Zutrittsrechte herrschen manuelle Prozesse, sind Zuständigkeiten unklar. Die Folge: verliert ein Mitarbeiter seinen Schlüssel, beginnt das Hoffen, dass nichts passiert.

Für Chief Information Security Officer (CISO) und Facility Manager ist dieser Zustand ein Albtraum. Sicherheit muss heute lückenlos nachweisbar und auditfähig sein. „Blinde Flecken“ solcher Insellösungen

sind ein unkalkulierbares Risiko. Die Sorge vor einer Fehlentscheidung, ausufernden Kosten und einem System-Chaos im laufenden Betrieb führt dazu, dass wichtige Entscheidungen verschoben werden – und damit das Sicherheitsrisiko bestehen bleibt.

Die „Alles-oder-nichts“-Illusion aufbrechen

Diese Zurückhaltung basiert auf einem weit verbreiteten Irrglauben: Viele Unternehmen denken Zutrittskontrolle noch immer von der Tür aus. Sie glauben, eine ganzheitliche Lösung bedeute, jede einzelne Tür im Gebäude aufwendig verkabeln zu müssen. Weil das unwirtschaftlich ist, bleibt man bei Insellösungen – und nimmt den organisato-

rischen Ausnahmezustand zähneknirschend in Kauf.

Moderne Zutrittskontrolle erfordert jedoch keinen Komplettumbau, sondern einen Paradigmenwechsel. Als Experte für ganzheitliche Sicherheitslösungen rät Interflex Datensysteme zu einem pragmatischen Ansatz: Analysieren (Wo fehlen Übersicht und Kontrolle?), Priorisieren (Kritische Zugänge zuerst absichern) und Erweitern (Bestehende Strukturen nutzen und Lücken gezielt schließen). Zutrittskontrolle darf nicht von der Tür, sondern muss von der Organisation aus gedacht werden. Das Prinzip lautet: Nicht jede Tür braucht teure Technik – aber jede Tür braucht eine zentrale Regel.

Das Fundament dafür bildet die Management- und Systemplattform IF-6040 als die zentrale Steuerungssoftware für alle rollenbasierten Zutrittsberechtigungen. Ändert die HR-Abteilung beispielsweise die Rolle eines Mitarbeitenden aufgrund eines Standort- oder Abteilungswechsels, ändern sich die entsprechenden Zutrittsrechte automatisch – ohne manuelle Aufwände.

Der pragmatische Ermöglicher in der Fläche

Doch wie integriert man die restlichen Türen – die abgelegenen Büros, Bestands-

Schnelle Montage und moderne Technik: Mit der Funktion der freien Spindwahl lassen sich bis zu 50 Spindschlösser komfortabel ansteuern



Hohe Effizienz: Bluetooth Low Energy ermöglicht – je nach Gebäudebeschaffenheit – eine Reichweite von bis zu 50 Metern zwischen Gateway und Schließkomponente

bauten oder Low-Traffic-Bereiche – in dieses zentrale System, ohne Wände aufzureißen? Genau hier schließt Interflex die Lücke mit der Produktlinie Opendor.

Die Air-Variante von Opendor ist kein isoliertes Hardware-Produkt, sondern der Baustein, der ganzheitliche Sicherheit erst realistisch und bezahlbar macht. Die batteriebetriebenen, kabellosen Schließkomponenten (wie Zylinder, Türbeschläge und -drücker bzw. Spind- und Vorhängeschlösser) lassen sich in wenigen Minuten installieren. Die technische Raffinesse liegt in der nahtlosen Anbindung: Über Gateways kommunizieren die kabellosen Komponenten direkt mit dem IF-6040 System.

Das Ergebnis: flächendeckende Kontrolle ohne umfangreiche Baumaßnahmen und aufwendige Verkabelungen. Selbst bei einem Netzwerkausfall sorgt ein dreistufiges Sicherheitskonzept dafür, dass Gateways und Schließkomponenten autonom weiterarbeiten und die Zugänge gesichert bleiben.

Ganzheitlich aus der Praxis

Dass die Kombination aus zentraler Plattform und kabelloser Opendor-Technologie in der Praxis funktioniert, zeigen Unternehmen unterschiedlichster Branchen wie etwa diese:

■ **Der stark wachsende Maschinenbauer:** Ein süddeutscher Weltmarktführer im Maschinenbau kämpfte durch rasantes Wachstum mit einem massiven Verwaltungsaufwand bei mechanischen Schlüsseln. Mit Interflex wurde das Prinzip „Ein Ausweis für alles“ eingeführt. Neben der vernetzten Zutrittskontrolle an den Außentüren wurden an die Innentüren mit kabellosen Opendor-Zylindern ausgestattet. Der Schlüssel-Verwaltungsaufwand für das Facility Management sank drastisch. Bei Verlust eines Ausweises reicht nun ein einziger Klick im System, und die Karte ist in Sekundenschnelle gesperrt.

■ **Der globale Technologiekonzern:** Ein international agierendes Hightech-Unternehmen mit sensiblen Forschungsbereichen benötigte eine lückenlose Nachweisbarkeit. Statt Gebäude aufwendig umzubauen, nutzte der Konzern Opendor air, um die bestehende, verkabelte Interflex-Infrastruktur tief in die Gebäude hineinzuverlängern. Wegen strenger Sicherheitsvorgaben wurden selbst die Umkleideschränke der Mitarbeiter mit Opendor-Spindschlössern versehen. Über die „Self Select“-Funktion buchen sich die Angestellten ihren Spind einfach mit dem Firmenausweis.

■ **Der expandierende Industriehersteller:** Ein führender Hersteller von Industriebauteilen erweiterte seinen Campus um neue Logistik- und Produktionshallen. Die Herausforderung: Ein Mix aus stark frequentierten Toren und wenig genutzten Innentüren. Die Lösung war ein hybrider Ansatz. Online-Terminals sichern die Peripherie, während Opendor die Kosten für die Absicherung der Innenbereiche massiv senkte.

Sicherheitsrisiko Komplexität

Wer heute noch versucht, fragmentierte Systeme und mechanische Schlüssel manuell zu verwalten, verliert unweigerlich die Kontrolle. Interflex bietet mit der IF-6040 Plattform und den smarten Opendor-Komponenten einen schrittweisen, pragmatischen Wachstumspfad an, bei dem Unternehmen ihre Zutrittskontrolle unterbrechungsfrei und ganzheitlich modernisieren und erweitern können. **GIT**



Interflex Datensysteme GmbH
www.interflex.com



Moderne Haustüren mit dunklen Oberflächen heizen sich in der Sonne stark auf – das Material arbeitet, und der Türflügel kann sich verziehen

ZUTRITT

Automatisch verriegelt

Intuitive Sicherheit für Gebäudezugänge

Automatische Mehrfachverriegelungen koppeln den gesicherten Zustand direkt an den Schließvorgang. Ein Beispiel dafür ist die Automatik-Türverriegelung Auto Lock AV4D von Winkhaus, die sich bei Bedarf um die motorische Lösung Blue Matic EAV ergänzen lässt.

■ Die Wohnungstür ist der zentrale Kontrollpunkt zwischen Innen und Außen. Deshalb gelten für deren Sicherheit spezielle Normen und Richtlinien, die bei der Planung berücksichtigt werden müssen. Im Alltag ist oftmals jedoch ein kleiner Moment entscheidend: Wird die Tür nur zugezogen oder wirklich verriegelt? Denn wenn der Schlüsseldreh ausbleibt, entsteht zwischen geplantem und tatsächlichem Schutzniveau eine Lücke, die sich mit Routine allein kaum schließen lässt.

Die tatsächliche Nutzung einer Wohnungs- und Eingangstür entspricht im Alltag nicht immer den angedachten Sicherheitsstandards. Offizielle Konzepte und Richtlinien sehen eine verriegelte Haustür als Regelfall vor – oftmals zeigt sich aber ein anderes Bild: Türen werden nur zugezogen, insbesondere bei kurzen Wegen und hoher Nutzungsfrequenz. Das aktive Abschießen mit dem Schlüssel findet im Alltag häufig

nicht statt, obwohl die Tür dafür ausgelegt ist. Aus diesem Unterschied zwischen vorgesehenem und tatsächlichem Umgang mit der Haustür entsteht immer wieder dieselbe Sicherheitslücke.

Gleichzeitig soll die Tür mehr leisten als nur schließen: Sie soll leise laufen, dauerhaft dicht bleiben und sich mit geringem Kraftaufwand bedienen lassen. Sonne und Temperaturwechsel setzen dem Material zu, der Flügel arbeitet, das Öffnen kann schwerer werden. Vor allem dunkle Haustüren erhitzen sich im Sommer stark und neigen eher zum Verzug. In dieser Mischung aus Verhalten und Technik entscheidet sich, wie sicher ein Gebäudezugang tatsächlich ist.

Zwei Ansätze für eine sichere Haustür

Es gibt zwei Wege, um einen sicheren Zustand an der Haustür zu erreichen: Der vertraute Ansatz setzt auf das aktive

Abschließen mit dem Schlüssel. Er ist technisch unkompliziert, verlangt aber bei jedem Weg durch die Tür Aufmerksamkeit und bewusstes Handeln.

Die andere Option verlegt den gesicherten Zustand in den Schließvorgang selbst. Die Tür erreicht beim Zuziehen ein höheres Schutzniveau, auch wenn der Schlüssel nicht aktiv umgedreht wird. So sinkt die Abhängigkeit vom menschlichen Faktor, und es entsteht ein Grundsicherheit, der der tatsächlichen Nutzung entspricht. Dabei stellt sich jedoch die Frage, wie Komfort und eine geordnete Zugangsorganisation bewahrt werden können.

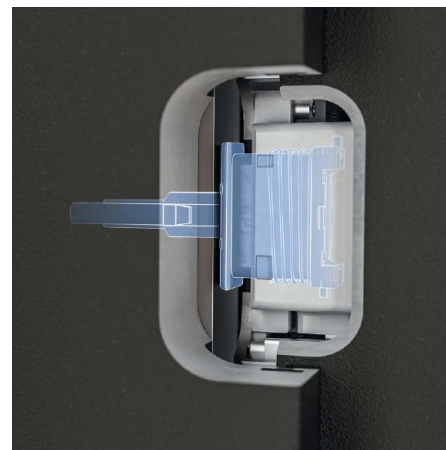
Genau dort setzt Winkhaus an: Auto Lock AV4D ist eine mechanische Automatik-Mehrfachverriegelung, die den gesicherten Zustand in den Schließvorgang verlegt. Türen verriegeln beim Zuziehen automatisch, liegen stabil im Rahmen und bleiben leichtgängig. Die Verriegelung eignet sich für moderne Haustüren aus Kunststoff, Holz



Die Dichtigkeitselemente von Auto Lock AV4D halten den Türflügel in einer definierten Endlage, sorgen für einen dichten Abschluss und wirken Verzugstendenzen entgegen



Die Tagesfalle erhöht den Komfort und sorgt dafür, dass eine Tür vorübergehend unverriegelt bleibt



Der rahmenseitige Magnetauslöser erkennt die bündig geschlossene Tür und startet erst dann die Verriegelung

und Aluminium – unabhängig davon, ob es sich um helle oder dunkle Oberflächen handelt.

„Die Mehrfachverriegelung verriegelt die Tür zuverlässig und möglichst dicht – schon beim Zuziehen, ohne dass man mit dem Schlüssel abschließen muss“, sagt Torsten Meyer, Leiter Produktmanagement Sicherheits-Tür-Verriegelungen bei Winkhaus. Ein zentral liegender Magnetauslöser ist für den leichtgängigen Schließmechanismus verantwortlich und verhindert effektiv Fehlbedienungen.

Wer zusätzlichen Komfort oder eine Anbindung an Zutrittskontrollsysteme wünscht, kann die mechanische Basis dank modularer Bauweise um die motorische Entriegelung Blue Matic EAV ergänzen. So entsteht ein System, das für Sicherheit im Alltag sorgt und sich bei Bedarf um Komfortfunktionen erweitern lässt.

Funktionsweise von Automatik und Motorik

Die Automatik setzt an einem klar definierten Punkt an: Erst wenn der Türflügel bündig im Rahmen anliegt, erkennt der rahmenseitige Magnetauslöser die geschlossene Position und startet den Verriegelungsvorgang. So lassen sich Fehlbedienungen vermeiden und Schleifspuren an den Schließblechen reduzieren. Auto Lock AV4D arbeitet dabei mit zwei zentralen Komponenten: Dichtigkeitselementen für den Anpressdruck und massiven Schwenkriegeln. Beim Zuziehen der Tür werden zunächst die Dichtigkeitselemente ausgelöst, sie halten das Türblatt in einer definierten Endlage und stabilisieren es im Rahmen. Anschließend fahren die Massivschwenkriegel aus, greifen tief hinter die Schließbleiste und sind gegen Zurückdrücken gesperret. Die Tür ist damit dicht verriegelt, ohne dass Nutzende zwingend nachriegeln müssen.

Wer darüber hinaus Zugänge geordnet steuern möchte, kombiniert AV4D mit der motorischen Lösung Blue Matic EAV. Innen bleibt die Bedienung über den Türdrücker vertraut, außen steuert ein Zutrittssystem die Freigabe – beispielsweise per Finger-Print, Code, Transponder, Funk oder über die Türsprechanlage. Die mechanische Automatik stellt den sicheren Grundzustand her, die Motorik ergänzt ihn um Komfort und Steuerbarkeit. Bei vorbereiteten Türen ist eine Nachrüstung möglich. „Auf dieser Basis können Betreiber Sicherheit und Komfort schrittweise ausbauen: von der rein mechanischen Automatik bis zur motorischen Lösung mit Zutrittskontrolle“, betont Torsten Meyer.

Alltagstaugliche Funktionen

Sicherheitstechnik muss zum Alltag passen. Mit der Tagesfalle Ta Fa kann die Tür kurzfristig unverriegelt bleiben. Das ist unter anderem dann von Vorteil, wenn häufig ein- und ausgegangen wird oder Einkäufe ins Haus getragen werden. Die Umstellung erfolgt direkt an der Tür mittels einer einfachen Ein-Hand-Bedienung und lässt sich ebenso leicht zurücknehmen. Für längere Abwesenheiten steht eine Sperrfunktion zur Verfügung, die das Öffnen von innen erschwert. In Ferienzeiten oder bei längeren Reisen wird das Sicherheitsniveau damit angehoben.

Ein optionaler Türwächter ermöglicht eine Spaltöffnung, sodass Gespräche an der Tür in kontrollierter Stellung stattfinden können.

Varianten und typische Einsatzfelder

Um unterschiedliche Anforderungen abzudecken, gibt es AV4D in mehreren Ausführungen: Varianten mit drei Verriegelungspunkten bilden ein solides Grundschutzniveau und erfüllen in stabilen

Elementen gängige Anforderungen an Einbruchhemmung. In entsprechend stabilen Türelementen lässt sich damit ein Schutzniveau nach RC2 erreichen. Ausführungen mit zusätzlichen Verriegelungspunkten adressieren höhere Sicherheitsansprüche.

Für Mehrfamilienhäuser stehen Konfigurationen als AV4D OR zur Verfügung, bei denen die Tür von außen automatisch verriegelt und von innen jederzeit auch ohne Schlüssel zu öffnen ist. So lassen sich Sicherheitsanforderungen und Fluchtwegregeln verbinden.

Alltagstaugliches Konzept

Die Haustür ist eine besonders kritische Stelle vieler Gebäude. Sicherheit scheitert dort häufig nicht an fehlender Technik, sondern an Alltagssituationen und Gewohnheiten. Konzepte, die ausschließlich auf konsequentes Abschließen setzen, stoßen im Betrieb an Grenzen. Automatik-Türverriegelungen koppeln den gesicherten Zustand an das Schließen der Tür und reduzieren die Abhängigkeit vom menschlichen Faktor.

Die Automatik-Türverriegelung auto-Lock AV4D verbindet einen definierten Dichtschluss, eine stabile Türlage und eine leichte Bedienung und lässt sich bei Bedarf mit Blue Matic EAV zu einem komfortablen, medienbasierten System erweitern. Für Sicherheitsverantwortliche, Planende und Betreiber entsteht so eine praxisnahe Grundlage für Entscheidungen in der Gebäude- und Zutrittssicherheit – von der mechanischen Basissicherung bis zur integrierten, motorisch angesteuerten Lösung. **GIT**



Aug. Winkhaus SE
www.winkhaus.com



SCHNELLAUFTORE

Hinein ins Waschparadies!

Schnellauftore für Autowaschanlage in Füssen

Thomas Bunz, Geschäftsführer des „Waschparadies Bunz – Waschanlagen in Lindenberg“, vergleicht seine Anlage mit einem Fünfsterne-Restaurant. Dazu gehört ein störungsfreier Betrieb – und dafür hat er seine Hallen an den Ein- und Ausfahrten mit den Schnellauftoren EFA-STT-S von Efaflex ausgestattet.

■ Wer sein Auto hier wäscht, kann es nach der Reinigung in der hochmodernen effizienten Anlage auch pflegen – und das auch geschützt vor Regen, Wind, Kälte oder Sonne, sagt Thomas Bunz, Betreiber von Waschstraßen in Lindenberg, Wangen, Kaufbeuren und Füssen, nicht ohne Stolz. Als er die Waschanlage in Füssen gekauft hat, arbeitete sie bereits mit Toren von Efaflex. Die Pflegehalle ist an seinen Betrieben Standard – und so erhielt auch der in Füssen einen Anbau, der ebenfalls mit Schnellauftoren des Herstellers ausgestattet wurde. „Die Waschanlagen haben sich in den vergangenen Jahren verändert“, so der Eigentümer und Betreiber. Viele wollen, so Bunz, auch bei schlechtem Wetter ihr Fahrzeug reinigen. Und „wenn es hier Winter ist, dann ist es Winter. Da wäscht und putzt draußen niemand sein Auto. In der heißen Sommersonne macht das ebenfalls keinen Spaß. Die meisten Kunden kommen inzwischen nicht nur zum Waschen ihrer Fahrzeuge, sondern auch zum Pflegen.“ Die Waschzahlen hätten sich seit dem Anbau

der Pflegehalle erhöht, der Umsatz sei um 20 Prozent gestiegen.

Tore öffnen bis zu 600 Mal am Tag

An vielen Tagen im Jahr müssen die Aggregate und Geräte in der Anlage Höchstleistungen vollbringen. „Sie muss immer funktionieren. Denn ein Kunde, den wir wegen einer Störung nicht bedienen können, geht uns für den Monat verloren. Im Schnitt waschen die Deutschen ihre Autos acht bis zehn Mal pro Jahr. Deshalb sind alle Aggregate in der Waschstraße doppelt. Nur eben die Tore nicht. Die müssen ohne Störung funktionieren.“ Er sei bereits seit langen Jahren Kunde bei Efaflex, sagt Thomas Bunz. Nach seinen Erfahrungen gibt es nicht viele Hersteller, deren Tore diese hohe Frequenz an Öffnungszyklen leisten können. „Wir haben hier bei Vollbetrieb 600 und mehr Öffnungen und Schließungen pro Tag. Diese Tore können alles, sie sind schnell, sie sind zuverlässig.“

Die Klarsichtlamellen der beiden Tore sorgen für ausreichend Tageslicht in der

Pflegehalle. Die Torblätter halten auch hohe Windgeschwindigkeiten aus. Durch seine Produkteigenschaften, wie die moderne, klarsichtige Optik, die schnellen Öffnungsgeschwindigkeiten von bis zu 3,0 m/s und Baugrößen bis 8.000 x 7.800 Millimeter, ist das Tor für die verschiedensten Anwendungsbereiche geeignet. Außerdem können die Lamellen individuell gestaltet und das Tor so an den gewünschten Einsatzzweck angepasst werden.

Die Spirale wickelt das Torblatt nicht auf einer Welle auf, sondern hält es platzsparend auf Abstand. Durch diese Konstruktion werden höchste Öffnungsgeschwindigkeiten, Langlebigkeit und Effektivität miteinander kombiniert. Dank der Spirale laufen die Tore leise und verschleißfrei und sehen über Jahre hinweg aus wie neu. **GIT**



Elaflex Hiby GmbH & Co. KG
www.efaflex.com

Wer? Wann? Wo?

Physical Identity & Access Management (PIAM) für mehr Sicherheit, Compliance und Effizienz

Mit einer Physical Identity & Access Management (PIAM)-Plattform zentralisieren Unternehmen die Verwaltung aller physischen Identitäten und Zutrittsrechte über Standorte und Systeme hinweg. Die integrierte PIAM-Suite von ID-ware automatisiert die Vergabe sowie den Entzug von Zutrittsberechtigungen, verbindet HR-, Zutrittskontroll- und Drittsysteme, reduziert Fehlerquellen und stärkt Compliance.



Neben dem Kern aus Ausweis- und Zutrittsmanagement lassen sich dedizierte Module für Besucher- und Fremdfirmen-Management ergänzen



Mit einer Physical Identity & Access Management (PIAM)-Plattform zentralisieren Unternehmen die Verwaltung aller physischen Identitäten und Zutrittsrechte über Standorte und Systeme hinweg

Noch immer verwalten viele Organisationen Zutrittsberechtigungen und Ausweiskarten für Mitarbeiter, Besucher und Fremdfirmen mit nicht integrierten Einzellösungen und manuellen Abläufen. Das Ergebnis: Sicherheitslücken, doppelter Verwaltungsaufwand und fehlende Transparenz darüber, wer Zutritt zu welchen Bereichen oder Standorten hat – und für welchen Zeitraum.

Hier setzt Physical Identity & Access Management (PIAM) an. Die PIAM-Suite von ID-ware zentralisiert die Verwaltung aller physischen Identitäten, Ausweise und Zutrittsberechtigungen: für Mitarbeiter, Besucher und Fremdfirmen, standort- und systemübergreifend.

Nahtlose Anbindung

Der Schlüssel liegt in der Integration. HR-Systeme, Zutrittskontrollsysteme, Parkraumverwaltung, Bezahlssysteme, Schließfächer und weitere Drittsysteme werden nahtlos angebunden. Daten werden automatisch synchronisiert: Rollenänderungen werden sofort übernommen und

bei Vertragsablauf oder Besuchsende werden Zutrittsberechtigungen unverzüglich gesperrt, ohne dass jemand manuell eingreifen muss. Das reduziert Fehler, schließt Sicherheitslücken an der Schnittstelle von IT und physischer Infrastruktur und entlastet die Verwaltung spürbar.

Der modulare Aufbau der PIAM-Suite von ID-ware ermöglicht eine schrittweise Einführung und Erweiterung der Plattform. Neben dem Kern aus Ausweis- und Zutrittsmanagement lassen sich dedizierte Module für Besucher- und Fremdfirmen-Management ergänzen: flexibel, skalierbar und zukunftssicher.

Compliance-Anforderungen erfüllen

Gleichzeitig steigen Transparenz und Nachvollziehbarkeit. Rollenbasiertes Zutrittsmanagement, zentrale Berichterstattung und detaillierte Audit-Trails unterstützen Organisationen dabei, Compliance-Anforderungen aus Vorgaben wie NIS2, DORA, ISO 27001 oder DSGVO zu erfüllen.

Verfügbar als SaaS oder On-Premises-Lösung passt sich die PIAM-Suite von ID-ware jeder IT-Strategie an und schafft die Grundlage für ein integriertes, effizientes und skalierbares Sicherheitsmanagement.



Weitere Informationen ...

finden Sie auch im persönlichen Gespräch der GIT mit Alexander Biederer von ID-ware.

Die PIAM-Suite von ID-ware ist Finalist beim GIT SICHERHEIT AWARD 2027. Jetzt in Kategorie E (Sicherheitsmanagement, Gebäudesicherheit & Perimeter-schutz) abstimmen.



idware
Identity • Access • Control

Kontakt
ID-ware
Deutschland GmbH
www.id-ware.com



SCHLIESSYSTEME

Ständig in Bewegung

Schließtechnik bei der Messe Berlin

Internationale Leitmessen, Kongresse, Gastveranstaltungen, Aufbau, Abbau, Logistik und Service: Auf dem Gelände der Messe Berlin greifen täglich unterschiedlichste Abläufe ineinander. Türen, Tore, Aufzüge, technische Bereiche, Schränke oder Drehtüren müssen zuverlässig gesichert und zugleich für wechselnde Nutzergruppen zugänglich bleiben. Dies wird gewährleistet durch die Cliq-Schließtechnik von Assa Abloy.

Auf dem Gelände der Messe Berlin müssen unterschiedlichste Zugänge zuverlässig gesichert und zugleich für wechselnde Nutzergruppen zugänglich bleiben

■ Messegelände befinden sich permanent in Bewegung, sind geprägt von synchron verlaufenden Ereignissen. Während in einer Halle eine internationale Leitmesse vorbereitet wird, finden nebenan Kongresse, Aufbauarbeiten, Logistikprozesse oder interne Service-Arbeiten statt. Mitarbeiter Aussteller, Dienstleister, Handwerker, Reinigungsteams, Sicherheitskräfte und temporäre Veranstaltungspartner benötigen Zugang zu unterschiedlichen Bereichen – häufig kurzfristig, innerhalb vorgegebener Zeitfenster und möglichst immer klar nachvollziehbar.

Das Schließsystem für die Messe Berlin muss deshalb zuverlässig regeln, wer wann wohin darf. Gleichzeitig muss es flexibel genug sein, um auf wechselnde Nutzungen, kurzfristige Änderungen und die Dynamik eines laufenden Veranstaltungsbetriebs zu reagieren. Eben hier spielt die Cliq-Technologie ihre Stärken aus. Sie verbindet robuste mechanische Sicherheit mit elektronischer

Intelligenz und ermöglicht eine präzise, zentrale Verwaltung der Zutrittsrechte.

Seit mehr als zwei Jahrzehnten setzt die Messe Berlin auf eine mechatronische Verso Cliq-Schließanlage der Marke Ikon von Assa Abloy. Bereits 2003 wurde die Cliq-Technologie eingeführt; heute umfasst die Anlage rund 11.500 Schließzylinder und Hangschlösser, etwa 3.700 Schlüssel sowie 29 Wandprogrammiergeräte. Betreut wird das Projekt durch Knorr Sicherheitstechnik aus Berlin. Die Lösung verbindet robuste mechanische Sicherheit mit elektronischer Flexibilität – und unterstützt so eine präzise, effiziente Zutrittsorganisation auf einem der dynamischsten Messegelände Europas.

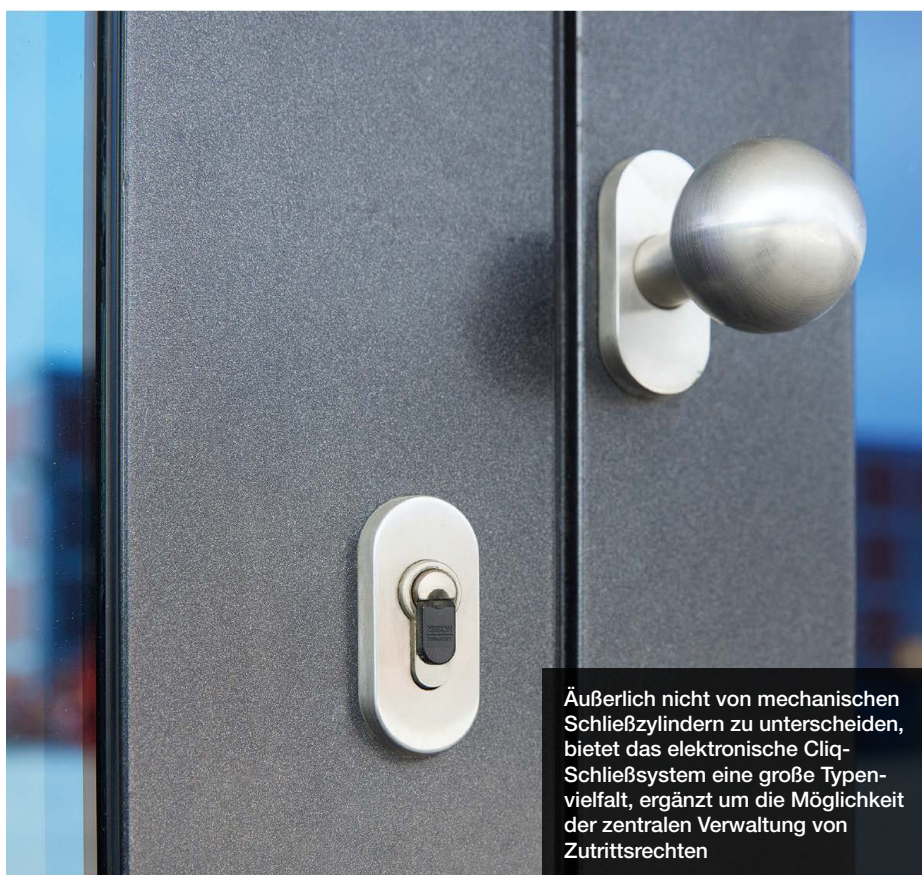
Mechanisch robust, elektronisch flexibel

Die Technologie sichert unterschiedlichste Anwendungen – vom Zugang zu Hallen, Büros und technischen Bereichen über

Aufzüge und Drehtüren bis hin zu Schränken oder weiteren dezentralen Verschlusspunkten. Damit unterstützt sie die Sicherheit eines weitläufigen Geländes, ohne die Abläufe unnötig zu verkomplizieren.

Wesentlicher Bestandteil dieses Prinzips ist die intuitive und flexible Programmierung. Berechtigungen lassen sich vergeben, ändern, zeitlich begrenzen oder entziehen. Geht ein Schlüssel verloren, muss nicht die gesamte Anlage ausgetauscht werden: Der betroffene Schlüssel kann einfach ausprogrammiert werden. Das erhöht die Sicherheit und vermeidet zugleich aufwendige und kostenintensive mechanische Anpassungen.

Auch im Betrieb überzeugt die Lösung durch ihre Alltagstauglichkeit. Da die Energieversorgung über die Batterie im Schlüssel erfolgt, benötigen die Zylinder keine eigene Verkabelung oder einen aufwendigen Tausch der Energiezellen vor Ort. Gerade in einer gewachsenen und weitläufigen Infrastruktur



wie der Messe Berlin ist das ein entscheidender Vorteil – sowohl bei der Installation als auch in der laufenden Wartung.

Berechtigungen aktualisieren, wo sie gebraucht werden

Verwaltet wird die Anlage über den Cliq Web Manager. Zusätzlich sind 29 Wandprogrammiergeräte über das Gelände verteilt. Über sie können Schlüsselinhaber ihre Berechtigungen aktualisieren lassen – unkompliziert, schnell und ohne lange Wege über zentrale Ausgabestellen.

Ergänzend kommt ein Cliq Updater zum Einsatz. Er ermöglicht die komfortable Aktualisierung von Zutrittsdaten und erweitert die Möglichkeiten der dezentralen Berechtigungsverwaltung. Gerade im Außenbereich oder an stark frequentierten Punkten bietet diese Lösung zusätzlichen Komfort: Nutzerinnen und Nutzer können ihre Schlüssel dort aktualisieren, wo der Bedarf entsteht. Das entlastet die Organisation, beschleunigt Abläufe und unterstützt einen reibungslosen Betrieb – ein wichtiger Faktor auf einem Gelände, das jährlich Millionen Besucher sowie Aussteller aus aller Welt empfängt.

Eine Lösung für komplexe Organisationswelten

Am Beispiel der Messe Berlin wird deutlich, wofür Cliq entwickelt wurde: für Sicher-



heitsumgebungen mit vielen Nutzergruppen, wechselnden Anforderungen und unterschiedlichsten Schließpunkten. Hier muss ein System dauerhaft zuverlässig funktionieren und zugleich flexibel anpassbar bleiben, wie Oliver M. Friedrich, Teamleitung Badge, Fleet, Key and Post Services, Messe Berlin, unterstreicht: „Wir setzen seit über 20 Jahren erfolgreich auf die Cliq-Technologie und haben damit sehr gute Erfahrungen gemacht.“

Dass eine Schließlösung über einen so langen Zeitraum hinweg im täglichen Betrieb überzeugt, verweist zugleich auf einen Grundsatz, der die Marke Ikon seit jeher

prägt, wie der Hersteller betont. Sicherheit muss verlässlich sein – und sich dennoch weiterentwickeln können. Im Jahr ihres 100-jährigen Jubiläums wird genau diese Verbindung besonders sichtbar. **GIT**



Assa Abloy Sicherheitstechnik GmbH
www.assaabloy.com

ZUTRITT

Kirchgang digital

Elektronisches Schließsystem für katholisches Pfarrzentrum in Velbert



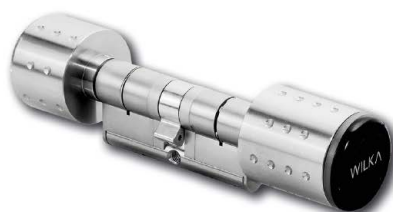
Kirchliche Einrichtungen stehen heute vor der Herausforderung, unterschiedlichsten Nutzergruppen einen sicheren und zugleich flexiblen Zugang zu ihren Gebäuden zu ermöglichen. Beim Neubau des Pfarrzentrums der katholischen Kirchengemeinde St. Michael und Paulus in Velbert wurde diese Anforderung konsequent umgesetzt – mit einer elektronischen Schließlösung von Wilka.

Im neuen Pfarrzentrum St. Marien sorgt das elektronische Schließsystem Easy Access für eine sichere und komfortable Zutrittsorganisation verschiedener Nutzergruppen

Die katholische Kirchengemeinde St. Michael und Paulus in Velbert suchte ein System, das nicht nur den aktuellen Anforderungen gerecht wird, sondern sich auch perspektivisch auf weitere Liegenschaften der Gemeinde erweitern lässt. Die Entscheidung fiel auf Wilka Schließtechnik. Bereits in der Planungsphase begleitete der Hersteller die Kirchengemeinde intensiv und stellte das elektronische Schließsystem Easy Access ausführlich vor. Die Umsetzung erfolgte durch den Fachhandelspartner Keycept Sicherheitstechnik aus Mönchengladbach. Von der ersten Beratung bis zur finalen Installation vergingen rund neun Monate.

Zentrale Verwaltung für maximale Flexibilität

Im Fokus stand eine flexible und komfortable Vergabe von Zutrittsrechten für verschiedene Nutzergruppen. Das elektronische Schließsystem ermöglicht die Erstellung individueller Zeit- und Nutzerprofile – so kann beispielsweise mehreren Vereinen an unterschiedlichen Tagen und Zeiten gezielt



Elektronische Zylinder



Elektronischer Türbeschlag



Wandleser



Transponder



Nutzerkarte

Das elektronische Schließsystem vereint elektronische Zylinder, Wandleser, Türbeschläge und moderne RFID-Identmedien zu einer flexiblen und skalierbaren Zutrittslösung

Zutritt gewährt werden. Ein weiterer Vorteil ist die standortübergreifende Verwaltung der Anlage. „Unser elektronisches Schließsystem Easy Access ist serverbasiert und kann aus der Ferne verwaltet werden“, erklärt Manuel Immach von Wilka.

Easy Access vereint elektronische Zylinder, Wandler und eine zentrale Verwaltungssoftware zu einem modularen Gesamtsystem. Dadurch eignet sich die Lösung sowohl für kleinere Objekte als auch für komplexe, standortübergreifende Anlagen.

Die intuitive Software ermöglicht eine einfache Verwaltung sämtlicher Zutrittsrechte – von der Vergabe über Änderungen bis hin zum Entzug. Je nach Ausbaustufe lassen sich Anlagen mit bis zu 64.000 Türen und Nutzern steuern.

„Das Easy Access System ist ein sehr ausgereiftes, netzwerkfähiges und benutzerfreundliches System“, so Keycept Sicherheitstechnik Geschäftsführer Michael Schulte. „Die Struktur ist klar und zweckorientiert aufgebaut.“ Für die sichere Identifikation der Nutzer kommen moderne RFID-Transponder mit Mifare Desfire-Technologie zum Einsatz. Diese gewährleisten eine verschlüsselte Datenübertragung und damit ein hohes Sicherheitsniveau. Gleichzeitig sorgt die kontaktlose Bedienung für Komfort im täglichen Gebrauch. Ereignisspeicher ermöglichen zudem eine transparente Nachvollziehbarkeit aller Zutrittsvorgänge.

Praxisgerechte Ausstattung im Gebäude

Am Haupteingang des Pfarrzentrums wurde ein Wandler des Typs Easy Access E231 installiert, der den Zutritt per Transponder

ermöglicht. Änderungen an Berechtigungen werden online übertragen und aktualisieren sich bei der nächsten Nutzung automatisch.

Im Gebäude kommen verschiedene elektronische Zylinder zum Einsatz, darunter Varianten mit ein- und beidseitiger Elektro-

Kirchengemeinde in der Lage, das System eigenständig zu verwalten und flexibel anzupassen. „Keycept ist ein absoluter Profi im Objektgeschäft und ein verlässlicher Wilka-Partner“, betont Manuel Immach. Die Mitarbeiter verfügten über umfassende Expertise



Die katholische Kirchengemeinde St. Michael und Paulus in Velbert setzt bei der Zutrittskontrolle auf eine moderne elektronische Schließlösung von Wilka

nik sowie spezielle Panikzylinder für Fluchttüren. Ergänzend wurden auch mechanische Lösungen integriert, etwa für persönliche Schränke von Pfarrern und Mitarbeitenden.

Nach der erfolgreichen Installation übernahm der Fachhandelspartner Keycept Sicherheitstechnik die Schulung der Verantwortlichen vor Ort. Dadurch ist die

in der Sicherheitstechnik und sorgen für eine professionelle und partnerschaftliche Umsetzung unserer Projekte. **GIT**



Wilka Schließtechnik GmbH
www.wilka.de

© Bilder: Wilka Schließtechnik GmbH

Neuaufgabe des BHE-Praxis-Ratgebers Sicherungstechnik erschienen

Der BHE Bundesverband Sicherheitstechnik e. V. hat die 6. Auflage seines etablierten Praxis-Ratgebers Sicherungstechnik veröffentlicht. Die umfassend aktualisierte Publikation bietet auf mehr als 200 Seiten einen praxisnahen Überblick über alle wesentlichen Gewerke der Sicherungstechnik – von der Planung über die Projektierung bis hin zur Umsetzung.

Die Neuaufgabe wurde sorgfältig überarbeitet und um aktuelle Themenfelder ergänzt. Erstmals behandelt der Ratgeber auch die Bereiche Schranken und Personensperren, Blitz- und Überspannungsschutz, Sicherheit Kritischer Infrastrukturen, Kleindrohnenabwehr sowie Robotiksicherheit. Damit trägt das Werk der zunehmenden Bedeutung ganzheitlicher Sicherheitskonzepte Rechnung.

Der Praxis-Ratgeber stellt für Errichter, Planer, Betreiber und Anwender ein hilfreiches Nachschla-

gewerk dar. Neben fundierten Informationen zu modernen sicherheitstechnischen Lösungen enthält das Buch zahlreiche Normenverweise, Planungshinweise, Checklisten und praktische Umsetzungstipps für den Arbeitsalltag.

Die Themen reichen von Einbruch- und Brandschutz über Video- und Zutrittssysteme bis hin zur Perimetersicherheit. Ergänzend werden Netzwerk- und Leitstellentechnik sowie aktuelle Herausforderungen wie Cybersicherheit im KRITIS-Umfeld oder rechtliche Rahmenbedingungen der Drohnenabwehr praxisorientiert erläutert.

Die neue Ausgabe des BHE-Praxis-Ratgebers Sicherungstechnik ist erstmals sowohl in digitaler als auch in gedruckter Version erhältlich. Bestellungen sind über den BHE-Shop shop.bhe.de oder per E-Mail an info@bhe.de möglich. **www.bhe.de**



QUANTENCOMPUTING

Europas Moment der Quantensouveränität

Von wissenschaftlicher Exzellenz zu strategischer Infrastruktur

Amerikanische Unternehmen dominierten die Cloud-Revolution, chinesische Konzerne skalierten industrielle Kapazitäten in rasantem Tempo, und Europa fand sich häufig in der Rolle wieder, die Zukunft zu regulieren, anstatt sie selbst zu gestalten. Quantencomputing könnte der erste große Technologiezyklus werden, in dem sich dieses Muster verändert.

■ In Brüssel, Berlin, Paris und Helsinki werden Quantentechnologien längst nicht mehr als entfernte wissenschaftliche Kuriositäten betrachtet. Stattdessen gelten sie zunehmend als Instrumente wirtschaftlicher Resilienz, industrieller Wettbewerbsfähigkeit und geopolitischer Souveränität. Die Sprache rund um den Sektor hat sich deutlich verändert: weg von rein akademischen Ambitionen, hin zu Infrastruktur, Cybersicherheit und strategischer Autonomie.

Diese Entwicklung ist von zentraler Bedeutung, da Quantencomputing an der Schnittstelle mehrerer Herausforderungen steht, die derzeit die europäische Politik prägen. Die Abhängigkeit von ausländischer Cloud-Infrastruktur, zunehmende Cyberbedrohungen, Fragen der Energiesicherheit, Probleme in den Halbleiter-Lieferketten sowie die Stärkung der Verteidigungsfähigkeit Europas haben sich seit der Pandemie und dem Krieg in der Ukraine deutlich verschärft.

Die 2025 vorgestellte „Quantum Europe Strategy“ der Europäischen Kommission macht diesen Wandel deutlich. Brüssel verfolgt das Ziel, Europa bis 2030 zu einem globalen Marktführer im Quantenbereich zu

entwickeln – nicht nur durch Forschungsstärke, sondern durch industrielle Umsetzung und strategische Infrastruktur. Die Strategie definiert fünf zentrale Säulen: Forschung und Innovation, Quanteninfrastruktur, Industrialisierung des Ökosystems, Dual-Use-Verteidigungsanwendungen sowie Fachkräfteentwicklung.

Strategie technologischer Souveränität

Bemerkenswert ist dabei, wie stark dieser Ansatz Europas umfassender Strategie technologischer Souveränität ähnelt. Die Roadmap der Kommission umfasst den Ausbau der EuroHPC-Quantenkapazitäten, den Aufbau eines Pilotprojekts für ein „Europäisches Quanteninternet“, die Stärkung sicherer Quanten-Lieferketten sowie die Integration von Quantenkommunikation in Programme wie Galileo und IRIS. Quantencomputing hat sich damit von einem Forschungsthema zu einem industrie- und sicherheitspolitischen Schwerpunkt entwickelt.

Die Zahlen verdeutlichen, weshalb Brüssel überzeugt ist, dass dieses Zeitfenster noch offensteht. Laut Europäischer Kommission haben EU-Institutionen und Mit-

gliedstaaten in den vergangenen fünf Jahren rund 11 Milliarden Euro in Quantentechnologien investiert. Gleichzeitig verfügt Europa über tiefgreifende Kompetenzen in Bereichen wie Photonik, supraleitende Systeme, industrielle Mathematik und Hochleistungsrechnen.

Im Gegensatz zu früheren Technologierevolutionen startet Europa diesmal mit echten strukturellen Vorteilen. Das europäische Quantenökosystem wird zunehmend dichter und koordinierter. Die Fraunhofer-Institute in Deutschland, das niederländische QuTech-Ökosystem, finnische Forschung im Bereich supraleitender Technologien, staatlich unterstützte Quanteninitiativen in Frankreich sowie Europas starke industrielle Fertigungsbasis bilden gemeinsam ein Fundament, das während früherer digitaler Umbrüche nicht existierte. Das European Quantum Industry Consortium (QuIC), gegründet zur Vernetzung von Start-ups, Industrieunternehmen, Investoren und Forschungseinrichtungen, verdeutlicht zudem, dass Europas Herausforderung heute weniger in wissenschaftlicher Glaubwürdigkeit als vielmehr in kommerzieller Skalierung und Umsetzung liegt.

Wachsende Dynamik

Das finnisch-deutsche Unternehmen IQM bereitet sich darauf vor, über eine geplante SPAC-Transaktion und ein mögliches Dual-Listing in Helsinki das erste börsennotierte europäische Quantencomputing-Unternehmen zu werden. Das Unternehmen gibt an, bereits Systeme an mehrere führende Supercomputing-Zentren weltweit geliefert zu haben und eine wachsende kommerzielle Dynamik im europäischen Hochleistungsrechner-Ökosystem zu verzeichnen. Gleichzeitig kündigte der niederländische Prozessor-Spezialist QuantWare kürzlich eine Finanzierungsrunde über 152 Millionen Euro an, um nach eigenen Angaben die weltweit größte spezialisierte Fertigungsanlage für Quantenchips in Delft auszubauen.

Beide Entwicklungen zeigen deutlich, wohin sich die Branche bewegt. Der Sektor entwickelt sich zunehmend von experimentellen Laborerfolgen hin zur Industrialisierung. Fertigungskapazitäten, Software-Orchestrierung, Energieeffizienz, Infrastrukturintegration und Cybersicherheit gewinnen ebenso an Bedeutung wie theoretische Fortschritte bei der Qubit-Leistung.

Deutschland gilt dabei zunehmend als klarster Ausdruck europäischer Quantenambitionen. Lange vor dem aktuellen Hype um generative KI und souveräne Rechenkapazitäten legten die Fraunhofer-Institute bereits die Grundlagen für angewandte Quantenforschung. Bereits 2021 installierte IBM gemeinsam mit einem Fraunhofer-Konsortium den ersten kommerziellen Quantencomputer Europas in Deutschland – ein früher Versuch, Quantencomputing aus der theoretischen Wissenschaft in industrielle Anwendungen zu überführen.

Testfeld deutsche Industrie

Die deutsche Industrie entwickelte sich früh zu einem Testfeld praktischer Quantenanwendungen. Volkswagen setzte D-Wave-Quantenannealer zur Simulation von Verkehrsflüssen ein, während BMW Optimierungslösungen im Bereich Fertigungsrobo-



Quantencomputing könnte der erste große Technologiezyklus werden, in dem die Europäer dominieren

tik untersuchte. Der Reiz liegt auf der Hand: Quantensysteme eignen sich besonders zur Lösung hochkomplexer Optimierungsprobleme, die klassische sequenzielle Computersysteme nur schwer effizient verarbeiten können.

Prof. Anita Schöbel, Direktorin des Fraunhofer-Instituts für Techno- und Wirtschaftsmathematik (ITWM) in Kaiserslautern, betonte, dass die bedeutendsten Durchbrüche möglicherweise weniger aus abstrakter Rechenleistung als vielmehr aus angewandter industrieller Mathematik entstehen werden. „Wir arbeiten an Projekten mit stochastischen partiellen Differentialgleichungen wie den Fokker-Planck-Gleichungen“, erklärte sie in einem Fraunhofer-Interview. „Diese werden genutzt, um Lithium-Ionen-Batterien und Windturbinen zu entwickeln, Granulatströme zu berechnen oder Preise im quantitativen Finanzwesen zu bestimmen. Diese Gleichungen lassen sich in quantenmechanische Gleichungen umwandeln, die Quantencomputer vermutlich wesentlich schneller lösen können.“ Dieser Fokus auf industriellen Nutzen statt technologischer Inszenierung entwickelt sich zunehmend zur europäischen Quantenphilosophie.

Impuls aus der Cybersicherheit

Die kurzfristig größte Auswirkung des Quantencomputings könnte weniger aus

Durchbrüchen in der Pharmaforschung oder Künstlichen Intelligenz resultieren, sondern vielmehr aus massiven Veränderungen im Bereich der Cybersicherheit – insbesondere durch die Sorge, dass zukünftige Quantensysteme die kryptografischen Grundlagen moderner digitaler Infrastruktur untergraben könnten.

Die Diskussion um sogenannte „Harvest Now, Decrypt Later“-Angriffe hat sich rasch von theoretischen Szenarien hin zu konkreter strategischer Planung entwickelt. Das Prinzip ist einfach: Gegnerische Akteure könnten bereits heute verschlüsselte Kommunikation und sensible Daten sammeln, um diese zukünftig mit leistungsfähigen Quantencomputern zu entschlüsseln. Informationen über Verteidigungssysteme, Finanztransaktionen, Gesundheitsdaten, industrielles geistiges Eigentum oder Energieinfrastruktur könnten auch in Jahrzehnten noch strategischen Wert besitzen.

Für Europa wären die Konsequenzen erheblich. Die europäische Wirtschaft basiert stark auf vernetzter Infrastruktur, regulierten Industrien und grenzüberschreitenden digitalen Systemen. Ein zukünftiger Zusammenbruch kryptografischer Sicherheit würde nicht nur IT-Probleme verursachen, sondern Verwundbarkeiten in Finanzwesen, Energieversorgung, Transport und öffentlicher Verwaltung offenlegen. Vor diesem Hintergrund gewinnt Post-Quantum-Kryptografie zunehmend strategische Bedeutung innerhalb Europas.

Eine neue Klasse von Unternehmen

In diesem Umfeld entsteht eine neue Klasse von Unternehmen – nicht primär als Hersteller von Quantenhardware, sondern als Infrastruktur-Enabler zwischen Hochleistungsrechnen und industrieller Anwendung. Eines davon ist SuperQ Quantum Computing, ein kanadisches Unternehmen, das sich über Partnerschaften, hybride Computing-Lösungen und Initiativen im Bereich quantensicherer Verschlüsselung



Europa versteht es besser als fast jede andere Region, Technologien in kritische Infrastruktur, industrielle Prozesse und souveräne Systeme zu integrieren

Bitte umblättern ►

zunehmend an Europas industriellen und sicherheitspolitischen Prioritäten orientiert.

Im Gegensatz zu Unternehmen, die ausschließlich Quantenprozessoren entwickeln, konzentriert sich die Strategie von SuperQ auf Orchestrierung und Zugänglichkeit. Die Plattform „Super“ sowie die ChatQLM-Architektur sollen Rechenlasten dynamisch zwischen klassischen Hochleistungsrechnern, Optimierungssystemen, Quantenannealern und gatebasierten Quantenplattformen verteilen – und dies über dialogbasierte Benutzeroberflächen statt hochspezialisierter Programmiersprachen.

Diese Positionierung spiegelt eine zentrale Entwicklung der Branche wider: Die meisten Unternehmen benötigen nicht zwingend direkten Zugang zu Quantenhardware. Sie benötigen vielmehr Systeme, die entscheiden können, wann Quantentechnologien sinnvoll einsetzbar sind, wie Rechenlasten verteilt werden und wie sich fortschrittliche Rechenverfahren in bestehende industrielle Prozesse integrieren lassen.

Besonders relevant ist zudem SuperQs Fokus auf Post-Quantum-Cybersicherheit durch die Initiative „SuperPQC“ und Partnerschaften rund um quantensichere Verschlüsselungsstandards. Der Schwerpunkt auf „Harvest Now, Decrypt Later“-Risiken passt eng zur Entwicklung europäischer und amerikanischer Cybersicherheitsstrategien, in denen die Migration hin zu quantenresistenter Kryptografie zunehmend beschleunigt wird.

Besondere Bedeutung besitzt in diesem Zusammenhang die jüngste Partnerschaft mit dem Fraunhofer-Institut für Techno- und Wirtschaftsmathematik (ITWM) in Deutschland. Fraunhofer ist weit mehr als

nur eine Forschungseinrichtung – es bildet das Rückgrat des deutschen Modells angewandter industrieller Innovation.

Die Vereinbarung verschafft SuperQ direkten Zugang zu einem der einflussreichsten industriellen Forschungsökosysteme Europas – genau zu jenem Zeitpunkt, an dem Brüssel versucht, Quantencomputing von akademischer Forschung in operative Infrastruktur zu transformieren. Entscheidend dabei: Die Zusammenarbeit konzentriert sich nicht auf spekulative Narrative rund um „Quantum Supremacy“, sondern auf hybride Quanten-Klassik-Workflows für Logistik, Fertigung, Energieoptimierung und verteidigungsnahe Anwendungen.

Das Fraunhofer ITWM spielt hierbei eine zentrale Rolle. Das Institut ist spezialisiert auf industrielle Mathematik, Simulation und Hochleistungsrechnen – Kernbereiche der europäischen Industrie. Im Rahmen der Partnerschaft wird Fraunhofer die Orchestrierungstechnologien von SuperQ in industriellen Simulationsumgebungen evaluieren und Anwendungen in Logistik, Finanzwesen, Fertigung und Energiesystemen untersuchen. Damit positioniert sich Quantencomputing nicht als isolierter Technologiesektor, sondern als nächste Optimierungsschicht innerhalb der europäischen Industrie.

Vor schwierigen Aufgaben

Dennoch bleibt Vorsicht angebracht. Der Quantencomputing-Sektor zieht weiterhin Bewertungen und Erwartungen an, die oft schneller wachsen als die kommerzielle Realität. Selbst Europas stärkste Quantenunternehmen stehen vor der schwierigen Aufgabe, den Übergang von Forschungsexzellenz zu nachhaltigen Industrieunterneh-

men zu schaffen. SuperQ steht vor ähnlichen Herausforderungen. Die angestrebte Orchestrierungsebene gilt strategisch als attraktiv, ist jedoch stark umkämpft. Technologiekonzerne, Cloud-Hyperscaler und spezialisierte Start-ups konkurrieren gleichermaßen darum, die Schnittstelle zwischen Unternehmen und hybriden Quantensystemen zu definieren. Ob Unternehmen diese Technologien tatsächlich im großen Stil einsetzen oder zunächst vorsichtig in Pilotprojekten testen werden, bleibt offen. Der übergeordnete Trend scheint jedoch zunehmend unumkehrbar.

Das Rennen um Quantencomputing entwickelt sich zu weit mehr als einem Wettbewerb um die höchste Anzahl an Qubits. Es wird zu einem Wettkampf darüber, wer die Infrastruktur, Standards und Sicherheitsarchitektur der nächsten Rechenära kontrolliert. Für Europa könnte dies ein überraschend günstiges Spielfeld darstellen.

Die europäischen Stärken in industriellen Systemen, regulierter Infrastruktur, angewandter Mathematik und Cybersicherheit könnten im Quantenzeitalter wertvoller werden als jene Dominanz von Konsumentenplattformen, die frühere digitale Revolutionen geprägt hat. Europa versteht es besser als fast jede andere Region, Technologien in kritische Infrastruktur, industrielle Prozesse und souveräne Systeme zu integrieren. Genau das könnte letztlich wichtiger sein als die lautesten Schlagzeilen. **GIT**



SuperQ Quantum Computing Inc.
www.superq.co

Hacker-Alarm im Krankenhaus

Das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) bietet besonders realitätsnahe Cyber-Krisen-Planspiele speziell für Krankenhäuser an. In ganztägigen Übungen trainieren Teams aus Technik, Medizin und Verwaltung gemeinsam, wie sie einen Cyberangriff erkennen, kommunizieren und bewältigen. Erste Erfahrungen mit Kliniken zeigen: Die Teilnehmer machen deutliche Fortschritte, und das unter echtem Druck. Die Ergebnisse fließen außerdem in ein Forschungsprojekt ein, damit auch andere aus den Planspielen lernen können. Ransomware verschlüsselt Patientendaten, die Telefonanlage bricht zusammen, Journalisten stehen im Eingangsbereich des Krankenhauses, und der Krisenstab muss dafür sorgen, dass der Betrieb weiterläuft. Genau solche Szenarien simulieren die neuen Cyber-Krisen-Planspiele des Fraunhofer SIT.

www.sit.fraunhofer.de



IDENTITÄTSMANAGEMENT

Vertrauen dank

ZERO TRUST

Mit integriertem Identitätsmanagement werden SuperApps sicher

Sie vereinfachen das digitale Leben, sind aber auch ein potenzielles Sicherheitsrisiko: SuperApps. Europäische Alternativen haben großes Potenzial – wenn sie bei den Nutzern Vertrauen durch Sicherheit schaffen. Erfolgreiche Beispiele gibt es bereits.

Autor:
Ismet Koyun
CEO und Gründer,
Kobil Gruppe



■ SuperApps zeigen, wie praxistauglich digitale Transformation sein kann. Sie bündeln unterschiedliche Dienste in einer einzigen Anwendung – einschließlich Bezahlungsfunktionen, Messaging, E-Commerce, Mobilität, Behördenservices und mehr. Mit nur einem Login bewegt man sich durch ein digitales Ökosystem, ohne zwischen verschiedenen Plattformen zu wechseln. In Asien sind SuperApps längst etabliert, europäische Verbraucher bleiben skeptisch. Zu Recht. Denn der Blick nach Asien zeigt die Schattenseiten vieler SuperApps: Datenmonopole, Intransparenz, Überwachung.

Hier liegt die Chance für europäische Lösungen, die sicher und compliant mit Richtlinien wie der DSGVO sind. Das ist keine regulatorische Hürde, sondern ein Wettbewerbsvorteil. Mit einem vertrauenswürdigen europäischen Gegenentwurf kann ein SuperApp-Modell entstehen, von dem Nutzer, Unternehmen und öffentliche Institutionen gleichermaßen profitieren. Die nötige Basis: hohe Datenschutzstandards, sichere Architektur und verifizierte Identitäten.

Sicherheit und ID-Management als Grundbedingungen

Ob Nutzerdaten, Payment oder Chats – in SuperApps laufen viele Datenströme zusammen. Jeder ist ein potenzielles Einfallstor für Angriffe und Datenlecks. Umso wichtiger ist ein Sicherheitskonzept, das Nutzer von der ersten Anmeldung bis zum Ausloggen kontinuierlich schützt. Das Herzstück einer solchen Architektur ist die digitale Identität.

Jede Transaktion, jede Autorisierung steht und fällt mit der Frage: Wer handelt – und darf er das? Identität ist die Grundlage für Vertrauen und Verbindlichkeit. Es braucht ein System, das digitale Identitäten eindeutig und fälschungssicher absichert. Am besten ist die Identität zudem universell einsetzbar und ohne zusätzliche Hürden für die Nutzer.

Wie es nicht funktioniert, zeigt die elektronische ID in Deutschland: kompliziert, wenig intuitiv, nicht flächendeckend integriert – entsprechend gering ist deren Nutzung. Digitale Identität muss alltagstauglich sein. Sonst leidet die Akzeptanz.

Wie geht sichere digitale Identität?

Zero-Trust-Architekturen sind das Fundament sicherer Identitätslösungen. Kein Nutzer und keine Interaktion wird per se als vertrauenswürdig eingestuft. Entscheidend ist die kontinuierliche Verifikation: Nicht nur beim Login, sondern über den gesamten Nutzungsprozess hinweg muss die ID überprüfbar bleiben. Dahinter steht bei ein mehrstufiges Identitätsmanagement. Adaptive Multi-Faktor-Authentifizierung passt die Sicherheitsanforderungen dynamisch an das Risiko an. Gerätebindung verhindert Missbrauch durch kompromittierte Zugangsdaten.

Bei der Risikoeinschätzung, der Betrugserkennung, aber auch bei anderen Aspekten der Authentifizierung spielt auch künstliche Intelligenz (KI) eine wichtige Rolle. Ein Beispiel: Verhaltensbiometrie. KI-Systeme analysieren in Echtzeit, wie Nutzer ihre Endgeräte verwenden – Tippgeschwindigkeit, Mausbewegungen, Scrollverhalten. Das Muster ist so individuell wie ein Fingerabdruck, greift aber weniger in Persönlichkeitsrechte ein als biometrische Daten. So entstehen Sicherheitslösungen, die Vertrauen fördern, statt invasiv Daten zu sammeln.

Europäische Erfolgsmodelle

Dass SuperApps ebenso sicher wie nutzerfreundlich sein können, zeigen erprobte Beispiele. Die Stadt Worms führte eine City-App ein, in der Bürger unter anderem digitale Verwaltungsdienste, Kommunikation, Bezahlvorgänge und Dokumentenaustausch nutzen können – auf Basis einer verifizierten digitalen Identität.

Weitere Beispiele sind die SuperApp Istanbul Senin mit über fünf Millionen Nutzern sowie die Spark SuperApp für urbane Mobilität, die auch in Deutschland verfügbar ist.

Diese Plattformen basieren auf einer Sicherheitsinfrastruktur mit Ende-zu-Ende-Verschlüsselung, Gerätebindung und flexibler Authentifizierung – entwickelt von Kobil, dem laut Gartner, einem international agierenden, US-amerikanischen Beratungsunternehmen für Marktforschung und Analyse im Bereich der Informationstechnologie, einzigen SuperApp-Anbieter in Europa. Es gibt sie also schon: fertige Alternativen, die ein sicheres und nahtloses digitales Ökosystem bilden.

Handlungsempfehlungen für Entscheider

Für Entscheidungsträger in Wirtschaft, Verwaltung und IT-Security gilt: Jetzt ist der Zeitpunkt, tragfähige Sicherheitsstrukturen zu schaffen. SuperApps sind ein erfolgversprechender Ansatz, damit digitale Services technisch überzeugen, aber auch geschützt und vertrauenswürdig sind. Drei Schritte sind entscheidend:

- Sicherheit als Basisanforderung definieren – Privacy by Design und Security by Design sind Grundvoraussetzungen.
- Auf europäische Anbieter setzen, die DSGVO-konform sind – nachträgliche Compliance-Maßnahmen sind teuer und riskant.
- Nutzer von Anfang an einbeziehen – Akzeptanz entsteht durch Vertrauen und Vertrauen durch Transparenz. **GIT**



Kobil GmbH
www.kobil.com



HB-Wildfire 2.0: Schutz und Tragekomfort für effektive Brandbekämpfung im Gelände. Jacke optional mit Rückenkoller, Hose optional mit Trägern



HB-Wildfire 2.0 von HB Protective Wear: Schutzbekleidung mit Warnwestenbefreiung für Wald- und Flächenbrandbekämpfung

FEUERWEHRBEKLEIDUNG

Flammenschutz im freien Gelände

PSA: Sicheres und bequemes Outfit für steigende Anforderungen an Einsatzkräfte

Mit HB-Wildfire 2.0 bringt HB Protective Wear eine Schutzbekleidung mit Warnwestenbefreiung für Wald- und Flächenbrandbekämpfung sowie Technische Hilfe auf den Markt.

Der Klimawandel ist längst in Europa angekommen. Extreme Wetterlagen lassen dabei auch hierzulande die Temperaturen ansteigen. Die Folge: Böden und Wälder trocknen immer weiter aus, wodurch sich die Brandgefahr signifikant erhöht. Denn selbst in kühleren Monaten können sich viele Flächen nicht mehr von dem zunehmenden Hitzestress erholen. Gleichzeitig sind die ausgetrockneten Böden bei Regen nicht in der Lage, ausreichend Wasser aufzunehmen. Inzwischen reicht meist schon ein kleiner Funke, um große Flächen zu entzünden. Zusätzlich breiten sich die Feuer mehr aus und dauern länger an, weil sie schwerer einzudämmen sind.

Widrige Bedingungen

Die Feuerwehrleute stehen vor immer größeren Herausforderungen, um unsere Wälder zu schützen. Die körperliche und mentale Belastung der Einsatzkräfte, die

unter diesen besonders widrigen Bedingungen arbeiten, nimmt dementsprechend zu. Um sie bei ihrer Arbeit wirkungsvoll zu unterstützen, hat HB Protective Wear die Kollektion HB-Wildfire 2.0 entwickelt, die neben der EN ISO 11612 gleichzeitig auch die neuen Normanforderungen der EN 15384 berücksichtigt.

Entstanden ist eine PSA, die exakt auf die Anforderungen von Einsatzkräften bei der Brandbekämpfung im freien Gelände zugeschnitten ist – sie bietet zuverlässigen Schutz vor Flammen und überzeugt zugleich durch ein besonders angenehmes Tragegefühl sowie eine spürbare körperliche Entlastung.

Leicht und strapazierfähig

Zu nennen ist hier das leichte und strapazierfähige Modacryl/Tencel-Obermaterial, das ebenso wie die Reflexbestreifung vielen Wäschchen standhält. Des Weiteren das Innenfutter mit hydrophiler Ausstattung: Es

nimmt Feuchtigkeit sehr gut auf und gibt sie gleichmäßig in Form von Verdunstungskälte wieder ab. Dadurch kommt der Träger nicht so schnell ins Schwitzen. Zusätzlich erfüllt HB-Wildfire 2.0 die Kriterien der Warnwestenbefreiung gemäß DGUV-Information 205-020, da die Anforderungen an die Warnbestreifung übertroffen werden.

Die aufwendige Verarbeitung mit speziellen Formnähten und segmentierten Reflexstreifen sorgt für Bewegungsfreiheit. Besonders beanspruchte Bereiche wie Ellbogen, Knie und Säume sind zusätzlich mit einem Silikon-Carbon-beschichteten Besatz verstärkt und sämtliche Taschen mit Klettverschluss verarbeitet.

Die Kollektion besteht aus Jacke und Hose plus optionalem Funktionskennzeichnungskoller und anknöpfbaren Hosenträgern. Sie ist auch für den Einsatz in der technischen Hilfe geeignet und in drei Farben sowie als Normal-, Lang- und Kurzgröße erhältlich. **GIT**



HB Protective Wear GmbH & Co. KG
www.hb-online.com

KI-VIDEO-LÖSUNGEN

Millionenschäden vorbeugen

Videotechnik und KI heben Brandschutz auf ein neues Level

Alle zwei bis drei Minuten kommt es in Deutschland rechnerisch zu einem Feuerschaden. Neben der Gefahr für Leib und Leben summieren sich allein die wirtschaftlichen Schäden bei privaten Wohngebäuden nach Angaben der Versicherungswirtschaft mittlerweile auf über zwei Milliarden Euro jährlich. Hinzu kommen nach Expertenschätzung Jahr für Jahr zirka 200 Großbrände in Unternehmen. Ganzheitliche Sicherheit, wie sie Kötter Sicherheitssysteme durch integrierte Techniklösungen inklusive Aufschaltung auf die eigene Notruf- und Serviceleitstelle plus personelle Maßnahmen (z. B. Betriebs- und Werkfeuerwehren) bietet, ist daher von größter Relevanz.



■ Die Kosten von Produktionsausfällen, Know-how-Verlusten etc., die auf Feuerschäden zurückzuführen sind, werden auf bis zu 25 Milliarden Euro geschätzt. Nach Statistiken führender Sachversicherer gehen viele Unternehmen aufgrund dieser oft kaum zu bewältigenden Konsequenzen binnen zwei Jahren nach dem Schadensereignis insolvent.

Bei Lösungen rund um Sicherheitstechnik und Brandschutz wird der digitale Fortschritt – u. a. durch Cloud-Lösungen oder Künstliche Intelligenz (KI) – immer mehr zum Treiber für noch höhere Sicherheits- und Qualitätsstandards. Dies zeigt exemplarisch die vernetzte Nutzung von Brandschutz- und Videotechnik plus KI, die Prävention und Abwehr von Brandgefahren auf ein neues Level heben.

KI-basierte Videotechnik

So analysiert KI-basierte Videotechnik relevante Daten in Echtzeit, erkennt typische Bewegungen durch Infrarot, Brandschutz-Gefahrenmuster wie etwa Temperaturänderungen und unterscheidet zudem

zuverlässig zwischen echten Bränden und harmlosen Wärmequellen. „Ein deutliches Upgrade gegenüber herkömmlichen Kameras“, verdeutlicht Jörg Marmann, Geschäftsführender Direktor von Kötter Sicherheitssysteme. Das Schutzergebnis:

- Früherkennung statt Reaktion – selbst minimale Veränderungen werden wahrgenommen, bevor Rauch entsteht.
- Gezielte Alarmierung – Einsatzkräfte werden schneller und genauer informiert.
- Daraus resultierend: mehr Sicherheit – für Menschen, Anlagen und Prozesse.

Welchen physischen Anforderungen die technischen Systeme, aber auch die ausführenden Techniker, dabei gegenüberstehen, wird u. a. etwa beim Einsatz in der Industrie oder Logistik deutlich. Herausfordernde und extrem belastete Umgebungen – bspw. durch Luft, die mit Säuredämpfen, Staub oder Feuchtigkeit angereichert ist – machen Brandmeldeanlagen (BMA) elementar – sei es aufgrund von Versicherungsanforderungen oder aus dem berechtigten Schutzbedürfnis der Betreiber. Gepaart mit KI-Video-Lösungen – die u. a. auch erhöhte

oder untypische Bewegungsfrequenzen von Menschen und Maschinen registrieren – verbessern sie die Sicherheit deutlich.

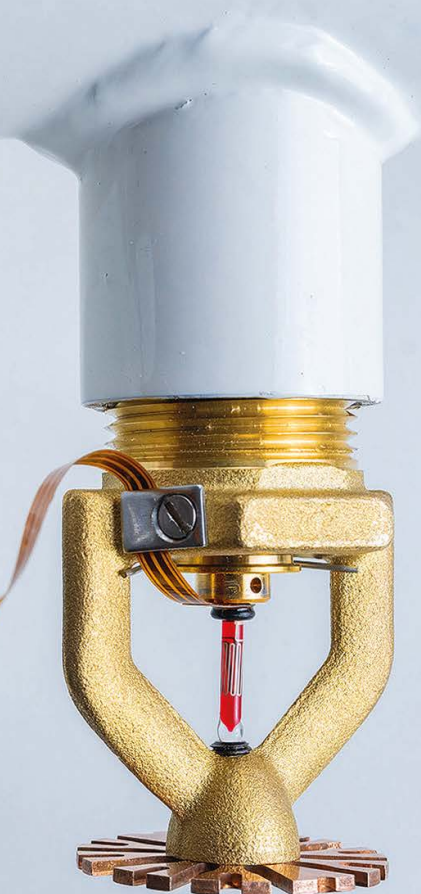
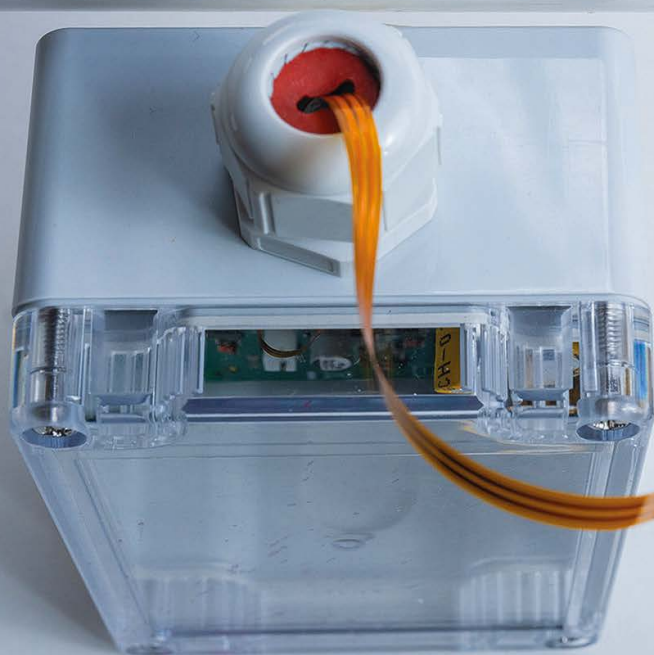
Die Implementierung in solchen Umgebungen ist kein Standard: Melder müssen besonders widerstandsfähig und fehlerarm sein; Videokameras kommen in sensiblen Bereichen zum Einsatz und liefern zusätzliche Funktionen und Vorteile für den Brandschutz. Modernisierungs- und Wartungsmaßnahmen – oft bei laufendem Betrieb und an schwer zugänglichen Stellen – verlangen dabei häufig individuelle, spezielle und dennoch nachhaltige Lösungen.

„Digitaler Fortschritt im Brandschutz ist also längst viel mehr als ein Trend“, so Jörg Marmann. Integration von Künstlicher Intelligenz sei ein entscheidender Schritt hin zu intelligenten, proaktiven Sicherheitslösungen. **GIT**



Kötter GmbH & Co. KG
Verwaltungsdienstleistungen
www.koetter.de

SmartFit bietet gezielten Brandschutz genau dort, wo Gefahr entsteht



SPRINKLERANLAGEN

Brandschutz, der mitdenkt

Smarte Sprinklerlösungen, die schneller reagieren, gezielter löschen und Werte effektiv schützen

Herkömmliche Sprinkleranlagen löschen dort, wo der Brand bereits intensiv tobt. Doch zur Bekämpfung von Rauchausbreitung oder zum Schutz von besonders leicht brennbaren Materialien gibt es effizientere Wege. Intelligente Smart Sprinkler mit digitaler Anbindung an die Brandmeldezentrale ermöglichen automatisierten und intelligenten Brandschutz, der sich an den individuellen Bedarf anpassen lässt.

Komplexe automatisierte Logistikgebäude benötigen Hochleistungslöschkonzepte und Brandschutzanlagen, um sensible Materialien oder große Sachwerte zu schützen. Die Systeme müssen derart ausgelegt sein, dass sie auch in den automatisierten Bereichen für eine effiziente Brandbekämpfung sorgen – denn die Feuerwehr dringt in diese Bereiche im Brandfall aus Selbstschutz nicht vor. Diese Gemengelage kann jedoch dazu führen, dass die Löschanlage nicht allen Risiken gerecht wird. Die Folge: hohe Investitions- und Wartungskosten. Zudem kann ein zu großer Wassereintrag hohe wirtschaftliche Schäden nach sich ziehen, wenn beispielsweise hochwertige Güter durch das Wasser zerstört werden. Daher ist es von großer Bedeutung, Brandschutzsystem so auszulegen, dass das Verhältnis zwischen den eingesetzten Löschmitteln und den zu erwartenden Auswirkungen auf das Gebäude und die gelagerten Mittel optimal ist.

Die Königsdisziplin des Brandschutzes

Je komplexer die Gebäudearchitektur und je schwerer zugänglich der zu löschende Bereich ist, umso schwieriger ist es, die Löschanlage optimal zu dimensionieren. Ein besonders extremes Beispiel stellen roboterbetriebene Würfellagersysteme dar, in denen Waren abmessungsoptimiert untergebracht werden, um den vorhandenen Platz optimal zu nutzen. Diese Lager sind in der Regel für die Brandbekämpfung durch die Feuerwehr nicht zugänglich. Wenn dann noch leicht entzündliche oder explosive Materialien gelagert werden, stoßen herkömmliche Brandschutzsysteme an ihre Grenzen.

Die Fire Protection Solutions Gruppe bringt zu diesem Zweck die Vorteile der Digitalisierung und Automatisierung in den Brandschutz und die Sprinklertechnologie ein. Brandschutzsysteme auf Basis der sogenannten Smart Sprinkler ermög-

lichen eine bidirektionale Kommunikation zwischen jedem individuellen Sprinkler und der Brandmeldezentrale. Nach Bedarf können die Sprinkler auf diese Weise gezielt elektrisch ausgelöst werden, um den Brandherd noch effektiver einzudämmen. Hierzu sendet die Brandmeldezentrale ein Signal an das Modul, welches anschließend durch einen elektrischen Impuls den Heizdraht, der auf dem Glasfässchen des Sprinklers aufgebracht ist, erhitzt, es so zum Platzen bringt und den Löschvorgang auslöst. In der Folge verkürzt sich die Reaktionszeit auf einen Brand deutlich. Zugleich sind ein präziseres Löschen und die effiziente Eindämmung von giftigen Gasen und Rauch möglich.

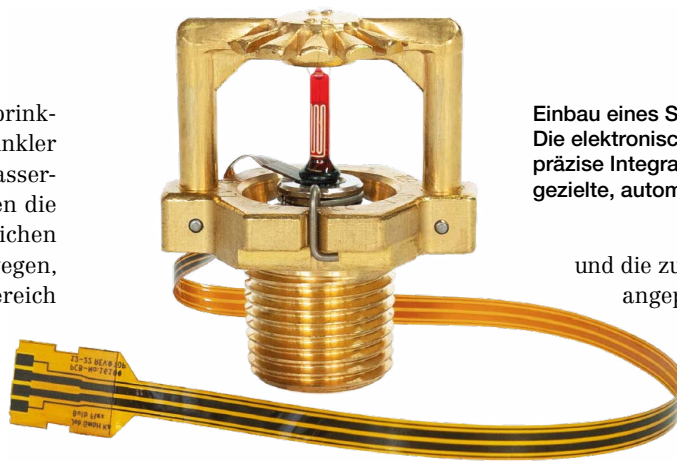
Automatisierte Sprinklerauslösung

Denn mit einem solchen System lassen sich automatisierte Löschmuster realisieren und Brände extrem genau orten. Auf diese Weise

können beispielsweise spezifische Sprinklergruppen oder individuelle Sprinkler angesteuert werden, um gezielt Wasservorhänge zu schaffen. Diese dämmen die Rauchentwicklung ein und ermöglichen das bewusste Schaffen von Fluchtwegen, falls sich Menschen im sensiblen Bereich aufhalten. In jedem Fall wird deutlich weniger Wasser benötigt, um einen Brand schnellstmöglich zu löschen.

Durch die beidseitige Verbindung und Kommunikation der Smart Sprinkler mit der Brandmeldezentrale ist beim ersten Auslösen eines Sprinklers sofort klar, wo das Feuer entsteht und wie es sich ausbreiten kann. Somit ist eine individuelle Reaktion auf jedes Brandereignis möglich. Hochentzündliche oder sonstige sensible Materialien in der Umgebung können durch gezieltes und schnelleres Auslösen von Sprinklern im Umfeld heruntergekühlt und die Entzündung somit verhindert werden. Herkömmliche temperaturabhängige Löschanlagen würden die Sprinkler im Umfeld in einem solchen Fall nicht auslösen. Außerdem wird das in einfacheren Löschanlagen häufig durch den Kühleffekt des Löschwassers auftretende Überspringen der nächstgelegenen Sprinkler verhindert.

Alle SmartSprinkler haben neben der elektrischen Auslösung die Möglichkeit, thermisch auszulösen – und das mit einem RTI(Response-Time-Index)-Wert <30 sogar schneller als der Industrie Standard Fast Response RTI<50. Durch die geringe Ansprechzeit werden hohe Temperaturen vermieden und gefährliche Pyrolyseprodukte wie brennbare Gase können erst gar nicht entstehen. So kann wertvolle Zeit für die Rettung von Menschenleben gewonnen werden.



Einbau eines SmartFit Sprinkler:
Die elektronische Anbindung und präzise Integration ermöglichen eine gezielte, automatisierte Auslösung

und die zu überwachenden Gegebenheiten angepasst werden kann.

Durch diese Individualisierung lassen sich auch alle vorgelagerten Systeme passgenau konfektionieren. Beispielsweise können Pumpen oder Wasserbehälter kleiner dimensioniert werden. Auch Rohrquerschnitte lassen sich auf diese Weise reduzieren. Die Anschaffungs- und Montagekosten dieser Komponenten sinken somit.

Für hochkomplexe Strukturen wie die eingangs erwähnten automatisierten und roboterbetriebenen Lagersysteme werden mit dieser Technologie neue Wege für hocheffiziente Löschsysteme geschaffen. Die hängend oder stehend montierbaren Sprinkler mit flexiblen Sprühcharakteristiken gewährleisten die Realisierung von Löschanlagen, die genau am richtigen Ort in dem Maß löschen, wie es für das jeweilige Gebäude und zu schützende Material optimal ist.

Abschließend bleibt festzuhalten, dass eine Brandschutzanlage mit Smart-Sprinkler-Technologie Brände schneller orten, automatisiert und hochpräzise bekämpfen und Kosten in der wasserführenden Löschinfrastruktur verringern kann. Menschenleben und große Sachwerte werden durch die minimale Ansprechzeit der Systeme und die intelligenten Löschmuster besser geschützt.



Fire Protection Solutions
www.fire-protection-solutions.com

© Bilder: Fire Protection Solutions

Schraner-Group präsentierte Portfolio auf der FeuerTrutz

Die FeuerTrutz in Nürnberg war auch in diesem Jahr trotz der hohen Temperaturen ein Besuchermagnet. Mit dabei war auch wieder die Schraner-Group mit ihren sieben Unternehmen und einer Vielzahl an technischen und digitalen Lösungen rund um das Thema Brandschutz. Basketball verbindet und erleichtert den Einstieg in das gemeinsame Netzwerken. Und so war es auch nicht verwunderlich, dass der Messestand der Schraner-Group auf der FeuerTrutz in Nürnberg in diesem Jahr erneut ein Publikumsmagnet war.

Unter der professionellen Anleitung von BBL-Rekordspieler und Markenbotschafter der BMA365 Bamberg Baskets, Karsten Tadda, hatten die Messebesucher die

Gelegenheit, ihre Treffsicherheit am Korb unter Beweis zu stellen. Zu gewinnen gab es dafür einen Basketball. Seit 2023 sind die erfolgreichen Bamberger Basketballer Teil der Unternehmensgruppe. Als besonderes Highlight brachten sie den in dieser Saison gewonnenen BBL-Pokal mit und stellten ihn am Stand aus.

Die Aktion kam an und war häufig der Einstieg in fachlich tiefe und sehr gehaltvolle Gespräche. „Es waren wieder sehr viele Besucher an unserem Stand und wir ziehen insgesamt eine positive Bilanz“, sagte Marketingleiterin Kerstin Hilpert vom Erfolgslabor der Schraner-Group im Nachgang über die Messe. www.schraner-group.de



V.l.n.r.: Malte Riks, Business Development Manager, Tunc Kurnaz, Salex Executive, und Aljona Ijoschina, Geschäftsführerin bei Datolution

TOP PLAYER

GEFAHRSTOFF-HANDLING

Günther
Rossdeutscher

Geschäftsführer, Asecos



Mit der Weiterentwicklung der Ion-Line Sicherheitsschränke und neuen Lösungen wie dem Core Store adressieren Sie die steigenden Risiken durch Lithium-Ionen-Akkus. Wie verändern Sie die Sicherheitsstandards in Laboren und Industrie?

Günther Rossdeutscher: Beim Thema Lithium-Akkus sehen wir aktuell noch einen klaren Unterschied zwischen Laboren und Industrie: Während Akkus in der Industrie bereits weit verbreitet sind, spielen sie in Laboren meist noch eine eher indirekte Rolle – und betreffen dort vor allem Arbeitsgeräte außerhalb des eigentlichen Laborbetriebs. Dennoch gilt: Es braucht sichere, geprüfte Lagerlösungen. Genau hier setzen wir an und ermöglichen mit unseren Ion-Line Modellen die verlässliche Einhaltung der Sicherheitsstandards in beiden Bereichen.

Asecos investiert aktuell stark in die Forschung von Filtrationssystemen für Gefahrstoffarbeitsplätze und engagiert sich gleichzeitig intensiv in Normungsgremien. Welche strategische Rolle spielt dies für Ihre Position als Marktführer in der Gefahrstofflagerung?

Günther Rossdeutscher: Als Marktführer in der sicheren Gefahrstofflagerung und der sicheren Lagerung von Lithium-Akkus verfügen wir über ausgewiesene Expertise. Damit unser praxiserprobtes Wissen und unsere bewährten Lagerlösungen in Standards einfließen und normativ berücksichtigt werden, arbeiten wir in VDMA-, EN- und ISO-Gremien mit. Parallel dazu investieren wir in den beiden genannten Kernbereichen sowie in der Absaugung von gesundheitsschädlichen Dämpfen gezielt in Forschung – als Grundlage unserer Produktentwicklung.

Welche Entwicklungen werden aus Ihrer Sicht die Gefahrstofflagerung und das Gefahrstoffhandling in den nächsten Jahren prägen? Welche Märkte – vertikal und regional – sind für Sie am vielversprechendsten?

Günther Rossdeutscher: Bei der Auswahl der richtigen Produkte gewinnen digitale Tools an Bedeutung. Dem begegnen wir mit unserem 3D-Ion-Line-Konfigurator: Über fachspezifische Fragen gelangen Kunden Schritt für Schritt zur passgenauen Lösung für die sichere Lagerung von Lithium-Akkus. Bei Bedarf begleiten wir die Konfi-

guration im persönlichen Gespräch. Perspektivisch erweitern wir unser Online-Tool um weitere Produktgruppen wie Gefahrstoffarbeitsplätze. Die letzte Frage nach einer Marktprognose lässt sich für uns nur schwer pauschal beantworten, da wir mit unserem breiten Angebot in vielen Bereichen präsent sind.



Asecos GmbH
www.asecos.com

TOP PLAYER

GEFAHRSTOFF-MANAGEMENT

Horst Rose

Managing Director / CSO, Denios

Mit neuen Lösungen wie Power Safe, Power Store und erweiterten IoT-Funktionen für Sicherheitsschränke und Sicherheitsräume für Batteriespeicher reagiert Denios auf die stark steigende Nachfrage nach Lithium-Ionen-Sicherheit. Welche Neuerungen – etwa bei Brandfrüherkennung, Kühlung oder digitalem Monitoring – sind für Ihre Kunden aktuell besonders entscheidend?

Horst Rose: Die Sicherheit im Umgang mit Lithium-Ionen-Batterien ist für viele Unternehmen zu einer zentralen Herausforderung geworden. Unsere Kunden wünschen sich heute vor allem ganzheitliche Lösungen, die über die reine Lagerung hinausgehen und Risiken frühzeitig erkennen sowie aktiv minimieren.

Besonders gefragt sind daher intelligente Sicherheitskonzepte mit integrierter Brandfrüherkennung, permanenter Temperaturüberwachung und digitalem Monitoring. Mit unseren IoT-Lösungen können relevante Betriebszustände in Echtzeit überwacht und kritische Veränderungen frühzeitig erkannt werden. Dadurch erhalten Anwender die Möglichkeit, schnell zu reagieren und potenzielle Gefahren bereits im Entstehungsstadium einzudämmen.

Insgesamt beobachten wir, dass die Nachfrage nach vernetzten, transparenten und skalierbaren Sicherheitslösungen kontinuierlich wächst. Kunden möchten jederzeit wissen, in welchem Zustand sich ihre Energiespeicher befinden, und gleichzeitig die Gewissheit haben, dass Menschen, Umwelt und Sachwerte bestmöglich geschützt sind.

Denios verfolgt mit der Vision Zero einen ganzheitlichen Sicherheitsansatz und baut gleichzeitig Engineering-Kompetenz und internationale Präsenz weiter aus. Welche strategischen Prioritäten setzen Sie, um Ihre Rolle als globaler Marktführer für Gefahrstofflagerung und Lithium-Ionen-Sicherheit zu stärken?

Horst Rose: Unsere strategische Ausrichtung folgt einem klaren Ziel: Wir wollen

Unternehmen weltweit dabei unterstützen, Menschen, Umwelt und Sachwerte bestmöglich zu schützen. Die Vision Zero – also das Ziel von null Unfällen, null Umweltschäden und maximaler Sicherheit – bildet dabei die Grundlage unseres Handelns. Um unsere Position als weltweit führender Anbieter für Gefahrstofflagerung weiter auszubauen, setzen wir auf drei zentrale Schwerpunkte: Erstens investieren wir kontinuierlich in die Entwicklung neuer Produkte und Lösungen. Insbesondere die sichere Lagerung und das Laden von Lithium-Ionen-Batterien sowie digitale Sicherheitslösungen und IoT-Anwendungen bieten großes Potenzial, um Risiken frühzeitig zu erkennen und Sicherheitsstandards weiter zu erhöhen. Zweitens bauen wir unsere Engineering-Kompetenz konsequent aus. Viele Kunden benötigen heute individuelle und standortspezifische Lösungen, die technische, regulatorische und betriebliche Anforderungen gleichermaßen berücksichtigen. Hier unterstützen wir mit umfassender Beratung, Planung und Umsetzung aus einer Hand. Drittens stärken wir unsere internationale Präsenz, um Kunden weltweit mit einheitlich hohen Qualitäts- und Sicherheitsstandards zu begleiten. Gleichzeitig ermöglichen uns unsere lokalen Teams, regionale Anforderungen und Marktgegebenheiten optimal zu berücksichtigen. Unser Anspruch ist es, nicht nur Produkte zu liefern, sondern als langfristiger Partner ganzheitliche Sicherheitslösungen anzubieten. Genau darin sehen wir den Schlüssel, um unsere Marktführerschaft nachhaltig auszubauen.

Welche Entwicklungen werden aus Ihrer Sicht die nächsten Jahre den Bereich Gefahrstofflagerung prägen? Welche Märkte – vertikal und regional – sind für Sie am vielversprechendsten?

Horst Rose: Die Anforderungen an die Gefahrstofflagerung werden in den kommenden Jahren weiter steigen. Treiber sind insbesondere strengere regulatorische Vorgaben, höhere Nachhaltigkeitsanforderungen, die fortschreitende Digitalisierung



sowie die zunehmende Elektrifizierung von Industrie, Logistik und Mobilität.

Ein zentrales Zukunftsthema bleibt die sichere Handhabung von Lithium-Ionen-Batterien. Mit dem Wachstum der Elektromobilität, stationärer Energiespeicher und batteriebetriebener Geräte steigt weltweit der Bedarf an sicheren Lösungen für Lagerung, Laden, Transport und Recycling. Gleichzeitig erwarten Unternehmen zunehmend integrierte Sicherheitskonzepte, die bauliche Schutzmaßnahmen mit digitalem Monitoring und vorausschauender Wartung verbinden.

Auch die Digitalisierung wird die Branche nachhaltig verändern. Vernetzte Systeme, Echtzeitüberwachung und datenbasierte Services werden dazu beitragen, Risiken früher zu erkennen, Prozesse effizienter zu gestalten und die Betriebssicherheit weiter zu erhöhen.

Unabhängig von Branche oder Region erwarten wir, dass Unternehmen Sicherheit künftig noch stärker als strategischen Erfolgsfaktor betrachten werden. Anbieter, die regulatorische Expertise, innovative Technologien und ganzheitliche Lösungen miteinander verbinden, werden von dieser Entwicklung besonders profitieren.



Denios SE
www.denios.de

TOP PLAYER

MASCHINEN- UND ANLAGENSICHERHEIT

André Hartmann

Head of German Sales, Bihl+Wiedemann GmbH

Sie haben Ihr Portfolio zuletzt um neue ASi-5 und ASi-3 Module, Gateways und Safety-Komponenten erweitert. Welche technologischen Fortschritte ermöglichen diese Lösungen – und welchen konkreten Mehrwert bieten sie Maschinenbauern und Betreibern in Bezug auf Diagnose, Effizienz und Flexibilität?

André Hartmann: Im vergangenen halben Jahr lag unser Fokus insbesondere auf der Weiterentwicklung unseres ASi-5 Safety Portfolios. Mit ASi-5 Safety schaffen wir neue Möglichkeiten hinsichtlich Skalierbarkeit und Effizienz in sicherheitsgerichteten Anwendungen. Ein wesentlicher Vorteil besteht darin, dass mehrere sichere Signale über eine einzige ASi-5 Safety-Adresse übertragen werden können. Während bei ASi-3 zum Beispiel acht sichere zweikanalige Eingänge auch acht ASi-Adressen belegen, lassen sich diese Signale heute mit nur einer ASi-5 Safety-Adresse abbilden. Dadurch stehen Anwendern deutlich mehr Ressourcen innerhalb des Netzwerks zur Verfügung, was insbesondere bei komplexen Maschinen und modularen Anlagenkonzepten erhebliche Vorteile bietet.

Neben der Weiterentwicklung unseres Produktportfolios haben wir in den vergangenen Monaten intensiv an der Umsetzung der Anforderungen des Cyber Resilience Act (CRA) gearbeitet. Auch wenn daraus nicht unmittelbar neue Produkte entstanden sind, war dies ein strategisch wichtiger Schritt. Unser Ziel war es, unsere bestehenden Produkte und Entwicklungsprozesse frühzeitig an die neuen regulatorischen Anforderungen anzupassen und gleichzeitig die langfristige Verfügbarkeit unserer Lösungen sicherzustellen.

Für unsere Kunden bedeutet dies vor allem Investitionssicherheit und Verlässlichkeit. Sie können darauf vertrauen, dass unsere Produkte auch künftig den gesetzlichen Anforderungen entsprechen und ohne Einschränkungen weiter eingesetzt werden

können. Damit unterstützen wir Maschinenbauer und Anlagenbetreiber nicht nur technologisch, sondern auch dabei, zukünftige regulatorische Anforderungen sicher und planbar zu erfüllen.

Bihl+Wiedemann positioniert sich zunehmend als Komplettanbieter für dezentrale Automatisierungslösungen. Welche strategische Rolle spielen dabei Themen wie Interoperabilität, einfache Integration in bestehende Feldbuswelten und die Weiterentwicklung von ASi Safety at Work?

André Hartmann: Wir sehen uns nicht als Komplettanbieter für die Automatisierungstechnik. Unsere Vision ist es, weltweit das individuelle Nervensystem in Maschinen, Anlagen und Gebäuden zu sein. Genau daraus leitet sich auch unsere Strategie ab. Interoperabilität und die einfache Integration unserer Lösungen sind für uns keine Zusatzfunktionen, sondern Grundvoraussetzungen. Es spielt keine Rolle, welche Standardsteuerung, welche Feldbus- oder Industrial-Ethernet-Technologie, welche Sensorik oder welche Antriebstechnik unsere Kunden einsetzen. Unsere Aufgabe ist es, diese Komponenten effizient miteinander zu verbinden und den Datenaustausch bis in die Feldebene hinein so einfach wie möglich zu gestalten. Unser Fokus liegt dabei konsequent auf der Reduzierung von Verdrahtungsaufwand und Komplexität. Denn genau hier können Maschinenbauer und Anlagenbetreiber erhebliche Kosten einsparen, die Inbetriebnahme beschleunigen und die Flexibilität ihrer Maschinen und Anlagen steigern. Dies trägt unmittelbar zur Wettbewerbsfähigkeit unserer Kunden bei. Deshalb entwickeln wir gemeinsam mit unseren Partnern einfache, robuste und ressourcenschonende Lösungen für die Automatisierungstechnik. Die kontinuierliche Weiterentwicklung von ASi und ASi Safety ist dabei ein wesentlicher Bestandteil



unserer Strategie. Unser Ziel ist es nicht, möglichst viele Technologien anzubieten, sondern die beste und effizienteste Verbindung zwischen Feldgeräten und Steuerung zu schaffen – unabhängig von der eingesetzten Automatisierungswelt.

Welche Entwicklungen werden aus Ihrer Sicht in den nächsten Jahren die industrielle Automatisierung prägen? Welche Märkte – vertikal und regional – sind für Sie am vielversprechendsten?

André Hartmann: Aus meiner Sicht werden die industrielle Automatisierung in den kommenden Jahren vor allem zwei Entwicklungen prägen, die sich zunehmend überlagern: die steigenden Anforderungen an Cybersecurity – insbesondere im Zuge des Cyber Resilience Act (CRA) – sowie die verstärkte Nutzung von Künstlicher Intelligenz im Kontext von Industrie 4.0.

Beide Themen basieren auf einer gemeinsamen Voraussetzung: der Verfügbarkeit hochwertiger Daten aus dem Produktionsprozess. Genau hier sind wir seit vielen Jahren sehr gut aufgestellt. Unser Ansatz besteht darin, Signale direkt dort zu digitalisieren, wo sie entstehen – unmittelbar an Sensoren und Aktoren in der Maschine oder Anlage. Dafür bieten wir hochgranulare Automatisierungslösungen an, bei denen bereits die Anbindung eines

einzelnen IO-Link-Sensors oder Aktors wirtschaftlich sinnvoll umgesetzt werden kann. So schaffen wir die Grundlage für eine durchgängige Datentransparenz bis in die Feldebene und ermöglichen es unseren Kunden, die Potenziale von Industrie 4.0 und zukünftigen KI-Anwendungen optimal zu nutzen.

Gleichzeitig rückt das Thema Cybersecurity immer stärker in den Fokus. Auch hier bietet unser Ansatz entscheidende Vorteile. Im Vergleich zu vielen anderen Architekturen ist es in zahlreichen Anwendungen nicht

erforderlich, Ethernet-basierte Feldbusnetzwerke flächendeckend innerhalb der Anlage zu verteilen. Dadurch reduziert sich die Komplexität der Kommunikationsinfrastruktur und die Anzahl potenzieller Angriffspunkte. Dies erleichtert die Umsetzung robuster Security-Konzepte und unterstützt unsere Kunden dabei, die Anforderungen des CRA effizient und nachhaltig zu erfüllen. Gerade vor diesem Hintergrund sehen wir großes Potenzial in Branchen mit einem hohen Automatisierungsgrad und einer großen Anzahl dezentraler Feldgeräte. Dazu

zählen beispielsweise die Intralogistik, die Robotik, die Verpackungs- und Fördertechnik sowie die Halbleiterindustrie. Hier können unsere Lösungen einen wesentlichen Beitrag leisten, um Datenverfügbarkeit, Effizienz und Cybersecurity gleichermaßen zu verbessern.



Bihl + Wiedemann GmbH
www.bihl-wiedemann.de

TOP PLAYER

FEUERLÖSCHER

Achim Giesselmann

Sale Director Gloria

Gloria hat sein Portfolio zuletzt um modernisierte Feuerlöscher-Generationen und Lösungen für Lithium-Ionen-Brände erweitert. Welche technologischen Neuerungen sind dabei besonders relevant für den professionellen Brandschutz?

Achim Giesselmann: Zum Zeitpunkt der Einführung im Jahr 2020 gab es noch keine Feuerlöscher-Norm für Lithiumbrände. Daher wurden von uns seinerzeit belastbare und erfolgreiche Tests in Zusammenarbeit mit der niederländischen KIWA durchgeführt. Die Norm für Lithiumbrände steht nun kurz vor der Verabschiedung und wir sind zuversichtlich, dass unsere bisherige Löscherkonfiguration der neuen Norm entsprechen wird. Wichtig ist auch weiterhin die Erkenntnis, dass ein tragbarer Feuerlöscher weiterhin als wesentliche Eigenschaft am Lithiumbrand eine Kettenreaktion durch Kühlen – nicht durch Löschen – verhindern soll. Lithiumbrände sind weiterhin höchst komplex und für nicht ausgebildete Personen ohne Schutzausrüstung sehr gefährlich

und nur begrenzt einsetzbar (z. B. an Akkus für E-Bikes).

Sie setzen stark auf Qualität, Normenkonformität und ein flächendeckendes Servicenetz. Welche strategischen Schwerpunkte verfolgen Sie aktuell, um Ihre Position im professionellen Brandschutz weiter auszubauen?

Achim Giesselmann: Wir setzen neben Qualität, Beratung sowie Normkonformität für die Ausrüstung von Arbeitsstätten vor allem auf Nachhaltigkeit und wartungsfreundliche Produkte mit langer Lebensdauer. So haben wir unser Unternehmen und den Vertrieb schon Ende 2024 komplett auf fluorfreie Löschmittel umgestellt. Noch in diesem Jahr werden wir ein weiteres, sehr wartungsfreundliches Schaumlöschgerät als Kartuschenlösung einführen.

Für Folgeschulungen in Betrieben entwickeln wir zudem konsequent unseren VR-Fire-Trainer weiter. Mit Einführung von Augmented Reality setzen wir in dem Bereich wieder neue Maßstäbe.



Welche Entwicklungen werden im kommenden Jahr aus Ihrer Sicht den Brandschutz prägen? Welche Märkte – vertikal und regional – sind für Sie am vielversprechendsten?

Achim Giesselmann: Die Antwort ist einfach: Die Branche wird bis zum Jahr 2030 mit der Fluorfrei-Transformation und der Entsorgung fluorhaltiger Löschmittel zu tun haben.



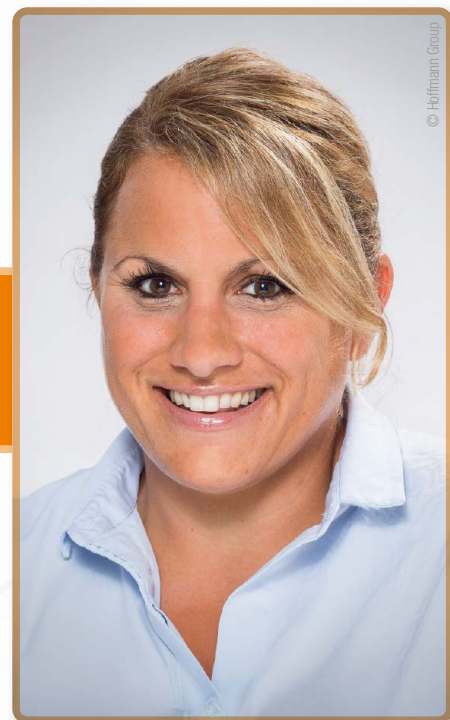
Gloria GmbH
www.gloria.de

TOP PLAYER

PSA

Alexandra Kovacs

Category Managerin, Hoffmann Group



Wie beurteilt die Hoffmann Group die aktuelle Marktlage und welche Konsequenzen zieht sie daraus?

Alexandra Kovacs: Wir erleben volatile Preise, Verfügbarkeitsprobleme und eine insgesamt schwierige wirtschaftliche Situation in wichtigen Industriezweigen. Besonders in der Metallverarbeitung und der Automobilindustrie sehen wir derzeit deutliche Einschnitte. Unsere Aufgabe besteht darin, kreative Lösungen zu entwickeln und unsere Kunden dabei zu unterstützen, ihre Ziele trotz dieser Rahmenbedingungen zu erreichen. Die Hoffmann Group versteht sich als Partner, der Beschaffungssicherheit gewährleistet. Als global agierendes Handelsunternehmen können wir Lieferfähigkeit sicherstellen und gleichzeitig helfen, Kostensteigerungen abzufedern. Unsere Mehrmarkenstrategie mit den großen PSA-Herstellern und unseren Eigenmarken schafft zusätzliche Sicherheit für die Kunden.

Mit elektronischen Bestellplattformen, Ausgabesystemen und digitalen Lösungen unterstützen wir Unternehmen dabei, ihre Prozesse effizienter und widerstandsfähiger zu gestalten.

Tobias Zöllkau: Die Kunden müssen sich ständig an veränderte Marktbedingungen

anpassen. Genau dabei wollen wir sie unterstützen. Es geht um Versorgungssicherheit, Kostenkontrolle und die Fähigkeit, die eigene Produktion trotz schwieriger Rahmenbedingungen aufrechtzuerhalten. Unser Anspruch ist es, nicht nur Lieferant zu sein, sondern ein Partner, der den Kunden hilft, sich zukunftsicher aufzustellen.

Welche Herausforderungen treiben die Kunden im Bereich Arbeitssicherheit derzeit besonders um?

Tobias Zöllkau: Die Kunden stehen heute unter erheblichem Druck. Sie müssen ihre Arbeitsplätze sicher gestalten, gleichzeitig Kosten kontrollieren und immer komplexere Anforderungen erfüllen. Hinzu kommen neue gesetzliche Vorgaben, veränderte Normen und technologische Entwicklungen. Viele Unternehmen suchen deshalb nach Partnern, die nicht nur Produkte liefern, sondern den gesamten Prozess begleiten. Das betrifft die Versorgung der Mitarbeiter ebenso wie die Digitalisierung von Beschaffungs- und Ausgabesystemen.

Ein weiterer wichtiger Punkt ist die Akzeptanz von persönlicher Schutzausrüstung. Früher wurde PSA häufig als notwendiges Übel betrachtet. Heute erwarten die Mitarbeiter Komfort, Ergonomie und modernes Design. Unternehmen erkennen

gleichzeitig, dass hochwertige Schutzausrüstung ein Instrument der Mitarbeiterbindung und Wertschätzung sein kann. Ein guter Sicherheitsschuh oder eine hochwertige Schutzkleidung sind längst nicht mehr nur Mittel zur Unfallverhütung. Sie signalisieren dem Mitarbeiter, dass seine Gesundheit und sein Wohlbefinden ernst genommen werden.

Alexandra Kovacs: Wir beobachten, dass die Anforderungen an die Arbeitsplätze kontinuierlich steigen. Deshalb müssen Produkte heute nicht nur Schutz bieten, sondern auch ergonomisch und komfortabel sein. Die Nutzer akzeptieren Schutzausrüstung wesentlich stärker, wenn sie angenehm zu tragen ist und gleichzeitig modern aussieht.

Welche technologischen Entwicklungen treiben Sie im PSA-Bereich voran?

Alexandra Kovacs: Ein besonders wichtiges Thema für uns ist die Digitalisierung im Bereich Sicherheitsschuhe und Ergonomie. Wir haben die Prozesse kontinuierlich weiterentwickelt. Heute kommt unser Fachberater mit einem 3D-Scanner direkt zum Kunden. Die Füße werden digital vermessen, und das System empfiehlt automatisch geeignete Modelle auf Basis von Größe, Gewicht, Einsatzbereich und Sicherheitsan-



Tobias Zöllkau

Regionalvertriebsleiter, Hoffmann Group

forderungen. Das System erkennt außerdem mögliche Fehlstellungen und kann Hinweise auf orthopädischen Unterstützungsbedarf geben.

Tobias Zöllkau: Technologie darf nie Selbstzweck sein. Sie muss dazu beitragen, dass die Mitarbeiter gesünder arbeiten können und die Unternehmen ihre Prozesse effizienter gestalten. Der 3D-Scan ist dafür ein gutes Beispiel, weil er Ergonomie, Gesundheitsschutz und digitale Prozesse miteinander verbindet.

Wo sieht die Hoffmann Group die wichtigsten Wachstumstreiber?

Alexandra Kovacs: Wir betrachten das aus zwei Perspektiven. Zum einen können wir aus dem sehr breiten Portfolio der Hoffmann Group schöpfen. Wir bieten nicht nur persönliche Schutzausrüstung an, sondern auch Betriebseinrichtungen, ESD-Lösungen, Handwerkzeuge und viele weitere Produkte rund um die industrielle Arbeitswelt. Dadurch können wir unseren Kunden ganzheitliche Sicherheits- und Arbeitsplatzkonzepte anbieten.

Zum anderen sehen wir Wachstum in neuen Märkten. Besonders stark entwickelt sich derzeit die Nachfrage aus dem Bereich der erneuerbaren Energien. Gleichzeitig

steigt der Bedarf an europaweiten und internationalen Versorgungskonzepten. Viele Unternehmen möchten ihre Techniker weltweit mit einheitlicher PSA ausstatten. Dafür entwickeln wir zentrale Konzepte, die international ausgerollt werden können.

Tobias Zöllkau: Darüber hinaus entsteht Wachstum durch kontinuierliche Veränderungen bei Normen, Gesetzen und Produktionsverfahren. Jede Veränderung führt dazu, dass Unternehmen ihre Sicherheitskonzepte überprüfen und anpassen müssen. Genau dabei unterstützen wir sie.

Wie wird sich der PSA-Markt in den kommenden Jahren entwickeln?

Tobias Zöllkau: Der PSA-Markt wächst seit Jahren kontinuierlich. Ein wichtiger Grund dafür ist die deutlich gestiegene Akzeptanz. Persönliche Schutzausrüstung wird heute ganz anders wahrgenommen als früher. Sie ist ein wesentlicher Bestandteil der Mitarbeitermotivation. Wer hochwertige Ausrüstung erhält, empfindet das als Wertschätzung. Wenn die Kleidung zusätzlich personalisiert ist oder das Firmenlogo trägt, stärkt das die Identifikation mit dem Unternehmen.

Gleichzeitig dürfen wir nie vergessen, worum es eigentlich geht: den Schutz von Menschen.

Interessant ist dabei ein Phänomen, das wir als ‚Overprotection‘ bezeichnen. Viele Unternehmen entscheiden sich bewusst für höhere Schutzstandards, als sie rein formal benötigen würden. Früher stand oft die Frage im Vordergrund, wie man möglichst wenig investieren kann. Heute beobachten wir häufiger die Haltung: Lieber etwas mehr Schutz als zu wenig.



SicherMacher
Der GIT-Talk mit den Marktführern



Jetzt ansehen:
das vollständige
Interview in unserem
Video-Podcast



Hoffmann SE
www.hoffmann-group.com

TOP PLAYER

BRANDMELDETECHNIK

Simon Schurr

Abteilungsleiter Produktmanagement
Brandmeldetechnik, Telenot

Telenot hat sein Portfolio im Bereich Brandmeldetechnik zuletzt erweitert. Welche Neuerungen sind für Ihre Kunden aktuell besonders relevant?

Simon Schurr: Mit der EBLCloud haben wir unser Portfolio um eine zukunftssichere digitale und vor allem normkonforme Serviceplattform erweitert. Sie ermöglicht Fachbetrieben digitale Services wie Fernwartung, Ferndiagnose, digitale Prüfprotokolle und die zentrale Verwaltung aller Kundenanlagen aus einer Hand anzubieten. Gleichzeitig eröffnet die EBLCloud neue Geschäftsmodelle für Errichter. Betreiber profitieren von transparenten Anlageninformationen, automatischen Benachrichtigungen sowie einem digitalen Betriebsbuch, während Fachbetriebe zusätzliche Service- und Betreuungsleistungen anbieten können. Ein weiteres wichtiges Thema ist die Vereinfachung und Beschleunigung der Inbetriebnahme von Brandmeldeanlagen. Der zunehmende Fachkräftemangel erfordert intelligente Werkzeuge, die unsere Partner im Arbeitsalltag unterstützen. Mit der neuen App Hiscan 4000 haben wir genau dafür eine praxisorientierte Lösung geschaffen. Sie ermöglicht es, Projekte direkt vor Ort digital anzulegen, Komponenten per Smartphone-Kamera zu erfassen und alle relevanten Informationen wie Meldergruppe, Meldernummer und Kundentext unmittelbar zu dokumentieren. Die Daten können anschließend nahtlos in die Parametriersoftware compas-F 4000 übernommen werden. Dadurch lassen sich Inbetriebnahmeprozesse

um bis zu 50 Prozent beschleunigen und Fehlerquellen deutlich reduzieren.

Sie setzen im Brandschutz stark auf zertifizierte Qualität, ein bundesweites Fachpartnernetzwerk und Lösungen für anspruchsvolle KRITIS und Gewerbeumgebungen. Welche strategischen Schwerpunkte verfolgen Sie, um Ihre Position im professionellen Brandschutz weiter auszubauen?

Simon Schurr: Wir sehen es als gemeinsame Herausforderung, die komplexen regulatorischen Anforderungen wie Kritis-Dachgesetz und NIS-2 effizient umzusetzen, die wir mit unseren Partnern angehen. Diese strengen Vorgaben bieten jedoch gleichzeitig die große Chance, sich durch nachweisbare Cyber-Resilienz klare Wettbewerbsvorteile und neues Wachstum zu sichern. Gemeinsam entwickeln wir die passenden Lösungen, wobei wir unseren Partnern mit der EBLCloud das perfekte Werkzeug an die Hand geben, um Compliance und Zukunftsfähigkeit sicher zu vereinen.

Welche Entwicklungen werden aus Ihrer Sicht die nächsten Jahre des Brandschutzes prägen? Welche Märkte – vertikal und regional – sind für Sie am vielversprechendsten?

Simon Schurr: Vertikal sehen wir Potenzial in zwei Kernbereichen: Erstens im Bildungs- und öffentlichen Sektor (Schulen), wo wir durch staatliche Sonderver-

mögen und Investitionspakete den akuten Investitionsstau auflösen können. Zweitens in der Industrie, wo Unternehmen unter dem Druck von NIS-2 und dem Schutz ihrer Produktion massiv in resiliente, zukunfts-sichere Infrastruktur investieren müssen. Aktuell bedienen wir schwerpunktmäßig den sehr heterogenen Markt in Deutschland. In Zukunft soll auch die komplette DACH-Region von unserer Brandmeldetechnik profitieren und unser Partner-Netzwerk dahingehend ausgebaut werden.



Telenot Electronic GmbH
www.telenot.com

TOP PLAYER

SENSOREN

Dr. Henning Grözin

CTO, Leuze-Gruppe



Mit neuen Sensorserien wie der 5B Baureihe und erweiterten IO-Link-fähigen Modellen haben Sie Ihr Portfolio zuletzt deutlich ausgebaut. Wie unterstützen Sie Maschinenbauer und Betreiber bei Präzision, Verfügbarkeit und smarter Diagnose?

Dr. Henning Grözin: Aktuell liegt unser Fokus auf dem Sicherheits-Laserscanner RSL 200, dem kleinsten Sicherheits-Laserscanner in unserem Portfolio, der mit dem GIT Award 2026 ausgezeichnet wurde. Im Mittelpunkt stehen dabei insbesondere Anwendungen in mobilen Fahrerlosen Transportsystemen (FTS) und autonomen mobilen Robotern (AMR). Dieses Produkt werden wir kontinuierlich weiterentwickeln, um den steigenden Anforderungen moderner Intralogistik- und Automatisierungslösungen gerecht zu werden. Ein weiterer Schwerpunkt ist unser Barcode-Positioniersystem FBPS. Es vereint als einzigartige Lösung am Markt die sichere Geschwindigkeitsüberwachung von Fahrzeugen mit präziser Positionierung und trägt so für unsere Kunden maßgeblich zu maximaler Effizienz und hoher Arbeitssicherheit in automatisierten Materialflussprozessen bei.

Leuze positioniert sich seit Jahren als 'The Sensor People' und investiert stark in internationale Expansion sowie branchenspezifische Lösungen. Welche strategischen Schwerpunkte setzen Sie aktuell?

Dr. Henning Grözin: Wir erweitern unser Angebot konsequent von einzelnen Komponenten hin zu ganzheitlichen Lösungsansätzen. Neben innovativen Safety-Lösungen entwickeln wir maßgeschneiderte Applikationslösungen, die unsere Kunden bei konkreten Herausforderungen in ihren Automatisierungsprozessen unterstützen. Ein Beispiel hierfür sind Übergabestationen zwischen Fahrerlosen Transportsystemen (FTS) und Roboterzellen, bei denen Sicherheit, Verfügbarkeit und Effizienz optimal aufeinander abgestimmt werden müssen.

Gleichzeitig bauen wir unsere Branchenkompetenz kontinuierlich aus und entwickeln gezielt Lösungen für ausgewählte Industrien. Ein besonderer Fokus liegt dabei auf der Verpackungsindustrie. Für diesen Bereich bieten wir ein umfassendes Edelstahlportfolio an, das sowohl Anforderungen im Wash-Down-Bereich als auch im Hygienic Design erfüllt und damit höchste Standards hinsichtlich Reinigbarkeit, Produktsicherheit und Anlagenverfügbarkeit unterstützt.

Welche Entwicklungen werden aus Ihrer Sicht die nächsten Jahre der industriellen Sensorik prägen? Welche Märkte – vertikal und regional – sind für Sie am vielversprechendsten?

Dr. Henning Grözin: Aus Marktsicht sehen wir insbesondere in der Intralogistik großes Potenzial. Die zunehmende Verbreitung von Fahrerlosen Transportsystemen (FTS) und autonomen mobilen Robotern (AMR)

eröffnet attraktive Wachstumschancen, für die wir mit unserem Portfolio sehr gut aufgestellt sind. Darüber hinaus werden wir einen besonderen Fokus auf die Bereiche Robotics, Batteriefertigung und die Verpackungsindustrie legen.

Regional bleibt China ein zentraler Wachstumsmarkt und ist bereits heute unser zweitstärkster Markt weltweit. Gleichzeitig sehen wir eine hohe Dynamik in Südostasien. Die Region entwickelt sich sehr positiv, und dank unseres Werks inklusive Distributionszentrum in Malaysia können wir diesen Markt schnell und effizient bedienen.

Technologisch wird Künstliche Intelligenz eine immer wichtigere Rolle spielen. Bereits heute ist sie aus kamerabasierten Sensorsystemen nicht mehr wegzudenken und wird zunehmend auch in anderen Sensorlösungen eingesetzt. Besonders bei der Verarbeitung komplexer Daten, etwa von Punktwolken, bietet KI großes Potenzial. Darüber hinaus wird sie auf Systemebene die intelligente Verknüpfung und Auswertung von Sensordaten weiter vorantreiben.



Leuze electronic GmbH + Co. KG
www.leuze.com

TOP PLAYER

BAULICHER BRANDSCHUTZ

Tobias Vähjunker

CEO von Kirotec (bis vor kurzem Vorstandsvorsitzender der Priorit, Tochter von Kirotec)

Wie beurteilen Sie die aktuelle wirtschaftliche Lage und welche strategischen Schlüsse ziehen Sie daraus?

Tobias Vähjunker: Die gesamtwirtschaftliche Entwicklung ist geprägt von einer hohen Dynamik und gleichzeitig einer hohen Unsicherheit. Das trifft letztendlich alle Unternehmen. Wir sind im vorbeugenden Brandschutz aktiv und damit eng an die Bauwirtschaft angelehnt. Dort sehen wir Investitionszurückhaltung, hohe Finanzierungskosten, permanente Kostensteigerungen und lange, schleppende Planungs und Genehmigungsverfahren.

Der Brandschutz ist stark regulatorisch getrieben, und diese Regulatorik steigt stetig. Genau das ist für uns ein stabiler Nachfragetreiber. Betreiber von Immobilienportfolios, Produktions und Industrieimmobilien müssen kontinuierlich nachrüsten. Brandschutz kann nicht aufgeschoben werden, er ist ein Dauerbrenner, und Compliance ist verpflichtend.

Für uns bedeutet das, dass wir eine Balance zwischen Absatz und Beschaffungsmärkten finden müssen. Nachfrageschwankungen beantworten wir mit flexiblen Wertschöpfungsstrukturen. Entscheidungen treffen wir nicht auf Basis vermeintlicher Gewissheiten oder alter Routinen, sondern auf Basis von Zahlen, Daten und Fakten. Wir wollen keine Entwicklungen verschlafen und keine Fehlentscheidungen treffen. Strategisch heißt das für uns: noch stärkerer Kundenfokus, der Ausbau des Sanierungsgeschäfts und Investitionen in neue Produkte und Nischenmärkte, die durch die Dynamik gerade entstehen.

Welche Herausforderungen sehen Sie bei Ihren Kunden, Partnern und Lieferanten – und wie reagieren Sie darauf?

Tobias Vähjunker: Unsere Kunden stehen vor der permanenten Herausforderung, die Brandschutzvorschriften einzuhalten. Der regulatorische Druck steigt kontinuierlich. Dazu kommen die permanenten Kostensteigerungen, die bei langen Projektlaufzeiten besonders kritisch sind. Wenn die Informationslage zu Beginn schlecht ist, wenn Brandschutzlösungen unzuverlässig sind, wenn Produkte Mängel haben oder die Service Delivery schwach ist, dann werden Projekte teurer und der Aufwand steigt. Das ist eine Realität, die wir häufig sehen.

Wir müssen unsere Kunden deshalb noch früher unterstützen. Wir bringen unser Knowhow ein, wir unterstützen technisch, wir schaffen Planungssicherheit. Unser Qualitätsversprechen – sowohl technisch als auch zeitlich – ist entscheidend, um stabile Projektumsetzungen zu ermöglichen und Unsicherheiten bei Kosten und Compliance zu reduzieren.

Gleichzeitig erleben wir einen Strukturwandel. Einzelkämpfertum wird schwieriger. Gerade im kleineren und mittleren Mittelstand mit 50 bis 250 Mitarbeitern stellt sich immer häufiger die Zukunftsfrage. Kooperationen oder die Zugehörigkeit zu einer Gruppe sind für viele eine sehr sinnvolle Antwort.

Wo sehen Sie Wachstumspotenziale – im Inland, im Export und in Ihrem Produktportfolio?

Tobias Vähjunker: Wir sehen Chancen in mehreren Bereichen: mehr Unterstützung für unsere Kunden, der Ausbau des Sanierungsgeschäfts und die Verbreiterung unseres Produktportfolios. Besonders großes Potenzial haben wir im Export. Es gibt Länder, die eine höhere Wachstumsdynamik als Deutschland haben, und dort wollen



wir unseren Anteil ausbauen. Um dieses Wachstum zu ermöglichen, investieren wir jährlich einen siebenstelligen Betrag in die Entwicklung neuer Produkte. Außerdem haben wir in den letzten 15 Monaten vier Partnerschaften mit Unternehmen aufgebaut, die ein komplementäres Geschäftsmodell haben – sowohl in der Entwicklung als auch im Vertrieb. Von diesen Partnerschaften erwarten wir viel.

Ein weiterer Baustein ist unsere Zukaufstrategie. Im Verbund mit der Priorit und unserem Partner, der Aurelius Wachstumskapital bauen wir eine Gruppe auf, die Ressourcen bündelt, Synergien hebt und resilienter gegenüber Nachfrageschwankungen ist. Digitalisierung, Investitionen, Effizienz – all das lässt sich in einer Gruppe besser stemmen. Das Produktportfolio der Priorit ist in über 25 Jahre gewachsen, aber es gibt immer Verbesserungsbedarf. Anwenderfreundlichkeit und Montageprozesse sind für uns zentrale Themen, um dem steigenden Kostendruck zu begegnen. Außerdem führen wir für alle unsere Produkte EPDs ein, um ein klares Zeichen im Bereich Nachhaltigkeit zu setzen.

Ein konkretes Beispiel ist unser neuer LithiumIonenSchrack. Wir haben ihn nach den VDMA-Prüfgrundsätzen getestet, er befindet sich im Zertifizierungsverfahren und wird eine sehr interessante Lösung für Industrie und öffentliche Kunden. Und

ja – wir waren maßgeblich daran beteiligt, überhaupt erst zu definieren, was ein solcher Schrank leisten muss. Das gab es vorher nicht. Wir haben ein großartiges Team aus Entwicklung, Zulassung, Vertrieb und Export, das diese Themen gemeinsam vorantreibt.

Gerade im internationalen Geschäft profitieren wir davon, dass wir die hohen deutschen und europäischen Standards erfüllen. Gleichzeitig ticken Behörden in anderen Ländern anders, und man braucht langen Atem. Deshalb bauen wir Schulungsangebote für internationale Märkte aus – und machen damit sehr gute Erfahrungen.

Wie sehen Sie die Entwicklung der Branche in den nächsten fünf Jahren?

Tobias Vähjunker: Wenn ich mich im Markt umhöre, gehen Viele von einer moderaten

Erholung aus. Einige Bereiche werden überproportional wachsen: Infrastruktur, Sanierung, Wirtschaftsbau – und ganz besonders Rechenzentren. Allein in Frankfurt entstehen mehrere neue Anlagen. Die Investitionssummen sind extrem hoch, und Brandschutz spielt eine gewaltige Rolle. Das Risiko der Brandausbreitung muss minimiert werden, um diese Investitionen abzusichern. Wir haben dafür sehr interessante Lösungen, etwa Revisionsöffnungsverschlüsse und Systeme zur Unterteilung von Räumen. Wir führen aktuell sehr spannende Gespräche und sehen großes Potenzial.

Unabhängig von der Konjunktur gibt es Megatrends, die enorme Chancen bieten: Digitalisierung durch KI, Automatisierung, der demografische Wandel und der ökologische Umbau der Wirtschaft. Diese Entwicklungen werden die Branche prägen.

Und der Strukturwandel wird weitergehen. Kooperationen, Partnerschaften, Gruppenmodelle – das wird für viele Unternehmen der Weg sein, um die nächsten fünf Jahre und darüber hinaus erfolgreich zu gestalten.



SicherMacher

Der GIT-Talk mit den Marktführern



Jetzt ansehen:
das vollständige
Interview in unserem
Video-Podcast



Priorit AG
www.priorit.de

50 Jahre Innovation im Brandschutz: Wagner feiert Jubiläum

Die Wagner Group GmbH blickt 2026 auf 50 Jahre Unternehmensgeschichte zurück. Seit seiner Gründung im Jahr 1976 hat sich das Unternehmen von einem spezialisierten Ingenieurbüro zu einem international führenden Lösungsanbieter im anlagentechnischen Brandschutz entwickelt. Heute ist Wagner in 15 Ländern vertreten und beschäftigt weltweit über 800 Mitarbeiter. Das Jubiläum steht unter dem Leitmotiv „Zukunft gestalten. Sicherheit leben.“ – ein Anspruch, der sich in der technologischen Entwicklung des Unternehmens seit fünf Jahrzehnten widerspiegelt. Wagner zählt zu den Technologieführern in der Brandfrüherkennung und Brandvermeidung. Zu den wegweisenden Entwicklungen gehören hochsensible, täuschungsalarmsichere Ansaugrauchmelder zur Brandfrüherkennung sowie Sauerstoffreduzierungssysteme zur aktiven Brandvermeidung.

www.wagnergroup.com



Geschäftsführung, Belegschaft und persönliche Wegbegleiter der Gründerfamilie feierten im Schloss Herrenhausen das 50-jährige Firmenjubiläum der Wagner Group GmbH



Die Geschäftsführer der Hekatron Unternehmen:
Petra Riesterer und Arno Hohmann

Hekatron Unternehmen im Aufwärtstrend

Nach einem herausfordernden Jahr konnten die Hekatron Unternehmen 2025 wieder an ihre guten Geschäftsergebnisse anknüpfen: Mit einem konsolidierten Umsatz von 260 Millionen Euro und einer Umsatzsteigerung von rund 14 Prozent zum Vorjahr befanden sich die zur Schweizer Securitas Gruppe gehörenden Brandschutzexperten und Produktionsspezialisten insbesondere ab Jahresmitte spürbar im Aufwind. Einen wesentlichen Beitrag zu dieser positiven Entwicklung hatte ihre konsequente und weiterhin andauernde Transformation. In den Standort sowie den Bereich Forschung und Entwicklung investierten die Sulzburger dabei erneut 8 Prozent. Die Sulzburger Brandschutzexperten blicken mit großer Zufriedenheit auf ihr Jahresergebnis 2025. Trotz weiterhin schwächelnder Baubranche gelang es ihnen, insbesondere durch das Bestandsobjektgeschäft im anlagentechnischen Brandschutz, geplante Umsatzziele nicht nur zu erreichen, sondern sogar zu übertreffen.

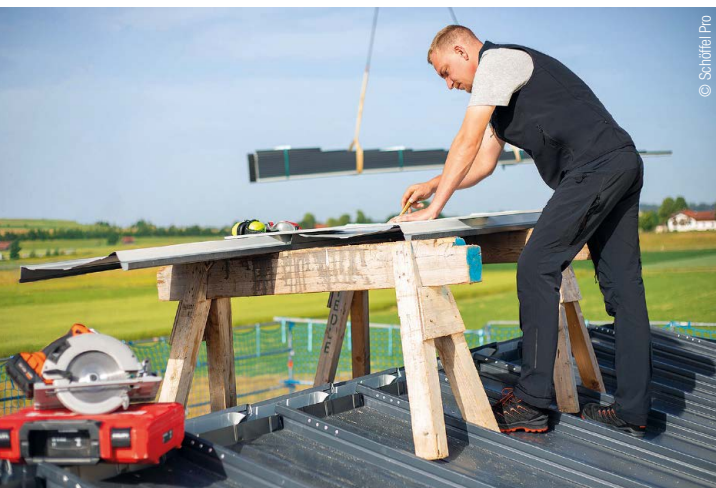
www.hekatron.de

Warnschutz-Sommermodelle

Schöffel Pro hat sein Produktportfolio um neue Warnschutz-Sommermodelle ergänzt, die nicht nur leicht und zugleich strapazierfähig sind, über ausgezeichneten Feuchtigkeitstransport verfügen, sondern auch höchste Bewegungsfreiheit und Sichtbarkeit gewährleisten.

Bei der „WS Meistermacher kurz“, einer Warnschutz-Shorts mit 2-Wege-Stretch trifft hohe Performance auf Nachhaltigkeit. Für die Arbeitshose wurde ein nachhaltiger Materialmix aus der Sorona Faser, deren natürlicher 2-Wege-Stretch (ohne Elasthan) für ein Novum und für höchsten Tragkomfort im Segment der Polycottonhosen sorgt und eine Waschbarkeit bei höheren Temperaturen (60°C) ermöglicht, recyceltem Polyester und Bio-Baumwolle verwendet. Diese hochwertigen Materialien sorgen für ein angenehmes Körperklima, eine hohe Atmungsaktivität und Wasserabweisung. Sie beinhalten nachwachsende Rohstoffe und kombinieren Robustheit mit Umweltbewusstsein.

Zudem ist die „WS Meistermacher kurz“ nach EN 20471 Klasse 1 zertifiziert. Die Arbeitshose ist auch als nicht Warnschutzmodell „Meistermacher kurz“ mit den gleichen Performance- und Materialeigenschaften in sieben verschiedenen Farben erhältlich.



Neu für den Sommer 2026 sind auch die Schöffel Pro Warnschutz-Oberteile „WS Warnheld T-Shirt“ und „WS Warnheld Polo“. Beide Modelle verbinden hohe Sichtbarkeit mit Tragkomfort und eignen sich für warme Arbeitstage im Freien. Die verwendete Coolmax EcoMade Faser bietet permanente feuchtigkeitstransportierende Eigenschaften, die dafür sorgen, dass die Feuchtigkeit vom Körper abgeleitet wird, sodass der Träger während der gesamten Arbeitszeit kühl, trocken und komfortabel und auch bei Hitze konzentriert bleibt. Zudem besteht die Faser zu 100 % aus recyceltem Material.

Der integrierte UV-Schutz (UPF 50+) schützt zuverlässig vor Sonnenstrahlen. Die antibakterielle Ausrüstung hält das Shirt auch nach langen Einsätzen frisch, während eine insektizide Wirkung zusätzlichen Schutz bei Outdoor-Arbeiten bietet. Für etwas kühlere Temperaturen oder wenn lange Ärmel benötigt werden, gibt es das Langarm-Modell „WS Warnheld Longsleeve“ mit identischen Funktionalitäten. Erhältlich sind die „WS-Warnheld“-Modelle, wie die gesamte Warnschutzkollektion des Herstellers als Damen- und Herrenmodelle in den Farben Neongelb sowie Neonorange, kombiniert mit Dunkelblau und Dunkelgrau.

www.schoeffel-pro.com

Avacon zu Gast bei Denios

Wie praxisnah moderne Gefahrstofflagerung und Arbeitssicherheit heute aussehen können, das erlebten rund 30 Abfallkoordinatoren der Avacon AG bei einem Erfahrungsaustausch am Hauptsitz der Denios SE. Das Unternehmen für Gefahrstofflagerung und betriebliche Sicherheit öffnete seine Türen für intensive Fachgespräche, praxisorientierte Einblicke und persönlichen Austausch.

Seit inzwischen 40 Jahren verfolgt Denios ein klares Ziel: Unternehmen dabei zu unterstützen, Mensch und Umwelt nachhaltig vor Schäden zu schützen. Dieses Leitbild bündelt das Unternehmen heute unter der Vision „Vision Zero“ – einer Welt ohne Schäden an Mensch und Umwelt. Der Besuch der Avacon-Abfallkoordinatoren zeigte eindrucksvoll, wie dieser Anspruch in der täglichen Praxis gelebt wird.

Die Avacon AG ist ein regionales Energieversorgungsunternehmen mit Sitz in Helmstedt (Niedersachsen). Der Versorgungsbereich erstreckt sich von der Nordseeküste bis Südhessen und umfasst große Teile Niedersachsens und Sachsen-Anhalts. Avacon ist Teil des E.ON-Konzerns und erzielt einen Jahresumsatz von mehr als 2 Milliarden Euro.



Das Team von Avacon bekam bei Denios Einblicke rund um die Themen Gefahrstofflagerung und Arbeitssicherheit

Sicherheit zum Anfassen statt Theorie auf Papier

Im Mittelpunkt des Besuchs stand neben dem internen Erfahrungsaustausch insbesondere der praxisnahe Gefahrstoffparcours. Dort konnten die Teilnehmer ihr Wissen rund um sichere Gefahrstofflagerung anhand realitätsnaher Szenarien und verschiedener Lagersituationen vertiefen und überprüfen. Die positiven Rückmeldungen der Gäste bestätigten den hohen Praxisnutzen des Formats.

Darüber hinaus erhielten die Teilnehmer bei einem Produktionsrundgang spannende Einblicke in die Fertigungsprozesse der unterschiedlichen Denios-Raumsysteme. Dabei wurden die hohen Qualitäts- und Sicherheitsstandards des Herstellers deutlich.

Auch der moderne Showroom des Unternehmens bot Gelegenheit, zahlreiche Produkte und Sicherheitslösungen direkt vor Ort zu erleben und zu testen. Abgerundet wurde der Tag durch ein gemeinsames Mittagessen, bei dem die Gäste ihre Eindrücke vertiefen und weitere Gespräche führen konnten.

www.denios.de

GIT

SICHERHEIT

INNENTITEL – ARBEITSSCHUTZ

ION-LINE:

**FÜR DAS SICHERE LAGERN
UND LADEN VON LITHIUM-
IONEN-AKKUS**

asecos®



www.asecos.com



Sicherheitsschränke wie die der Asecos Ion-Line können ein zentraler Baustein im vorbeugenden Brandschutz sein

INNENTITEL

Sicher lagern und laden

Welche Anforderungen Sicherheitsschränke für Lithium-Akkus erfüllen sollten

Lithium-Akkus sind fester Bestandteil vieler betrieblicher Arbeitsprozesse. Mit ihrer Verbreitung steigen jedoch auch die Anforderungen an den Arbeits- und Brandschutz, denn defekte Akkus können Brände verursachen. Sie sollten daher in speziell entwickelten Sicherheitsschränken gelagert und geladen werden, etwa in den Modellen der Asecos Ion-Line.



In den Ion-Line Sicherheits-schränken können Lithium-Ionen-Akkus sicher gelagert und geladen werden

■ Energiespeicher wie Lithium-Ionen-Akkus bieten viele Vorteile und gelten bei ordnungsgemäßem Betrieb als sicher. Sind die Zellen jedoch beschädigt oder thermisch überlastet, können sie ein Brandrisiko darstellen. Besonders kritisch ist der Ladevorgang, da instabile Akkus ihre Energie unkontrolliert in Form von Wärme freigeben. Beim Laden steigt die Hitze weiter an, was zu einem thermischen Durchgehen der Zellen (Thermal Runaway) führen kann: Ab einer kritischen Temperatur schmilzt der Separator der Zelle und es kommt zu einem inneren Kurzschluss, oft mit einer Kettenreaktion auf benachbarte Zellen.

Um Schutz bei diesem Szenario zu bieten, hat Asecos die Ion-Line-Sicherheitsschränke zum Lagern und Laden von Lithium-Akkus entwickelt, deren Modelle Pro und Ultra auch VDMA-zertifiziert sind.

Sicherheitsregeln

Angesichts des Gefährdungspotenzials der Energiespeicher sollten präventive Maßnahmen frühzeitig ansetzen. Die Basis dafür bilden Sicherheitsregeln für den Umgang mit Lithium-Akkus, deren konsequente Umsetzung die Voraussetzung für einen sicheren Betrieb schafft.

- Kurzschlüsse vermeiden: Batteriepole müssen zuverlässig vor Kontakt und Kurzschluss geschützt werden.
- Regelmäßige Prüfung: Akkus sind in regelmäßigen Intervallen auf sichtbare Schäden, Aufblähungen oder Verformung zu kontrollieren.
- Keine Manipulationen: Niemals dürfen Eigenbauten oder die Akkus anders verwendet werden, als vom Hersteller vorgegeben.
- Sichere Ladeumgebung: Akkus sollten nicht auf brennbarem Untergrund, in der Nähe entzündbarer Materialien oder unbeaufsichtigt geladen werden.
- Tiefentladung verhindern: Vollständige Entladung kann die Lithium-Akkus dauerhaft schädigen und instabil machen.

Der Gesamtverband der deutschen Versicherungswirtschaft (GDV) empfiehlt in seinem „Merkblatt zur Schadenverhütung“, Lithium-Ionen-Akkus grundsätzlich wie Gefahrstoffe zu behandeln. Entsprechend ist ein ganzheitliches Brandschutzkonzept erforderlich, das sowohl technische als auch organisatorische Maßnahmen umfasst. Dazu zählen beispielsweise die Begrenzung der Akkus am Arbeitsplatz auf das notwendige Minimum sowie der Ausbau und die fachgerechte Lagerung nicht genutzter Akkus – idealerweise in geprüften Sicherheitsschränken.



Isolierte Fachböden verhindern eine Brandausbreitung von einer Lagerebene zur nächsten

Bitte umblättern ►



Transportsockel ermöglichen im Ernstfall die kontrollierte Evakuierung eines Sicherheitsschranks

Doppelter Brandschutz

Typ-90-Sicherheitsschränke erfüllen die baulichen Anforderungen für feuerbeständig abgetrennte Bereiche (F90) und sind diesen gleichwertig. Sie sind somit eine sichere Wahl für das Aufbewahren und Laden von Lithium-Akkus.

Entscheidend ist hierbei jedoch nicht allein der Feuerwiderstand gegenüber äußerer Brandbeanspruchung, sondern – aufgrund des Risikos eines Thermal Runaways – der Feuerwiderstand von innen. Zusätzlich zur Brandprüfung von außen nach DIN EN 14470-1 ist daher auch der Nachweis einer Brandprüfung von innen erforderlich, etwa in Anlehnung an die DIN EN 1363-1.

Eine Feuerwiderstandsfähigkeit von 90 Minuten für beide Szenarien gilt als Mindeststandard. Sie verschafft wertvolle Zeit, um Personen zu evakuieren und Rettungskräfte zu alarmieren. Entsprechende Nachweise sollten durch den Hersteller dokumentiert sein.

VDMA-Prüfung für zusätzliche Sicherheit

Das VDMA-Einheitsblatt 24994:2024-08 beschreibt einheitliche Prüfanforderungen für feuerwiderstandsfähige Sicherheitsschränke zum Lagern und Laden von tragbaren bzw. abnehmbaren Lithium-Akkus. Ziel der Prüfung ist es, das Verhalten der

Schränke im Fall eines Thermal Runaway der eingelagerten Akkus realitätsnah zu bewerten. Dazu wird ein sogenannter Realbrandversuch durchgeführt: Durch gezieltes Erhitzen der eingelagerten Akkus kommt es zu einer Kettenreaktion, bei der die Zellen ausgasen, sich entzünden und teilweise explosionsartig zerplatzen. Dabei können kurzzeitig Temperaturen von über 700 °C im Schrank entstehen. Der Schrank muss diesem Worst-Case-Szenario standhalten, ohne dass Flammen oder Splitter austreten.

Auf die bestandene Prüfung folgt ein Audit der Produktionsstätte. Erst danach erhalten die Schränke die Zertifizierung, die die Konformität von Prüfung und Produkt gemäß VDMA 24994:2024-08 sicherstellt. Zertifizierte Modelle wie der Ion-Line Pro und Ultra sind anschließend entsprechend gekennzeichnet.

Sicherheitsfunktionen für den Ernstfall

Zu den wichtigsten Ausstattungsmerkmalen für Akku-Sicherheitsschränke zählen Branddetektion und Alarmweiterleitung. Besonders bei unbeaufsichtigtem Betrieb – etwa außerhalb der Arbeitszeiten – ist die Alarmweiterleitung an eine zentrale Leitstelle oder definierte Rufnummern unverzichtbar. Nur so kann im Ernstfall rasch gehandelt werden, um Folgeschäden zu begrenzen.

Weitere Merkmale erhöhen das Sicherheitsniveau und erweitern die Handlungsoptionen. So verfügen Ion-Line-Modelle über Transportsockel und schnelllösende Steckverbindungen, wodurch sie sich im Bedarfsfall schnell evakuieren lassen. Einsatzkräfte können somit situationsbedingt entscheiden, ob sie den Schrank am Aufstellort löschen oder dafür ins Freie bringen.

Im Brandfall schalten sich integrierte Steckdosenleisten automatisch ab, wodurch zusätzliche Hitzeentwicklung vermieden wird. Zudem verhindern geprüfte, isolierte Fachböden mit Brandschutzmaterial eine Brandausbreitung zwischen den einzelnen Lagerebenen (Propagation). Dank einer kontrollierten Abführung der Ladeabwärme und einer schnellen Rauchdetektion wird das Gesamtrisiko eines Brandes weiter reduziert.

Bei den Modellen Pro und Ultra erhöht eine überarbeitete Türkonstruktion mit Drei-Punkt-Verriegelung außerdem die Widerstandsfähigkeit bei Bränden im Innenraum. **GIT**

Schulung und Weiterbildung



Der sichere Umgang mit Lithium-Akkus erfordert neben geeigneten technischen Schutzmaßnahmen auch fundiertes Fachwissen. Um Risiken realistisch bewerten und geeignete Schutzmaßnahmen umsetzen zu können, sind aktuelle Kenntnisse zu Richtlinien, technischen Entwicklungen und bewährten Verfahren unerlässlich. Mit Weiterbildungsangeboten wie der zweitägigen „Asecos online Expo – Lithium Special“ am 29. und 30. September 2026 möchte Asecos Unternehmen dabei unterstützen, das Wissen der Teilnehmer zu aktuellen Entwicklungen und Sicherheitsanforderungen im Umgang mit Lithium-Akkus zu vertiefen. Weitere Informationen und Anmeldemöglichkeiten zur kostenlosen Veranstaltung finden Sie über den QR-Code.



Asecos

www.asecos.com



„Im Job brauchst
Du Partner,
auf die Du Dich
verlassen kannst.“

Mewa. Berufskleidung im Rundum-Service.

Maximale Entlastung bei höchster Qualität. Mit Mewa können Sie sich auf professionell gepflegte Berufskleidung verlassen. Von Holen und Bringen zu Waschen und Pflegen – der Rundum-Service nimmt Ihnen alles ab. So können Sie sich auf das Wesentliche konzentrieren: Ihre Arbeit.

Vereinbaren Sie jetzt einen kostenlosen Anprobetermin unter 0800 450030 oder besuchen Sie uns unter www.mewa.de.

MATERIALIEN

Materialien für Jahrzehnte

Vor einem halben Jahrhundert wurde Gore-Tex Fabrics gegründet

Lange Wege, enge Schiffsrümpfe, hohe Temperaturen: Die Werkfeuerwehr der Meyer Werft arbeitet unter Bedingungen, in denen Schutzkleidung mehr leisten muss als normgerechten Hitzeschutz

Gore-Tex ist einer jener Begriffe, die so allgemein bekannt geworden sind, dass man sie als Synonym für Materialien mit ganz bestimmten Schutzfunktionen verwendet – aber auch mit Komfort und Langlebigkeit. Geniale Einfälle waren Initialzündungen für deren Entwicklung – und der innovative Geist des Unternehmens hält bis heute an. GIT SICHERHEIT sprach anlässlich des Jubiläums mit Achim Löffler, Global Business Leader für das Gore-Tex Ingredient Business.

■ Herr Loeffler, zunächst einmal: herzlichen Glückwunsch zum 50-jährigen Jubiläum von Gore-Tex Fabrics, das Sie bei Gore in diesem Jahr begehen – wobei die erste Gründung des Unternehmens Gore ja bereits ins Jahr 1958 fällt...?

Achim Löffler: Vielen Dank. Das stimmt: W.L. Gore & Associates wurde 1958 von Bill und Vieve Gore gegründet. Aus diesem Unternehmen ist über die Jahrzehnte ein globaler Innovationstreiber der Materialwissenschaften entstanden, der heute in sehr unterschiedlichen Bereichen aktiv ist – von Medizinprodukten über Industrie- und Elektronikanwendungen bis hin zu Textilien.

Die Marke Gore-Tex geht auf die 1970er-Jahre zurück. 1976 kamen die ersten Produkte auf den Markt – und damit ein grundlegender Wandel im Verständnis von Wetterschutz. Bis dahin bedeutete trocken

bleiben oft auch, im eigenen Schweiß zu stehen. Materialien hielten Wasser zwar weitgehend ab, ließen aber keine Feuchtigkeit von innen entweichen. Mit Gore-Tex-Produkten wurde erstmals eine Lösung eingeführt, die beides vereinte: wasserdichter Schutz, der gleichzeitig atmungsaktiv ist.

Heute steht die Marke nicht nur für eine Membran. Sie steht für ein System aus Materialtechnologie, Entwicklung, Tests, Qualitätsstandards und Partnerschaften mit Herstellern. Im professionellen Bereich geht es dabei immer um Schutz, Komfort und Verlässlichkeit unter realen Einsatzbedingungen.

Am Beginn standen ja klassische geniale Tüftler, insbesondere Bill Gore – und später etwa dessen ältester Sohn Bob Gore. Dessen genialitätsbefeuerte Zufallsentdeckung wird noch heute in Ihrem Besucherzentrum in Delaware

vorgeführt: Da hat ein kleiner Wutausbruch eine Rolle gespielt. Können Sie das mal kurz beschreiben?

Achim Löffler: Bob Gore arbeitete mit PTFE, also Polytetrafluorethylen. Er versuchte, erhitzte PTFE-Stangen zu dehnen, um die Materialstruktur zu verändern und neue Eigenschaften wie höhere Flexibilität und bessere Verarbeitbarkeit zu erreichen. Zunächst rissen sie immer wieder. Eines Abends zog er aus Ärger ruckartig an dem Material. Dieses Mal riss es nicht. Es dehnte sich schlagartig auf ein Vielfaches seiner ursprünglichen Länge.

So entstand expandiertes PTFE, kurz ePTFE. Das Material hatte eine mikroporöse Struktur. Es bestand zu einem großen Teil aus Luft, war aber zugleich sehr stabil. Aus dieser Struktur ergaben sich Eigenschaften, die später für Gore-Tex-Produkte zentral wurden: Schutz vor Wasser von außen und

gleichzeitig die Möglichkeit, Wasserdampf von innen nach außen entweichen zu lassen.

Es war kein fertiges Produkt, sondern ein Materialdurchbruch. Aus ihm ließ sich erstmals ein Material entwickeln, das Regen zuverlässig abhält und gleichzeitig Schweiß nach außen entweichen lässt – die Grundlage für moderne, atmungsaktive Schutz- und Funktionsbekleidung.

Diese Entdeckung eröffnete eine Vielzahl von Anwendungsmöglichkeiten und Weiterentwicklungen. Können Sie ein paar wichtige Meilensteine nennen?

Achim Löffler: Ein früher Meilenstein war der Transfer in Schutzkleidung für Feuerwehrleute. 1979 wurde eine atmungsaktive Nässesperre für Feuerwehrschutzkleidung kommerziell eingeführt. Sie verhindert, dass Wasser, Blut, Körperflüssigkeiten oder bestimmte Chemikalien von außen in das Bekleidungssystem eindringen. Gleichzeitig lässt sie Wasserdampf von innen nach außen entweichen. 1981 setzte Globe als erster Kunde in den USA Gore-Tex Moisture Barrier Fabric in Feuerwehrschutzkleidung ein.

Ein weiterer Meilenstein war die Entwicklung von flammhemmenden Technologien. Die Produkttechnologie Gore-Tex Pyrad wurde für Situationen entwickelt, in denen Beschäftigte plötzlich Hitze, Flammen oder auch Störlichtbögen ausgesetzt sein können – etwa im Militär, in der Öl- und Gasindustrie oder bei Energieversorgern. Sie verbindet Schutz vor Hitze- und Flammeneinwirkung mit leistungsfähigen, leichten und komfortablen textilen Konstruktionen.

In den letzten Jahre kam das Obermaterial Extraguard hinzu. Diese Technologie ermöglicht leichte, robuste und atmungsaktive Schuhe, die ihre Eigenschaften auch bei langanhaltender Nässe beibehalten. Im trockenen Zustand ist die Konstruktion rund 40 Prozent leichter als Leder und trocknet zudem schneller. Gerade bei Sicherheits- und Einsatzstiefeln ist das relevant, da zusätzliches Gewicht am Fuß bei jedem Schritt beschleunigt und abgebremst werden muss.

Die Bandbreite der Anwendungsgebiete ist heute kaum noch überschaubar – Ihre Materialien waren sogar auf dem Mond. Wann kamen die Bereiche Arbeitssicherheit und PSA hinzu – und welcher materialtechnischen Durchbrüche bedurfte es hier noch?

Achim Löffler: PSA kam nicht als ein einzelner Schritt hinzu. Es war eher eine konsequente Weiterentwicklung. Sobald klar war,

dass unsere Produkttechnologien zuverlässigen Wetterschutz und Atmungsaktivität ermöglichen können, stellte sich die nächste Frage: Wie lassen sich diese Eigenschaften für Menschen nutzen, die unter besonders harten Bedingungen arbeiten?

Im Feuerwehrbereich begann dieser Weg Ende der 1970er-Jahre mit atmungsaktiven Nässesperren. Im Arbeitsschutz kamen später weitere Anforderungen hinzu: Schutz gegen Hitze und Flammen, Schutz gegen Flüssigkeiten, Schutz gegen Blut und Körperflüssigkeiten, Schutz gegen Chemikalien, Abriebfestigkeit, Beweglichkeit und lange Nutzungsdauer.

Der eigentliche Fortschritt lag dabei nicht nur in der Membran. Er lag im Systemaufbau. PSA besteht aus mehreren Lagen. Obermaterial, Nässesperre, Isolation, Futter, Nähte, Tape, Schnittführung und Verarbeitung müssen zusammenpassen. Bei professioneller Schutzkleidung reicht es nicht, ein Material gut zu machen. Das gesamte Bekleidungssystem muss unter Normbedingungen und im harten Alltag funktionieren.

Ihr Geschäftsmodell in diesem Sektor basiert ja stark auf Partnerschaften mit PSA-Herstellern. Können Sie das anhand eines Beispiels darstellen?

Achim Löffler: Die Marke Gore-Tex ist eine Ingredient Brand. Unsere Technologien sind Bestandteil von Produkten, die von spezialisierten Herstellern entwickelt und produziert werden. Unsere Rolle geht dabei weit über die eines Materiallieferanten hinaus. Wir bringen Materialwissen, Testkompetenz, Normenverständnis und die Erfahrung aus dem engen Austausch mit Endanwendern ein.

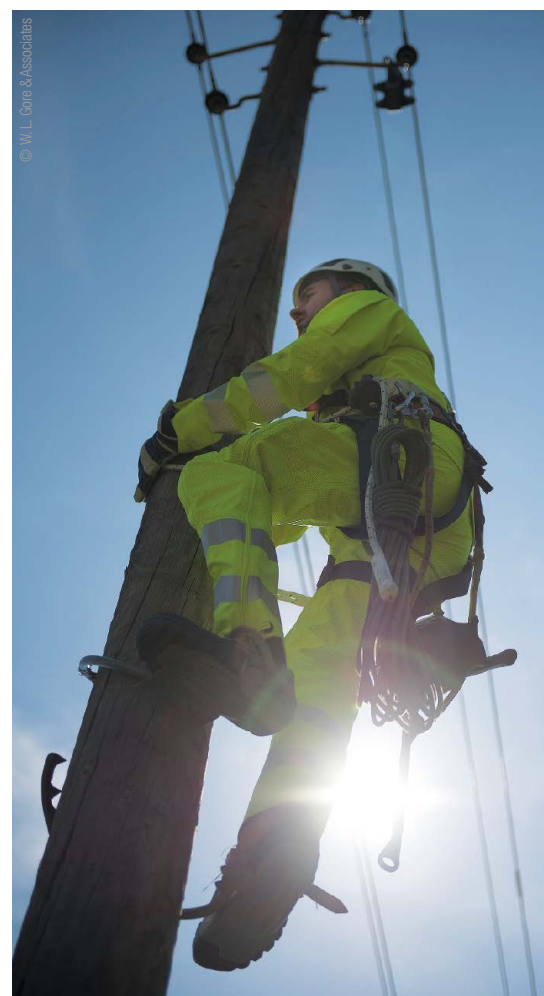
Ein gutes Beispiel ist die Zusammenarbeit mit S-Gard und der Werkfeuerwehr der Meyer Werft in Papenburg. Die Feuerwehr arbeitet dort unter extremen Bedingungen: lange Anmarschwege, hohe Temperaturen und enge Schiffsrümpfe. Gemeinsam wurde eine Schutzbekleidung entwickelt, die genau auf diese Anforderungen zugeschnitten ist. S-Gard entwickelte das Bekleidungssystem, Gore steuerte die Produkttechnologie Gore-Tex Crosstech Parallon sowie Material- und Testkompetenz bei. Das Ergebnis: Die Feuerwehrleute bleiben auch unter extremen Bedingungen länger leistungsfähig und können ihre Arbeit sicherer ausführen. Genau dieses partnerschaftliche Entwicklungsmodell zeichnet unsere Zusammenarbeit mit PSA-Herstellern aus.

In Zusammenarbeit mit der Feuerwehr in New York haben Sie Schutzanzüge entwickelt, die in diesem Bereich die Sicherheit deutlich verbessert haben. Wie kam es zu dieser Zusammenarbeit und was waren die Ergebnisse?

Achim Löffler: Das Fire Department of the City of New York arbeitet unter extremen Bedingungen: hohe, enge Gebäude, enorme Bevölkerungsdichte, hohe Einsatzfrequenzen und im Sommer große Hitze. Nicht umsonst gilt das FDNY weltweit als eine der legendärsten Feuerwehren – geprägt durch seine lange Geschichte, seine Einsätze unter außergewöhnlichen Bedingungen und seine besondere Stellung im öffentlichen Bewusstsein. Die körperliche Belastung der Feuerwehrleute ist entsprechend hoch.

FDNY und Gore arbeiten seit über 30 Jahren eng zusammen. Die Feuerwehr nutzt Schutzbekleidung, Stiefel und Handschuhe mit Gore-Tex-Produkttechnologien. Das Gewicht der Ausrüstung ist dabei entscheidend – darf aber nie zulasten der Schutzleistung gehen. Schutz und Komfort müssen zusammen gedacht werden. Der kontinuierliche Austausch mit den Einsatzkräften ist zentral: Ihre Erfahrungen fließen direkt in die Weiterentwicklung unserer Produkttechnologien ein.

Bitte umblättern ►



Pyrad: Bei Arbeiten an elektrischen Anlagen muss der Schutz vor thermischen Risiken eines Störlichtbogens mit hohem Tragekomfort vereint werden



© W.L. Gore & Associates

Als Bob Gore erhitztes PTFE ruckartig dehnte, riss es nicht – sondern expandierte schlagartig auf ein Vielfaches seiner ursprünglichen Länge – so entstand ePTFE



1979 wurde eine atmungsaktive Nässebarriere für Feuerwehrschutzkleidung kommerziell eingeführt

Es geht bei Feuerwehreinsätzen vor allem um den Umgang mit extremer thermischer Belastung. Dazu kommen Feuchtigkeit und Atmungsaktivität. Wie arbeiten Ihre Materialien hier genau?

Achim Löffler: Feuerwehrschutzkleidung muss zwei Dinge gleichzeitig leisten: Sie schützt vor äußeren Gefahren wie Hitze, Flammen, Wasser und Schadstoffen. Zugleich muss sie dafür sorgen, dass die Einsatzkraft durch eigene Körperwärme und Feuchtigkeit nicht übermäßig belastet wird.

Entscheidend ist dabei das Zusammenspiel von Schutz und Atmungsaktivität. Moderne Materialien verhindern das Eindringen von Flüssigkeiten und ermöglichen gleichzeitig, dass Schweiß nach außen entweichen kann. So bleibt die Belastung für den Träger geringer und der thermische Schutz stabil. Wichtig ist aber: Es gibt nicht die eine Lösung für alle Feuerwehreinsätze. Brandbekämpfung, technische Hilfeleistung, Rettungsdienst oder Vegetationsbrandbekämpfung stellen unterschiedliche Anforderungen. Deshalb müssen Materialsysteme auf den jeweiligen Einsatz abgestimmt sein.

Ich durfte während Ihrer Presseveranstaltung einen der Schutzanzüge der New Yorker Feuerwehr selbst einmal anziehen: Sie sind überraschend leicht. Auch das ist ja ein beträchtlicher Fortschritt?

Achim Löffler: Ja. Gewicht ist bei PSA kein Nebenthema. Es wirkt direkt auf die körperliche Belastung. Eine Einsatzkraft trägt Schutzkleidung nicht für ein Foto, sondern

unter Stress, Hitze, Zeitdruck und körperlicher Arbeit. Leichtere Schutzsysteme können deshalb zu besserer Beweglichkeit, geringerer Ermüdung und längerer Leistungsfähigkeit beitragen. Dabei darf geringeres Gewicht aber nie zulasten der Schutzleistung gehen. Das ist die eigentliche Entwicklungsaufgabe: Schutz, Gewicht, Atmungsaktivität, Robustheit und Beweglichkeit müssen in Balance gebracht werden.

Die Entwicklungen in diesem Zusammenhang haben Sie auch auf viele andere Bereiche übertragen. Können Sie ein paar Beispiele nennen?

Achim Löffler: PSA funktioniert nur dann richtig, wenn sie korrekt getragen wird und über einen längeren Zeitraum komfortabel ist, damit der Körper leistungsfähig und konzentriert bleibt. Gerade bei Hitze, Flammen oder Störlichtbögen sind Leichtigkeit, Atmungsaktivität und Bewegungsfreiheit deshalb sicherheitsrelevant.

Ein gutes Beispiel ist die Energieversorgung. Beschäftigte, die an elektrischen Anlagen arbeiten, können unerwartet einem Störlichtbogen ausgesetzt sein. Die neue Pyrad Uniform by Gore-Tex Labs mit Störlichtbogenschutz verbindet Schutzklasse 2 mit einer leichten, weniger sperrigen und hoch atmungsaktiven Konstruktion. So wird Schutz vor den thermischen Auswirkungen eines Störlichtbogens möglich, ohne die Kleidung übermäßig schwer oder voluminös und damit heiß zu machen.

Nun geht die Entwicklung weiter. Wir haben kürzlich auf unserem GIT

SICHERHEIT-Portal zum Beispiel Ihre Innovationen im Bereich Störlichtbogenschutz gezeigt. Woran wird in der sicherheitsrelevanten Materialkunde heute vor allem gearbeitet?

Achim Löffler: Der zentrale Fortschritt liegt heute darin, Schutzkleidung präziser auf den jeweiligen Einsatz abzustimmen. Die Anforderungen unterscheiden sich deutlich – etwa bei Störlichtbogen, Hitze und Flammen, Flüssigkeiten, Chemikalien, Wetter, mechanischen Risiken oder biologischen Gefährdungen. Moderne PSA muss diese Risiken differenziert adressieren und zugleich tragbar, beweglich und langlebig bleiben. Die erwähnte Pyrad Uniform mit Störlichtbogenschutz zeigt, wie sich hohe Schutzanforderungen mit einer leichten, atmungsaktiven und weniger sperrigen Konstruktion verbinden lassen – ein Ansatz, der für den praktischen Einsatz entscheidend ist.

Daraus ergeben sich drei Entwicklungsrichtungen: besser abgestimmte Systemarchitekturen sowie geringeres Gewicht und bessere Beweglichkeit bei verlässlicher Schutzleistung. Hinzu kommen Materialien mit geringerer Umweltwirkung, ohne Performance und Langlebigkeit aus dem Blick zu verlieren.

Kommen wir noch zum Thema Nachhaltigkeit. Können Sie uns kurz Ihre Responsible-Performance-Strategie vorstellen?

Achim Löffler: Responsible Performance beschreibt unseren Anspruch, Produktleis-

tung und Verantwortung zusammenzubringen. Für die Marke Gore-Tex ist Nachhaltigkeit kein neues Zusatzthema. Sie ist seit vielen Jahren Teil der Entwicklung: über langlebige Produkte, Reparatur, Pflege, zertifizierte Materialien, soziale Verantwortung in der Lieferkette und die Reduktion von Emissionen.

Daraus ergeben sich unsere zentralen Handlungsfelder – CO₂-Reduktion, Chemikalienmanagement, Kreislaufwirtschaft und menschenrechtliche Sorgfaltspflicht. Viele dieser Themen begleiten uns seit den frühen 1990er-Jahren und prägen bis heute unsere Nachhaltigkeitsarbeit.

Im Bereich CO₂-Reduktion beispielsweise haben wir uns konkrete, messbare Ziele gesetzt, ausgehend vom Basisjahr 2019. Für Scope 1 und 2 – also direkte Emissionen aus eigenen Quellen sowie indirekte Emissionen aus eingekaufter Energie – haben wir unser ursprüngliches Reduktionsziel von 60 Prozent bereits erreicht und auf 80 Prozent bis 2030 erhöht. Für Scope 3, also Emissionen entlang der vor- und nachgelagerten Wertschöpfungskette, verfolgen wir ein Reduktionsziel von 35 Prozent. Insgesamt ergibt sich daraus ein unternehmensweites Ziel von 40 Prozent weniger Treibhausgasemissionen bis 2030.

Langlebigkeit ist ja ebenfalls ein zentraler Nachhaltigkeitsfaktor?

Achim Löffler: Langlebigkeit ist einer der größten Hebel für Nachhaltigkeit. Das gilt besonders bei PSA. Denn ein großer Teil der Umweltwirkung entsteht bereits in der Her-



stellung. Wenn ein Produkt länger genutzt werden kann, sinkt die Umweltwirkung pro Nutzung. Gleichzeitig sinken häufig auch die Kosten über die Lebensdauer.

Was ist aus Ihrer Sicht nach 50 Jahren Gore Tex Fabrics der wichtigste Blick nach vorn?

Achim Löffler: Schutzkleidung wird noch spezifischer und leistungsfähiger werden. Gleichzeitig steigen die Anforderungen an Nachhaltigkeit, Langlebigkeit und nachvollziehbare Produktverantwortung, während

Einsatzkräfte, Beschäftigte und Sicherheitsorganisationen in zunehmend komplexen Umgebungen arbeiten.

50 Jahre sind deshalb kein Schlusspunkt, sondern ein Versprechen für die Zukunft: Wir entwickeln weiterhin wegweisende Produkttechnologien, die Menschen zuverlässig schützen, wenn es darauf ankommt. **GIT**



W. L. Gore & Associates, Inc.
www.gore.com

Mewa führt flächendeckend KI-gestützte Größenvermessung ein

Bei Mewa ist der Startschuss für die flächendeckende Einführung der digitalen Größenvermessung gefallen. Der Textildienstleister setzt auf das Tool des rumänischen Start-ups Esenca Digital Workwear, bei dem Mewa seit 2024 Mehrheitsanteile hält. Nach erfolgreicher Pilotphase wird die Software zunächst an allen Mewa-Standorten in Deutschland ausgerollt und soll bis Ende 2026 in allen europäischen Ländern zum Einsatz kommen, die Kunden mit Berufs- und Schutzkleidung versorgen. Die KI-basierte Anwendung ermöglicht, Träger von Arbeitskleidung vollständig digital zu vermessen, um sie mit Hosen, Jacken und Shirts in der richtigen Konfektionsgröße zu beliefern. Die Digitalisierung bringt erhebliche Vorteile für beide Seiten: Die Vermessung kann voll bekleidet durchgeführt werden und es wird keine Musterkleidung benötigt, um die richtige Größe zu ermitteln.

www.mewa.de



SICHERHEITSSCHUHE

Sicherheit trifft Sneaker-Style

Jalas Flex verbindet S3S-Schutz mit leichter Bauweise und sportlichem Design

Mit der Jalas Flex Kollektion stellt Ejendals eine neue Generation von Sicherheitsschuhen vor, die Komfort und Optik moderner Sneaker mit Arbeitssicherheit verbindet. Die Jalas-Modelle decken unterschiedliche Tragepräferenzen ab, ohne Einbußen an Schutz oder Ergonomie. In sicherheitskritischen Bereichen wird sowohl ein einheitliches Erscheinungsbild sowie die Gesundheit der Beschäftigten berücksichtigt.

Die Flex Kollektion richtet sich an Arbeitsplätze, in denen Mitarbeitende viel auf den Beinen sind und ein zeitgemäßer visueller Auftritt gefragt ist. Der sportliche Charakter der Schuhe unterstützt die Trageakzeptanz bei persönlicher Schutzausrüstung (PSA). Gleichzeitig erfüllen die Modelle die Norm EN ISO 20345:2022 S3S SR FO SC (S3S: Schutzklasse mit Durchtrittshemmung und wasserabweisendem Schaft; SR: Rutschhemmung; FO: Beständigkeit der Sohle gegen Kraftstoff; SC: Abriebschutz im Zehenbereich) und bieten damit zentrale Schutzfunktionen für unterschiedliche Arbeitsumgebungen. Die metallfreie Konstruktion unterstützt zudem den Einsatz in Bereichen mit Metalldetektion oder sensiblen Produktions- und Logistikprozessen.

Leicht, dämpfend und alltagstauglich

Komfort ist ein wichtiges Entwicklungsziel der Kollektion: Ein Schaft aus strapazierfähiger, wasserabweisender Mikrofaser mit einem Anteil biobasierter Materialien sorgt dafür, dass die Füße auch bei längeren Schich-

ten trocken bleiben und belüftet werden. Die PU/PU-Laufsohle (Polyurethan in zwei Dichten) ist auf Grip und Haltbarkeit ausgelegt und trägt durch ihre große Kontaktfläche zu einer hohen Rutschhemmung bei. Ergänzend verteilt die FX2 Pro-X Einlegesohle mit Poron XRD die Belastung beim Gehen und Stehen gleichmäßiger und trägt so dazu bei Überlastungen an Füßen und Knien zu reduzieren.

Zwei Ausprägungen für unterschiedliche Ansprüche

Der Jalas Flex 1055 ist als Schnürschuh in Schwarz mit dunkelgrauer Laufsohle gestaltet und richtet sich an Träger, die eine fein einstellbare Passform wünschen. Seine Mikrofaser mit verstärktem Zehenbereich, Komposit-Zehenschutzkappe, ESD-Funktion (Schutz vor elektrostatischer Entladung) und eine durchtrittshemmende Einlage mit

Recyclinganteil machen ihn zu einem vielseitigen Modell.

Der Jalas Flex 1065 verfolgt einen ähnlichen Ansatz bei Schutz und Komfort, setzt jedoch mit schwarzen Obermaterialien, roten Akzenten und roter Laufsohle auf eine sportlichere Optik. Er nutzt ein Drehverschlussystem (Boa Fit System), das ein schnelles und reproduzierbares Schließen ermöglicht.

Mit Größen von 35 bis 48 deckt die Jalas Flex Kollektion ein breites Spektrum an Nutzergruppen ab. In Kombination mit ergänzenden Maßnahmen wie Gefährdungsanalysen und Schulungen kann sie Teil eines präventiven Arbeitsschutzkonzepts sein. Ziel ist es, Arbeitsunfälle und Belastungen der Füße zu reduzieren sowie die Nutzung von PSA im betrieblichen Alltag zu unterstützen. **GIT**



Ejendals AB
www.ejendals.com

Der Jalas Flex 1065 kombiniert sportliches Sneaker-Design mit leichter, metallfreier Bauweise, Drehverschlussystem und ergonomischem Tragekomfort für lange Arbeitstage



SICHERHEITSSCHUHE

Sicherer Schritt trotz schmalen Fuß

ESD-Einlegesohlen verbessern Passform und Halt in Sicherheitsschuhen für schmale Füße

Für viele Beschäftigte gehören Sicherheitsschuhe zur täglichen persönlichen Schutzausrüstung. Dennoch passen gängige Leistenformen nicht immer optimal zu unterschiedlichen Fußtypen. Insbesondere bei schmalen Füßen kann ein zu großes Innenvolumen im Schuh zu eingeschränktem Halt und funktionalen Nachteilen führen.

Ingo Wietrzychowski,
Orthopädienschuh-
Techniker bei Baak

Die neue ESD-Einlegesohle „ComfyFit“ (l.) ist voluminöser als beispielsweise die Softstep-Einlegesohle (r.)



Ist der Schuh zu weit, fehlt es an Führung. Der Fuß kann im Schuh rutschen, wodurch Ausgleichsbewegungen erforderlich werden. Diese können Muskeln und Gelenke zusätzlich beanspruchen, die Ermüdung beschleunigen und die Trittsicherheit beeinträchtigen. Damit wird deutlich, dass die Passform nicht nur eine Komfort-, sondern auch eine Sicherheitsfrage ist.

Ansatz über angepasste Einlegesohlen

Eine Möglichkeit zur Verbesserung der Passform besteht im Einsatz angepasster Einlegesohlen. Die neue ESD-Einlegesohle „ComfyFit“ (ESD: elektrostatische Ableitfähigkeit) von Baak wurde gezielt für schmale und schlanke Fußformen entwickelt. Ziel ist es, überschüssigen Raum im Schuh zu reduzieren und den Fuß stabil zu führen.

Die Einlegesohle ist im Vergleich zu anderen Varianten voluminöser ausgeführt. Dadurch wird das Innenvolumen des

Schuhs ausgeglichen, ohne die Schutzfunktionen zu beeinträchtigen. Der Fuß wird stärker fixiert, was zu einer stabileren Position im Schuh beitragen kann. „Gerade bei schmalen Füßen geht im Schuh oft entscheidende Stabilität verloren“, erklärt Ingo Wietrzychowski, Orthopädienschuh-Techniker bei Baak. „Mit ComfyFit schaffen wir gezielt mehr Halt und unterstützen ein natürliches Gangbild, auch an langen Arbeitstagen.“

Ergonomische Aspekte

Die Konstruktion der Einlegesohle orientiert sich an der natürlichen Fußform. Ziel ist es, dass sich Sicherheitsschuhe und Zubehör an den Menschen anpassen – nicht umgekehrt. Eine ausgeprägte Fersenpartie („Kugelferse“) kann den Halt im Rückfußbereich verbessern und das Rutschen im Schuh reduzieren. In der Folge können unnatürliche Ausgleichsbewegungen vermindert und die Stabilität bei dynamischen Bewegungsabläufen unterstützt werden.

Solche Anpassungen sind insbesondere in Tätigkeitsbereichen mit hohen Gehanteilen relevant, etwa in Bau, Handwerk, Industrie oder Logistik.

Technische Eigenschaften und Regelwerke

Die Einlegesohle ComfyFit ist ESD-fähig und kann orthopädisch angepasst werden. Die Anpassbarkeit orientiert sich an der DGUV-Regel 112-191, die Anforderungen an orthopädische Veränderungen von Sicherheitsschuhen beschreibt. Atmungsaktive und antibakterielle Materialien unterstützen zudem ein ausgeglichenes Fußklima. Seit Mai erhalten ausgewählte Modelle der Bau-Serie die „ComfyFit“-Einlegesohle serienmäßig und ohne Aufpreis. Dadurch wird deren Weite von 12 auf 11 reduziert. **GIT**



Baak GmbH & Co KG
<https://baak.de>

Beim Modell Uvex Phynomic DX HV (Cut Level D) werden die Reißkräfte durch die integrierten Sollbruchstellen um 70 % im Vergleich zu klassischen Schnittschutzhandschuhen reduziert

Als Teil der Uvex Phynomic Serie ist der Uvex Phynomic x-foam HV speziell für Montagearbeiten konzipiert

SCHNITTSCHUTZ

Eingebaute Notbremse

Sollbruchstellen in Schnittschutzhandschuhen reduzieren Einzugsrisiken bei rotierenden Maschinenteilen

Die Arbeit an Maschinen mit rotierenden Teilen stellt besondere Anforderungen an den Handschutz. Insbesondere in Bereichen wie Metallverarbeitung, Maschinenbau oder Instandhaltung besteht das Risiko, von sich drehenden Komponenten erfasst zu werden. Klassische Schnittschutzhandschuhe bieten zwar Schutz vor mechanischen Einwirkungen, können jedoch in bestimmten Situationen selbst zum Risiko werden, wenn sie von rotierenden Teilen erfasst werden.

■ Rotierende Maschinenteile wie Wellen, Bohrer oder Fräser entwickeln hohe Kräfte. Werden Handschuhe in solche Bewegungen einbezogen, kann dies zu schweren Verletzungen führen. Das Material des Handschuhs überträgt die Zugkräfte direkt auf die Hand. Dadurch können Quetschungen, Frakturen oder sogar das Abtrennen von Gliedmaßen die Folge sein.

Aus diesem Grund wird in einigen Arbeitsbereichen grundsätzlich empfohlen, auf Handschuhe zu verzichten – etwa bei der Bedienung von Drehmaschinen. In anderen Tätigkeitsfeldern, in denen Schnitenschutz erforderlich ist, entsteht jedoch ein Zielkonflikt zwischen Schutz vor Schnittverletzungen und der Vermeidung von Einzugsgefahren.

Ansatz: Sollbruchstellen in Handschuhen

Ein Lösungsansatz besteht in der Integration von Sollbruchstellen in Schnitenschutzhandschuhen. Diese sind so konzipiert, dass sie bei Überschreiten einer definierten Zugkraft gezielt aufreißen. Ziel ist es, die Kraftübertragung auf die Hand zu reduzieren und so das Risiko schwerer Verletzungen zu minimieren.

Die Sollbruchstellen befinden sich typischerweise an strategisch ausgewählten Bereichen des Handschuhs, etwa zwischen einzelnen Materialschichten oder entlang bestimmter Nahtverläufe. Im Fall eines Ein-

zugs gibt das Material nach, bevor kritische Kräfte auf die Hand wirken.

Funktionsweise und Grenzen

Die Funktionsweise basiert auf einem kontrollierten Materialversagen. Dabei bleibt der grundlegende Schnitenschutz im regulären Einsatz erhalten. Erst bei außergewöhnlichen Belastungen – etwa durch das Erfassen in einer rotierenden Maschine – tritt die Sollbruchfunktion in Kraft.

Wichtig ist jedoch die Einordnung dieser Technologie: Sollbruchstellen stellen keinen vollständigen Schutz vor allen denkbaren Unfallmechanismen dar. Sie können das Risiko reduzieren, ersetzen jedoch keine Gefährdungsbeurteilung oder geeignete organisatorische Maßnahmen. Auch bleibt es entscheidend, die Einsatzgrenzen der Handschuhe zu beachten.

Normen und Auswahlkriterien

Bei der Auswahl von Schnitenschutzhandschuhen spielen Normen eine zentrale Rolle. Relevante Prüfverfahren sind unter anderem in der Norm EN 388 festgelegt, die mechanische Risiken wie Abrieb, Schnitt, Weiterreißen und Durchstich bewertet. Ergänzend können weitere Prüfmethoden herangezogen werden, um spezifische Eigenschaften – etwa das Verhalten unter Zugbelastung – zu beurteilen.

Neben den normativen Anforderungen sollten Anwender folgende Aspekte berücksichtigen:

- Art der Tätigkeit und Gefährdungssituation
- Nähe zu rotierenden Maschinenteilen
- erforderliches Maß an Fingersensibilität und Tragekomfort
- Schulung der Beschäftigten im sicheren Umgang

Schnitenschutzhandschuhe mit integrierten Sollbruchstellen können einen Beitrag zur Risikoreduzierung bei Arbeiten mit mechanischen Gefährdungen leisten. Sie adressieren insbesondere den Zielkonflikt zwischen Schnitenschutz und Einzugsgefahr bei rotierenden Teilen. Dennoch bleibt ihre Wirksamkeit an den konkreten Anwendungsfall gebunden. Eine ganzheitliche Betrachtung der Arbeitssituation, inklusive technischer und organisatorischer Maßnahmen, ist weiterhin erforderlich. **GIT**



Uvex Arbeitsschutz GmbH
www.uvex-safety.com

© Bilder: Uvex

Sicherheitsschuh-Linie Puma Safety Trail Protect

Mit der Puma Safety Trail Protect Linie bringt PIP EMEA frische Impulse in das Segment Performance-Sicherheitsschuhe. Unter dem Claim „Work is your trail“ richtet sich die Kollektion an alle, die sich täglich neuen Herausforderungen stellen und dabei auf hohe Performance, Komfort und Sicherheit angewiesen sind. Inspiriert von der Dynamik des Trailrunnings vereinen die Modelle modernste Technologien mit robuster Funktionalität und sportlichem Design.

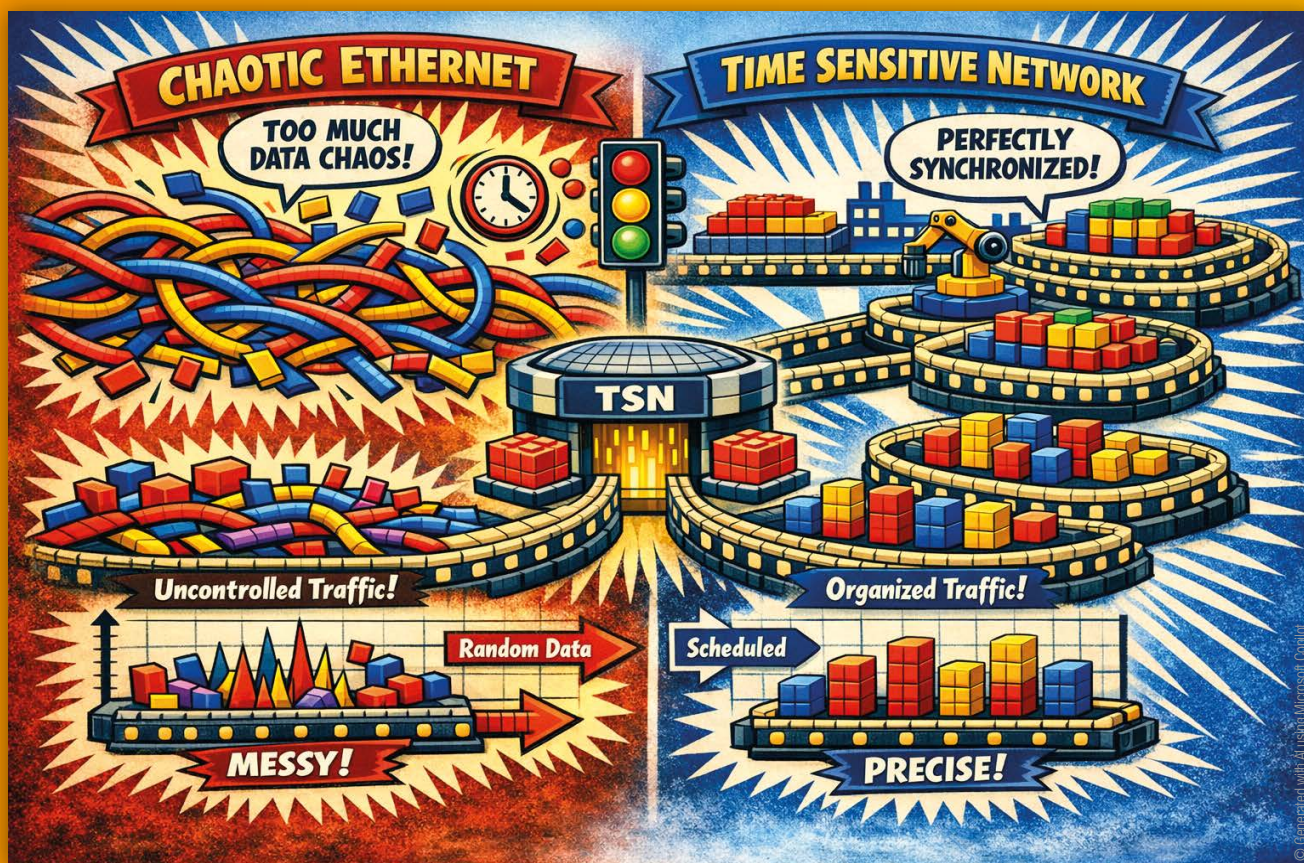
Die Trail Protect Linie wurde dafür entwickelt, den Arbeitsalltag in jedem Gelände souverän zu meistern. Ob auf unebenem Untergrund, in der Industrie oder im Handwerk – diese Sicherheitsschuhe bieten guten Grip, zuverlässige Stabilität und einen hohen Tragekomfort. Die innovative Impulse.Blast Zwischensohle unterstützt durch ihre besonders reaktionsfreudige Energierückgabe jeden Schritt und sorgt gleichzeitig für effektive Dämpfung.

Herzstück der Trail Protect Modelle ist die leistungsstarke XTS Trail Laufsohle, die speziell für anspruchsvolle Untergründe konzipiert wurde. Die strapazierfähige Gummilaufsohle bietet dank ihres ausgeklügelten Stollenprofils guten Grip auf unterschiedlichsten Böden und ist mit selbstreinigenden Eigenschaften ausgestattet.

Breite Flexkerben unterstützen die natürliche Abrollbewegung und verbessern gleichzeitig die wasserverdrängenden Eigenschaften, sodass jederzeit optimale Bodenhaftung gewährleistet ist. Ergänzt wird dieses Konzept durch die Impulse.Blast Zwischensohle. Sie nimmt die beim Auftreten entstehenden Kräfte auf, speichert diese und gibt sie unmittelbar wieder ab. Das Ergebnis ist ein besonders weiches, gleichzeitig dynamisches Laufgefühl, das den Träger spürbar entlastet und aktiv bei jedem Schritt unterstützt.

www.ism-europa.de





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 Ethernetbasierten 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 Technologiethemata wie Steuerungstechnik und Funktionale Sicherheit in der Anwendung im Maschinenbau.

MASCHINEN- UND ANLAGENSICHERHEIT

Time-Sensitive Networking – TSN in der Anwendung

OPC UA und TSN – vernetzte Produktion mit deterministischer Kommunikation

Offene und zuverlässige Kommunikation ist eine zentrale Voraussetzung für die vernetzte Industrie. Standards wie OPC UA und Ethernet TSN schaffen die technische Basis, um Maschinen, Anlagen sowie IT- und Cloud-Systeme sicher und herstellerübergreifend zu verbinden. Während OPC UA für die strukturierte Beschreibung und Semantik industrieller Informationen steht, schafft TSN die Voraussetzungen für deterministische, vorhersagbare Datenübertragung in Echtzeit. Gerade im Maschinenbau ergeben sich dadurch neue Möglichkeiten, Daten nicht nur zu transportieren, sondern gezielt nutzbar zu machen – bis hinunter zur Feldebene und über Systemgrenzen hinweg.



Herbert Köbel,
R&D – Senior Software Expert bei
Leuze electronic GmbH + Co. KG



Peter Lutz, Director Field Level
Communications bei der
OPC Foundation

OPC UA Companion Specification

Companion Specifications standardisieren die Informationen, die zwischen Maschinen und Systemen ausgetauscht werden. Sie legen fest, welche Daten übertragen werden, wie sie heißen, welche Strukturen und Datentypen sie besitzen und welche Funktionen oder Zustände unterstützt werden. Dadurch können unterschiedliche Komponenten herstellerübergreifend dieselbe Sprache sprechen.

■ Mit zunehmender Digitalisierung müssen Maschinen, Anlagen und IT-Systeme enger zusammenarbeiten. Dafür braucht es Kommunikationsstandards, die unabhängig vom Hersteller funktionieren und Informationen zuverlässig übertragen. Eine zentrale Rolle übernimmt dabei OPC UA (Open Platform Communications Unified Architecture, nach IEC 62541). Der Standard konzentriert sich nicht darauf, wie eine Maschine technisch gebaut ist, sondern wie sie ihre Daten bereitstellt. Ziel ist eine gemeinsame Sprache für die Industrie – sicher, erweiterbar und für unterschiedliche Geräte und Anwendungen geeignet.

OPC UA als semantisches Fundament

OPC UA wird überall dort eingesetzt, wo Produktionsdaten zwischen verschiedenen Ebenen ausgetauscht werden. Auf der einen Seite verbindet der Standard Maschinen mit übergeordneten Systemen wie MES (Produktionsleitsysteme zur Überwachung und Steuerung der Fertigung) oder ERP (Systeme

zur betriebswirtschaftlichen Planung). Auf der anderen Seite ermöglicht er die direkte Kommunikation zwischen Maschinen und Anlagen.

Darüber hinaus bildet OPC UA die Verbindung zur IT-Welt, etwa zu Edge-Systemen oder Cloud-Anwendungen. So können Maschinendaten nicht nur zur Steuerung, sondern auch für Auswertungen, Wartungskonzepte oder Optimierungen genutzt werden.

Ein entscheidender Vorteil von OPC UA ist, dass nicht nur Zahlenwerte übertragen werden, sondern auch deren Bedeutung. Daten sind strukturiert beschrieben, zum Beispiel mit Namen, Einheiten oder Beziehungen zu anderen Daten. Dadurch ist klar, was ein Wert aussagt – sowohl für andere Maschinen als auch für Softwareanwendungen.

Companion Specifications und Interoperabilität

Damit diese Verständlichkeit auch herstellerübergreifend funktioniert, werden

sogenannte Companion Specifications von Branchenorganisationen wie dem VDMA entwickelt. Sie definieren gemeinsame Datenmodelle für bestimmte Branchen oder Gerätetypen, etwa für Maschinen, Roboter oder Identifikationssysteme. So können unterschiedliche Geräte dieselben Informationen auf gleiche Weise bereitstellen und nutzen.

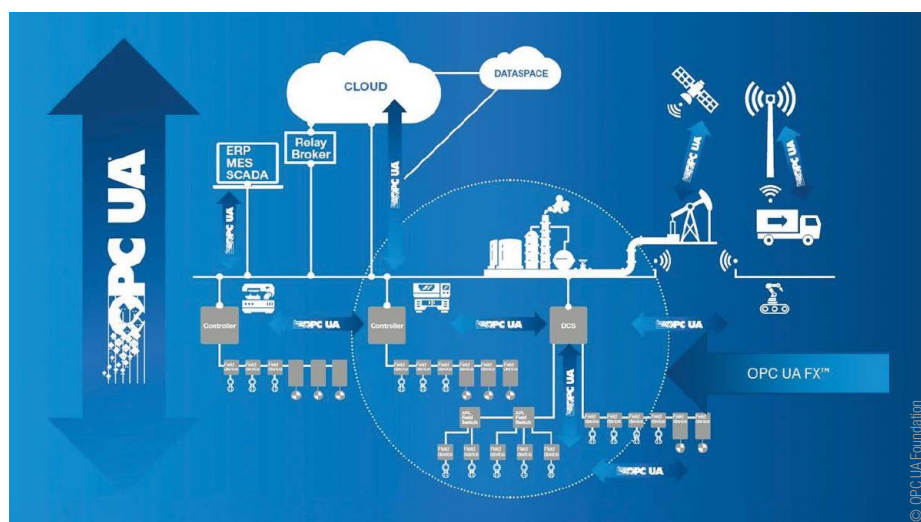
Integrierte Sicherheit

Sicherheit ist fester Bestandteil von OPC UA und erstreckt sich über alle Kommunikationsebenen bis hin zur Feldebene. Der Standard bringt Mechanismen für verschlüsselte Datenübertragung, eindeutige Identitäten und geregelte Zugriffsrechte mit. Dadurch lässt sich genau festlegen, wer welche Daten lesen oder ändern darf. Das ist besonders wichtig, wenn Produktionsdaten über Werksgrenzen hinaus oder in Cloud-Umgebungen genutzt werden.

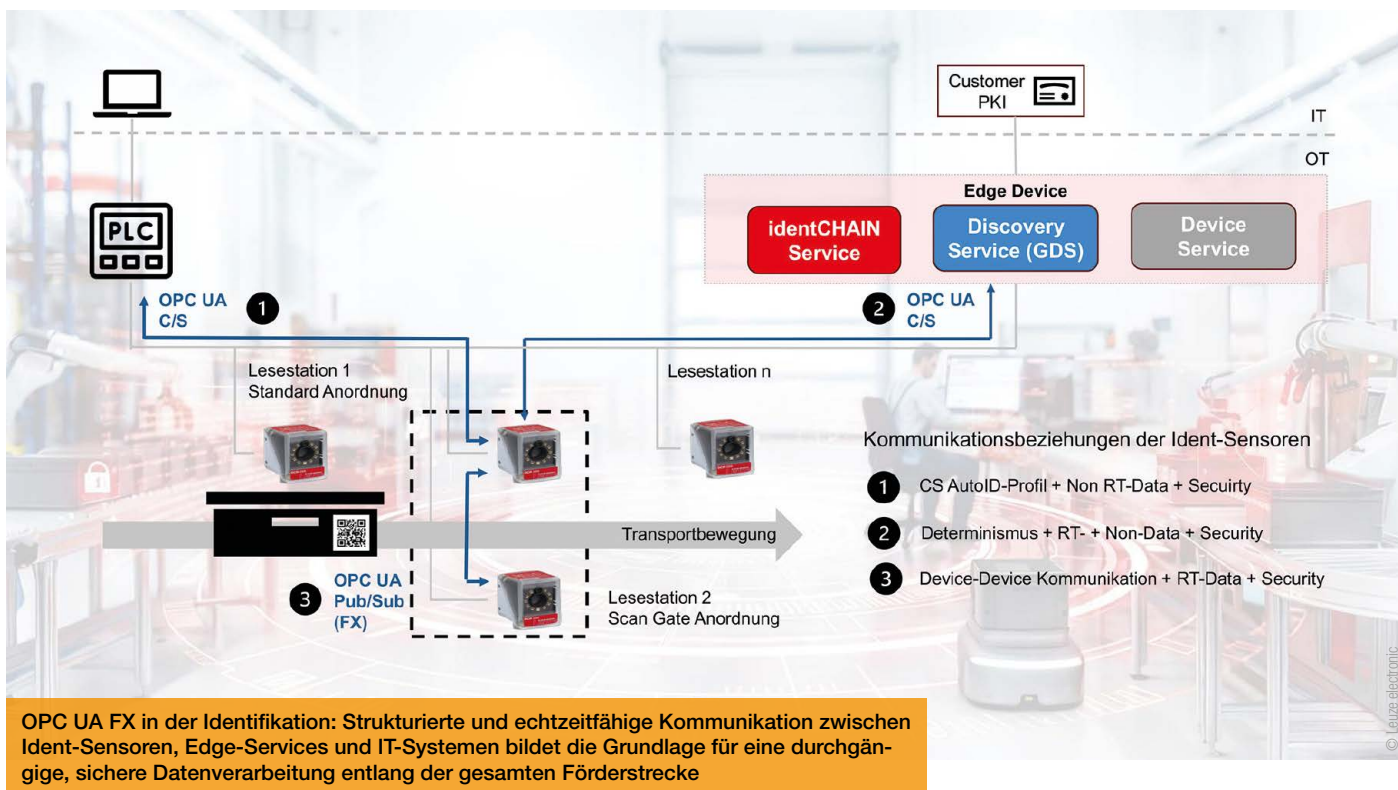
Kommunikationsmodelle: Client-Server und Publish-Subscribe

OPC UA unterstützt verschiedene Kommunikationsformen. Klassisch ist das Client-Server-Modell: Ein System fragt gezielt Daten bei einem anderen System ab. Ergänzend gibt es das Publish-Subscribe-Modell (Pub-Sub). Dabei senden Geräte ihre Daten aktiv ins Netzwerk, andere Systeme empfangen diese, ohne direkt verbunden zu sein. Das reduziert den Kommunikationsaufwand und eignet sich besonders für größere, verteilte Systeme.

Bitte umblättern ►



OPC UA FX erweitert OPC UA um eine echtzeitfähige Kommunikation auf der Feldebene mittels TSN und ermöglicht eine durchgängige Skalierung bis zur Cloud



Für die Anbindung an IT- und Cloud-Plattformen wird häufig MQTT genutzt, ein Protokoll, das sich in skalierbaren IoT-Architekturen für den Datentransport etabliert hat. OPC UA sorgt dabei für die strukturierte Beschreibung der Inhalte, MQTT für die flexible Verteilung der Daten. Die entsprechenden Erweiterungen für Cloud-Konnektivität werden unter dem Begriff OPC UA CX (Cloud eXchange) zusammengefasst.

OPC UA FX – Kommunikation bis zur Feldebene

Während OPC UA lange vor allem oberhalb der Steuerungsebene eingesetzt wurde, erweitert OPC UA FX (Field eXchange) den Standard gezielt auf die Feldebene. Ziel ist eine durchgängige Kommunikationsarchitektur vom Feldgerät über die Steuerung bis hin zu IT- und Cloud-Systemen – und das auf Basis offener, herstellerübergreifender Standards.

Für Anwender liegt der zentrale Nutzen von OPC UA FX darin, dass erstmals ein einheitlicher Kommunikationsansatz bis auf die Feldebene definiert wird, ohne bestehende Feldbus- oder Industrial-Ethernet-Systeme grundsätzlich abzulösen. Vorhandene Geräte und Anlagen können weiter betrieben werden, während neue, OPC UA FX-fähige Komponenten schrittweise ergänzt werden. Damit unterstützt OPC UA FX ausdrücklich den Schutz bestehender Investitionen.

Ein wesentlicher Mehrwert ist die durchgängige Datenstruktur. Informatio-

nen müssen nicht mehr auf jeder Ebene neu übersetzt oder interpretiert werden. Daten behalten ihre Bedeutung vom Feldgerät über die Steuerung bis in übergeordnete Systeme. Für Anwender reduziert sich damit der Integrations- und Engineering-Aufwand, insbesondere bei modularen Anlagen oder bei späteren Erweiterungen.

Technische Grundlage für OPC UA FX ist unter anderem Ethernet TSN (Time Sensitive Networking). TSN erweitert Ethernet so, dass zeitkritische Daten zuverlässig und planbar übertragen werden können. Vereinfacht gesagt, erhält wichtige Kommunikation im Netzwerk Vorrang, ohne dass dafür separate Netze notwendig sind. In der Prozessindustrie ergänzt Ethernet-APL diese Entwicklung, indem Ethernet-Kommunikation auch über große Distanzen und in explosionsgefährdeten Bereichen ermöglicht wird.

OPC UA FX unterstützt verschiedene Kommunikationsszenarien, etwa den direkten Datenaustausch zwischen Steuerungen oder die Anbindung von Feldgeräten. Auch Funktionale Sicherheit kann mit OPC UA Safety über dieselbe Infrastruktur realisiert werden. Für Anwender entsteht so perspektivisch die Möglichkeit, Steuerung, Safety-Funktionen, Diagnose und IT-Dienste über eine gemeinsame technische Basis zu betreiben.

Gleichzeitig ist der aktuelle Reifegrad von OPC UA FX realistisch einzuordnen. In der Praxis befindet sich die Technologie noch in einer frühen Phase. Erste Spezifikationen,

insbesondere für Controller-Controller-Kommunikation, sind verfügbar und werden in Demonstratoren und Pilotprojekten erprobt. Breite Serienanwendungen auf der Feldebene sind derzeit noch nicht die Regel. Für Anwender bedeutet das: OPC UA FX ist weniger als sofort flächendeckend einsetzbare Lösung zu verstehen, sondern als strategischer Entwicklungspfad mit wachsender Bedeutung.

Gerade darin liegt jedoch der Nutzen. Unternehmen können sich frühzeitig mit den Konzepten vertraut machen, erste Anwendungen evaluieren und ihre Automatisierungsarchitektur langfristig darauf ausrichten – ohne kurzfristigen Migrationsdruck oder Systembrüche.

Anwendungsbeispiel: Objekt-Tracking mit OPC UA und TSN

Ein anschauliches Beispiel findet sich in der Intralogistik: Hier müssen Behälter, Werkstücke oder Pakete zuverlässig durch Förder- und Sortiersysteme verfolgt werden. Damit Steuerungen schnell reagieren können, müssen relevante Informationen direkt auf der Feldebene verfügbar sein.

Typischerweise werden Objekte über eine Identifikationsnummer, wie z. B. über einen kostengünstigen Barcode verfolgt. Für die lokalen Entscheidungen werden zunehmend weitere Informationen übertragen – etwa der aktuelle Status, Prozessdaten oder Zeitstempel. Diese Daten werden nicht auf dem Objekt selbst gespeichert (wie bei einem beschreibbaren RFID-Tag), son-

den zentral in einer lokalen Datenbank auf einem Edge-System direkt in der Feldebene verwaltet und stehen über eine gesicherte Verbindung allen berechtigten Sensorsystemen zur Verfügung. Die Struktur der Daten orientiert sich an standardisierten OPC UA-Modellen, sodass sie unmittelbar über die Profile der Sensoren zeitnah nutzbar sind.

Bei schnell bewegten Objekten oder Lesevorgängen über mehrere Identensysteme gleichzeitig ist eine präzise Abstimmung notwendig. Hier ermöglicht die Kombination aus OPC UA Publish-Subscribe und TSN eine zeitlich abgestimmte, vorhersehbare Kom-

munikation. Gleichzeitig bleiben die Daten eindeutig beschrieben und damit über alle Ebenen hinweg interpretierbar.

Parallel dazu können Diagnose oder Visualisierungsfunktionen genutzt werden. TSN stellt sicher, dass diese zusätzlichen Daten den zeitkritischen Betrieb nicht beeinträchtigen.

Insgesamt entsteht so eine gemeinsame Kommunikationsbasis, die Echtzeitfähigkeit, Verständlichkeit der Daten und Sicherheit verbindet – und damit eine tragfähige Grundlage für moderne, vernetzte Intralogistik und Produktionssysteme schafft. **GIT**



OPC Foundation
<https://opcfoundation.org>

Leuze electronic
GmbH + Co. KG
www.leuze.com

Vernetzt, flexibel, zukunftssicherer

Sichere Automation: Jetzt die passende Lösung mit Schmersal finden

ADVERTORIAL

Der Maschinenbau steht vor einem Paradigmenwechsel: Modulare Anlagen, flexible Produktion und Digitalisierung erfordern neue Ansätze für die funktionale Sicherheit. Schmersal treibt diesen Wandel voran und verknüpft Sicherheitstechnik mit modernen Kommunikationsarchitekturen.

Drei Technologien prägen die nächste Generation: dezentrale Sicherheitskonzepte mit der Sicheren Feldbox (SFB), IO-Link Safety sowie perspektivisch Single Pair Ethernet (SPE) als durchgängige Infrastruktur vom Sensor bis in die Cloud.

Dezentrale Sicherheit mit der Sicheren Feldbox

Mit der SFB werden Sicherheitsfunktionen in Maschinenmodule verlagert. Das reduziert Verdrahtungsaufwand, vereinfacht die Inbetriebnahme und ermöglicht skalierbare Architekturen. Besonders bei modularen Anlagen entstehen neue Freiheitsgrade.

Markteinführung erster IO-Link-Safety-Produkte

IO-Link Safety ermöglicht eine durchgängige, sichere bidirektionale Kommunikation bis auf Sensor- und Aktorebene. Neben den sicheren Prozessdaten stehen Diagnose-, Status- und Betriebsdaten, sowie die sichere Konfiguration und Parametrierung der Gerätefunktionen zur Verfügung.



Schmersal versteht Sicherheit als vernetztes System und gestaltet die digitale Produktion aktiv mit

Mit dem AZM42 und RSS362 bringt Schmersal die ersten IO-Link-Safety-fähigen Produkte auf den Markt. Standardisierte Steckverbindungen reduzieren den Engineering-, Wartungs- und Serviceaufwand erheblich.

Single Pair Ethernet als Zukunftsinfrastruktur

Langfristig eröffnet Single Pair Ethernet neue Perspektiven. Die Technologie ermöglicht die durchgängige Ethernet-Kommunikation über nur ein Adernpaar und schafft die Grundlage für einheitliche Sensor2Cloud-Netzwerke.

Im Zusammenspiel entstehen flexible, effiziente und zukunftssichere Maschinen. Schmersal versteht Sicherheit als vernetztes System und gestaltet die digitale Produktion aktiv mit.

SCHMERSAL
THE DNA OF SAFETY

Kontakt

K. A. Schmersal GmbH & Co. KG
www.schmersal.com

Der Ethernet-APL Field Switch von FieldConnex: Informationen über angeschlossene Geräte sowie die Qualität der Installation

MASCHINEN- UND ANLAGENSICHERHEIT

Vom blinden Fleck zur Datenquelle

Infrastrukturdiagnose mit Ethernet-APL

Die Verkabelung im Feld einer Prozessanlage altert unbemerkt: Klemmen korrodieren, Schirmungen lassen nach, doch ihren physischen Zustand sieht in der klassischen 4...20-mA-Welt niemand, bis eine Messstelle ausfällt. Ethernet-APL macht diese Übertragungsphysik erstmals durchgängig sichtbar und verwandelt die Infrastruktur in eine überwachbare Datenquelle – für Sicherheit, Compliance und Verfügbarkeit.

Es beginnt mit einer Messstelle, die zickt: Mal steht der Wert sauber, mal flackert er, dann ist er für einige Sekunden weg. Der Instandhalter misst, findet nichts und quittiert die Störung. Zwei Wochen später dasselbe Spiel an einer Nachbarstelle. Was hier altert, ist nicht das Messgerät, sondern die Übertragungsstrecke: eine korrodierende Klemme, eine nachlassende Schirmung, eine Leitung, eine mangelhafte Dichtung am Gehäuse, an der die Feuchtigkeit arbeitet – mögliche Ursachen sind vielfältig. Doch genau diese physikalische Ebene – Spannung, Strom, Signalqualität – sieht in der klassischen 4...20-mA-Welt niemand. Sie ist unsichtbar, bis sie ausfällt. Und dann steht im schlimmsten Fall die Produktion.

Dieses Grundproblem ist bekannt. Die Feldbustechnik half, die Infrastruktur transparent zu machen, und bei eingeweihten Anwendern bewährte sich das: Mit dem Advanced Diagnostic Module (ADM) zeigte Pepperl+Fuchs früh, dass sich die Alterung

der Feldinstallation erfassen lässt und dass sich daraus belastbare Prognosen ableiten lassen. Doch in der Breite setzte sich der Feldbus in der Prozessindustrie nie durch. Er galt als zu komplex, das Betriebspersonal war kaum geschult und weil die alten 4...20-mA-Schleifen so stabil liefen, rüsteten manche Anwender Feldbusinseln sogar wieder auf Analogtechnik zurück. Der Preis dieser Stabilität: keine Sicht auf den Zustand der Infrastruktur und ein latentes Risiko für Betrieb, Sicherheit und Audit.

So sieht die Realität in den meisten Bestandsanlagen aus. Dort dominieren zwei Konzepte: die klassische 4...20-mA-Stammkabel-Verdrahtung und die Anbindung von 4...20-mA-Geräten über Remote-I/O-Stationen im Feld. Beide Konzepte bringen das Signal zuverlässig zur Steuerung, haben jedoch denselben blinden Fleck. Ob ein Übergangswiderstand wächst, ein Schirm seine Wirkung verliert oder eine Leitung an ihrer Spezifikationsgrenze arbeitet, bleibt verborgen, und der Messwert sieht nur noch

plausibel aus. Die Remote-I/O-Variante verlagert die Wandlung näher ans Feld und spart Kabel, ändert am Kern aber nichts: Die analoge Strecke zwischen Sensor und I/O-Karte bleibt eine Blackbox. Diagnose über den Zustand der Übertragungsphysik liefert keines der beiden Konzepte.

Ein Netzwerk für das Feld

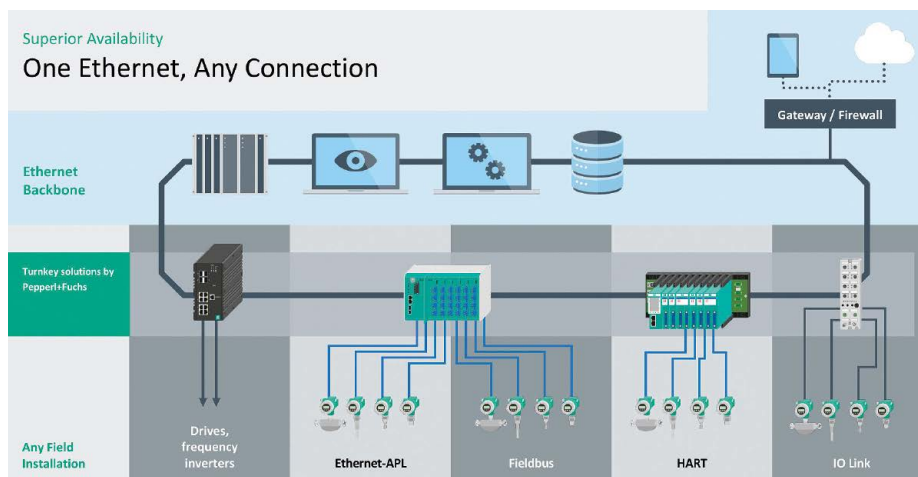
Den Ausweg liefert eine Technologie, die niemand mehr erklären muss: Ethernet. Mit dem Advanced Physical Layer (APL) zieht es bis ins Feld – auch in explosionsgefährdete Bereiche. Basis ist die bewährte Zweidrahtleitung für Speisung und Kommunikation; Redundanzkonzepte wie das Media Redundancy Protocol (MRP) sind Teil von Ethernet und damit integriert. Ethernet ist auch im Haushalt Alltag, das Know-how ist in der Belegschaft längst vorhanden. Hinzu kommen handfeste Vorteile: eine präzise, driftfreie Übertragung ohne Messbereichsskalierung, eine schnelle parallele Kommunikation und mehrere Messwerte je Feldgerät. Letzteres senkt die Investitionskosten spürbar, da weniger Geräte weniger Verrohrung, Raum und Fläche benötigen.

Die Infrastruktur wird zur Datenquelle

Hier setzt der Ethernet-APL-Field-Switch von FieldConnex an. Im Feld installiert, überwacht er die angeschlossenen Geräte, den Uplink und sich selbst und macht so die

Übertragungsphysik zu einem planbar wartbaren Anlagenteil. Er misst kontinuierlich die physikalische Ebene jeder Verbindung: Spannung, Strom, Signalpegel, Rauschen, Jitter und das Signal-Rausch-Verhältnis (SNR). Jede Veränderung wird erfasst und dokumentiert, sodass der Zustand jeder Leitung über die Zeit nachvollziehbar bleibt. Hinzu kommen Temperaturüberwachung und interne Verschleißanzeige. Wiederkehrende Snapshots speisen Asset-Management- und Historiensysteme, sodass eine stets gepflegte Bestandsaufnahme entsteht. Damit kehrt der ADM-Gedanke zurück: Wer vor einem Migrationsprojekt wissen möchte, welche Kabel ausgetauscht werden müssen, kann dies zukünftig aus den Langzeitdaten ableiten, statt auf Verdacht zu erneuern.

Zur Transparenz kommt die Selbstdokumentation. An jedem Anschluss identifiziert der Switch das Feldgerät über seine eindeutige ID. Wird ein Gerät getauscht oder ergänzt, ermöglicht eine Ethernet-Verbindung, dass sich die Dokumentation automatisch aktualisiert und eine manuelle Nachpflege entfällt. Auf diese Weise wird in Asset Management Systemen eine Langzeitüberwachung ermöglicht, die Inkonsistenzen vermeidet und eine revisionssichere Datenbasis liefert. Hinzu kommt, dass sich Switch und Remote-I/O als anschlussfertige, zertifizierte Gehäuselösungen vorverdrahtet und geprüft auf die Baustelle liefern lassen. Das beschleunigt die Inbetriebnahme und entlastet die Investitionsseite.



Kontinuierlich wird die physikalische Ebene jeder Verbindung gemessen: Spannung, Strom, Signalpegel, Rauschen, Jitter und das Signal-Rausch-Verhältnis (SNR). Jede Veränderung wird erfasst und dokumentiert, sodass der Zustand jeder Leitung über die Zeit nachvollziehbar bleibt

Sicherheit ohne Infrastruktur-Ballast

Noch grundlegender wirkt Ethernet-APL bei der funktionalen Sicherheit. Da Prozess- und Sicherheitssignale dieselbe physikalische Infrastruktur und dasselbe Protokoll nutzen können, lässt sich Safety über genau diese Architektur realisieren. Möglich macht das der „schwarze Kanal“: Auf Protokollebene erkennen Mechanismen wie Telegrammzähler und starke Prüfsummen Übertragungsfehler in der Infrastruktur und falsche Reihenfolgen mit einer für SIL 3 geeigneten Sicherheit. Die Übertragung sicherheitsrelevanter Signale wird damit unabhängig von der darunterliegenden Kommunikation.

Die Konsequenz ist erheblich: Die Infrastruktur ist nicht mehr Teil der sicherheitstechnischen Bewertung. Bei einem Sicherheitskreis zählen nur noch Sensor, Steuerung und Aktor; die Kommunikation bleibt als reiner für SIL 3 geeigneter Transportkanal außen vor. Das vereinfacht Planung und Nachweisführung. Zudem wird ein bekanntes Ärgernis gelöst: Wird nach einer HAZOP-Studie ein Betriebsmesspunkt zur Sicherheitsmessstelle aufgewertet, bedeutet das in der analogen Welt den kompletten Rückbau auf 4...20 mA – neue Geräte, neue Verdrahtung, verlorene

Bitte umblättern ▶

MADE IN GERMANY

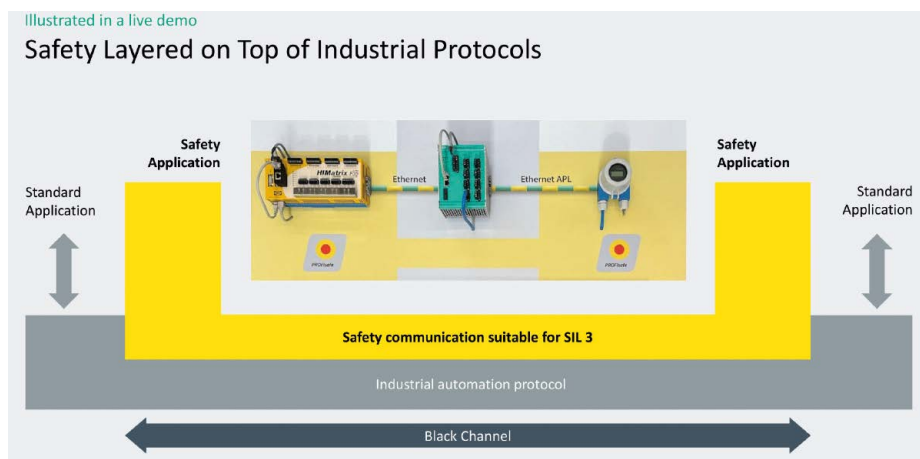


FLEXITAST DIE INNOVATIVE DISPLAYTASTE

- HIGH-KONTRAST:** Innovative ZBD-Technologie für perfekte Darstellung.
- DYNAMIC-CONTENT:** Symbole und Texte jederzeit flexibel anpassen.
- PURE-COLOR:** Brillante Farben und echtes Weiß dank RGBW-LEDs.
- ZERO-POWER-SAFE:** Informationen bleiben auch ohne Strom dauerhaft sichtbar.
- EFFIZIENZ-PLUS:** Komplexität reduzieren, Energie sparen und Kosten nachhaltig senken.



SCHLEGEL®
ELEKTROKONTAKT
www.schlegel.biz



Im Feld installiert, überwacht der Ethernet-APL Field Switch die angeschlossenen Geräte, den Uplink und sich selbst und macht so die Übertragungsphysik zu einem planbar wartbaren Anlagenteil

Diagnose. Auf einheitlicher Ethernet-APL-Basis genügt im Idealfall, die Sicherheitskommunikation des Feldgeräts zu aktivieren.

Für die Infrastruktur selbst zählt damit nur noch eine Größe: ihre Verfügbarkeit. Dafür sorgen Medienredundanz und die kontinuierliche Diagnose der Übertragungsqualität. Akute Meldungen ermöglichen zudem schnelle Eingriffe. Dass Ethernet auch im rauen Umfeld robust ist, ist keine Glaubensfrage: In einem frühen Test wurde ein 100 Meter langes Patchkabel mehrfach um einen Schweißtransformator gelegt – von über 538 Millionen Telegrammen in 16 Tagen wurden nur 15 gestört.

Allerdings ist die sicherheitsgerichtete Kommunikation über Ethernet-APL in der Praxis noch Zukunftsmusik. Standardseitig ist der Weg geebnet: Profisafe als TÜV-geprüftes SIL-3-Protokoll setzt auf dem

schwarzen Kanal auf und ist vom Übertragungskanal unabhängig. Erste Erfahrungen damit sammelte die BASF in einer Testanlage. Was noch fehlt, sind serienreife Geräte: SIL-zertifizierte Sensoren für Ethernet-APL sind derzeit noch nicht am Markt erhältlich. Anwender wie die BASF drängen darauf, dass die Hersteller nachziehen. Erste Geräte sind für die kommenden Jahre angekündigt.

Vom Diagnosewerkzeug zur Managementgrundlage

Der eigentliche Hebel liegt jenseits der Einzeldiagnose. Eine durchgängige digitale Ethernet-Kommunikation bis zu den Feldgeräten ist die Grundlage für die Anlagensoptimierung – zunehmend auch mit KI. Während bislang von jedem Gerät nur der eine, fürs Regeln nötige Messwert nach oben gelangte, liefert ein Feldgerät mehrere Prozesswerte auf einmal. Eine Fülle

zusätzlicher Alarm- und Diagnosedaten werden über einen zweiten Kanal ausgewertet, ohne die Prozessführung anzutasten – etwa im Sinne der NAMUR Open Architecture (NOA), die solche Daten an der Automatisierungspyramide vorbei für Monitoring und Optimierung erschließt. Daraus speisen sich Langzeitanalysen wie die Alterungsprognose, die Auffälligkeiten früher erkennen als ein Mensch. Die stets aktuelle Selbstdokumentation der Feldgeräte zahlt zugleich auf Compliance und Betriebskosten ein, beschleunigt die Inbetriebnahme und sichert so im laufenden Jahr Umsatz.

Die Bandbreite eröffnet zudem Möglichkeiten, die mit Analogtechnik nicht realisierbar sind. Weil ein Feldgerät via Ethernet-APL viele Daten in hoher Qualität liefert, lassen sich Messprinzipien neu definieren: Möglich wäre beispielsweise ein Drucksensor, der zugleich als Mikrofon arbeitet und Geräusche im Rohr oder Tank erkennt. So wird aus dem Messpunkt ein intelligenter Knoten im Anlagennetz. Damit ist die Transparenz der Übertragungsphysik die gemeinsame Grundlage für Sicherheit, Compliance und einen wirtschaftlichen, hochverfügbaren Betrieb. Wer sie nutzt, tauscht die Blackbox gegen Klarsicht. **GIT**



Pepperl+Fuchs SE
www.pepperl-fuchs.com

© Bilder: Pepperl+Fuchs



Hilscher und Schwarz Digits starten Edge-to-Cloud-Plattform

Die Hilscher Gesellschaft für Systemautomation mbH und Schwarz Digits haben eine Kooperation zur Bereitstellung souveräner europäischer Edge-to-Cloud-Lösungen für die Industrie bekannt gegeben. Kern ist die Kombination aus Hilschers Edge- und Device-Management-Plattform netFIELD und der europäischen Cloud-Infrastruktur STACKIT Cloud von Schwarz Digits. Ziel ist eine offene, skalierbare Infrastruktur für Industrieunternehmen, Maschinenbauer, OEMs und Systemintegratoren, um digitale Services schneller auszurollen – bei voller Kontrolle über sensible Betriebs-, Prozess- und Produktdaten. Je nach Bedarf können Anwendungen in Public Cloud, Private Cloud oder On-Premise betrieben werden. Die Plattform verbindet Maschinen und Anlagen sicher mit Cloud-Ressourcen in Europa und erleichtert auch die Einbindung bestehender Maschinenparks. <https://www.hilscher.com>

Neuer Vorstand für VDMA Elektrische Automation

Der VDMA Elektrische Automation hat einen neuen Vorstand für die Amtsperiode 2026 bis 2030 gewählt. Jessica Bethune, Schneider Electric GmbH, übernimmt den Vorsitz und Gerd Hoppe, Beckhoff Automation GmbH & Co. KG, wurde zum stellvertretenden Vorsitzenden benannt.

Die Veranstaltung wurde durch ein Vorabendprogramm und hochkarätige Fachbeiträge begleitet. Thilo Brodtmann, Hauptgeschäftsführer des VDMA, ordnete die aktuelle Lage im Maschinen- und Anlagenbau ein. VDMA-Chefvolkswirt Dr. Johannes Gernandt beleuchtete die konjunkturellen Entwicklungen, während Nikolai Ensslen, Co-Founder & CEO der Vesoma GmbH, Impulse zu humanoider Robotik in Verbindung mit Künstlicher Intelligenz gab. Ein Workshop mit den Mitgliedsunternehmen lieferte wichtige Impulse für die neue Amtsperiode des Vorstands: Hier kamen die relevanten Themen und Handlungsfelder für die kommende Amtsperiode zur Sprache – u. a. mit Fokus auf Innovation, Resilienz und Wettbewerbsfähigkeit.

Mit großem Dank für sein langjähriges Engagement und seine wertvollen Verdienste wurde der bisherige Vorsitzende Jörg Freitag, Siemens AG, nach Erreichen der maximalen Amtszeit verabschiedet. www.vdma.eu



BVSW: Peer-Austausch Auslandssicherheit

Der BVSW veranstaltete einen Peer-Austausch zum Thema Auslandssicherheit. Auf der Agenda standen Prävention, Krisenmanagement und Best Practices für internationale Geschäftsreisen und Auslandseinsätze. Anlass für den Start dieses neuen Veranstaltungsformats ist eine Herausforderung, mit der sich immer mehr Unternehmen konfrontiert sehen: Die Sicherheit von Geschäftsaktivitäten im Ausland zu gewährleisten wird angesichts zunehmender geopo-

litischer Spannungen zunehmend schwieriger. „Gewissenhafte Vorbereitung, Zugang zu aktuellen Informationen sowie ein belastbares Netzwerk im Ernstfall gewinnen an Bedeutung. Mit unserem neuen Peer-Austausch schaffen wir ein Format, das unseren Mitgliedern Einblicke in aktuelle Ereignisse bietet und einen vertrauensvollen Erfahrungsaustausch ermöglicht“, so BVSW-Geschäftsführerin Caroline Eder. www.bvsw.de

Grünes Licht für Neubau: Schlegel erweitert am Standort

Das Elektrotechnik-Unternehmen Georg Schlegel stellt die Weichen für seine Zukunft und erweitert am Standort Dürmentingen: Schlegel investiert einen Millionenbetrag in einen Neubau und setzt damit das größte Bauprojekt seiner Geschichte um. „Der Neubau ist ein klares Bekenntnis zum Standort Dürmentingen sowie zur Zukunft der Produktion ‚Made in Germany‘“, betonen die Geschäftsführer Christoph Schlegel, Wolfgang Weber und Eberhard Schlegel.

Bereits 2023 konnte das Unternehmen das benachbarte Grundstück erwerben. Die Pläne für das Projekt liegen seit 2024 in der Schublade. Voraussetzung für die Umsetzung war jedoch eine stabile wirtschaftliche Entwicklung. Nachdem sich die Auftragslage zuletzt deutlich stabilisiert hat, fiel nun die Entscheidung für den Baustart.

Mit dem Neubau reagiert das Elektrotechnik-Unternehmen mit seinen rund 250 Mitarbeitern vor allem auf die zunehmende Platznot. Die bestehenden Gebäude sind inzwischen vollständig ausgelastet, zahlreiche Abteilungen arbeiten unter beengten Bedingungen. Der Neubau schafft rund 2.800 Quadratmeter zusätzliche Nutzfläche. Damit wächst die verfügbare Fläche des Unternehmens um knapp 50 Prozent – von derzeit rund 5.700 auf künftig etwa 8.500 Quadratmeter. Damit schafft das Unternehmen die räumlichen Voraussetzungen für weiteres Wachstum und zukünftige Entwicklungen.

Automatisierung wichtiger Baustein

Ein wichtiger Schwerpunkt liegt dabei auf der Automatisierung. Sie gilt als entscheidender Baustein, um die Wettbewerbsfähigkeit des Standorts langfristig zu sichern. „Automatisierung ist ein wichtiger Ansatz, um langfristig erfolgreich produzieren zu können“, betonen die Geschäftsführer. Ziel sei es, die Produktion in Dürmentingen

nachhaltig zu stärken und die Voraussetzungen für weiteres Wachstum zu schaffen. Schlegel entwickelt und produziert Elektrotechnik-Komponenten zur Steuerung von Maschinen und Anlagen, die weltweit eingesetzt werden.



Schlegel investiert einen Millionenbetrag in den geplanten Erweiterungsbau (im Vordergrund), der auch einen neuen Eingangsbereich beinhaltet

Baubeginn im Spätsommer

Die Bauarbeiten sollen nach aktueller Planung im August oder September beginnen. Mit den Rohbauarbeiten wurde die Firma Fritschle aus Uttenweiler beauftragt, die auch den Erweiterungsbau im Jahr 2014 realisiert hat. Die Fertigstellung des Rohbaus ist für das Frühjahr 2027 vorgesehen, die Inbetriebnahme des Neubaus für Herbst 2028. www.schlegel.biz

MASCHINEN- UND ANLAGENSICHERHEIT

Cybersecurity wird Teil der Maschinenzulassung

CRA und Maschinenverordnung machen Cybersecurity zur Pflicht im gesamten Produktlebenszyklus.

Das System 2BSecure schützt externe Schnittstellen wie USB- oder Ethernet-Ports vor schadhaftem Zugriff

SCHLEGEL
ELEKTRONIK

Jürgen Leng,
Business Development
Manager bei Schlegel

Die EU-Maschinenverordnung 2023/1230 und der Cyber Resilience Act (CRA) setzen neue Maßstäbe für Maschinensicherheit. Hersteller müssen nicht nur funktionale Sicherheit, sondern künftig auch den Schutz vor Cyberrisiken systematisch berücksichtigen und dokumentieren. Im Interview erklärt der Normungsexperte Jürgen Leng, Business Development Manager bei Schlegel, worauf Unternehmen achten müssen – und wie Schlegel mit 2BSecure einen praxisnahen Schutz bietet.

■ GIT SICHERHEIT: Herr Leng, CRA und Maschinenverordnung – worauf müssen sich Unternehmen in puncto Maschinensicherheit einstellen?

Jürgen Leng: Mit der neuen EU-Maschinenverordnung (EU) 2023/1230 und dem Cyber Resilience Act (CRA) wird Cybersicherheit erstmals zu einem verbindlichen Bestandteil der Maschinensicherheit. Neben der funktionalen Sicherheit müssen Hersteller künftig auch den Schutz vor Cyberrisiken systematisch berücksichtigen und dokumentieren.

Eine wichtige Neuerung ist der in Anhang III, Abschnitt 1.1.9 der Maschinenverord-

nung geforderte Schutz gegen sogenannte „Korrumpierung“. Das ist ein Begriff aus der Normung und bezeichnet die Manipulation oder unbefugte Veränderung von Maschinen, Software oder Parametern, die sicherheitsrelevante Funktionen beeinträchtigen kann.

Was verbirgt sich konkret dahinter?

Jürgen Leng: Die Norm prEN 50742 „Schutz von Maschinen gegen Korrumpierung“ gibt Herstellern praxisnahe Leitlinien. Sie definiert, wie Maschinen konzipiert und betrieben werden, dass sowohl unbeabsich-

tigte als auch vorsätzliche Manipulationen verhindert werden.

Im Fokus stehen insbesondere:

- Zugriffsschutz für Maschinen und Steuerungen
- Absicherung von externen Schnittstellen
- Schutz vor manipulierten Softwareständen
- Sicherstellung der Integrität sicherheitsrelevanter Funktionen

Parallel fordert der CRA klare Nachweise über die Cybersecurity von vernetzten Maschinen – ein Novum für die EU.

Welche konkreten Anforderungen bringt der Cyber Resilience Act für Maschinenhersteller?

Jürgen Leng: Der CRA verpflichtet Hersteller dazu, Cybersicherheit über den gesamten Produktlebenszyklus hinweg sicherzustellen – von der Entwicklung bis zum Ende der Nutzung.

- Zu den wichtigsten Anforderungen gehören: Security by Design & Default: Cybersicherheit muss bereits bei der Entwicklung berücksichtigt werden. Produkte dürfen keine Standardpasswörter haben und ungenutzte Schnittstellen müssen deaktiviert sein.
- Risikobewertung und Schwachstellenmanagement: Eine systematische Cyber-Risikobewertung ist für den Hersteller vor der Markteinführung verpflichtend. Gefundene Schwachstellen müssen dokumentiert und schnell behoben werden.
- Verpflichtende Sicherheitsupdates: Sicherheitsupdates müssen mindestens fünf Jahre oder über die erwartete Lebensdauer des Produkts bereitgestellt werden.
- Transparenz: Offenlegung aller Softwarekomponenten (inkl. Open Source), um Transparenz über die Lieferkette zu schaffen (Software Bill of Materials – SBOM).
- Meldepflichten: Schwerwiegende Sicherheitsvorfälle müssen an die Behörden gemeldet werden.
- Konformitätsbewertung & CE-Kennzeichnung: Je nach Risikoklasse sind Selbstbewertungen oder externe Prüfungen erforderlich. Zudem werden die CRA-Anforderungen Teil der CE-Konformitätsbewertung.

Für Maschinenbauer bedeutet das: Cybersecurity wird künftig zu einem festen Bestandteil der Produktzulassung.

Welche Produkte sind vom CRA betroffen?

Jürgen Leng: Der CRA gilt für alle Produkte mit digitalen Elementen, die in der EU hergestellt, importiert oder vertrieben werden. Der Anwendungsbereich ist also ziemlich weit gefasst, weil er alle Produkte betrifft, die mit Netzwerken oder Geräten verbunden sind.

Welche Produkte fallen unter den CRA? Hier geht's zum Text vom TÜV Süd



Die Produkte werden dabei in verschiedene Risikoklassen eingeteilt. Bei der Einstufung spielt vor allem ihr mögliches Schadenspotenzial eine Rolle. Produkte, die etwa in kritischen Infrastrukturen, der industriellen Produktion oder im Energieumfeld eingesetzt werden, fallen in eine höhere Risikokategorie. Für Hersteller bedeutet das: Die Verfahren zur Konformitätsbewertung werden umfassender und anspruchsvoller.

Wer prüfen will, welches seiner Produkte unter den CRA fällt, dem sei ein Test von TÜV Süd auf dessen Homepage empfohlen. Anhand weniger Fragen wird ermittelt, ob der Cyber Resilience Act für eigene Produkte relevant ist:

Wie hoch ist aktuell das Gefährdungspotenzial durch Cyberangriffe?

Jürgen Leng: Das Risiko ist bereits heute hoch. Das ist den Unternehmen auch bewusst. Laut Branchenverband Bitkom (Wirtschaftsbericht 2025) schätzten 72 % der Befragten die Bedrohungslage als hoch ein, zudem waren in den vergangenen zwölf Monaten rund 66 % der deutschen Unternehmen von Datendiebstahl betroffen. Rund 70 % der Angriffe werden der organisierten Kriminalität zugerechnet. Die Schadenshöhe durch Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen ist von 2024 auf 2025 um fast 20 Milliarden auf 73,3 Milliarden Euro gestiegen.

Das Thema ist also sehr aktuell. Das gilt auch für den Zeitplan des CRA: Die Meldepflicht für Schwachstellen und Sicherheitsvorfälle im Rahmen des CRA tritt am 11. September 2026 in Kraft. Am 11. Dezember 2027 müssen dann alle neuen Produkte vollständig CRA-konform sein.

Die Absicherung von externen Schnittstellen ist Teil der Norm zum Schutz vor Korruption. Warum bleiben diese Schnittstellen oft unbeachtet?

Jürgen Leng: Das Risiko durch physische Schnittstellen an Maschinen wird tatsächlich oft unterschätzt. Mit der zunehmenden Vernetzung von Maschinen im Zuge von Industrie 4.0 steigt auch das Risiko von Cyberangriffen über USB- oder Ethernet-Ports. Diese sind in vielen Fällen notwendige Servicezugänge, aber auch potenzielle Einfallstore. Über diese Zugänge können Schadprogramme eingeschleust, Daten ausgelesen oder Maschinenparameter verändert werden. Hier können technische Schutzmaßnahmen viel bewirken.

Schlegel hat mit 2BSecure ein System entwickelt, das offene Schnittstellen schützt. Wie funktioniert dies konkret?

Jürgen Leng: 2BSecure ist als kompakte Hardwarelösung konzipiert, die zwischen Schnittstelle und Endgerät installiert wird und ist für gängige USB-A-, USB-C- sowie Ethernet-Schnittstellen ausgelegt. Das System verfolgt einen präventiven Ansatz: Schnittstellen werden standardmäßig deaktiviert und lassen sich nur über Schlüsselschalter oder RFID durch autorisierte Personen gezielt freischalten. Nur berechtigte Personen können damit Ports aktivieren und Daten übertragen, der Zugriff wird dadurch kontrollierbar und Manipulationen können wirksam verhindert werden. Die Lösung schützt sowohl die Maschinensteuerung als auch sensible Daten im Netzwerk.

Ist für die Nutzung ein größerer Umrüstaufwand notwendig?

Jürgen Leng: Nein, die Lösung ist einfach integrierbar. Sie kann sowohl in neuen Maschinen als auch in Bestandsanlagen eingesetzt werden und lässt sich ohne großen Aufwand in vorhandene Maschinen- und IT-Infrastrukturen einbinden. Damit folgt sie dem Prinzip „Security by Design“.

Inwiefern spielen gesetzliche Vorgaben bei der Entwicklung eine Rolle?

Jürgen Leng: Die regulatorischen Anforderungen durch die neue Maschinenverordnung oder den CRA waren ein wesentlicher Treiber. Durch die kontrollierte Absicherung physischer Schnittstellen kann 2BSecure dazu beitragen, diese Anforderungen technisch umzusetzen und Risiken nachweisbar zu reduzieren.

Herr Leng, vielen Dank für das Gespräch. **GIT**



In **GIT Business Partner**, dem „Who is who in Sachen Sicherheit“, präsentieren sich Ihnen die kompetentesten Anbieter aus allen Bereichen der Sicherheit. Die hier vertretenen Firmen freuen sich über Ihre Kontaktaufnahme.

Alle Präsentationen, Einträge, Infos zum Unternehmen und Berichte über das jeweilige Unternehmen finden Sie auch im dazugehörigen Company Channel auf <https://git-sicherheit.de/de/business-partner> – mit Links zu den Unternehmen.

Sie gehören selbst zu den wichtigen Anbietern und wollen mit jeder Ausgabe mehr als 25.000 Entscheider direkt erreichen? Dann kontaktieren Sie uns für eine Präsentation.



© Vitaya_25 - stock.adobe.com

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 Switche für Video

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

Sicherheitsmanagement



BOSCH

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

Sicherheitsmanagement



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 Sicherheitsfachrichter.

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 Zufahrtskontrollsysteme;
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, Implementierung 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

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.

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

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

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

Gebäudesicherheit



Uhlmann & Zacher GmbH **ASSA ABLOY**
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.

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



Perimeterschutz



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



Videoüberwachung



ABUS Security-Center GmbH & Co. KG
Linker Kreuthweg 5 · D-86444 Affing
Tel.: +49(0)8207/95990-0
Fax: +49(0)8207/95990-100
info.de@abus-sc.com · www.abus.com

ABUS Security-Center ist Hersteller innovativer Alarmanlagen, Videoüberwachungssysteme und Zutrittskontrollsysteme. Als Teil der ABUS Gruppe ist das Unternehmen sowohl auf branchenspezifische Sicherheitsbedürfnisse, als auch auf die Anforderungen von Privatanwendern spezialisiert.

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

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 EMEA B.V.
Herikerbergweg 292 · 1101CT Amsterdam
Netherlands
<https://i-pro.com/eu/en>
Hochwertige CCTV-Lösungen (IP & analog), Video-Automatisierung und KI, Technologien für hohe Ansprüche (FacePro, Personen-Maskierung), Schutz vor Cyber-Angriffen im Einklang mit DSGVO, VMS: Video Insight

Videoüberwachung



LivEye GmbH
Europa-Allee 56b
54343 Föhren

liveye.com

ZEIT ZUTRITT

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

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.assaabloentrance.de
Speedgates, Durchgangs- und Sicherheitsschleusen,
Drehkreuze, Schwenktüren, Sicherheits-Karussell-
türen und -Portale für die Sicherheits-Zutritts-
kontrolle und Personenvereinzelung.

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

 **DoorBird**
Technology meets Design.

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

Zeit + Zutritt

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

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

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

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

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.

Zeit + Zutritt

gantner **N**
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

phg
Die richtige Verbindung

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

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

salto **A**
INSPIRED ACCESS

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

Zeit + Zutritt

TKH **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

Zeit + Zutritt

**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



Fernwirk-Sicherheitssysteme
Oldenburg
FSO
Ihr Security-Provider

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.

BRAND SCHUTZ

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

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

Brandschutz



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

ARBEITS SICHERHEIT

GEFAHRSTOFF MANAGEMENT

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.

Arbeitssicherheit



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

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,
Sicherheitsschränke, Chemikalien- und Umluft-
schränke, Druckgasflaschenschränke, Gefahrstoffar-
beitsplätze, Absauganlagen, Raumluftreiniger uvm.

Brandschutz



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
Schlüsseldpots, Feuerwehr, Schlüsselmanager,
Feuerwehrperipherie, Feststellanlagen, Störmeldezentralen

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

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



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



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 Betriebs-
 ausstattung, Gefahrstoff-Leckage-Warnsystem

MASCHINEN ANLAGEN SICHERHEIT

Maschinen + Anlagen



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

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, Auffang-
 wannen, Bodenschutzsysteme, Gasflaschenlagerung,
 Gasflaschencontainer, Gasflaschenbox, Kleingebinderegale
 Unser Online-Shop: www.fladafi.de

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



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

GASMESS TECHNIK

Ihr Eintrag in der Rubrik



Schicken Sie einfach eine E-Mail
 an miryam.reubold@wiley.com

Wir beraten Sie gerne!

Maschinen + Anlagen



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

Gasesstechnik



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
 Gaswarttechnik, Sensoren, tragbare und
 stationäre Gasesstechnik

Maschinen + Anlagen



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

Jetzt

Newsletter abonnieren



Ihre
Nummer 1
seit mehr als
35 Jahren

inklusive
e-Ausgabe!



Nachrichten für
Entscheider und
Führungskräfte in
Sachen Sicherheit

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

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

SicherMacher

Der GIT-Talk mit den Marktführern



GIT SICHERHEIT

Kontakt:
Miryam.Reubold@Wiley.com

WILEY



atlas

FAST

SERIES



FAST 10 PLATINUM | ESD

EN ISO 20345 S1PS SR | Art. 77500



FAST 12 BLACK | ESD

EN ISO 20345 S1PS SR | Art. 28200



FAST 14 GREEN | ESD

EN ISO 20345 S1PS SR | Art. 83300



**ULTRA
LEICHT**



**EASY
SLIP-EINSTIEG**



**HEEL-BOX FÜR
PERFECTE
PASSFORM**



**OPTIMALE
LUFTZIRKULATION**



**ERGONOMISCHE
SCHAFTGESTALTUNG**