35. JAHRGANG | April 2026 | AUSGABE 4 | 17 €

GIT SICHERHEIT

30 926

MAGAZIN FÜR SAFETY UND SECURITY

Titelthema Seite 62:

Sieben Schritte zur reibungslosen Betriebsbegehung

Wie Anlagenbetreiber Sicherheitslücken systematisch schließen

Ausgabe ONLINE lesen:

HEFT IM HEFT

VIDEO | ZUTRITT ab S. 24

WILEY

Smart messen mit X-meas

Im Turnaround, während der Revision und im Tagesgeschäft: Mit X-meas effizient und präzise freimessen, automatisch dokumentieren und digital freigeben. Der smarte Messassistent koordiniert Aufgaben via App und speichert Messprotokolle sicher in der Cloudsoftware.

Dräger

Technik für das Leben

Zwischen Kamera, Karte und Kontrolle

Die aktuelle Ausgabe von GIT SICHERHEIT richtet den Blick zunächst auf das Heft im Heft „Video & Zutritt“ (ab Seite 24). Im Mittelpunkt steht das Zusammenspiel von Videoüberwachung, Zutrittsorganisation und Kontrolle – also genau jene Schnittstellen, an denen moderne Sicherheitskonzepte heute ansetzen müssen. Die Beiträge zeigen, wie sich beide Disziplinen technisch und organisatorisch verzahnen lassen und welche Rolle sie für Übersicht, Nachvollziehbarkeit und Handlungsfähigkeit spielen.

Wie praxisnah solche Konzepte überprüft werden können, verdeutlicht unser Beitrag „Testen zwischen Zaunlinien“ - gleichzeitig Auftakt einer neuen GIT-Serie (ab Seite 30). Anhand eines Testgeländes zeigen wir zusammen mit den Sachverständigen Markus Piendl und Hannes Dopler, wie Perimeter, Video und Inte grationslösungen unter realen Bedingungen bewertet werden.

Diese Perspektive führt unmittelbar zum Thema KRITIS. In den Beiträgen „Was Betreiber jetzt tun müssen“ (ab Seite 10) und „Keine Kritis ist eine Insel“ (ab Seite 8) wird deutlich, dass physische Sicherheit zunehmend Teil regulatorischer Anforderungen ist – und dass auch viele Unternehmen außerhalb klassischer KRITIS-Definitionen systemrelevant eingebunden sind.

Einen weiteren Praxisakzent setzt der Brandschutz. Mit dem angekündigten Test „Zwischen Norm und Praxis“, den GIT SICHERHEIT gemeinsam mit der EPS Vertriebs GmbH durchführt (ab Seite 54), rückt die Alltagstauglichkeit normkonformer Brandwarntechnik in den Fokus.

Im Bereich Maschinen und Anlagensicherheit verdichten sich viele dieser Fragestellungen. Hier ist auch das Titelthema dieser Ausgabe verortet: „Sieben Schritte zur reibungslosen Betriebsbegehung“ (ab Seite 62). Der Beitrag zeigt, wie Betreiber Sicherheitslücken systematisch erkennen und beheben können. Ergänzt wird der Schwerpunkt durch das Interview „Fit für neue Vorgaben“ (ab Seite 64) sowie den Innentitel „Euchner geht die letzten Meter der Automatisierung“ (ab Seite 60), der neue Ansätze sicherer Kommunikation in der Automatisierung beleuchtet.

Abgerundet wird das Heft durch die Rubrik Arbeitssicherheit. Der Innentitel „Sicherheit trifft Umweltbilanz“ (ab Seite 76) verbindet Schutzkleidung mit Nachhaltigkeit. Mit dem GIT Lesertest „Sicherheitsschuhe“ gemeinsam mit Atlas (ab Seite 78) lädt die Redaktion zudem zur aktiven Beteiligung ein.

Wir wünschen Ihnen eine erkenntnisreiche Lektüre.

Herzlichst,
Ihr

Dr. Timo Gimbel
für das Team GIT SICHERHEIT

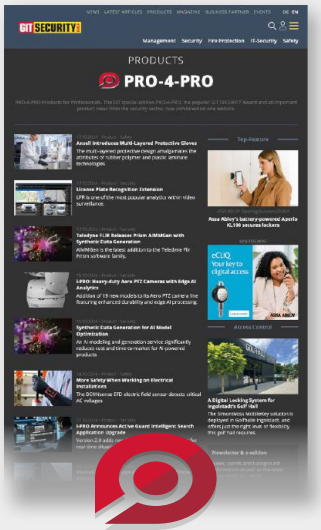
TITELTHEMA

Sieben Schritte zur reibungslosen Betriebsbegehung

Wie Anlagenbetreiber Sicherheitslücken systematisch schließen

ab Seite 62

PRO-4-PRO für 2025/2026



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

Sam Berlemann

Oliver Rolofs

Gerhard Harand

Thomas Jensen

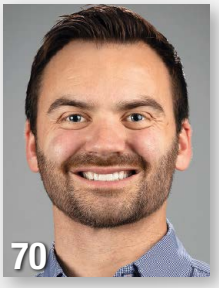
MANAGEMENT

SECURITY

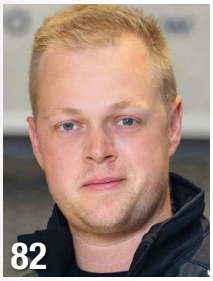
HEFT IM HEFT – VDEO I ZUTRITT

Joachim Mahlstedt

Matthias Bristle



Connor Doherty



Sven Traub

CYBER-SECURITY

PHYSISCHE SICHERHEIT

52 Wenn das rote Team für helle Aufregung sorgt
Fehlende Balance: „Fokus auf Cybersecurity verkennt physische Sicherheit“

BRANDSCHUTZ

TEST-REIHE

54 Zwischen Norm und Praxis
GIT SICHERHEIT und EPS Vertriebs GmbH untersuchen im Kundentest die Ajax Fire EN54 Brandwarnanlage

LITHIUM-IONEN-BATTERIEN

56 Von Fertigung bis Finishing
Risikobasierte Brandschutzstrategien in der Batterieproduktion

SAFETY

INNENTITEL MASCHINENSICHERHEIT

59 Euchner geht die letzten Meter der Automatisierung
IO-Link Safety: Sicherheit mit Daten

TITELTHEMA

62 Sieben Schritte zur reibungslosen Betriebsbegehung
Wie Anlagenbetreiber Sicherheitslücken systematisch schließen

64 Fit für neue Vorgaben
Wie Betreiber Bestandsmaschinen zukunftsfähig machen

EIGENSICHERE TABLETS UND SMARTPHONES

66 Deskless Worker im Kontext der Digitalisierung
Wie mobile Geräte und Augmented Reality die Arbeit von Deskless Workern in Industriebereichen verändern

INDUSTRIAL SECURITY

68 CRA: Mit der Ungewissheit umgehen
Wie Maschinenbauer ohne finale CRA-Vorgaben Risiken managen, Komponenten auswählen und OT Netzwerke absichern

DISTRIBUTION

70 First Call-Partner für Ingenieure und Integratoren
Im Gespräch mit Connor Doherty: Schnelle Teile, klare Daten, starke Systeme – wie DigiKey Automatisierung ganzheitlich und sicherheitsorientiert gestaltet

INNENTITEL ARBEITSSICHERHEIT

75 Sicherheit trifft Umweltbilanz
Wie Multinorm Green Sicherheit, Langlebigkeit und eine transparente Umweltbilanz verbindet

TEST-REIHE

78 Der GIT Lesertest: Sicherheitsschuhe
Atlas und GIT SICHERHEIT suchen Tester – Maximum Protection im harten Arbeitsalltag

ARBEITSSCHUTZ

80 Umweltschutz und Arbeitsschutz im Klimawandel
Herausforderungen und Lösungen in vier Punkten

SCHUTZKLEIDUNG

82 „Moderne PSA muss deutlich mehr können…“
Kübler-PSA-Experte Sven Traub erklärt, wie Schutz, Tragekomfort und Wirtschaftlichkeit in modernen PSA-Konzepten zusammenspielen

STÖRLICHTBOGENSCHUTZ

84 Praxisgerechter Störlichtbogenschutz im Arbeitsalltag
Effektiver Störlichtbogenschutz für Arbeiten an elektrischen Anlagen

EHS

86 Arbeitsschutz in Zeiten des Generationenwandels
Zielgruppengerechter Arbeitsschutz zwischen analogem Lernen und KI-gestützten Tools

88 Operation Risk
Wie Unternehmen Risikokompetenz neu denken

STÖRLICHTBOGENSCHUTZ

90 Klarer sehen und freier atmen
Die neue Störlichtbogenhaube von HB Protective für Schaltinstallateure sowie Netz- und Anlagentechniker

INDEX

QUICK-FINDER

ORGANISATIONEN, INSTITUTIONEN UND UNTERNEHMEN IM HEFT

NEWS

BDLS-Präsident Alexander Borgschulze wird 60 Jahre

© BDLS

Alexander Borgschulze

Der Bundesverband der Luftsicherheitsunternehmen (BDLS) gratuliert seinem Präsidenten Alexander Borgschulze anlässlich seines 60. Geburtstags am 13. Februar 2026. Alexander Borgschulze ist seit November 2023 Präsident des BDLS und vertritt die Interessen der deutschen Luftsicherheitsunternehmen gegenüber Politik, Behörden und Öffentlichkeit. Unter seiner Führung gestaltet der BDLS die Entwicklungen der Luftsicherheitsbranche aktiv – mit dem klaren Ziel, Sicherheit, Effizienz und internationale Kooperation im Luftverkehr zu stärken. „Mit seiner Vision, seiner Kompetenz und seinem unermüdlichen Einsatz für die Branche hat Alexander Borgschulze die Sicherheit im Luftverkehr und die Interessen der Mitglieder unseres Verbandes nachhaltig geprägt“, so die Geschäftsführerin des BDLS, Cornelia Okpara. **www.bdls.aero**

Hexagon: Octave startet neue Marke

© Hexagon

Matthias Stenberg, Chief Executive Officer von Octave

Octave, eine potenzielle Software-Ausgründung der Hexagon AB, stellt seine neue Markenidentität vor. Dies markiert einen großen Schritt hin zum Übergang zu einem eigenständigen Unternehmen. Bestehend aus der Hexagon Asset Lifecycle Intelligence Division sowie den Divisionen Safety, Infrastructure & Geospatial, zusammen mit den Einheiten Bricsys, ETQ und Projectmates steht die Marke Octave für eine klare Vision und Zielsetzung mit der Mission, Intelligenz großflächig freizusetzen. Die neue Marke vereint ein marktführendes Portfolio, das Komplexität entlang des gesamten Lebenszyklus auflöst und vereinfacht. Dies beginnt beim Design und Bau über den Betrieb bis zum Schutz von Menschen, Eigentum und Assets. „Octave existiert, damit Kunden fundierte Entscheidungen treffen, wenn die Komplexität hoch ist und viel auf dem Spiel steht“, erklärt Matthias Stenberg, Chief Executive Officer von Octave. **www.hexagon.com**

BVSW SecTec 2026: Technologie für die Sicherheit von morgen

Am 21. und 22. April 2026 lädt der Bayerische Verband für Sicherheit in der Wirtschaft zur BVSW SecTec ein. „Die digitalen Technologien entwickeln sich rasant und haben das Potenzial, Sicherheitssysteme zu verbessern. Gleichzeitig ist eine technologische und rechtliche Einordnung Voraussetzung für nachhaltige und rechtssichere Investitionsentscheidungen“, sagt Caroline Eder, Geschäftsführerin des BVSW. „Mit der BVSW SecTec bieten wir in diesem dynamischen Umfeld Orientierung und geben ein kompaktes und praxisorientiertes Update zu aktuellen Trends und marktrelevanten Entwicklungen.“

Ausgewählte Experten präsentieren in Fachvorträgen neue Technologien und erklären deren Relevanz für Unternehmen, KRITIS-Betreiber und Behörden. Thematisch spannt die BVSW SecTec 2026 einen weiten Bogen: Der Fachkongress beleuchtet den Einsatz von Drohnen bei KRITIS sowie die technischen Möglichkeiten und rechtlichen Grenzen zur Abwehr unbemannter Luftfahrtsysteme.

Außerdem erfahren die Teilnehmer, wie digitale Simulationen in unterschiedlichen Einsatzszenarien einen Beitrag zur Prävention von Gefahrenlagen leisten können. So lassen sich beispielsweise die Auswirkungen von Beschuss- oder Absprengszenarien am Computer nachstellen. Im öffentlichen Raum oder bei der Gebäudeplanung helfen Simulationen von Personenströmen, sicherheitskritische Engpässe zu ermitteln.

Künstliche Intelligenz entfaltet ihr Potenzial nicht nur in der Gefahrenprävention, sondern zunehmend auch im Personalwesen. Ein gemeinsamer Anwenderbericht eines Sicherheitsdienstleisters und eines KI-Anbieters wird zeigen, wie Künstliche Intelligenz schon heute beim High-Volume-Recruiting unterstützen kann. Für Sicherheitsdienstleister können solche Lösungen insbesondere bei der Vorbereitung von Großveranstaltungen oder bei temporären Auftragsspitzen zum Gamechanger werden.

© BVSW

Bei all den technischen Innovationen darf das Thema digitale Souveränität nicht fehlen: Prof. Dr. Gabi Dreo Rodosek von der Universität der Bundeswehr in München wird über die Schutzmöglichkeiten vor hybriden Angriffen im KI-Zeitalter referieren.

Neben dem hochwertigen Vortragsprogramm bietet die BVSW SecTec eine begleitende Fachausstellung. Hier haben die Teilnehmer die Gelegenheit, Produkte und Lösungen kennenzulernen und mit den Ausstellern und Entwicklern ins Gespräch zu kommen. Die limitierte Anzahl an Ausstellungsmöglichkeiten, die zwischen Catering- und Vortragsbereich platziert sind, fördert den interaktiven Charakter des Fachkongresses.

Darüber hinaus bietet die Veranstaltung im bewährten Lunch-to-Lunch-Format die Gelegenheit, sich zwischen den Vorträgen auszutauschen, neue Kontakte zu knüpfen und Kooperationen anzubahnen.

www.bvsw.de

NRW Sicherheitstag

24. Juni 2026

Unter der Schirmherrschaft des Ministers des Innern des Landes Nordrhein Westfalen Herbert Reul

Zwischen Geopolitik und Unternehmensrealität – Wirtschaftsschutz als Erfolgsfaktor

Anmeldungen sowie weitere Informationen zu Programm und Inhalten sind ab sofort unter obigem Link möglich.

DLR
Schutz terrestrischer Infrastrukturen

24. Juni 2026
Deutsches Zentrum für Luft- und Raumfahrt (DLR) in Köln-Wahn

ASW West

Allianz für Sicherheit in der Wirtschaft West e.V.
(ASW West e.V.)
info@aswwest.de
www.aswwest.de

KMU sind oft systemrelevant für Kritische Infrastrukturen – z.B. als Zulieferer, IT-Dienstleister, Wartungsbetrieb oder Spezialanbieter

KRITIS

Keine Kritis ist eine Insel

Kleine und mittlere Unternehmen sind nicht immer selbst Kritische Infrastrukturen – oft aber systemrelevant

Informationssicherheit, Cyber-Security, Resilienz; kaum ein mittelständisches Unternehmen bestreitet heute noch, dass diese Themen relevant sind. Firewalls wurden modernisiert, Backups eingerichtet, Zugänge eingeschränkt. Das Bewusstsein ist da. Und dennoch bleibt häufig das Gefühl: Wir tun etwas, aber wir wissen nicht genau, ob es reicht, ob es zusammenpasst oder ob wir im Ernstfall wirklich handlungsfähig wären. Dieses Spannungsfeld ist kein Versäumnis einzelner Unternehmen. Es ist eine strukturelle Herausforderung, mit der viele KMU konfrontiert sind. Ein Beitrag von Thomas Adenauer von VdS Cyber Security, einem Mitglied des Bundesverbands für den Schutz kritischer Infrastrukturen, BSKI.

Der Begriff „Kritische Infrastruktur“ wird häufig sehr eng verstanden: Energie, Wasser, Gesundheit, Verkehr. Was dabei leicht übersehen wird: Diese Infrastrukturen funktionieren nicht isoliert. Sie sind eingebettet in komplexe Liefer-, Dienstleistungs- und Wartungsketten. Viele kleine und mittlere Unternehmen sind Teil genau dieser Ketten: als Zulieferer, IT-Dienstleister, Wartungsbetriebe oder Spezialanbieter. Fällt ein solches Unternehmen aus, kann das Auswirkungen haben, die weit über den eigenen Betrieb hinausgehen. Nicht, weil es „kritisch“ im formalen Sinne ist, sondern weil Prozesse voneinander abhängen.

Die eigentliche Frage lautet daher nicht: Sind wir kritische Infrastruktur? Sie lautet vielmehr: Welche Rolle spielen wir in den Abläufen anderer und was passiert, wenn wir nicht liefern können?

Informationssicherheit: Mehr als Schutz vor Angriffen

In der öffentlichen Wahrnehmung wird Informationssicherheit oft auf Cyberangriffe reduziert, also auf Firewalls, Virenschutz und Angriffsabwehr. Das ist wichtig, greift aber zu kurz. Informationssicherheit bedeutet vor allem eines: Handlungsfähigkeit unter widrigen Umständen:

- Was passiert, wenn Schlüsselpersonen ausfallen?
- Wenn Kernprozesse ausfallen?
- Wenn Systeme zwar gesichert, aber Prozesse nicht dokumentiert sind?

Viele dieser Risiken haben wenig mit Cyberkriminalität zu tun, aber viel mit Organisation, Struktur und Klarheit.

Ein hilfreicher Vergleich ist der Flugverkehr: Dort wird nicht davon ausgegangen, dass niemals etwas passiert. Im Gegenteil. Es wird akzeptiert, dass Störungen eintreten können und genau deshalb gibt es Checklisten, definierte Rollen, Notfallverfahren und klare Abläufe. Sie sollen nicht etwa den Betrieb lähmen, sondern ihn auch unter Stress beherrschbar halten.

Managementsysteme als Ordnungsrahmen

Viele KMU investieren gezielt in Technik: neue Firewalls, neue Systeme, neue Tools. Das ist nachvollziehbar und oft sinnvoll. Problematisch wird es dort, wo diese Maßnahmen isoliert bleiben. Ohne übergreifende Struktur fehlt die Verbindung zwischen Technik, Organisation und Menschen. Dann bleibt unklar, welche Prozesse wirklich kritisch sind, wer im Ernstfall entscheidet, welche Prozesse priorisiert werden und wie Wissen dauerhaft verfügbar bleibt. Hier entsteht der Mehrwert eines Managementsystems.

Ein Informationssicherheitsmanagementsystem (ISMS) ist kein Selbstzweck und kein bürokratisches Konstrukt. Richtig verstanden ist es ein Werkzeug, um bestehende Maßnahmen sinnvoll zu bündeln, Lücken sichtbar zu machen und Verantwortlichkeiten klar zu regeln.

Ob ISO 27001, BSI-Grundschutz oder praxisorientierte Ansätze wie die VdS 10000er-Reihe: Entscheidend ist nicht das Regelwerk, sondern der Gedanke dahinter.

Ein ISMS übersetzt abstrakte Risiken in konkrete Fragen:

- Was ist für unseren Betrieb wirklich kritisch?
- Was müssen wir absichern, dokumentieren oder vorbereiten?
- Wie stellen wir sicher, dass wir auch im Ausnahmefall handlungsfähig bleiben?

Zertifizierungen können dabei helfen, den erreichten Stand nach außen nachvollziehbar zu machen. Der eigentliche Nutzen entsteht jedoch im Inneren: durch Klarheit, Struktur und regelmäßige Überprüfung.

Auditoren als Sparringspartner

Ein häufiges Missverständnis besteht darin, Audits als Kontrolle oder Bedrohung wahrzunehmen. In der Praxis ist ein externer Auditor vor allem eines: ein strukturierter Realitätsabgleich. Er bewertet nicht, ob ein Unternehmen „perfekt" ist, sondern ob es seine eigenen Risiken kennt, angemessen behandelt und nachvollziehbar steuert. Gerade für KMU kann dieser regelmäßige Blick von außen helfen, blinde Flecken zu erkennen und Prioritäten realistisch zu setzen ohne den laufenden Betrieb zu blockieren.

Organisationen wie der Bundesverband zum Schutz Kritischer Infrastrukturen (BSKI) und seine Mitglieder können hier eine vermittelnde Rolle einnehmen: durch Sensibilisierung, Austauschformate, praxisnahe Orientierung und den Zugang zu erprobten Vorgehensweisen. Nicht mit dem Anspruch, fertige Lösungen zu liefern, sondern um Unternehmen dabei zu unterstützen, ihren eigenen, passenden Weg zu finden.

> Ein häufiges Missverständnis besteht darin, Audits als Kontrolle oder Bedrohung wahrzunehmen.
>
> **Thomas Adenauer von VdS Cyber Security, einem Mitglied des Bundesverbands für den Schutz kritischer Infrastrukturen, BSKI**

Fazit

Die Frage ist nicht, ob KMU Informationssicherheit betreiben sollten. Diese Diskussion ist längst entschieden. Die entscheidende Frage lautet: Wie strukturiert und nachhaltig geschieht das? Wer Informationssicherheit als Managementaufgabe versteht, schafft die Grundlage für Resilienz, Vertrauen und langfristige Stabilität. Im eigenen Unternehmen und darüber hinaus in den Strukturen, von denen andere abhängen. GIT

Bundesverband zum Schutz Kritischer Infrastrukturen (BSKI)
www.bski.de

Kötter: Umsatzschwelle von dreiviertel Milliarde Euro übersprungen

Die Kötter Unternehmensgruppe hat im Geschäftsjahr 2025 ihre Leistungsstärke erneut nachhaltig unter Beweis gestellt. Der Umsatz stieg durch nahezu rein organisches Wachstum um 6,6 % auf 770 Millionen Euro, die Mitarbeiterzahl nahm auf 16.400 Beschäftigte zu (+ 2,5 %). Das Familienunternehmen stemmte sich damit weiter erfolgreich gegen die tiefste Wirtschaftskrise in der Geschichte der Bundesrepublik. Das gab die Dienstleistungsgruppe bekannt. Das Geschäftsjahr 2025 unterstrich die Verlässlichkeit als Innovationsmotor, Qualitätsgarant und Top-Player für 360-Grad-Lösungen, so Verwaltungsrat Friedrich P. Kötter. Diese Entwicklung sei kein Zufall. Im Gegenteil: Sie sei Ergebnis klarer strategischer Entscheidungen sowie hoher Einsatzbereitschaft der Mitarbeiter, denen sein besonderer Dank gilt. Gleichzeitig bedankte er sich bei den Kunden für die partnerschaftlichen Kooperationen und ihr Vertrauen in das Familienunternehmen.

www.koetter.de

© Berlemann Torbau GmbH

> „Viele Bestandsanlagen können wirtschaftlich sinnvoll aufgerüstet werden.

KRITIS

Was Betreiber jetzt tun müssen

Sam Berlemann erklärt, was jetzt zählt: Warum Freigeländesicherung für Betreiber zur Pflicht wird

Mit dem KRITIS-Dachgesetz hat die Bundesregierung einen zentralen Baustein zur Stärkung der physischen Sicherheit kritischer Infrastrukturen geschaffen. Die lang erwartete Regelung verpflichtet Betreiber nun, ihre Anlagen auch jenseits der IT gegen Angriffe zu schützen – ein Paradigmenwechsel, der die Sicherheitsbranche in Bewegung setzt. Was das konkret bedeutet, erklärt Sam Berlemann, Geschäftsführer der Berlemann Torbau GmbH.

Viele Betreiber wussten, dass ein Gesetz kommen würde – doch wie groß die Auswirkungen tatsächlich sind, zeigt sich erst jetzt. Für Sam Berlemann ist klar: „Es ist eine sehr gute Nachricht, dass die physische Resilienz endlich denselben Stellenwert bekommt wie die IT-Sicherheit." Der Schutz der Außenhaut, die sichere Organisation des Geländes und die robuste Auslegung von Anlagenkomponenten gelten ab sofort als unverzichtbare Elemente eines umfassenden Sicherheitskonzepts.

Physische Sicherheitslücken rücken in den Fokus

Ein Blick auf vergangene Ereignisse untermauert diese Notwendigkeit. Der Brandanschlag auf das Berliner Stromnetz hat eindrücklich gezeigt, wie anfällig kritische Prozesse sein können und welche Folgen ein physischer Angriff haben kann. „Der Handlungsbedarf war offensichtlich", so Berlemann. „Das KRITIS-Dachgesetz sorgt endlich für klare Prioritäten."

Zwischen Pflicht und Pragmatismus: Wo die Branche jetzt steht

Doch so klar die Richtung ist – das Gesetz lässt den Betreibern bewusst Spielraum. Es definiert keinen Katalog starrer Maßnahmen, sondern verpflichtet zu einer individuellen Risikoanalyse. Betreiber müssen sich nun drei zentrale Fragen stellen:

- Wo befinden sich die potenziellen Schwachstellen?
- Welche Bereiche der Anlage sind für den Betrieb besonders kritisch?
- Welche Angriffsszenarien sind wahrscheinlich – und mit welchen Folgen?

Berlemann betont: „Nicht jede Kläranlage muss wie ein Hochsicherheitsgefängnis geschützt werden. Es geht darum, angemessen zu handeln." Der Weg zur physischen Sicherheit sei ein kontinuierlicher Prozess, kein einmaliges Projekt.

Perimeterschutz: Vom Zaun bis zur intelligenten Sensorik

Eine der stärksten Hebelwirkungen entfaltet gut geplanter Perimeterschutz. Berlemann Torbau hat dafür ein klar strukturiertes Programm entwickelt, das in verschiedene Sicherheitslevel gegliedert ist.

Level I umfasst robuste, engmaschige Sicherheitsstabgitter, die je nach Bedarf mit angespitzten Überständen ergänzt werden können. Höhere Level setzen auf abgewinkelte Stabgitter, spezielle Aufnahmen für Stachel- oder NATO-Draht und weitere mechanische Verstärkungen für den physischen Übersteigschutz.

Doch allein mit Mechanik ist es nicht getan. „Wird der Zaun überwunden, kann ein Angreifer sich oft lange unbemerkt

bewegen“, erklärt Berlemann. Deshalb plädiert er für integrierte Lösungen: Mechanische Barrieren kombiniert mit aktiver Sensorik zur Übersteig- und Durchbruchsdetektion. Diese erkennt Manipulationen in Echtzeit und alarmiert sofort.

Entwickelt werden die Sensorkomponenten von der Schwesterfirma PeriNet GmbH – abgestimmt auf die mechanischen Systeme, skalierbar und individuell anpassbar auf die spezifische Umgebung.

Zugänge als neuralgische Punkte

Der Zaun ist häufig im Fokus – ein weiterer kritischer Baustein der Freigeländesicherung sind jedoch auch Tore, Schranken, Durchfahrten: „Besonders schützenswerte Objekte haben häufig auch besondere Anforderungen an die Objektzugänge wie Schiebe-, Falt- und Drehflügeltore. Diese Anforderungen können sowohl mechanischer als auch steuerungstechnischer Art sein“, erläutert Sam Berlemann – und führt weiter aus: „Wir rechnen mit einem deutlichen Anstieg an Sonderlösungen.“ Betreiber erwarten nicht nur stabile Tore, sondern auch vernetzte Systeme, die sich nahtlos in bestehende Sicherheitsarchitekturen einfügen.

Gute Nachrichten: Vieles lässt sich nachrüsten

Ein häufig geäußerter Irrtum lautet, man müsse komplette Zaunanlagen austauschen, um KRITIS-konform zu werden. Berlemann widerspricht energisch: „Das stimmt so nicht. Viele Bestandsanlagen können wirtschaftlich sinnvoll aufgerüstet werden.“

Dazu zählen beispielsweise:

- Erhöhung oder Abwinkelung vorhandener Zäune
- Ergänzung um Stachel- oder NATO-Draht
- Nachrüstbare Zaun- und Wanddetektionssysteme – oft schon ab ca. 20 Euro pro Laufmeter

Die meisten Betreiber profitieren von pragmatischen, modularen Lösungen, die Sicherheit und Wirtschaftlichkeit zusammenbringen. „Unsere Erfahrung zeigt: Mit intelligenten Erweiterungen lassen sich Schutzwirkung und Resilienz erheblich steigern – ohne finanzielle Hürden, die Projekte ausbremsen würden.“

Fazit: Die Chance zur neuen Sicherheitskultur

Mit dem KRITIS-Dachgesetz beginnt für Betreiber eine Phase der Neuorientierung – nicht aus Pflicht, sondern aus strategischem Vorteil. Wer frühzeitig investiert, stärkt Betriebssicherheit, minimiert Risiken und erfüllt regulatorische Anforderungen lange vor dem Stichtag.

Und die Hersteller? Sie erleben eine Branche im Wandel. „Wir sehen ein wachsendes Bewusstsein für ganzheitliche Sicherheitskonzepte“, sagt Sam Berlemann. „Mechanik und Elektronik greifen heute ineinander. Genau diese Kombination wird künftig entscheiden, wie resilient kritische Infrastrukturen wirklich sind.“ GIT

Weiterführende Infos zum Thema Sicherheitszäune

Berlemann Torbau GmbH
www.berlemann.de/

Kabel, Kabeljau und Sabotage

Seekabel als Unterwasserschauplatz hybrider Kriegsführung

Es sind kritische Infrastrukturen unter Wasser – und, wie Oliver Rolofs, Mitgründer der Munich Cyber Security Conference (MCSC) und Managing Partner der Münchner Strategieberatung Commvisory im Gespräch mit GIT SICHERHEIT sagt, eine der Achillesfersen der modernen Menschheit: Die durch sämtliche Weltmeere verlaufenden Seekabel sind Garant unserer digitalen Wirtschaft.

GIT SICHERHEIT: Herr Rolofs, die Cloud ist im Prinzip ein einziges Unterwasserkabel, so haben Sie es als „Fun fact" auf den Punkt gebracht. Wenn sie sabotiert werden, hört der Fun allerdings irgendwann auf. Geben Sie uns vielleicht als erstes einmal einen Überblick über Umfang und Verlauf dieses gewaltigen submarinen Kabelsalats?

Oliver Rolofs: Tatsächlich ist es so: Die sogenannte „Cloud" – also alles, was wir online speichern, streamen, verschicken oder abrufen – basiert in Wirklichkeit auf physischen Infrastrukturen, vor allem auf einem weltweiten Netz von rund 550 Unterseekabeln. Diese erstrecken sich über eine Gesamtlänge von mehr als 1,4 Millionen Kilometern mit wachsender Tendenz, da bis zu weitere 50 Seekabel in den nächsten Jahren verlegt werden sollen. Sie verbinden Kontinente, laufen zwischen den Datenzentren der Weltwirtschaft hin und her – und transportieren rund 98 Prozent des internationalen Datenverkehrs. Anders gesagt: Ohne diese Kabel wäre digitale Kommunikation, wie wir sie kennen, nicht möglich.

Neben dem internationalen Datenverkehr rasen ja auch noch Öl und Gas per Pipeline an den Fischen vorbei. Und weil der Bedarf steigt, nimmt auch der Verkehr durch Poseidons Herrschaftsgebiet immer noch weiter zu...?

Oliver Rolofs: Genau. Die See wird zunehmend ein Schauplatz kritischer Infrastrukturen – nicht nur für Daten, sondern auch für Energie. Untersee-Pipelines, Stromtrassen, Offshore-Windparks: Das alles konzentriert sich in maritimen Räumen, die oft schwer zu kontrollieren sind. Mit dem zunehmenden Datenvolumen steigt auch der Druck auf die bestehenden Kabel. Um das mal in Zahlen auszudrücken: Berechnungen zufolge wird das weltweite digitale Datenvolumen bis 2027 auf 284 Zettabyte, 2028 gar auf 394 Zettabyte steigen. Hohe Datenmengen und Rechenzentren erfordern ebenso einen hohen Energiebedarf und entsprechende Kapazitäten. Der Energieausblick der US-amerikanischen Energy Information Administration (EIA) prognostiziert einen Anstieg des weltweiten Energieverbrauchs um 34 % bis 2050. Für den Transport von Strom aus erneuerbaren Energien werden ebenso mehr Kapazitäten und Unterwasserinfrastrukturen benötigt. Damit steigt überall die Verwundbarkeit kritischer Unterwasserinfrastrukturen und es wächst die Gefahr gezielter Angriffe oder

Sabotageakte – sei es aus politischen, wirtschaftlichen oder strategischen Motiven. Um Energienetze unter Wasser mache ich mir derzeit die größten Sorgen, vor allem in der Ostsee.

Betreiber sind Staaten, aber zunehmend auch Unternehmen – sprich vor allem Google, Meta und Co.?

Oliver Rolofs: Richtig. In den letzten Jahren haben große Tech-Konzerne wie Google, Meta, Microsoft und Amazon massiv in eigene Seekabel investiert. Das hat einerseits ökonomische Gründe: Wer die Infrastruktur besitzt, spart langfristig und sichert sich Kontrolle. Andererseits bringt es neue sicherheitspolitische Fragen mit sich. Denn diese privatwirtschaftlichen Akteure bauen eine Art „digitale Parallelwelt" auf, mit eigener Infrastruktur – oft jenseits staatlicher Kontrolle, was unserem Verständnis digitaler Souveränität zuwiderläuft.

Dann lassen Sie uns kurz mal virtuell die Büroklamotten gegen Taucheranzüge tauschen und zum Meeresboden runterpaddeln: Wie sieht das da eigentlich aus? Wie sind diese Kabel aufgebaut und wie robust sind sie?

Oliver Rolofs: Man darf sich diese Kabel nicht als fragile Glasfaser vorstellen, sondern eher wie armdicke Hightech-Schläuche. Sie bestehen aus mehreren Schichten Schutzmaterial, darunter Kupfer, Polyethylen, Stahl und Isolierung – im Inneren verläuft ein dünner Glasfaserkern. In flachen Gewässern sind sie mitunter vergraben, in der Tiefsee liegen sie einfach auf dem Boden. Und obwohl sie sehr robust wirken, können sie doch relativ leicht beschädigt werden – durch Anker, Fischerei oder gezielte Sabotage.

Wenn wir von Angriffen sprechen, dann geht es um zwei Dinge: Das Abhören durch Geheimdienste, wie es beispielsweise durch Edward Snowden einem großen Publikum bekannt wurde, bis hin zu physisch-zerstörerischen Sabotageakten. Können Sie einmal einen Überblick zur Lage geben?

Oliver Rolofs: Wir erinnern uns an den Besuch von Chinas Präsident Xi in Moskau im März 2023, bei dem er zu seinem Gastgeber Putin sagte: „In diesem Moment gibt es Veränderungen, wie wir sie seit 100 Jahren nicht mehr gesehen haben. Und wir sind es, die diese Veränderungen gemeinsam vorantreiben". Das beschreibt sehr gut die aktuelle Bedrohungslage. Europa bekommt diese Veränderungen immer stärker zu spüren. Ob die Beschädigung des Stromkabels EastLink 2 zwischen Finnland und Estland durch den russischen Tanker Eagle S, das beschädigte Datenkabel zwischen Schweden und Lettland oder der im Februar 2025 gemeldete Kabelbruch in Schweden, der das C-Lion1 betraf: Unterwasserkabel werden immer mehr zum Ziel feindlicher Akteure - als Teil hybrider Angriffe auf westliche Infrastrukturen.

Die Bedrohung für Unterseekabel kommt heute neben natürlichen Ursachen aus zwei Richtungen: Spionage und Sabotage. Das gezielte Abhören solcher Leitungen ist seit Jahrzehnten gängige Praxis großer Geheimdienste – man denke an die US-Operation Ivy Bells im Kalten Krieg oder die Enthüllungen von Edward Snowden. Dabei werden Kabel mithilfe spezieller U-Boote gezielt angezapft, um Kommunikationsdaten auszulesen – eine Praxis, die nicht nur von Russland oder China, sondern auch von westlichen Staaten betrieben wurde und wird.

Noch bedenklicher ist aber die physische Sabotage. Zwar können Schäden auch durch Naturereignisse wie Erdbeben oder starke Stürme entstehen – wie etwa beim Ausbruch des Unterwasservulkans bei Tonga 2022 oder während des Supersturms Sandy 2012 –, doch immer häufiger rücken gezielte Angriffe in den Vordergrund. Militärische Spezialeinheiten, etwa Kampftaucher, sind in der Lage, bis zu einer Tiefe von rund 50 Metern kritische Infrastrukturen wie Kabel oder Pipelines zu zerstören. In größeren Tiefen können ferngesteuerte Unterwasserroboter oder Unterwasserdohnen eine solche Operation zunehmend übernehmen.

Der Krieg um Seekabel ist also schon lange im Gange?

Oliver Rolofs: In der Tat. Solche Operationen haben eine lange Geschichte: Bereits 1898 kappte ein US-Kriegsschiff ein Seekabel zwischen den Philippinen und dem asiatischen Festland – und legte so die Kommunikationsinfrastruktur des Gegners lahm. Auch heute sind vergleichbare Szenarien keine Theorie mehr: In der Ostsee häufen sich seit Beginn des russischen Angriffskriegs gegen die Ukraine auffällige Zwischenfälle – beschädigte Strom- und Datenkabel, verdächtige Schiffsrouten mit bewussten Ankerwürfen, wo es eigentlich keinen Sinn macht und laufende Sabotageermittlungen. Beobachter wie das Europäische Zentrum zur Abwehr hybrider Bedrohungen sehen darin gezielte Nadelstiche, mit denen Akteure wie Russland nicht nur die Verwundbarkeit westlicher Infrastrukturen testen, sondern auch unsere Reaktionsfähigkeit ausloten. Die Lage ist ernst – Unterwasserkabel sind längst nicht mehr nur technologische Rückgrate der globalen Kommunikation, sondern geopolitische Zielscheiben.

Dabei ist es ja kein wirkliches Geheimnis, wie hier jeweils (Wal-)Ross und (Wellen-)Reiter dieser Angriffe heißen: Abgesehen von abhörenden amerikanischen Geheimdiensten sind das die Russen und Chinesen?

Bitte umblättern ▶

© Oliver Rolofs

Oliver Rolofs, Founder & Managing Partner, Executive Board Advisory, Commvisory

Oliver Rolofs: Richtig. Russland beispielsweise verfügt über spezielle U-Boote, die dafür ausgelegt sind, Kabel zu orten und zu manipulieren. Auch China investiert massiv in maritime Spionagekapazitäten. Die USA machen es kaum anders. Das Spielfeld ist groß, die Akteure sind zahlreich – und der Meeresboden ist ein ziemlich unregulierter Raum. All das macht ihn zum geopolitischen Brennpunkt des 21. Jahrhunderts, auf dem Europa als hilfloses und verwundbares Treibgut erscheint. Es zeigt schonungslos auf: Uns Europäern und europäischen NATO-Partnern fällt es schwer, auf hybride Angriffe zu reagieren. Denn wir haben verlernt, wie man einem Aggressor hart und entschlossen gegenübertritt und ihn abschreckt.

Für die Zukunft stehen die Zeichen also eher auf Tsunami als auf Stiller Ozean?

Oliver Rolofs: Leider ja. Die Bedrohungslage wird sich weiter verschärfen, vor allem was die aktuellen russischen hybriden Operationen gegen uns angeht. Mit kleinen Nadelstichen wie die Angriffe auf Seekabel und Energienetze auf dem Meeresboden kann Russland seine Fähigkeit testen, unsere Infrastruktur zu zerstören – und unsere Reaktion darauf. Mit dem Ziel, später einen größeren Angriff zu starten, der unsere Entscheidungsfähigkeit beeinträchtigt. Und da machen mir zum einen die Sicherheit der strategisch wichtigen Datenkabel im Nordatlantik und Stromkabel in Nord- und Ostsee Sorgen. Auch Taiwan ist in dieser Situation einer besonderen Bedrohung durch China ausgesetzt. Künftige Konflikte – sei es um Daten, Macht oder Rohstoffe – werden gerade bei massiv steigendem Datenvolumen und globalen Energiebedarf auch unter Wasser ausgetragen.

Gleichzeitig nimmt unsere Abhängigkeit von diesen Infrastrukturen weiter zu, während Staaten durch einen zunehmend privatisierten Seekabelmarkt in diesem Bereich kaum noch ihre Hoheitsrechte wahrnehmen können, sprich gar keine Kontrolle mehr auf diese privaten Betreiber haben. Cyberattacken reichen nicht mehr aus – wer heute gezielt destabilisieren will, greift auch physisch an. Und Seekabel sind da in unsicheren Zeiten wie diesen ein äußerst verwundbares Ziel, um weitere Unruhe zu schaffen.

Was kann man alles tun? Welche Lösungen gibt es?

Oliver Rolofs: Der Schutz von Seekabeln und Unterwasserinfrastrukturen erfordert ein umfassendes Maßnahmenpaket aus Politik, Technik und Kooperation mit dem Ziel der Abschreckung und Resilienz. Zentrale Grundlage ist der Aufbau von Redundanzen und resilienten Netzen, etwa durch zusätzliche Kabelrouten und geografisch kluge Verlegungen abseits geopolitisch sensibler Zonen. Bereits bei der Planung und Verlegung müssen Sicherheitsaspekte wie geschützte Anlandestationen und Schutzkonzepte integriert werden.

Zudem braucht es eine Reform öffentlicher Ausschreibungen: Der Betrieb oder die Arbeit an Kritischen Infrastrukturen darf nicht länger nach dem reinen Bestbieterprinzip vergeben werden, sondern muss europäischen oder NATO-kompatiblen Anbietern vorbehalten sein. Parallel dazu sollte die technische Überwachung massiv ausgebaut werden – mit Sensoren, Satelliten, Sonarsystemen und KI-gestützter Lagebilderstellung, etwa durch die Vernetzung von AIS, Radar und Marinedaten (z. B. im CISE-System). Schließlich gehört der Schutz der Unterwasserinfrastruktur in die Sicherheitsstrategien der NATO und EU – unterstützt durch militärische Präsenzmaßnahmen wie Drohnen, unbemannte Überwachungsfahrzeuge oder die NATO-Operation „Baltic Sentry".

Die Nato erprobt auch neue technischen Lösungen, etwa die Software Mainsail, die Leitungsstörungen erkennen und verorten soll. Sie testet auch Unterwasserdrohnen, so genannte „Seekatzen." Eine davon liegt in Bremerhaven beim Zentrum für die Sicherheit Maritimer Infrastrukturen der Deutschen Luft- und Raumfahrt (DLR). Gleichzeitig muss das institutionelle Mandat auf EU-Ebene erweitert werden, damit Agenturen wie EMSA oder Frontex auch für Unterwasserlagen zuständig sind. Europa sollte zudem seine industrielle Souveränität zurückgewinnen und die eigene Produktion sowie Verlegung von Seekabeln wieder stärken.

Braucht es nicht auch noch viel mehr internationale Kooperation?

Oliver Rolofs: In einer Welt von Putin, Trump, Xi und Co. ist das gerade schwierig. Aber keine Frage. Wir brauchen hier auch ergänzend neue völkerrechtliche Initiativen wie klar definierte Schutzzonen und Sabotageverbote sowie durch diplomatische Abschreckung gegenüber feindlichen Akteuren – eine Art neue „Kabeldiplomatie". Das schließt auch eine völkerrechtlich sinnvolle Fortführung des Kabelschutzabkommens aus dem Jahr 1884 mit ein; das braucht dringend ein Update! Nur durch diese Kombination aus Resilienz, Regulierung, Technologie und internationalem Schulterschluss lässt sich die Achillesferse der globalen Konnektivität wirksam schützen.

Das wird wieder mal teuer für alle Beteiligten?

Oliver Rolofs: Natürlich. Sicherheit gibt es nicht zum Nulltarif und dass die Bundesregierung und NATO auf fünf Prozent des BIPs für Verteidigungsausgaben gehen, ist nicht nur richtig, sondern angesichts der aktuellen Sicherheitslage dringend notwendig. Aber sie nicht zu haben, kommt uns im Ernstfall deutlich teurer zu stehen. Der Ausfall eines einzigen Kabels kann Milliardenschäden verursachen, etwa wenn es an den Börsenhandel angeschlossen ist.

Und es braucht noch mehr, nämlich hohe Investitionen in unsere eigene europäische technologische Souveränität. Europas Ferien von der Geschichte sind leider vorbei. Umso wichtiger ist es, jetzt zu investieren, bevor der Ernstfall eintritt. Wir dürfen nicht erst handeln, wenn es schon zu spät ist.

Wirtschaftlich spielen die erwähnten „Magnificent Seven" wie Google, Apple, Meta und Amazon die Hauptrollen. Sorgen sie auch für den Schutz ihrer Kabel?

Oliver Rolofs: Teilweise ja. Diese Unternehmen sichern ihre Kabeltrassen, bauen redundante Systeme ein, arbeiten mit privaten Sicherheitsdiensten. Aber das reicht nicht aus. Der Schutz kritischer Infrastruktur darf nicht allein den Marktmechanismen überlassen werden. Es braucht staatliche Rahmenbedingungen, klare Vorgaben – und am besten internationale Kooperation.

Wo stehen die Europäer in diesem Spiel – und was muss noch geschehen?

Oliver Rolofs: Europa hinkt deutlich hinterher. Weder bei der Infrastruktur selbst noch bei deren Schutz ist man gut aufgestellt. Wir brauchen mehr Eigenständigkeit – Stichwort digitale Souveränität –, mehr Investitionen in Überwachung und Verteidigung, und eine engere Verzahnung von Wirtschaft, Sicherheitsbehörden und Militär. Der Schutz der Seekabel ist keine technokratische Randfrage – er ist ein geopolitisches Kernanliegen. GIT

Commvisory
www.commvisory.de

Neue Perspektiven bei Video und Zutritt – BHE-Fachkongress

Beste Möglichkeiten, sich umfassend über die Chancen und Grenzen moderner Techniken zu informieren, bietet der BHE-Fachkongress „Videosicherheit/Zutrittssteuerung“, zu dem der BHE Bundesverband Sicherheitstechnik am 21./22. April 2026 nach Mainz einlädt.

Der Markt für Videosicherheit und Zutrittssteuerung entwickelt sich stetig weiter. Innovative Technologien und intelligente Systeme eröffnen neue Wege zur Bewältigung unterschiedlichster Sicherheitsrisiken. Besonders der Einsatz von Künstlicher Intelligenz schafft Perspektiven für zukunftsorientierte Sicherheitslösungen.

Im Mittelpunkt dieser etablierten Veranstaltung steht ein abwechslungsreiches Vortragsprogramm, bei dem renommierte Experten praxisnahe Einblicke in aktuelle Entwicklungen und erfolgreiche Projekte geben. Ein besonderes Highlight ist der Live-Hacking-Vortrag von Michael Topal und Yannis Knoll: Sie demonstrieren hautnah, welche Auswirkungen Cyberangriffe auf die Videosicherheit und Zutrittssteuerung haben können, und geben wertvolle Tipps zum Schutz vor digitalen Bedrohungen.

In einem Impulsvortrag zeigen Mirko Dohse und Monic Wölker, wie verschiedene Sicherheitssysteme beim Thema Einbruchsprävention in Industrie, Handel und KRITIS optimal zusammenspielen. Im Anschluss wird dieses Thema in einer Podiumsdiskussion, moderiert von GIT SICHERHEIT, aus unterschiedlichen Blickwinkeln weiter beleuchtet.

Wie der Einsatz von KI die Videosicherheit verändert, verdeutlichen Hardo Naumann und Luka Johnsen: Sie richten den Fokus auf aktuelle Trends, Praxisbeispiele und Anwendungsmöglichkeiten. Ergänzt wird das Programm durch eine Fachausstellung führender Anbieter. Der Kongress bietet somit das ideale Umfeld, um sich intensiv mit Experten über moderne Lösungen und Systeme auszutauschen.

Abgerundet wird das Programm durch einen Branchentreff am Abend des ersten Veranstaltungstags – eine Gelegenheit für wertvolle Kontakte und entspanntes Networking. Detaillierte Informationen erhalten Interessenten unter www.bhe.de/kongress-video-zutritt oder unter Tel.: 06386 9214–18. **www.bhe.de**

KRITIS-Tage 2026 – Informiert in die Zukunft

Die erfolgreiche Veranstaltungsreihe „KRITIS-Tage“ geht auch 2026 weiter und bietet Sicherheitsverantwortlichen, Beratern, Planern und Facherrichtern aktuelles Fachwissen rund um den Schutz kritischer Infrastrukturen und NIS-2-Einrichtungen. Die erste Veranstaltung findet am 14. April 2026 in Mainz statt, im Juni folgt ein weiteres Event in Frankreich. Die KRITIS-Tage 2026 thematisieren unter dem Motto „Informiert in die Zukunft: Sicherheit und Hochverfügbarkeit für kritische Infrastrukturen“ aktuelle Herausforderungen und Anforderungen aus Technik, Recht und Praxis. Experten informieren über den Stand gesetzlicher Vorgaben – wie etwa der NIS-2-Richtlinie und dem deutschen KRITIS-Dachgesetz – und geben praxisnahe Einblicke in Best Practices zur physischen und digitalen Sicherheit kritischer Infrastrukturen und von NIS-2-Einrichtungen. **www.dallmeier.com**

Klüh als Top Company ausgezeichnet

Das Düsseldorfer Familienunternehmen Klüh ist von der Arbeitgeber-Bewertungsplattform Kununu zum fünften Mal in Folge als Top Company ausgezeichnet worden. Das Arbeitgebersiegel würdigt Unternehmen, die durch besonders hohe Mitarbeiterzufriedenheit überzeugen. Grundlage der Auszeichnung bilden die unabhängigen Bewertungen der Mitarbeiter auf der Plattform. Das „Top Company“-Siegel sei ein starkes Signal an Talente, die nach ihrem idealen Arbeitgeber suchen. Es zeige: Klüh lebt eine Unternehmenskultur, in der Mitarbeiter wertgeschätzt werden und sich entwickeln können, so Nina Zimmermann, CEO von kununu. Ihre Zufriedenheit haben die Mitarbeiter von Klüh mit einer Empfehlungsrate von 74 % sowie einer Gesamtnote von 4,4 von 5 zum Ausdruck gebracht. Diese Note liegt deutlich über dem landesweiten Durchschnitt als auch über dem Durchschnitt der meisten Marktbegleiter und unterstreicht das anhaltende Engagement des Unternehmens für die Schaffung einer positiven Arbeitsumgebung. **www.klueh.de**

Auch zahlreiche Supermärkte müssen häufig Sicherheitslösungen den neuen Kritis-Regelungen anpassen

KRITISCHE INFRASTRUKTUREN

Reifeprüfung

Gesetzliche Kritis-Anforderungen sicher umsetzen

Mit der neuen RUN-Bewertung des BSI wird klar, was Kritis-Betreiber wirklich brauchen: zuverlässige Sicherheitslösungen – auch und besonders im Bereich der physischen Sicherheit. Telenot zeigt, wie Unternehmen mit zertifizierter Technik und klarer Struktur auf der sicheren Seite bleiben.

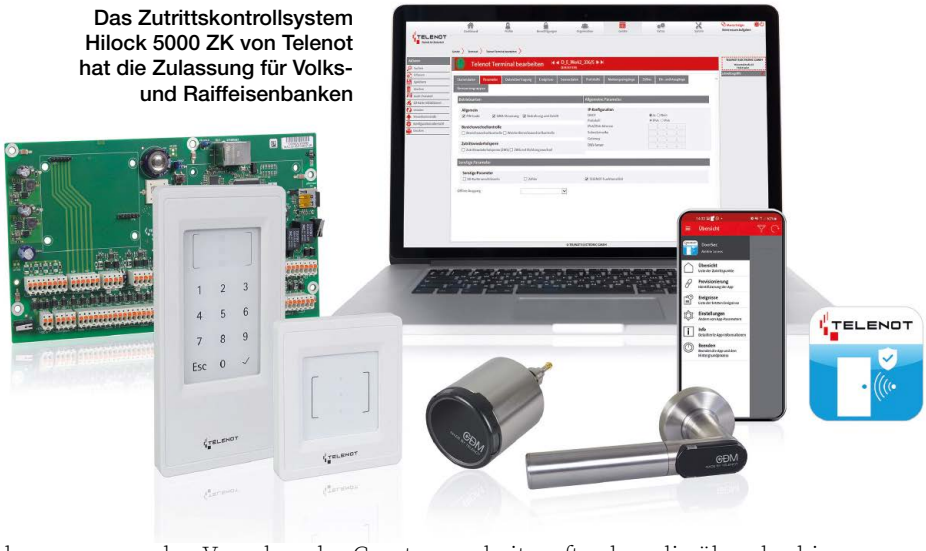
Was Unternehmen tun müssen, um die neuen Regularien des Kritis-Dachgesetzes zu erfüllen, liefert die Reife- und Umsetzungsgradbewertung (RUN) des Bundesamts für Sicherheit in der Informationstechnik (BSI). Mit diesem Dokument schafft das BSI mehr Transparenz für Betreiber Kritischer Infrastrukturen und vereinheitlicht die Nachweiserbringung gegenüber der Behörde. Hierzu hat das BSI die Anforderungen in sieben Hauptbereiche gegliedert, in denen jeweils bestimmte Kriterien erfüllt werden müssen.

Einer dieser Bereiche ist die physische Sicherheit. Betreiber Kritischer Infrastrukturen müssen unter anderem nachweisen, ob sie Maßnahmen zur Regelung und Kontrolle des Zugangs zu sensiblen Bereichen geplant oder bereits umgesetzt haben. Gleiches gilt für die Wartung physischer Sicherheitslösungen. So lässt sich bewerten, wie ausgereift und wirksam die physische Sicherheit eines Unternehmens ist – und wo eventuell nachgebessert werden muss, um gesetzeskonform zu bleiben und Strafzahlungen zu vermeiden.

Kritis-gemäße Sicherheitslösungen

Telenot aus dem süddeutschen Aalen verfügt als renommierter Hersteller elektronischer Sicherheitslösungen über langjährige Erfahrung in der Planung, Umsetzung und Betreuung von Sicherheitskonzepten für Unternehmen aus dem Kritis-Umfeld. Die Experten des Unternehmens wissen, welche Anforderungen eine elektronische Sicherheitslösung erfül-

Bereits in vielen Gebäuden im Einsatz, die unter die Regularien des Kritis-Dachgesetzes fallen: das Brandmeldesystem Hifire 4000 BMT



Das Zutrittskontrollsystem Hilock 5000 ZK von Telenot hat die Zulassung für Volks- und Raiffeisenbanken

len muss, um den Vorgaben des Gesetzes zu entsprechen. Zwar enthält das Kritis-Dachgesetz keine detaillierten technischen Spezifikationen – es nennt jedoch Beispiele, auf deren Basis sich konkrete Lösungen ableiten lassen. Hier setzt Telenot an.

So wurde beispielsweise die Verwaltungssoftware Compas Z 5500 als Bestandteil des Zutrittskontrollsystems Hilock 5000 ZK durch Atruvia, den Digitalisierungspartner der Volks- und Raiffeisenbanken, freigegeben. „Banken und Geldinstitute stellen verständlicherweise besonders hohe Anforderungen beim Thema Sicherheit – oft gehen die über das hinaus, was das Kritis-Dachgesetz vorgibt“, erklärt Telenot-Sicherheitsexperte Timm Schütz.

Auch Energieversorger setzen auf Sicherheitslösungen von Telenot. Das Brandmeldesystem Hifire 4000 BMT sowie die Gefahrenmelderzentrale hiplex 8400H erfüllen ebenfalls die Anforderungen des Gesetzes und noch mehr – inklusive aller zugehörigen Komponenten. Telenot zählt zu den wenigen Unternehmen der Branche, die sowohl Einzelbausteine als auch komplette Systeme auf ihre Zuverlässigkeit hin prüfen lassen.

Umsetzung in der Praxis

Wie Telenot bei der Planung einer Sicherheitslösung konkret vorgeht, erläutert Timm Schütz am Beispiel Einbruchschutz: „Zunächst klären wir gemeinsam mit dem Kunden, ob und inwieweit die jeweilige Einrichtung vom Gesetz betroffen ist. Anschließend ordnen wir das Objekt gemäß DIN VDE 0833-3 und der passenden VdS-Klasse ein. Danach begleiten wir den Kunden bei der Erstellung eines Sicherheitskonzepts und übernehmen die Musterplanung und die Umsetzung. Dazu gehört für uns auch die Erstellung eines Sicherheitshandbuchs.“

Dieses Handbuch dient nicht nur der gesetzlich geforderten Dokumentation, sondern ist ein zentrales Werkzeug für die Inbetriebnahme und Wartung durch Fachfirmen. „Darüber hinaus lassen sich die darin enthaltenen Daten auch als Grundlage für vergleichbare Sicherheitslösungen an weiteren Standorten nutzen“, ergänzt Schütz. GIT

Telenot
www.telenot.com

© Bilder: Telenot

VdS wird assoziiertes Mitglied im Branchenverband Euralarm

VdS Schadenverhütung ist neues assoziiertes Mitglied bei Euralarm. Der europäische Branchenverband vertritt die Interessen der Brand- und Sicherheitsbranche gegenüber Markt, Politik und Normung und bündelt Unternehmen, nationale Verbände und weitere Stakeholder aus ganz Europa. Gegründet 1970, repräsentiert Euralarm mehr als 5.000 Unternehmen der europäischen Brand- und Sicherheitswirtschaft. VdS wird sich künftig in allen vier Sektionen von Euralarm engagieren: Extinguishing, Fire, Security und Services. Mit der Mitgliedschaft baut VdS seine internationale Vernetzung weiter aus. Für das Unternehmen eröffnet die Zusammenarbeit zusätzliche Möglichkeiten, Entwicklungen in europäischen Märkten frühzeitig aufzugreifen, technische und regulatorische Themen auf europäischer Ebene enger zu begleiten und eigene Fachkompetenz in die Diskussion um Standards, Qualität und Zukunftsthemen der Sicherheitswirtschaft einzubringen. **www.vds.de**

VERBÄNDE

Manager Wirtschaftsschutz (IHK)

Qualifizierung für wirksamen Schutz vor Spionage, Extremismus und hybriden Bedrohungen

In Zeiten wachsender sicherheitspolitischer und gesellschaftlicher Unsicherheiten stehen Organisationen vor zunehmend komplexen Bedrohungen. Das Seminar vermittelt einen praxisorientierten Überblick über die Sicherheitsarchitektur der Bundesrepublik Deutschland und zeigt, wie sich daraus konkrete Schutzmaßnahmen für Organisationen ableiten lassen.

Teilnehmende lernen, Auswirkungen von Extremismus, Kriminalität sowie Wirtschafts- und Industriespionage zu erkennen und Risiken frühzeitig zu bewerten.

Ein besonderer Fokus liegt auf der realistischen Einschätzung hybrider Bedrohungen sowie der Entwicklung wirksamer, alltagstauglicher Sicherheitsstrategien. Zudem wird vermittelt, wie Wirtschaftsschutz systematisch in Organisationsstrukturen integriert und die Zusammenarbeit mit Sicherheitsbehörden effektiv gestaltet werden kann. Der VSW bietet gemeinsam mit der IHK für Rheinhessen die bundesweit einzigartige Möglichkeit, den IHK-Abschluss „Manager:in Wirtschaftsschutz“ zu erwerben.

Weitere Informationen finden Sie hier:

Verband für Sicherheit in der Wirtschaft Hessen - Rheinland-Pfalz - Saarland e.V.
www.vsw.de

… an Timo Keim, Leiter des Lehrgangs Manager Wirtschaftsschutz beim VSW Mainz

Herr Keim, für wen ist der Lehrgang gedacht?

Timo Keim: Der Lehrgang richtet sich an Mitarbeiter, Personalverantwortliche sowie Entscheider, die in folgenden Bereichen tätig sind: Unternehmenssicherheit / Corporate Security; Informationssicherheit; KRITIS-Organisationen sowie an Personen, die sich beruflich mit Prävention, Risikoanalyse, Spionageabwehr, Extremismusprävention oder organisatorischer Sicherheit befassen. Dabei eignet sich der Lehrgang sowohl für Berufserfahrene, die ihre Kompetenzen professionalisieren möchten, als auch für Einsteiger, die einen systematischen, IHK-zertifizierten Zugang zum Wirtschaftsschutz benötigen.

Was kann man dort lernen?

Timo Keim: Der Lehrgang „Koordinator Wirtschaftsschutz“ umfasst 54 Unterrichtseinheiten und vermittelt umfassendes, praxisnahes Wissen aus drei großen Themenbereichen:

1. Wirtschaftsschutz & Kriminalität
Die Teilnehmenden lernen u. a.: Aufbau und Funktionsweise der Sicherheitsorganisation in Deutschland; zentrale Dokumente, Konzepte und Netzwerke des Wirtschaftsschutzes; Grundlagen der organisatorischen und informationellen Sicherheit; Einschätzung und Bewertung von Extremismus, Terrorismus und organisierter Kriminalität.

2. Wirtschaftsschutz & Spionageabwehr
Die Teilnehmenden erwerben Wissen über: Formen, Methoden und Ziele der Wirtschafts- und Industriespionage; Akteure ausländischer Nachrichtendienste und hybride Bedrohungen, Spionageabwehr, inkl. Drohnenabwehr.

3. Anwendung & Praxisübungen
Mit realitätsnahen Trainings: Extremismus-, Spionage- und Cyberabwehr in Fallstudien; Awareness-Management und Sensibilisierung der Mitarbeiter; Stakeholder- und Netzwerkmanagement; Entwicklung konkreter Handlungsoptionen für interne und externe Sicherheitsprozesse.

Was kann man damit machen?

Timo Keim: Die Teilnehmer können nach Abschluss Bedrohungen wie Spionage, Extremismus, Kriminalität und Cyberangriffe einordnen, Wirtschaftsschutzkonzepte praxisnah anwenden und die Zusammenarbeit mit Sicherheitsbehörden gestalten.

Mit dem IHK-Zertifikat als Koordinator Wirtschaftsschutz können Absolventinnen und Absolventen als Sicherheitsverantwortliche oder Koordinatoren in Unternehmen arbeiten, Konzepte des Wirtschaftsschutzes eigenständig umsetzen, Sicherheitsrisiken professionell bewerten und präventive Maßnahmen entwickeln und in Sicherheitsabteilungen, Compliance, Risikomanagement oder KRITIS-Bereichen Verantwortung übernehmen.

Unternehmen profitieren durch Mitarbeiter, die in der Lage sind, Risiken durch Spionage, Extremismus, Kriminalität und Cyberangriffe frühzeitig zu erkennen, wirksame Schutzmaßnahmen umzusetzen, Sicherheitsstrukturen zu verbessern und Awareness-Programme aufzubauen sowie Behördenkontakte professionell zu managen. GIT

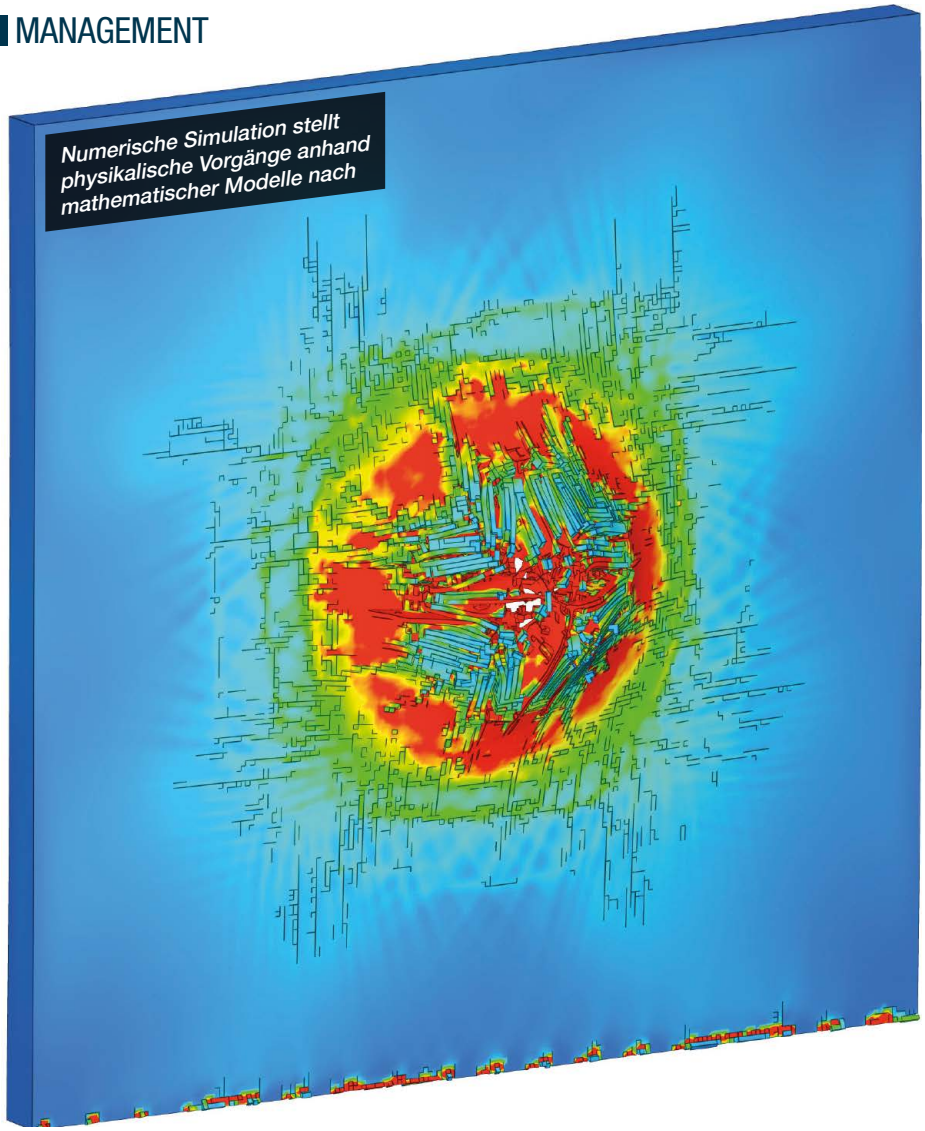
Primion hat an der Asis Europe 2026 teilgenommen

Primion, globaler Anbieter von Converged Security und Workforce Management -Lösungen, hat zum ersten Mal als Sponsor an der Asis Europe 2026 in Antwerpen teilgenommen und damit die Bedeutung von Converged Security als zukunftsweisendem Standard für die Unternehmenssicherheit in den Vordergrund gestellt. Primion CEO Francis Cepero hat zum Thema: „From Access Control to Workforce Advantage: Redesigning Security for the Human Era“ gesprochen. Mit seinem umfassenden Know-how unterstützt Primion Sicherheits- und Resilienz-Verantwortliche dabei, Risiken frühzeitig zu erkennen und wirksam zu steuern. Durch die nahtlose Verbindung von Identitätsmanagement, Zutrittskontrolle, OT-Security, Analytik und operativen Reaktionen entstehen aus zuvor getrennten Anwendungen ganzheitlich vernetzte Sicherheitsökosysteme und damit die Grundlage moderner Converged Security. **www.primion.eu**

Eudex bringt Politik, Militär und Industrie zusammen

Im September startet die Euro Defence Expo (Eudex) in der Messe Essen. Jetzt hat die neue internationale Fachmesse für die Sicherheits- und Verteidigungsindustrie ein starkes politisches Signal gesetzt. Beim Parlamentarischen Abend in der Deutschen Parlamentarischen Gesellschaft in Berlin kamen 120 hochrangige Vertreter aus Politik, Diplomatie, Militär, Verwaltung und Industrie zusammen, um zentrale Fragen der europäischen Sicherheitsarchitektur zu diskutieren. Vor dem Hintergrund der veränderten sicherheitspolitischen Lage in Europa knüpfte die Veranstaltung bewusst an die Debatte um die „Zeitenwende“ an und unterstrich den Anspruch der Euro Defence Expo, eine Plattform für strategischen Dialog und industrielle Innovationskraft zu schaffen und auch die zivil-militärische Zusammenarbeit zu fördern. **www.messe-essen.de**

© Messe Essen | Jens Ahner – www.jensahner.com



Numerische Simulation stellt physikalische Vorgänge anhand mathematischer Modelle nach

Der Fachkongress BVSW SecTec (21. und 22. April 2026) stellt technische Lösungen vor, die sich in der Sicherheitsbranche einsetzen lassen. Dieses Jahr steht unter anderem das Thema numerische Simulation von kurzzeitdynamischen Vorgängen auf der Agenda, etwa bei Beschuss, Anprall oder Ansprengungen. Referent ist Dr. Daniel Huber, Gründer von Simblast.

VERBÄNDE

Numerische Simulation

BVSW SecTec 2026 zeigt neue Möglichkeiten der Risikoanalyse

Wie verhält sich der Zufahrtsschutz an einem Stromwerk oder einem Mineralöllager, wenn ein Fahrzeug dagegen prallt? Sind Brücken, Flughäfen oder Rechenzentren im Ernstfall ausreichend geschützt? Fragen wie diese lassen sich mithilfe numerischer Simulation beantworten. Dabei handelt es sich um eine computerbasierte Berechnungsmethode, mit der sich komplexe physikalische Vorgänge durch mathematische Modelle nachstellen lassen.

Sicherheitsmaßnahmen überprüfen und optimieren

Computergestützte Simulationen eignen sich für die Überprüfung und Optimierung von Sicherheitsmaßnahmen. Deshalb präsentiert der BVSW das Thema auf seinem Fachkongress für Sicherheitstechnik, der BVSW SecTec.

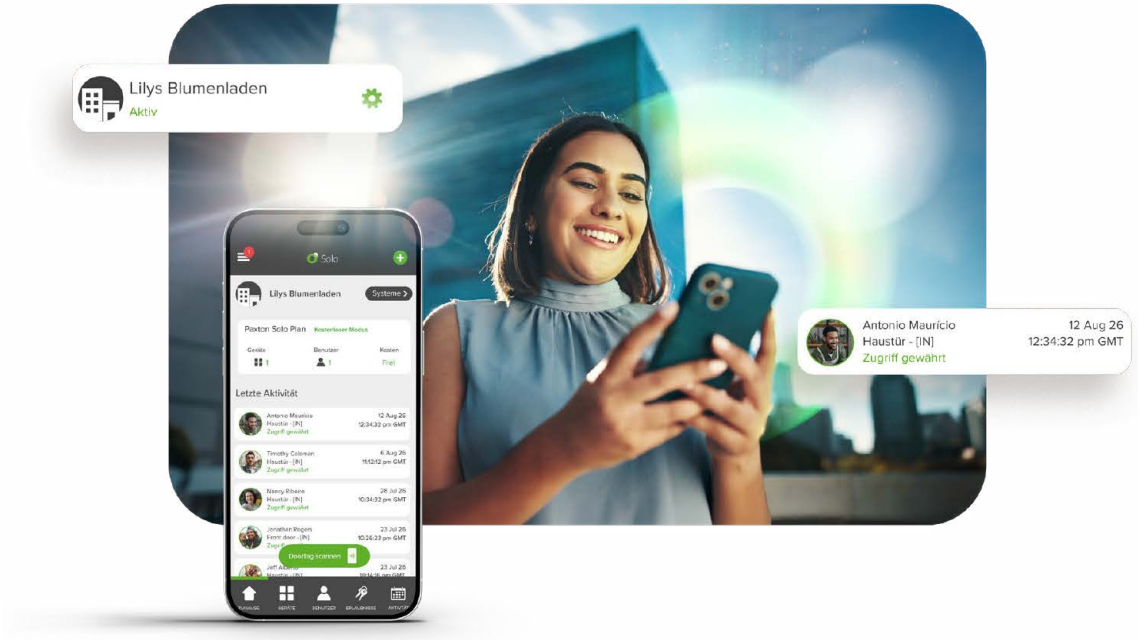
„Auf der BVSW SecTec wollen wir technische Lösungen vorstellen, die in der Sicherheitsbranche noch wenig bekannt sind, aber großes Potenzial für die Praxis bieten“, sagt BVSW-Geschäftsführerin Caroline Eder. „Die numerische Simulation gehört dazu. Wir freuen uns, für die diesjährige SecTec einen Experten gewonnen zu haben, der die Simulation kurzzeitdynamischer Vorgänge und ihre Bedeutung für die Sicherheitsbranche erklären wird.“

„Vor allem beim Zufahrts- und Gebäudeschutz gewinnt die numerische Simulation zunehmend an Bedeutung“, sagt Dr. Daniel Huber, Gründer und Inhaber der Firma Simblast. „Insbesondere Einrichtungen der kritischen Infrastrukturen müssen besser gegen Angriffe abgesichert werden, wobei eine nachträgliche Überprüfung der Wirksamkeit von Schutzmaßnahmen am bestehenden Objekt oft nicht möglich ist. Die numerische Simulation kann hier wertvolle Erkenntnisse liefern.“

So funktioniert numerische Simulation

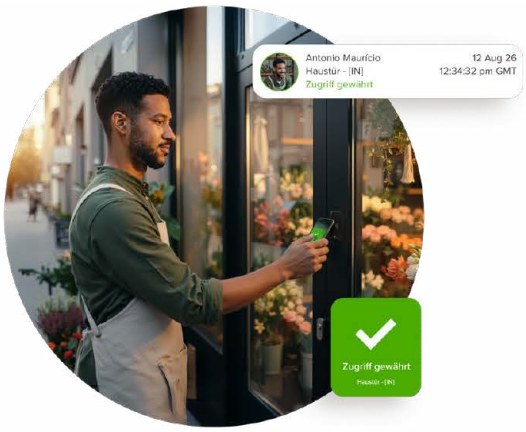
Jede numerische Simulation beginnt mit den vom Kunden bereitgestellten Geometriedaten. Dabei handelt es sich um digitale Beschreibungen eines Bauteils oder Systems, beispielsweise dem Aufbau eines Fensters, einer Sicherheitstür oder einer anderen Konstruktion. Die Geometriedaten bilden die Grundlage für das weitere Vorgehen.

Bitte umblättern ▶



Solo

Smartphone basiert, cloudgehostet.



Zutrittskontrolle. Neu gedacht.

Einfachheit von Standalone, Leistung eines vernetzten Systems

Ein echter Preis-Gamechanger

Nach höchsten Cybersicherheitsstandards entwickelt

Unbegrenzte Möglichkeiten

Besuchen Sie Paxton Live: Wir stellen Solo vor und sichern Sie sich Ihr **kostenloses Ein-Tür-Set.**

Paxton

Im nächsten Schritt, dem sogenannten Pre-Processing, erfolgt die Vernetzung der Geometrie. Das Modell wird dabei in sehr viele kleine Elemente zerlegt, oft anschaulich als kleine „Würfel“ bezeichnet. Gleichzeitig werden die Materialeigenschaften festgelegt, etwa, ob es sich um Glas, Kunststoff oder Metall handelt und wie sich diese Werkstoffe unter Belastung verhalten.

Darauf folgt die Definition der Randbedingungen. Dazu gehören die äußeren Einwirkungen, die untersucht werden sollen, wie Beschuss, Ansprengung oder andere mechanische Belastungen. Auch das umgebende Medium, etwa Luft, fließt in die Berechnung mit ein, da sich Druckwellen darüber ausbreiten, reflektiert werden und mit dem System wechselwirken.

Sobald Geometrie, Vernetzung, Werkstoffe und Randbedingungen feststehen, beginnt der Computer mit der Berechnung. Er analysiert dann Schritt für Schritt, was mit den einzelnen Elementen passiert. Wird einer dieser „Würfel“ stark belastet oder zerdrückt, berechnet der Computer, wie sich diese Veränderung auf die benachbarten Elemente auswirkt. Diese Schritte werden für jeden Zeitschritt über alle Elemente wiederholt, bis ein definiertes Abbruchkriterium erfüllt ist. Auf diese Weise lassen sich komplexe Prozesse, wie Verformungen, Rissbildung oder das Versagen ganzer Strukturen nachvollziehen.

Visualisierung unvorhergesehener Effekte

Die numerische Simulation kann bisweilen Unerwartetes sichtbar machen. Ein eindrucksvolles Beispiel dafür ist der sogenannte K-Effekt: Früher standen für die Entwicklung von Sonderschutzfahrzeugen keine numerischen Simulationen zur Verfügung. Die Wirksamkeit von Schutzmaterialien wurde deshalb experimentell überprüft. Dazu fanden klassische Beschussversuche statt: Ein Schutzblech wurde im Beschusskanal getestet, das Projektil traf die Platte und wurde wie erwartet zuverlässig gestoppt.

Sonderschutzfahrzeuge durchlaufen nach ihrer Entwicklung eine amtliche Zertifizierung, bei der das fertige Fahrzeug im Realversuch beschossen wird. Dabei zeigte sich in einigen Fällen ein überraschendes Ergebnis: Das zuvor im Beschusskanal positiv getestete Schutzblech wurde nun durchschossen, obwohl zusätzlich noch ein designgebende Karosserieblech davor lag. Das erscheint zunächst merkwürdig, wo doch noch mehr Material vorhanden ist.

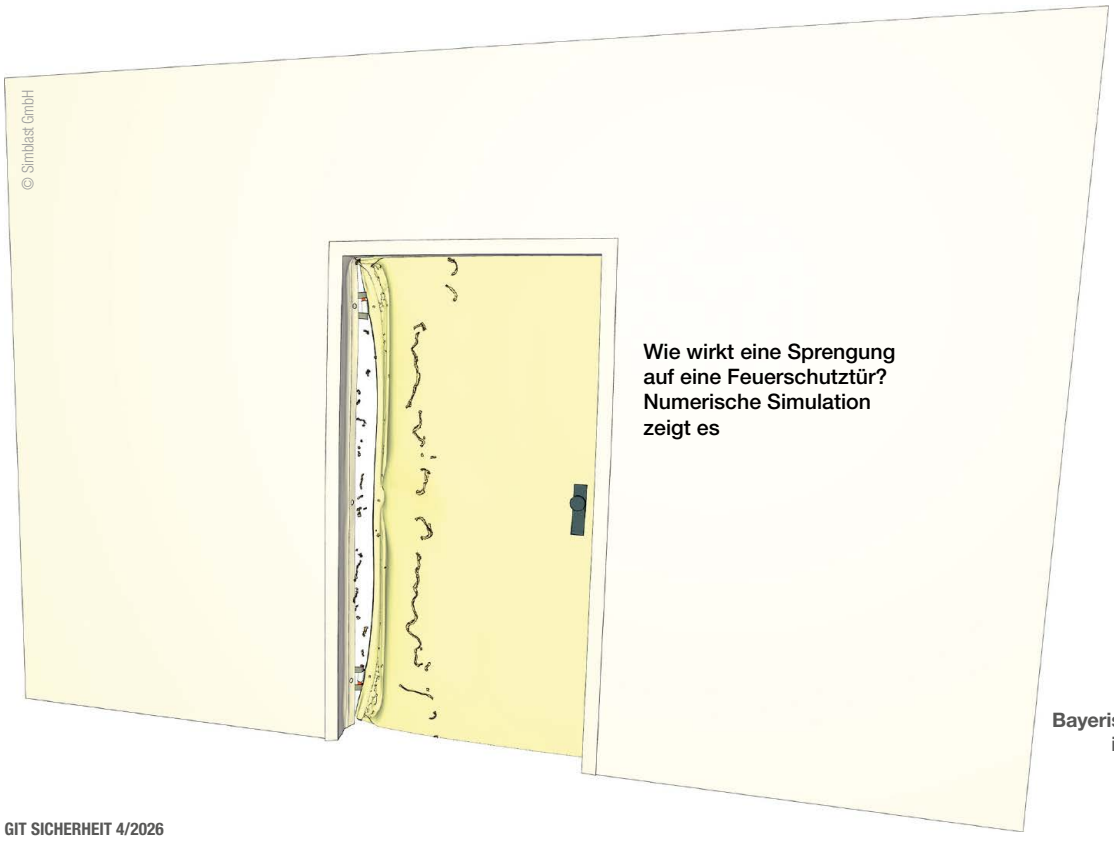
Die numerische Simulation liefert eine Erklärung dafür: Viele Projektile haben fertigungsbedingt einen kleinen Hohlraum in der Spitze. Trifft ein solches Projektil zuerst auf ein dünnes Blech, so wird dieser Hohlraum schlagartig zusammengedrückt oder die Spitze des Projektils direkt abgetragen. Dadurch verändert sich die Beschaffenheit des Projektils, insbesondere seine Querschnittsfläche, innerhalb kürzester Zeit. Diese Geometrieänderung im Projektil führt zu einem stanzähnlichen Wirken im nachgelagerten Schutzmaterial und verursacht kreisrunde Lochbilder. Das Versagen des Schutzmaterials erfolgt hierbei durch das sog. adiabate Scheren, bei dem Bereiche des Schutzblechs aufgeschmolzen werden.

Ohne numerische Simulation ist der K-Effekt kaum vorhersehbar, mit der numerischen Simulation aber lässt sich nachvollziehen, warum mehr Material zu weniger Schutz führt und wie konstruktive Gegenmaßnahmen im Einzelfall aussehen müssen.

Grenzen der numerischen Simulation

Obwohl sich die Rechenleistung permanent verbessert, ist sie es, die der numerischen Simulation momentan ein Limit setzt. Auch ab einer gewissen Größe der Modelle kommt numerische Simulation an ihre Grenzen. „Die Frage, wie sich beispielsweise ein Bewehrungsstahl im Fundament des Eiffelturms verhalten würde, wenn ganz oben eine Drohne mit der Spitze des Turms kollidiert, lässt sich schwer berechnen. Solche Szenarien würden riesige Modelle erfordern, bei denen die Struktur in sehr viele kleine Elemente zerlegt werden muss, um alle lokalen Effekte abzubilden. Selbst mit maximaler Rechenleistung würde eine vollständige Simulation solcher Größenordnungen zu lange dauern, um praktisch einsetzbar zu sein. Hier lassen sich aber sehr gute Ersatzmodelle finden und eine Aussage über die Kräfte im Fundament treffen“, erklärt Dr. Huber.

Auf der BVSW SecTec wird Dr. Huber am 21. April 2026 über die numerische Simulation der Schutzwirkung von KRITIS-Objekten referieren. Wer schon jetzt mehr über den Experten erfahren will, findet ein ausführliches Interview mit Dr. Huber auf der BVSW-Website. GIT



Wie wirkt eine Sprengung auf eine Feuerschutztür? Numerische Simulation zeigt es

Gerrit Fleischer wurde von Prosero Security zum Country Manager für Deutschland und die DACH-Region ernannt

Prosero ernennt Gerrit Fleischer zum Country Manager Deutschland

Prosero Security festigt die Präsenz in Deutschland mit der Ernennung eines Country Managers für den deutschen Markt. Damit unternimmt das Unternehmen einen bedeutenden Schritt in der langfristigen Strategie, sich als führender und bevorzugter Partner für Sicherheitstechnologie in Europa zu etablieren. Zur weiteren Verstärkung der deutschen Präsenz wurde Gerrit Fleischer zum Country Manager für Deutschland und die DACH-Region ernannt. In seiner Funktion wird Gerrit Fleischer eng mit den deutschen Standorten zusammenarbeiten und durch gemeinsame Initiativen, Cross-Selling und eine verstärkte Zusammenarbeit mit wichtigen Lieferanten den Erfolg von Prosero in Deutschland vorantreiben. Zentrale Aufgabe wird es sein, das weitere Wachstum und die Expansion des Unternehmens durch die Gewinnung starker Partner in der gesamten DACH-Region zu fördern.

www.prosero.com

Preisverleihung (v.l.n.r.) Markus Klein M&W Gruppe, Emma Wirth Pepperl+Fuchs, Patricia Reibert Pepperl+Fuchs, Victoria Klippel M&W Gruppe, Julian Lothring M&W Gruppe

Pepperl+Fuchs mit German Design Award ausgezeichnet

Das Messekonzept von Pepperl+Fuchs wurde während der „Ambiente“ in Frankfurt am Main mit dem German Design Award ausgezeichnet. Die „Winner“-Auszeichnung prämiert hervorragende Gestaltungsleistungen, die in ihrer jeweiligen Kategorie als wegweisend gelten. Entwickelt wurde das Messekonzept zusammen mit Saatchi & Saatchi und der M&W Gruppe, die als jahrzehntelanger Partner bei Messeauftritten die Umsetzung realisiert haben. Das Statement der Jury lautete wie folgt: „Modularität und Nachhaltigkeit werden bei ‚Pepperl+Fuchs – SPS 2022‘ konsequent als gestalterisches Prinzip interpretiert. Die Architektur überzeugt durch präzise Materialauswahl, flexible Systemkomponenten und ein wirkungsvolles Lichtkonzept. Die konsistente Wiederverwendbarkeit sämtlicher Elemente und die professionelle Reparaturstrategie markieren eine besonders relevante Antwort auf die Anforderungen zukunftsfähiger Messestände und zeichnen das Projekt als herausragend aus.“ **www.pepperl-fuchs.com**

ZUTRITT

Eine sichere Bank

Ratiodata stärkt physische Sicherheit mit moderner Schließtechnik

Für ihr neues Logistik- und Reparaturzentrum in Koblenz benötigte die Ratiodata SE eine moderne elektronische Schließlösung

Cyberangriffe gehören längst zu den größten Risiken für Banken und Finanzdienstleister. Die zunehmende Digitalisierung sensibler Prozesse, vernetzte Infrastrukturen und die veränderte geopolitische Lage sorgen dafür, dass das Thema Sicherheit heute ganzheitlich gedacht werden muss. Steigende regulatorische Anforderungen rücken daher neben IT-Systemen auch die physische Absicherung von Gebäuden, Rechenzentren und logistischen Knotenpunkten in den Fokus. Das schließt auch IT-Unternehmen ein, die Dienstleistungen für Banken erbringen. Hier setzt ein Projekt der Ratiodata SE an, die ihr neues Logistik- und Reparaturzentrum in Koblenz mit moderner Schließtechnik von Assa Abloy ausgerüstet hat.

Der IT-Dienstleister und Managed Service Provider entschied sich für eine eCliq-Schließanlage der Marke Ikon von Assa Abloy

Mit über 1.500 Mitarbeitern zählt die Ratiodata zu den führenden Systemhäusern und Dienstleistern für Bankentechnologie, SB-Infrastrukturen und Dokumentendigitalisierung in Deutschland. Als Partner zahlreicher Banken und Organisationen mit hohen regulatorischen Anforderungen betreibt das Unternehmen kritische Infrastrukturen, deren Schutz weit über klassische IT-Sicherheit hinausgeht. Um strategische Wachstumspotenziale zu realisieren, errichtete Ratiodata in Koblenz ein neues Logistik- und Reparaturzentrum in unmittelbarer Nähe zum bisherigen Standort in Mülheim-Kärlich. Das moderne Gebäude vereint erweiterte Reparaturkapazitäten, innovative Lager- und Fördertechnik, Büroflächen sowie ein Mitarbeiterkasino.

Operative Resilienz erfordert neue Sicherheitskonzepte

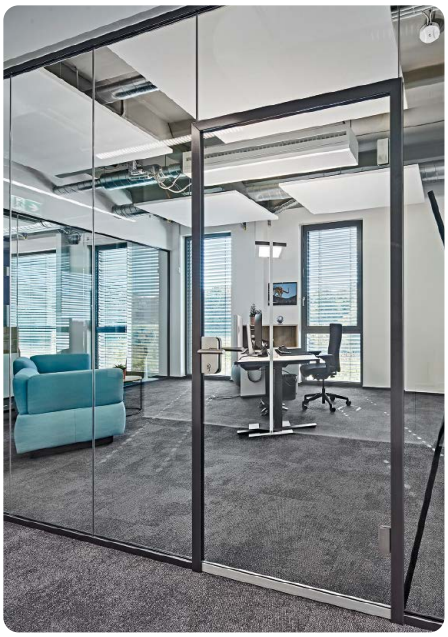
Mit dem Neubau stellte sich auch die Frage nach einem zeitgemäßen Zutrittskonzept. Die bisher eingesetzte mechanische Schließanlage sollte aus Sicherheits- und Flexibilitätsgründen durch eine elektronische Lösung ersetzt werden. Hintergrund ist nicht zuletzt die zunehmende Bedrohung durch Cyberangriffe auf die Finanzbranche, die auch regulatorisch adressiert wird. Mit der Richtlinie NIS2 (Network and Information Security Directive) und besonders der branchenspezifischen Verordnung DORA (Digital Operational Resilience Act) verlangt die Europäische Union von Finanzinstituten und deren Dienstleistern umfassende Maßnahmen zur operativen Widerstandsfähigkeit. Dazu zählt ausdrücklich auch die physische Sicherheit von Gebäuden und Rechenzentren als unterstützender Faktor für die IT-Sicherheit.

Von mechanischen zu elektronisch

Vor diesem Hintergrund entschied sich Ratiodata für das digitale Schließsystem eCliq der Marke Ikon von Assa Abloy. Mit der Planung, Beratung sowie der Lieferung und Installation wurde der erfahrene Assa Abloy-Partner Alfred Horn aus Neuwied beauftragt.

Äußerlich nicht von herkömmlichen Lösungen zu unterscheiden, ließen sich die elektronischen Schließzylinder ohne baulichen Aufwand und zusätzliche Verkabelung gegen die mechanischen Vorgänger tauschen

eCliq sichert nun den Zutritt vom Haupteingang ...



© Ratiodata SE

... bis zu einzelnen Büros

© Assa Abloy Sicherheitstechnik GmbH

Die große Typenvielfalt von eCkiq ermöglichte den flächendeckenden Einsatz im Außen- und Innenbereich des Betriebsgeländes

Zum Einsatz kamen rund 100 elektronische Schließzylinder und 100 programmierbare Schlüssel. Das rein elektronische System verfügt über eine AES-Verschlüsselung, ist nach den neuesten VdS- und DIN-Normen zertifiziert und bietet hohen Schutz gegen Manipulation und intelligente Angriffe. Durch seine kompakte Bauweise, ein robustes Design und langlebige Komponenten eignet sich eCliq zur Auslegung von Schließanlagen in jeder Größenordnung und in Objekten aller Art.

Flexile Lösung für komplexe Infrastrukturen

Da die Stromversorgung der Zylinder über eine leicht auszutauschende Standardbatterie im Schlüssel erfolgt, waren für den Wechsel keinerlei bauliche Maßnahmen oder zusätzliche Verkabelungen erforderlich. Damit empfiehlt sich das Schließsystem auch besonders für Versorgungs-, Industrie- und Infrastrukturunternehmen mit großflächigen Arealen und weitverzweigten Liegenschaften. Dank des umfangreichen Cliq-Typenprogramms, das einschließlich Schaltzylindern, Hangschlössern und Möbelolven über 60 Varianten umfasst, lassen sich die unterschiedlichsten Bereiche absichern – vom Einfahrtstor über Büros und Serverräume bis hin zum Aktenschrank.

Zutrittsrechte effizient und sicher verwalten

Entscheidend war für Ratiodata zudem, dass das System auch bei der Verwaltung von Zugangsberechtigungen mit hoher Flexibilität überzeugt. Nutzerspezifische Rollen und Rechte lassen sich schnell und präzise anpassen, zeitlich begrenzen oder bei Bedarf sofort entziehen. Verlorene Schlüssel können umgehend deaktiviert werden, ohne dass Zylinder ausgetauscht werden müssen. Die Steuerung erfolgt über den webbasierten Cliq-Web-Manager, der die dezentrale Verwaltung auch komplexer Zutrittsstrukturen ermöglicht und sich nahtlos in bestehende Prozesse integrieren lässt.

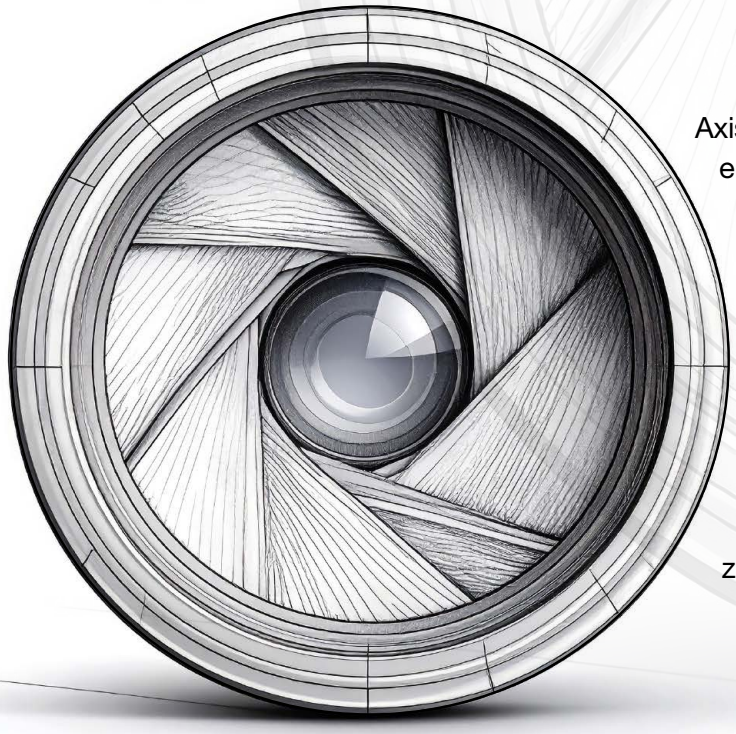
„Mit der eCliq-Schließanlage setzen wir auf ein System, das sehr hohe Sicherheitsstandards mit moderner, flexibler Verwaltung verbindet. Die Lösung passt perfekt zu unseren Anforderungen und unterstützt uns dabei, Zugangsberechtigungen effizient und zukunftssicher zu steuern“, bestätigt Michael Wagner, Ratiodata SE. GIT

Assa Abloy
www.assaabloy.com

VIDEO

Neue *Perspektiven*

Untersuchung zur Rolle intelligenter Videotechnologie



Axis Communications hat erstmals den nun jährlich erscheinenden „Axis Perspectives-Report“ veröffentlicht. Er basiert auf unternehmenseigenen, weltweiten Forschungsergebnissen, Expertenmeinungen und Anwendungsbeispielen aus der Praxis, und zeigt die Entwicklung intelligenter Videotechnologien und deren wachsende Bedeutung in verschiedenen Branchen auf. Er verdeutlicht zudem, welchen Beitrag intelligente Videotechnologien zur Verbesserung von Sicherheit, Schutz, betrieblicher Effizienz und Business Intelligence leisten.

Die Erkenntnisse aus dem Bericht weisen auf einen deutlichen Wandel hin: Obwohl für Unternehmen Sicherheit beim Einsatz von intelligenten Videotechnologien nach wie vor an erster Stelle steht, nutzen sie diese Technologien zunehmend auch als Business-Treiber zur Unterstützung ihrer Geschäftsprozesse. Videotechnologien fungieren dabei als intelligente Analysewerkzeuge, um sowohl betriebliche Abläufe zu optimieren als auch die strategische Unternehmensentwicklung voranzutreiben. Auf dieser Basis gewinnen Unternehmen wertvolle Informationen, mit denen sich Produktivität steigern, Kosten senken und Automatisierung in großem Maßstab realisieren lassen.

Strategischer Fahrplan

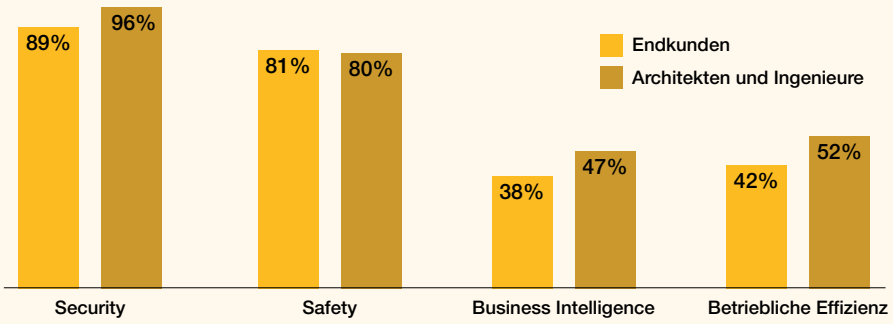
Der „Axis Perspectives-Report“ zeigt einen strategischen Fahrplan auf, wie Unternehmen Kameras aktiv in Entscheidungsprozesse integrieren und damit messbare Ergebnisse in kritischen Einsatzbereichen erzielen können. Wie dieser Mehrwert in der Praxis aussieht, wird über verschiedene Branchen hinweg deutlich: Im Einzelhandel reduzieren intelligente Videotechnologien zum Beispiel Inventurdifferenzen und unterstützen datenbasierte Entscheidungen zu Flächenplanung und Personaleinsatz. In Transport- und Logistikumgebungen erhöhen sie den Durchsatz, verbessern die Transparenz entlang der Lieferkette und minimieren Fehlerquellen. In der Industrie optimieren Kameras Maschinen- und Produktionsprozesse, erkennen frühzeitig Abweichungen und unterstützen Qualitätskontrollen ebenso wie Predictive Maintenance. Ein konkretes Beispiel liefert die BMW Group: Dort werden Kameras zur Unterstützung der KI-gesteuerten Qualitätsprüfung (AIQX) eingesetzt und ermöglichen so präzise, automatisierte Inspektionen zur Verbesserung der Produktqualität und betrieblichen Effizienz.

Wettbewerbsvorteile schaffen

Der Bericht bietet Unternehmen die Informationen, die sie benötigen, um integrierte, datengesteuerte Lösungen zu entwickeln, die konkrete Wettbewerbsvorteile schaffen. Um Unternehmen dabei zu unterstützen, stellt der Bericht zudem ein fünfstufiges Reifegradmodell für intelligente Videos vor,

Einsatzzwecke von Videoüberwachung

Inwieweit werden Videoüberwachungssysteme Ihrer Meinung nach zunehmend für die folgenden Zwecke eingesetzt? (Die Prozentangabe entspricht dem Anteil der Befragten, die „in hohem Maße“ und „in sehr hohem Maße“ geantwortet haben.)

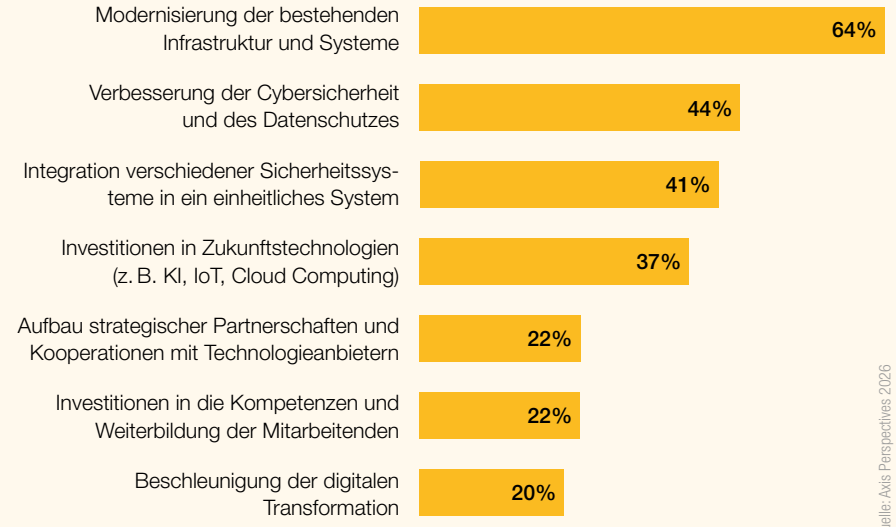


Quelle: Axis Perspectives 2026

Das Wichtigste auf einen Blick

- Mehr Einfluss auf das Gesamtgeschäft: Die Nutzung von intelligenten Videotechnologien für Business-Intelligence-Anwendungen, um beispielsweise Erkenntnisse über Kundenverhalten, Raumnutzung oder Performance zu gewinnen, hat sich in nur einem Jahr fast verdoppelt (von 20 auf 38 Prozent). 42 Prozent der befragten Unternehmen nutzen die Technologien mittlerweile aktiv zur Steigerung der betrieblichen Effizienz, um beispielsweise Arbeitsabläufe oder logistische Prozesse zu optimieren oder Ressourcen in Echtzeit zu verwalten (im Vergleich zu 38 Prozent 2024).
- Kundenprioritäten im Wandel: Die Modernisierung ihrer Infrastrukturen ist für 64 Prozent der befragten Endnutzer der wichtigste Treiber für die Nutzung von intelligenten Videotechnologien. Für 44 Prozent ist Cybersicherheit entscheidend.
- Schnellere Cloud-Implementierungen: Mit der zunehmenden Bedeutung neuer Anwendungsfälle wird die Cloud-Implementierung im Bereich physische Sicherheit voraussichtlich innerhalb der nächsten zwei Jahre von 27 auf 44 Prozent steigen – ein Anstieg von 17 Prozentpunkten.
- Zunehmende Nachfrage nach Plattform-Integration: 41 Prozent der Kunden verlangen mittlerweile einheitliche Plattformen. Dies unterstreicht noch einmal, wie wichtig Systemintegration als Erfolgsfaktor ist.

Welche Schlüsselbereiche erfordern in den nächsten 1–3 Jahren Ihre besondere Aufmerksamkeit, um in Ihrer Rolle erfolgreich zu sein?



Quelle: Axis Perspectives 2026

mit dem Unternehmen von passiven und reaktiven Systemen auf proaktive, prädiktive und letztendlich autonome Prozesse umsteigen können. Dieses Modell ermöglicht es Führungskräften, den aktuellen Reifegrad ihres Unternehmens zu bewerten und zeigt ihnen einen praxistauglichen Weg hin zu einer effektiveren Strategie für intelligente Videotechnologie auf.

„Aktuell beobachten wir, wie sich die Wahrnehmung von Videotechnologie in Unternehmen umfassend wandelt. Sie wird zunehmend als strategische Quelle für Daten, Erkenntnisse und Automatisierung im gesamten Unternehmen angesehen“, sagt Tobias Metsch, Regional Director Middle Europe bei Axis Communications. „Axis Communications verfügt über langjährige Erfahrung mit Innovationen im Bereich Netzwerk-Video – deshalb ist es aus unserer Sicht wichtig, die Entwicklung dieser Technologien und ihrer Anwendungsfälle strategisch zu betrachten“. GIT

Den vollständigen Report gibt es hier

Axis Communications
www.axis.com

Der Flughafen Paderborn/Lippstadt ist ein zentraler Arbeitgeber und regionaler Mobilitätspartner in der Region

VIDEO

Kameras am Start

Flughafen Paderborn/Lippstadt: Hybride Videoüberwachung für kritische Infrastruktur

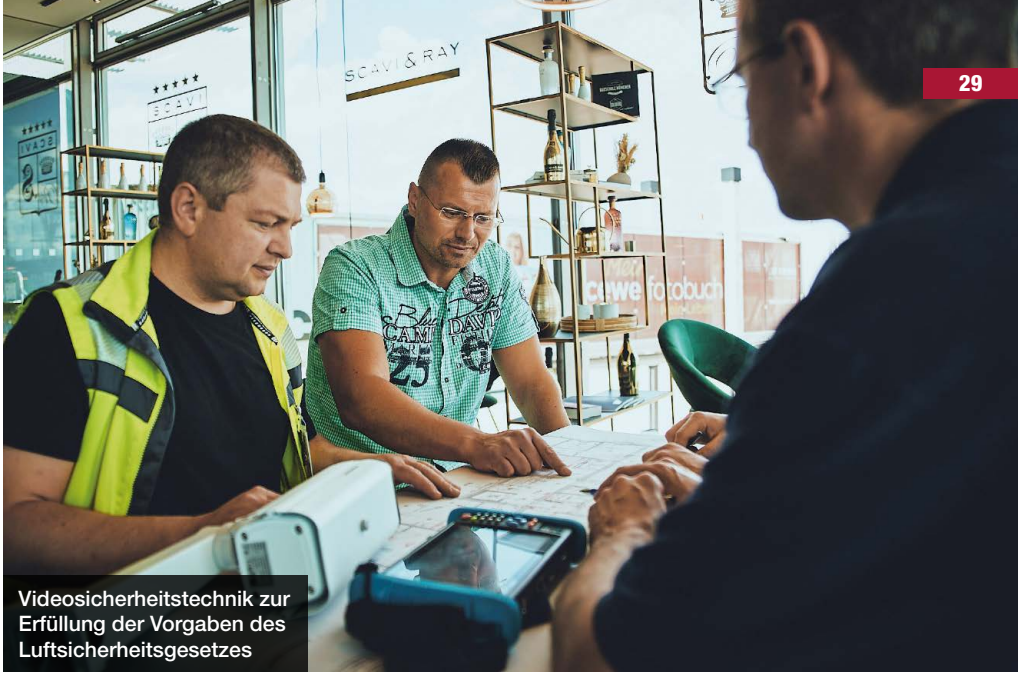
Um den gestiegenen Anforderungen des Luftsicherheitsgesetzes gerecht zu werden, hat der Flughafen Paderborn/Lippstadt sein bestehendes Videoüberwachungssystem modernisiert. Ziel war eine effektive Überwachung sicherheitsrelevanter Bereiche wie Vorfeld, Zufahrten und Parkplätze und Terminalzugänge – mit möglichst geringem Ressourceneinsatz. Gemeinsam mit dem Errichter Horn Sicherheitstechnik entwickelte Dallmeier eine Lösung, die eine schrittweise Erneuerung mit IP-Komponenten, wie z. B. dem Multifocal-Sensorsystem Panomera, ermöglicht, ohne dass vorhandene analoge Technik vollständig ersetzt werden muss.

Rund sechs Millionen Menschen leben im Einzugsgebiet des Flughafens Paderborn/Lippstadt. Als regionaler Verkehrsknotenpunkt stellt Paderborn/Lippstadt die Anbindung an touristische und geschäftliche Ziele sicher. Zum Tagesgeschäft zählen Linien- und Urlaubsflüge ebenso wie Business-, Privat- und Frachtverkehre. Damit übernimmt der Flughafen Verantwortung als Arbeitgeber und regionaler Mobilitätspartner. Ein reibungsloser Betrieb und die Umsetzung gesetzlicher Vorgaben – etwa aus dem Luftsicherheitsgesetz (§5 und §8), der Datenschutz-Grundverordnung (DSGVO) oder der NIS-2-Richtlinie – sind dabei unverzichtbare Grundlagen.

Modernisierung mit Augenmaß

Die Entscheidung zur Erweiterung und Erneuerung der Videosicherheitstechnik wurde vor dem Hintergrund wachsender regulatorischer Anforderungen und technologischer Weiterentwicklung getroffen. Im Mittelpunkt stand die zuverlässige Videoüberwachung der rund 65.000 Quadratmeter großen Vorfeldfläche (Apron) sowie von weiteren sicherheitskritischen Zonen wie Zufahrten, Parkplätzen oder Terminalzugängen und sogenannten Luftsicherheitsgrenzen (Übergang der Passagiere von Landside zu Airside). Analoge Systeme sollten dabei nicht abrupt ersetzt, sondern die Migration zur IP-Technologie sollte schrittweise erfolgen und sich flexibel an die baulichen und betrieblichen Gegebenheiten des Flughafens anpassen lassen.

Sicherheitsrelevante Außenbereiche am Flughafen unterliegen einer permanenten Überwachung



Videosicherheitstechnik zur Erfüllung der Vorgaben des Luftsicherheitsgesetzes

Hybride Lösung

Die Umsetzung erfolgte durch den erfahrenen Errichter Horn Sicherheitstechnik in Zusammenarbeit mit Dallmeier electronic. Herzstück des Systems ist eine hybride Lösung, die vorhandene analoge Komponenten mit modernen IP-Kameras verbindet. Die Aufzeichnung erfolgt über Recording Appliances wie DMS 2400 und IPS 10000, deren hybride Struktur den parallelen Betrieb beider Technologien möglich macht. Zur Überwachung der sensiblen Bereiche kommen verschiedene Kameramodelle zum Einsatz – darunter Domera, Fisheye- und Bullet-Kameras sowie Panomera-Systeme der W4- und S8-Serie. Die Panomera-Technologie erlaubt es, mit deutlich weniger Kameras große Bereiche detailgenau zu erfassen – ein entscheidender Vorteil insbesondere auf der weitläufigen Apron-Fläche, wo sowohl der Gesamtüberblick als auch Detailansichten mit hoher Bildqualität gefordert sind. Das Videomanagement basiert auf Semsy Compact in Verbindung mit dem Semsy Event Manager. Zusätzlich wurden die Tür- und Alarmkontakte über Moxa-Boxen eingebunden, um insbesondere an den Luftsicherheitsgrenzen funktionale Synergien und Aufschaltungen zu schaffen.

Sicherheit, Effizienz und Zukunftsfähigkeit

Mit der neuen Lösung erfüllt der Flughafen die Vorgaben des Luftsicherheitsgesetzes §5 und §8 – etwa in Bezug auf die Überwachung der Luftsicherheitsgrenzen, Zufahrten und sensiblen Betriebsbereichen. Die hybride Lösungsarchitektur erlaubt eine gezielte Weiterentwicklung der bestehenden Infrastruktur. Ein zentraler Vorteil: Dank der Panomera-Technologie ließ sich die Anzahl der benötigten Kameras erheblich verringern, ohne auf Sichtfelder oder Aufzeichnungsqualität verzichten zu müssen. Dies spart nicht nur Installations- und Betriebskosten, sondern reduziert auch den Wartungsaufwand erheblich. Der modulare Aufbau erlaubt eine schrittweise Migration und bietet Flexibilität für zukünftige Anpassungen.

„Mit der Lösung von Dallmeier konnten wir unsere bestehende Infrastruktur nahtlos modernisieren und zugleich neue Sicherheitsanforderungen effizient erfüllen. Besonders überzeugt hat uns die Möglichkeit, analoge und IP-Systeme flexibel zu kombinieren“, erklärt Paul Sawatzki, Leiter IT & Technik am Flughafen Paderborn/Lippstadt.

Regulatorische Sicherheit für kritische Infrastrukturen

Die eingesetzte Lösung von Dallmeier erfüllt sämtliche Anforderungen aus der DSGVO und der NIS-2-Richtlinie – insbesondere im Hinblick auf Datenschutz, IT-Sicherheit und Systemverfügbarkeit. Als ISO-zertifiziertes Unternehmen – unter anderem nach ISO/IEC 27001 für Informationssicherheits-Managementsysteme – bietet Dallmeier höchste Standards im Umgang mit sensiblen Daten. Diese Zertifizierungen bilden eine verlässliche Grundlage für die Einbindung der Technologie in Kritis-Umgebungen. Darüber hinaus schaffen die Entwicklung und Fertigung in Deutschland zusätzliche Transparenz und rechtliche Sicherheit für Betreiber.

Bereit für KI und Prozessoptimierung

Ein weiterer zentraler Aspekt der neuen Lösung ist ihre Zukunftsfähigkeit. Neben der reinen Überwachung rücken zunehmend Analysefunktionen für die Prozessoptimierung und Kostenersparnis in den Fokus. Der Flughafen plant den Einsatz KI-gestützter Technologien wie zum Beispiel den Dallmeier Attribut-Finder, die sich in bestehende Systeme integrieren lassen. GIT

Dallmeier electronic
www.dallmeier.com
www.panomera.com

Gerhard Harand, Geschäftsführer von Wehrhan TPS

SERIE: TESTGELÄNDE IM TEST – TEIL 1

Testen zwischen Zaunlinien

Radar und Video-Management für Perimeterschutz: Wiener Innenstadtgelände von Wehrhan TPS im Test

GIT TEST ZONE

Unsere neue Serie: Keine Showrooms, keine Powerpoint-Bühnen – sondern Umgebungen, in denen Sicherheitstechnik zeigen muss, was sie wirklich kann. Teil 1: Mit Markus Piendl und Hannes Dopler bei Wehrhan TPS.

Perimetersicherheit gewinnt angesichts steigender Anforderungen in urbanen Räumen und kritischen Infrastrukturen weiter an Bedeutung. Mit GIT SICHERHEIT waren die beiden Sachverständigen Markus Piendl und Hannes Dopler auf dem Testgelände der Wehrhan-TPS Sicherheitstechnik GmbH in Wien aktiv. Dort untersuchen sie Radarsensorik, Systemintegration und Täterprofile unter realen Bedingungen – und zeigen, welche Rolle praxisnahe Testumgebungen für Planung, Bewertung und Entscheidungsprozesse spielen.

Ein Testgelände mitten in der Stadt

Die Wehrhan-TPS Sicherheitstechnik GmbH verfügt über eine lange Unternehmensgeschichte, die bis in die 1920er Jahre reicht. Ursprünglich als traditioneller Sicherheitsbetrieb mit Schlüssel- und Schlosstechnik tätig, entwickelte sich das Unternehmen nach der Übernahme im Jahr 2004 zu einem Errichterbetrieb für Zutritts-, Alarm- und Videoanlagen. 2010 folgte der Zusammenschluss mit der TPS Technology, Planning, Security GmbH, wodurch Kompetenzen in Video- und Alarmmanagement sowie ein Großhandelsbereich hinzukamen. Heute beschäftigt das Unternehmen über 20 Mitarbeitende, die sich mit vielseitigen Lösungen rund um Sicherheitstechnik befassen.

Die Entscheidung für ein eigenes Testgelände fiel aus praktischen Gründen: Komplexe Video- und Perimetersysteme lassen sich nur bedingt in sterilen Laborumgebungen beurteilen. Notwendig sind realistische Bedingungen, um Fehlalarme, Abschattungen, tote Winkel oder die Kombination verschiedener Sensoren zuverlässig einzuschätzen. Dabei steht nicht allein die Technik im Fokus – auch menschliches Verhalten und unkonventionelle Bewegungsmuster müssen getestet werden.

v.l.: Renato Nordera, GPS Italia, Jovan Pajic und Gerhard Harand, beide Geschäftsführer von Wehrhan TPS und Sachverständiger Hannes Dopler

Firmengelände Wehrhan TPS: Testgelände mitten in der Stadt, realitätsnah wie beim Kunden

rung und erlaubt die simultane Verfolgung mehrerer Objekte. Neben reiner Detektion unterstützt das System konfigurierbare Alarm- und Ausschlusszonen sowie die Definition von Übertrittslinien.

Ein weiterer Schwerpunkt lag auf der Integration in das Milestone Video-Management-System. Über ein MIP-Plugin werden die Sensoren direkt an den Event-Server angebunden, was eine zentrale Darstellung im Smart Client inklusive Kartenansicht ermöglicht. Die Installation erfolgt serverseitig und ermöglicht ein vergleichsweise einfaches Hinzufügen weiterer GPS-Systemelemente.

Ablauf der Prüfungen: Täter, Profile und Manipulationen

Treppe rauf und rein in die Tests: Der Testtag startete im Schulungsraum im ersten Stock des Wehrhan-Gebäudes. Über mehrere Monitore verfolgen Endkunde, Herstellervertreter und das TPS-Team die Prüfsequenzen der Sachverständigen. Die beiden Experten simulieren währenddessen Einbrecherverhalten in unterschiedlichen Ausprägungen – mit und ohne Tarnung, langsam, schnell, sowie unter Einsatz von

Bitte umblättern ▶

Auslöser: Ein KRITIS-Projekt mit besonderen Anforderungen

Der Besuch unserer beiden Sachverständigen Markus Piendl und Hannes Dopler entstand aus einer konkreten Anfrage eines Unternehmens aus dem KRITIS-Umfeld, die an Markus Piendl herangetragen wurde. Die Aufgabe: eine Perimetersicherheitslösung für eine anspruchsvolle Stadtlage mit unregelmäßigen Zaunlinien, Mauern, Zufahrten und mehreren Eingangsbereichen. Der Endkunde verfügt über viel technisches Know-how und will Sensorik und Systemintegration vor der Beauftragung persönlich prüfen. Wie Gerhard Harand uns erläutert: „Markus Piendl hatte mich informiert, dass ein Unternehmen im KRITIS-Umfeld nach einer Perimetersicherheit-Lösung in einer Stadtlage mit schwierigem Zaunverläufen, Mauern und diversen Einfahrten sucht. Ein gutes Preis-Leistungsverhältnis war ebenso entscheidend wie die Tatsache, dass dieser Kunde sowohl die Sensoren als auch die Integration desselben in ein Video-Management-System vor der Beauftragung selbst sehen und persönlich ausprobieren wollte."

Sensorik im Fokus: Radar 077

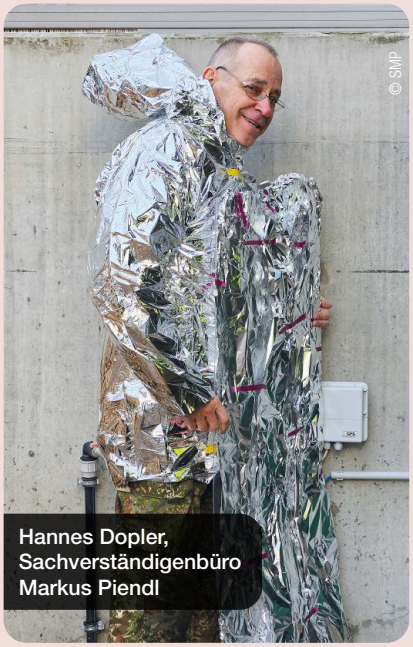
Für die Tests bereitet das Team den Radar 077 von GPS Italia vor – ein 77-GHz-Radarsystem mit zwei Betriebsmodi: einem 90 ° Wide-Modus mit Reichweiten bis zu 40 Metern sowie einer schmalen „Blade"-Variante mit circa 60 Metern Distanzabdeckung. Die Sensorik nutzt MIMO-Technologie, Machine-Learning-basierte Klassifizie-

„Verbesserung der Firmware aufgrund der Tests"

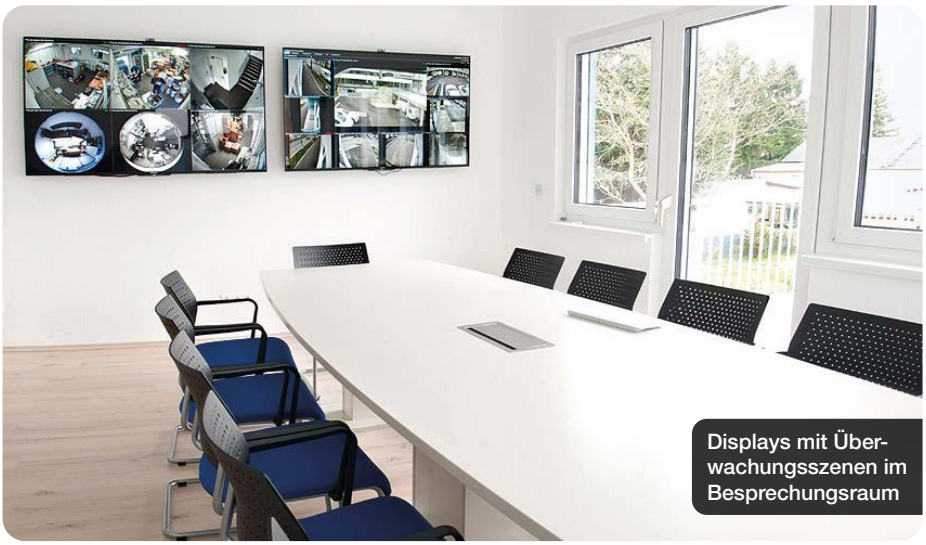
GIT SICHERHEIT: Hannes Dopler, Ihr Eindruck vom Testgelände?
Hannes Dopler: Die Flexibilität des Areals hat mich beeindruckt. Wir konnten verschiedene Täterprofile in kurzer Zeit durchspielen und Sensorpositionen schnell verändern.

Worauf achten Sie bei Perimetertests?
Hannes Dopler: Auf das Verhalten in Ausnahmesituationen – langsame Bewegungen, verdeckte Annäherungen oder untypische Fortbewegungsarten. Diese Szenarien zeigen, wie zuverlässig ein System wirklich arbeitet.

Was ist Ihr Fazit – und wie verlief die Zusammenarbeit mit den Beteiligten?
Hannes Dopler: Ein Testgelände in einer Großstadt zu betreiben ist aufgrund des begrenzten Platzes natürlich etwas Spezielles. Besonders beeindruckt war ich von den vielfältigen Möglichkeiten, Sensoren schnell und einfach zu installieren. Wir konnten die verschiedenen Tätervorgehen problemlos auf kurze und mittlere Distanzen nachstellen, etwa bei Liefereinfahrten, Parkflächen, Büroeingängen oder Tiefgaragen – und zwar ohne, dass wir von Dritten gestört wurden. Richtig gut gefallen hat mir auch, dass GPS unsere Vorschläge für die Firmware-Änderung direkt aufgenommen hat.



Hannes Dopler, Sachverständigenbüro Markus Piendl



Displays mit Überwachungsszenen im Besprechungsraum

Hilfsmitteln. Ziel: das Ansprechverhalten der Sensorik systematisch erfassen.

Und: testen, testen, testen. So sind Szenarien wie „Leopardieren“ und „Ozelotieren“ besonders anspruchsvoll – Kriech- und Rollbewegungen, die auf minimale Signatur ausgelegt sind. TPS-Chef Harand: „Ein Höhepunkt der Einbruchtests war das Ozelotieren und Leopardieren bei gleichzeitiger Deckung durch Leucht-, Blend- und Konfettigranaten sowie die Versuche, die Sensoren gezielt zu manipulieren zu stören.“ Knalleffekte also inklusive. Parallel kamen Videoanalysefunktionen zum Einsatz, die Verifikationsprozesse unterstützten.

In Zeitlupe rollend versucht Sachverständiger Hannes Dopler, die Sicherheitssysteme zu überlisten

Ergebnisse: Belastbare Daten und konkrete Optimierungen

Die wichtigen Einbruchversuche wurden erfolgreich absolviert. Die per Remote-Verbindung zugeschaltete Entwicklungsabteilung des Herstellers verfolgte die Tests live und konnte Auslöseschwellen sowie Ereignisse in Echtzeit analysieren. Rückmeldungen der Sachverständigen flossen unmittelbar in Firmware-Anpassungen und Optimierungen am Milestone-Plugin ein. Der Clou und eine besondere Leistung der Partner von Wehrhan TPS: Nur kurze Zeit später waren die vorgeschlagenen Änderungen implementiert.

Gerhard Harand: „Die für den Endkunden wichtigen Einbruchversuche wurden bravourös bestanden. Die Entwicklungsabteilung von GPS Italia war über eine sichere Internetverbindung zugeschaltet und verfolgte live, wie gut die Sensoren funktionierten und welche Auslöseschwellen in Echtzeit anschlugen. Ferner übertrugen wir einen Video-Live-Stream. Die beiden Sachverständigen gaben GPS und uns gute Tipps für die Verbesserung der Sensor-Firmware bei den Manipulationstests und steuerten auch für das Milestone Plug-In gute Ideen bei.“

Für den Endkunden ergab sich dadurch ein klares Bild über Funktionsweise, Grenzen und Integrationsfähigkeit des Systems – und letztlich die Entscheidung, das Projekt gemeinsam mit Wehrhan-TPS samt der ausgewählten Partner umzusetzen.

Partner GPS Standard: Lösungen für Perimeterschutz

Marco Capula, Business Development Strategist, mit GPS-Sensoren

GPS Standard gehört seit Jahrzehnten zu den europäischen Anbietern für Perimeterschutzlösungen und setzt dabei auf eine Kombination aus Sensorik, Datenfusion und modularen Sicherheitsarchitekturen.

„Mehr als Hochglanzbroschüren“

GIT SICHERHEIT: Gerhard Harand, welche Rolle spielt das Testgelände für Ihre Arbeit?
Gerhard Harand: Es hilft uns, Systeme so zu beurteilen, wie sie sich im tatsächlichen Einsatz verhalten. Viele Fragestellungen – etwa Grenzbereiche oder Fehlalarme – lassen sich ausschließlich unter realen Bedingungen bewerten.

Wie profitieren Sie von unabhängigen Tests?
Gerhard Harand: Sie erweitern den Blickwinkel. Fachleute wie Herr Dopler und Herr Piendl bringen andere Testmethoden ein und geben wertvolle Hinweise für Hersteller wie für uns als Errichter. Und das ist gut für das Projekt, den Kunden, den Betreiber!

Welche Bedeutung hat das für die Branche?
Gerhard Harand: Ich hoffe, dass viele Hersteller und Sicherheits-Errichter wie wir über kleine, größere und große Testgelände verfügen. Möglichst viele davon sollten im Rahmen dieser Serie bei der GIT SICHERHEIT vorgestellt werden! Wir können so viel voneinander lernen. Hochglanzbroschüren sind bekanntlich das eine – der Besuch auf einem Testgelände inklusive guter Nachbereitung ist hingegen klar zu bevorzugen.

Ing. Gerhard Harand, MSc, Geschäftsführer Wehrhan TPS

Das Unternehmen mit Hauptsitz in Italien entwickelt Radarsysteme, Zaunsensoren und Bodenmeldetechnologien, die auf unterschiedlichen physikalischen Prinzipien basieren. Durch diese Bandbreite lassen sich Perimeterlösungen flexibel an Geländeformen, Gebäudestrukturen und Umgebungsbedingungen anpassen – ein Aspekt, der im Industriesektor ebenso relevant ist wie im Bereich kritischer Infrastrukturen.

Ein Schwerpunkt des Unternehmens liegt auf der kontinuierlichen Weiterentwicklung eigener Radarplattformen. Systeme wie der im Test eingesetzte 77-GHz-Radar 077 basieren auf aktiver Detektionstechnologie, ergänzt um Klassifizierungsalgorithmen, die zwischen verschiedenen Objekttypen unterscheiden. Die Produkte unterstützen darüber hinaus die Integration in übergeordnete Video-Management- und Leitsysteme. Diese Offenheit erleichtert Errichtern die Kopplung mit bestehenden Infrastrukturen und schafft einheitliche Alarmierungs- und Dokumentationsprozesse.

Partner Milestone: Lösungen für Video-Management

Markus Poth, Channel Business Manager bei Milestone

Milestone Systems zählt zu den etablierten Anbietern offener Video-Management-Plattformen und entwickelt seit Ende der 1990er Jahre Softwarelösungen, die auf Skalierbarkeit und Integrationsfähigkeit ausgelegt sind. Das Unternehmen mit Hauptsitz in Dänemark setzt auf ein Ökosystemmodell, bei dem Video, Audio, Sensorik und Analysewerkzeuge verschiedener Hersteller über standardisierte Schnittstellen zusammengeführt werden können. Dieser Ansatz unterstützt Errichter, Planer und Betreiber dabei, unterschiedliche Systemlandschaften zu verbinden – von kleinen Installationen bis hin zu weitverzweigten Netzwerken.

Kern des Portfolios ist die XProtect-Plattform, die je nach Projektgröße als Basis-, Mittelstands- oder Premiumversion bereitsteht. Die Software erlaubt den Betrieb klassischer Überwachungsstrukturen ebenso wie die Einbindung moderner Analyseverfahren, darunter Objekterkennung, Bewegungsmusteranalysen oder Ereignisautomationen. Über das Milestone Integration Platform (MIP) SDK lassen sich externe Hardware und Sensorik – wie der getestete Radar 077 – direkt anbinden. Dadurch entsteht eine gemeinsame Ereignisstruktur, die sowohl visuelle als auch sensorische Daten synchronisiert darstellt.

Fazit: Mehrwert für Hersteller, Errichter und Kunden

Entscheidend ist auf dem Platz, um Trainerlegende Otto Rehagel zu zitieren. Dem können wir von GIT SICHERHEIT uns nur anschließen, denn gerade im Bereich Sicherheit ermöglichen Testgelände eine differenzierte Betrachtung, die weit über Hochglanz-Produktbroschüren hinausgeht. Sie bringen reale Bedingungen, klare Vergleichsmöglichkeiten und nachvollziehbare Systemreaktionen zusammen.

Auch unsere Experten betonten, dass Errichter damit angesichts des Preisdrucks einen qualitativen Mehrwert schaffen und sich gegenüber Mitbewerbern profilieren können.

Wenn dann noch wie im vorliegenden Fall gute Ergebnisse und das berühmte Sicherheitsplus für den Kunden und Betreiber erzielt werden kann – Sicherheitsherz, was willst du mehr. GIT

Demnächst nimmt GIT SICHERHEIT ein Testgelände unter die Lupe, das sich mit Drohnendetektion und Drohnenabwehr beschäftigt.

„Testgelände macht Kompetenz sichtbar“

GIT SICHERHEIT: Markus Piendl, welchen Nutzen hatte der Besuch für Ihre Bewertung?
Piendl: Die reale Umgebung half, die Systeme eindeutig einzuschätzen. Das ist aussagekräftiger als reine Theorie.

GIT SICHERHEIT: Was zeichnet das Testgelände aus?
Piendl: Die Kombination aus Schulungsraum und Testfeld ist praxisnah. Man sieht oben, was unten passiert – das erleichtert Bewertung und Austausch.

GIT SICHERHEIT: Welche Empfehlung geben Sie Errichtern?
Piendl: Ein Testgelände macht Kompetenz sichtbar. Es hilft, realistische Erwartungen zu setzen und Systeme verantwortungsvoll auszuwählen. Und speziell der Blick hier auf Wehrhan TPS: Die Logistik ist schon besonders. Dass Kunden im Schulungsraum komfortabel sitzen können, während unter ihnen gleichzeitig Sensoren getestet werden – einfach prima. In Pausen können Laien, aber auch Experten Einstellungen, diverse Einbruchmelde-Anlagen, IP-Sprechanlagen und Lautsprecher, Video- und Zutrittssysteme an Exponaten und im Live-Betrieb ausprobieren. Der Vergleich der verschiedenen Milestone-Versionen samt dem voll funktionsfähigen GPS-Plug-In hat mir sehr gefallen. Der integrierte Ansatz und der Verzicht auf Insellösungen wird gelebt. Sicherheits-Errichter stehen in vielen Projekten unter hohem Preisdruck: ein Testgelände ist eine sehr gute Möglichkeit, sich von Mitbewerbern abzusetzen. Das ist hier bei Wehrhan TPS auf kleinstem Raum hervorragend gelungen. Danke, dass wir vor Ort sein durften.

Markus Piendl, Sachverständigenbüro Markus Piendl

Wehrhan TPS Sicherheitstechnik GmbH
www.Wehrhan-TPS.at

Der zehnte Austrian Security Day (ASD) im Januar dieses Jahres

SICHERHEITSTECHNIK

Eine Branche im Umbruch

Beim 10. Austrian Security Day bei Wehrhan TPS standen NIS2 und RKEG im Mittelpunkt

Bereits zum 10. Mal lud Wehrhan TPS am 29. Januar zum Austrian Security Day (ASD) auf die Burg Perchtoldsdorf in Niederösterreich. Die Veranstaltung brachte Facherrichter, Hersteller, Betreiber und Experten zusammen, um zentrale Entwicklungen der Sicherheitstechnik zu analysieren. Im Mittelpunkt standen die Auswirkungen der NIS2 Richtlinie und des österreichischen „Resilienz kritischer Einrichtungen-Gesetzes“ (RKEG). Ergänzt wurde das Programm durch Fachvorträge, Podiumsdiskussionen und einen umfangreichen Ausstellerbereich.

v.l.n.r.: Harald Blauensteiner und Gerhard Harand, beide Wehrhan TPS Sicherheitstechnik, Jürgen Karlsböck, Siemens Österreich, Bernhard Steindl, ÖWD Security Systems, Martin Aigelsreiter, G4S Security Systems, Mischa Zöberer, Plenus Protect

Der 10. Austrian Security Day (ASD) von Wehrhan TPS zeigte eindrucksvoll, wie stark die österreichische Sicherheitsbranche im Umbruch steht. Im Zentrum der Tagung, zu der das Sicherheitstechnik-Unternehmen am 29. Januar 2026 eingeladen hatte, standen zwei Themen, die Unternehmen, Errichter und Hersteller in den kommenden Jahren maßgeblich prägen werden: die NIS2-Richtlinie und das neue RKE-Gesetz. Beide Regelwerke verlangen tiefgreifende organisatorische, technische und strategische Anpassungen – eben hier setzte die Veranstaltung an.

NIS2 und RKEG

Bereits die Eröffnungs-Keynote von Mischa Zöberer machte deutlich, wie eng NIS2 und RKE-Gesetz künftig miteinander verwoben sind. Die anschließenden Podiumsdiskussionen vertieften diese Perspektiven: Zunächst diskutierten Vertreter aus Industrie, Gesundheitswesen und Gasversorgung über praktische Herausforderungen und notwendige Maßnahmen. Im zweiten Panel standen die Facherrichter im Mittelpunkt, die vor allem strategische und technische Auswirkungen der neuen Vorgaben beleuchteten.

Ein besonderes Highlight war der Ausstellerbereich, der mit 20 Unternehmen so groß war wie nie zuvor. Die Bandbreite reichte von Perimeter- und Sensortechnik über moderne Kamerasysteme und Videoanalyse bis hin zu Zutrittslösungen, Netzwerktechnik und Visualisierung. Vertreten waren unter anderem Hanwha Vision Europe, Vivotek, Bosch/Iqsight, Teledyne Flir, Milestone Systems, Iseo, 2N, Barox Kommunikation, Eizo und viele weitere. Ergänzt wurde das Spektrum durch Forschungseinrichtungen wie die Donau-Universität Krems sowie Fachmedien.

Vernetzung und Austausch

Die Teilnehmerstruktur spiegelte die Vielfalt der Branche wider: Vertreter kritischer Infrastrukturen, Errichterbetriebe, Hersteller, Experten und Vortragende nutzten die Gelegenheit zum intensiven Austausch. Gerade dieser Vernetzungsaspekt – seit jeher ein Kern des ASD – prägte die Veranstaltung spürbar.

Der 10. Austrian Security Day machte deutlich, dass die Branche nicht nur vor großen Herausforderungen steht, sondern diese aktiv und gemeinschaftlich angeht. Die hohe Qualität der Diskussionen, die Rekordzahl an Ausstellern und das breite Themenspektrum unterstrichen die Bedeutung des ASD als zentrale Plattform für Wissenstransfer, Innovation und Kooperation. Die Veranstaltung setzte damit ein starkes Zeichen für die Zukunft der österreichischen Sicherheits- und Errichterlandschaft. GIT

Wehrhan TPS Sicherheitstechnik
www.wehrhan-tps.at

© Bilder: Wehrhan TPS Sicherheitstechnik

Salto: XS4 Com erhält German Design Award 2026

Beim German Design Award konnte Salto mit seiner intelligenten Video-Intercom-Lösung XS4 Com in der Kategorie „Building and Elements“ überzeugen und wurde für „Excellent Product Design“ ausgezeichnet.

XS4 Com setzt als umfassende Plattform für die Türkommunikation und Zutrittskontrolle auf einen modernen cloudbasierten Ansatz und integriert sich nahtlos in die moderne digitale Lebenswelt von Wohn-, Arbeits- und Geschäftsumgebungen. XS4 Com kombiniert innovative Kommunikationstechnologie mit dem bewährten Zutrittsmanagement von Salto. Anwender und Gebäudebetreiber profitieren von optimierten Prozessen, die ein Echtzeit-Zutrittsmanagement, die Ansteuerung von Zutrittspunkten aus der Ferne sowie eine nahtlose und sichere Kommunikation zwischen Gastgebern und Besuchern ermöglichen.

Die leichte Bedienbarkeit und der Funktionsreichtum machen die Plattform zur idealen Wahl für smarte Ökosysteme in einer Vielzahl von Anwendungen, etwa in der Wohnungswirtschaft, in modernen Büroumgebungen, in Shared Living Spaces, im Bildungswesen sowie im Gastgewerbe und Gesundheitswesen.

Der German Design Award zählt zu den angesehensten Preisen der Designlandschaft. Seit 2012 identifiziert der Award maßgebliche Gestaltungstrends, macht sie sichtbar und zeichnet sie aus. Jährlich werden herausragende Arbeiten aus den Bereichen Produktdesign, Kommunikationsdesign und Architektur prämiert. Nur Produkte, Projekte und Kommunikationsdesignleistungen, die von den Expertengremien des Rats für Formgebung nominiert wurden, können am Wettbewerb teilnehmen.

2026 wurden über 3.900 Einreichungen aus 57 Ländern registriert. Bewertet wird in einem mehrstufigen Verfahren, das in einer zweitägigen Jurysitzung mündet.

www.saltosystems.de

Mobiler Videotürme im Einsatz für einen Solarpark: Lösungen, die sich ebenso für Baustellen, Infrastrukturprojekte, Logistikflächen, Windparks oder andere weitläufige Areale eignen

VIDEOTÜRME

Zur Stelle, wenn man's braucht

Temporäre mobile Videoüberwachung in Deutschland

Innerhalb weniger als einem Jahrzehnt hat sich der Markt für temporäre mobile Videoüberwachung in Deutschland zu einem professionellen, skalierfähigen Industriezweig entwickelt. David Smyczek befasst sich mit seinem Beratungsunternehmen Smyczek Consulting mit diesem Thema seit vielen Jahren. Für GIT SICHERHEIT hat er einen Überblick zu diesem Markt und seinen Entwicklungen in Deutschland geschrieben.

Wo früher häufig klassische Baustellenbewachung durch Wachpersonal, Bestreifungen oder punktuelle Kontrollfahrten dominierte, sind heute mobile Videoüberwachungstürme vielerorts zum Standard geworden – insbesondere dort, wo Werte hoch, Risiken konkret und Reaktionszeiten entscheidend sind. Die Gründe: Material- und Maschinenwerte sind gestiegen, Projektvolumina werden größer, Baustellen liegen zunehmend in exponierten Lagen, und Täter agieren strukturierter. Gleichzeitig steigt der Druck auf Bauherren, Betreiber und ausführende Unternehmen, Standorte präventiv abzusichern – nicht erst nach dem ersten Schadenfall.

Von „früher erkennen" zu „aktiv verhindern"

Noch vor zehn Jahren war die Realität auf vielen Baustellen simpel: Sicherheit wurde über Wachpersonal abgebildet – teilweise stationär, teilweise über Bestreifungen, vereinzelt auch mit Diensthunden. Diese Maßnahmen hatten zwar einen Effekt: Ein Einbruch wurde häufig früher erkannt als erst am nächsten Morgen durch den Bauleiter. Der eigentliche Mehrwert blieb jedoch begrenzt, weil Täter die Abläufe häufig ausspähten und genau kalkulierten, wie viel Zeit zwischen zwei Runden bleibt, um beim Einbruch unbemerkt zu bleiben.

Gerade im Kontext kritischer Infrastrukturen zeigt sich der Nutzen temporärer Systeme besonders deutlich. Ereignisse wie der Anschlag in Berlin verdeutlichen, dass Sicherheitsmaßnahmen an neuralgischen Punkten nicht immer sofort dauerhaft umgesetzt werden können. Mobile Videoüberwachungssysteme können hier kurzfristig als wirksame Übergangslösung dienen, um gefährdete Bereiche schnell abzusichern, Lagebilder zu liefern und Resilienz aufzubauen – bis permanente Schutzmaßnahmen installiert sind.

Das Problem systematisch lösen

Die Entstehungsgeschichte der Videotürme lässt sich gut an einem typischen Praxisfall erklären: Ein Unternehmen das ursprünglich Baumaterialien verkaufte, erhielt montagmorgens regelmäßig Anrufe, dass am Wochenende Material entwendet wurde. Das führte zwar zu wiederholten Nachbestellungen – war aber gleichzeitig ein Symptom für ein strukturelles Problem: Die Baustellen waren nicht präventiv geschützt.

Was zur Lösung dieses Problems zunächst mit Teststellungen begann, entwickelte sich über die Jahre zu einem hochgradig skalierfähigen Produkt: einem mobilen System, das Kameratechnik, Router, Switch, Stromversorgung und zunehmend auch Analysefunktionen in einem standardisierten Setup bündelt.

Anbieterübersicht

AF Security Group | https://af-security.de

Alinotec | https://alinotec.de

Autosecure | https://autosecure.net

BauVision (B.O.S.S. Sicherheitsdienste & Service) | https://bauvision.de

BauWatch | www.bauwatch.com/de-de

Camcontrol (by TOI TOI & DIXI) | www.toitoidixi.de/camcontrol

Kooi | https://247kooi.com/de

LivEye | www.liveye.com

Securetask | https://securetask.de

Secontec | www.secontec.de

Sicherheitsdienst Sauermann | https://sicherheitsdienst-sauermann.de/perimeterschutz

TurmWatch | http://turmwatch.de

Videoguard | www.videoguard24.de/unternehmen

Watchtower | http://wt-security.com/de-de

180 ° Gruppe (Wisag Sicherheit & Service) | www.180-sicherheit.de/mobile-ueberwachung

© Tabea Flöhr

David Smyczek (rechts) und Alexander Lerch – Experten mit Herzblut für mobile Videoüberwachung

Live-Intervention statt nur Videobild

Entscheidend war jedoch nicht die Kamera an sich – denn reine Bilder liefern im Zweifel nur Beweismaterial „nach der Tat". Der wirkliche Durchbruch kam mit der Live-Intervention: Täteransprache, Verifikation in Echtzeit, Alarmprozesse, Eskalationslogiken. So konnte man nicht mehr nur den Einbrüche dokumentieren, sondern Einbrüche gleich verhindern. Parallel dazu entwickelte sich auch die Leitstellenlandschaft weiter: weg von klassischen Alarmaufschaltungen aus Einbruchmeldetechnik, hin zu videobasierten Prozessen, in denen Analyse, Priorisierung und Intervention zur Kernleistung wurden.

Marktüberblick: Zahlen, Dynamik und Wettbewerbsstruktur

Die Branche ist in den letzten Jahren deutlich gewachsen. Ende 2024 waren rund 17.000 Systeme im deutschen Markt aktiv. Ende 2025 lag der Bestand bereits bei rund 21.000 aktiven Videotürmen. Dieses Wachstum ist bemerkenswert, da nicht alle Teilmärkte (z. B. Wohnungsbau) konstant wachsen. Die Erklärung liegt in der zunehmenden Relevanz von temporärer Sicherheit auch außerhalb klassischer Baustellen – beispielsweise in Energieprojekten, Infrastrukturmaßnahmen, Logistikflächen oder bei kommunalen Objekten.

Im Zuge einer Marktanalyse wurden im September 2024 etwa 15.615 Systeme im Feld ermittelt. Auffällig war dabei die starke Marktkonzentration: Die Top-10-Anbieter vereinten zu diesem Zeitpunkt rund 90 % der Systeme auf sich – bei insgesamt etwa 70 Wettbewerbern. Diese Struktur war typisch für einen Markt, der stark von wenigen sehr großen Playern dominiert wird: bundesweite Präsenz, standardisierte Produktlinien, große Service-Hubs und hohe Skalierungsfähigkeit.

Evaluierung 2025: Regionale Anbieter gewinnen

Eine erneute Auswertung der Marktdaten 2025 zeigte eine wichtige Veränderung: Die Top 10 beanspruchten jetzt noch rund 83 % des Marktes. Das ist ein entscheidender Indikator für die Reifephase der Branche: kleinere und mittlere Anbieter gewinnen an Bedeutung, insbesondere durch regionale Vernetzung, kurze Wege, persönliche Beziehungen und schnellere Reaktionsfähigkeit vor Ort. Damit entsteht ein Markt, der sich zunehmend zweigeteilt entwickelt: große Anbieter mit bundesweiter Skalierung und stark standardisierten Prozessen, regionale Anbieter mit hoher Nähe zum Kunden und lokaler Stärke.

Neben den erfahrenen Playern im deutschen Markt BauWatch, Videoguard, LivEye, Kooi, Alinotec und Secontec haben sich jetzt auch Firmen wie z. B. AF Security Group Autosecure, BauVision als Teil von Boss Sicherheitsdienste & Service, Camcontrol by Toi Toi & Dixi, die 180 ° Gruppe als Teil von Wisag Sicherheit und Service, Sicherheitsdienst Sauermann, Securetask, TurmWatch sowie Watchtower, etabliert. (s. Anbieterliste)

Diese Unternehmen stehen exemplarisch für unterschiedliche Ausprägungen

Bitte umblättern ▶


© LivEye

Liveye-Videoturm bei der Überwachung einer Stadion-Baustelle

© Liveye

Alles im Blick: Videoturm von Liveye, hier in einer Variante mit Solarpanels zur Stromversorgung

im Markt – von reinen Vermietmodellen über hybride Ansätze bis hin zu verschiedenen technischen Strategien und Servicekonzepten. Der Markt wird sich verändern, in dem sich einige der Unternehmen durch Zusammenschlüsse konsolidieren – wie zuletzt Videoguard und Kooi.

Vom Videoturm zu Sicherheitsplattform

Die technische Evolution der Systeme schreitet kontinuierlich voran. Während die ersten Generationen vor allem Kamera und Übertragung abbildeten, werden heutige Systeme zunehmend zu einem Hub für weitere Sicherheitsfunktionen. Ein zentraler Trend ist der Einsatz von KI-gestützter Analyse. Cloudbasierte Filter und Analytics helfen dabei, relevante Ereignisse schneller von irrelevanten Bewegungen zu unterscheiden. Das entlastet Leitstellen und schafft die Grundlage für neue Modelle – bis hin zu teilautonomen oder autonomen Türmen.

Ein weiterer Treiber ist die Energieversorgung. Autarke Systeme waren 2016 in vielen Beständen noch die Ausnahme. Damals dominierten stromgebundene Varianten deutlich. Waren 2016 noch ca. 90 % stromgebunden und 10 % autark, arbeiten heute etwa 60 % stromgebunden und 40 % autark. Dies wird sich Richtung 50/50 ändern, möglicherweise mit weiterem Shift Richtung Autarkie. Dabei geht es nicht nur um Nachhaltigkeit, sondern vor allem um eine Antwort auf reale Baustellenbedingungen: fehlender Baustrom, entlegene Standorte, temporäre Projektphasen.

Service, Logistik und Prozesse als Engpass

Mit dem Wachstum des Marktes stiegen nicht nur die Systemzahlen – sondern auch die Anforderungen an Organisation, Service und Logistik. Denn in der Praxis entscheidet nicht allein die Technik über den Erfolg, sondern die Fähigkeit, Prozesse stabil zu betreiben: Auslieferung und Rückholung, Aufbau, Umsetzung, Wartung, Alarmprozesse und Eskalation. Gerade in Wachstumsphasen entstehen hier häufig die größten Schmerzen: Kapazitätsengpässe, unklare Verantwortlichkeiten, fehlende Standardprozesse oder ineffiziente Schnittstellen zwischen Vertrieb, Logistik, Leitstelle und Technik.

Analysten und Researcher, die den Markt unter anderem im Zuge von Übernahmen der letzten Jahre detailliert betrachtet haben, gingen ursprünglich von 25.000 bis 34.000 Systemen bis 2030 aus. Heute wird die Marke von 50.000 Systemen – teils sogar bis zu 70.000 – häufig als mögliches Marktsättigungsszenario diskutiert.

Smyczek Consulting und GuardUp

Mit der Professionalisierung des Marktes steigt auch der Bedarf an strukturiertem Aufbau – insbesondere bei Unternehmen, die neu einsteigen oder ihre bestehende Organisation skalieren wollen. Neben Technik und Vertrieb sind dabei Themen wie Prozesse, Service-Logistik, Datenschutz, Versicherung und organisatorische Verantwortlichkeiten entscheidend. Smyczek Consulting begleitet Unternehmen genau an dieser Schnittstelle: Wachstum planbar machen, Engpässe vermeiden und Strukturen so aufsetzen, dass Servicequalität auch bei steigenden Systemzahlen stabil bleibt.

Parallel dazu entsteht mit GuardUp ein neuer Ansatz, um den Markt effizienter zu machen: ein digitaler Marktplatz, der Produkte, Verfügbarkeiten, Preise und Prozesse vergleichbarer macht. Gerade in einem Markt mit vielen Anbietern und unterschiedlichen Logiken kann Transparenz ein entscheidender Hebel sein: weniger Abstimmung, schnellere Entscheidungen, klarere Vergleichbarkeit – und damit ein Beitrag zur weiteren Professionalisierung der gesamten Branche. GIT

Smyczek Consulting
www.smyczekconsulting.de

VSW
Verband für Sicherheit in der Wirtschaft
Hessen – Rheinland-Pfalz – Saarland

Save the date!

Nähere Informationen und Möglichkeit zur Anmeldung:

www.vsw.de/themen/vsw-sicherheitstag

VSW-Sicherheitstag

Gemeinsam die Sicherheit in der Wirtschaft stärken

Der jährliche VSW-Sicherheitstag ist eine hervorragende Plattform, um sich umfassend über Unternehmenssicherheit auszutauschen und wertvolle Netzwerke zu knüpfen. Dabei kommen Experten und Fachkräfte aus unterschiedlichen Bereichen – vom staatlichen Sicherheitssektor bis hin zur privaten Wirtschaft – zusammen, um aktuelle Sicherheits- und Gefährdungslagen zu diskutieren.

30. September 2026

Ort: Schloss Waldthausen bei Mainz

Verband für Sicherheit in der Wirtschaft
Hessen – Rheinland-Pfalz – Saarland e.V. (VSW-Mainz)
info@vsw-mainz.de | vsw.de

GESICHTSERKENNUNG

„Erklären statt polarisieren“

Gesichtserkennung: Ein Plädoyer für klare Regeln

Gesichtserkennung gehört zu den umstrittensten Themen moderner Videoanalyse. Auf der einen Seite steht die Sorge vor Eingriffen in die Privatsphäre, vor einer übermäßigen Überwachung und vor möglichen Verzerrungen in den Algorithmen. Auf der anderen Seite eröffnet diese Technologie Chancen für die Aufklärung schwerer Straftaten. Angesichts hoher Risiken und hoher Chancen braucht es einen verantwortungsvollen Umgang mit Gesichtserkennung. Wie kann ein Ausgleich zwischen technischer Weiterentwicklung und verantwortungsbewusster Anwendung gelingen? Dieser Frage geht Thomas Jensen, CEO von Milestone Systems, in seinem Beitrag für GIT SICHERHEIT nach.

Viele Menschen befürchten, Gesichtserkennung könne als flächendeckendes Kontrollinstrument missbraucht werden. Der Gedanke, jederzeit erfasst zu werden, widerspricht grundlegenden demokratischen Werten und stellt einen tiefen Eingriff in die Privatsphäre dar. Deshalb darf Gesichtserkennung nur in eindeutig gerechtfertigten Situationen eingesetzt werden. Dazu gehören Vergleiche mit klar definierten, rechtlich legitimierten Datenbanken wie den Fahndungslisten von Europol oder Interpol. Auch der Einsatz bei der Suche nach vermissten Personen ist sinnvoll, sofern Angehörige zustimmen.

Gesichtserkennung gehört zu den umstrittensten Themen moderner Videoanalyse

Es wäre höchst problematisch, Fotos aus sozialen Netzwerken ohne ausdrückliche und informierte Zustimmung zu verwenden. Persönliche Bilder wurden nie mit der Absicht veröffentlicht, später in Überwachungssystemen zu landen. Zudem wären alle Menschen potenzielle Treffer, wenn die Datenbanken ohne klare Zweckbindung befüllt würden.

Ein gutes Beispiel für eine datenschutzfreundliche Anwendung ist die Gesichtserkennung an automatisierten Grenzkontrollstellen in Flughäfen. Dort wird das Livebild einer reisenden Person lediglich mit dem im Pass gespeicherten biometrischen Foto abgeglichen. Die Daten werden lokal und nur für den Moment der Prüfung verarbeitet.

Ein weiterer wichtiger Punkt betrifft die Sicherheit biometrischer Daten. Moderne Systeme speichern keine Rohbilder. Stattdessen entsteht aus einem Gesicht eine digitale Signatur, die für andere Systeme kaum verwertbar ist und sich nicht zurückrechnen lässt. Trotzdem bleiben hohe Sicherheitsstandards unverzichtbar, etwa starke Verschlüsselung, Zugriffsbegrenzungen und strikte Regeln zur Datenminimierung.

Algorithmische Verzerrungen

Kritiker weisen zurecht darauf hin, dass Gesichtserkennung Menschen falsch zuordnen kann. Besonders betroffen sind Gruppen, die in Trainingsdaten unterrepräsentiert sind. Studien des MIT Media Lab und des US National Institute of Standards and Technology zeigen Unterschiede bei Frauen, älteren Menschen und Personen mit dunklerer Hautfarbe.

Umso wichtiger ist es, Verzerrungen systematisch zu überprüfen und zu reduzieren. Entwickler sollten Verfahren zur Fairness-Prüfung fest integrieren. Außerdem sollten Systeme regelmäßig mit vielfältigen Datensätzen getestet werden, die die tatsächliche Bevölkerung abbilden. Transparenz zu Genauigkeitswerten in verschiedenen Gruppen ist eine grundlegende Voraussetzung.

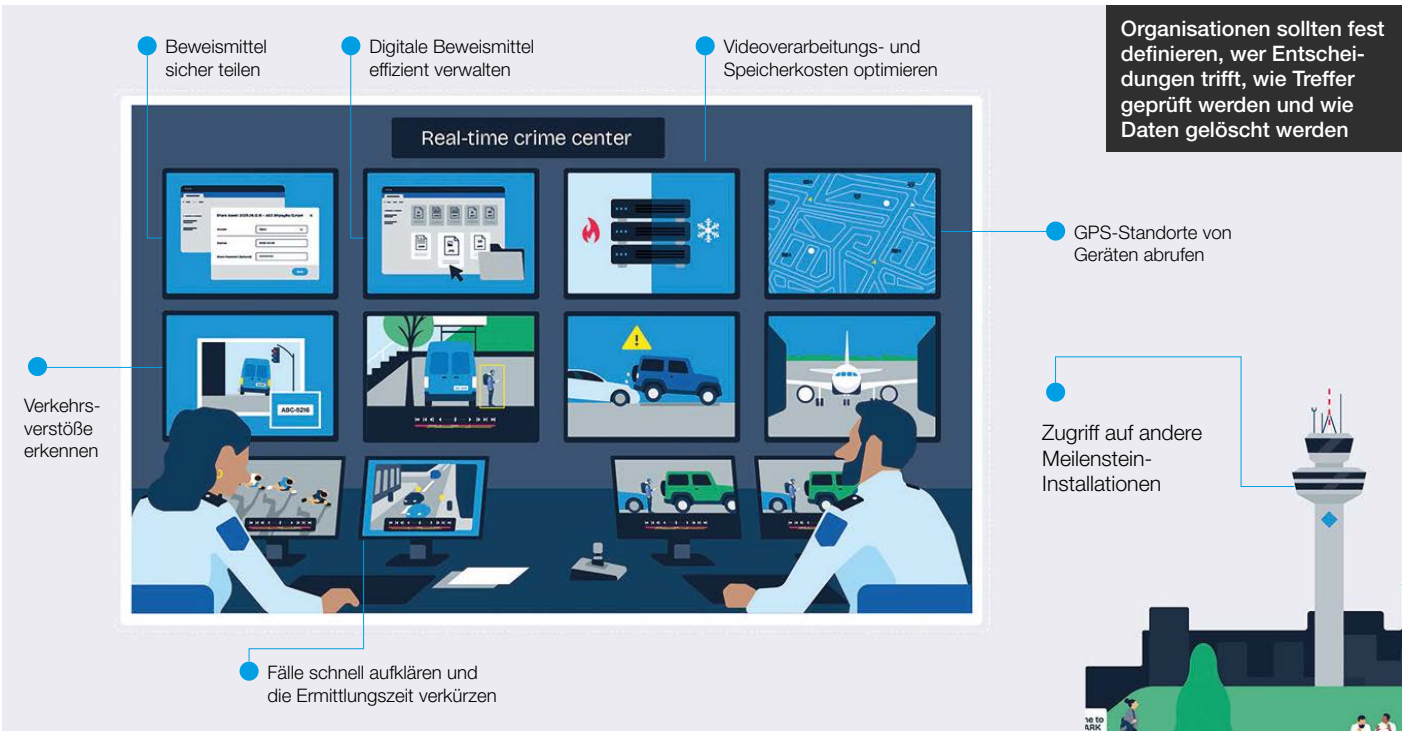
Klare Verfahren und rechtliche Grenzen

Gesichtserkennung gehört in Bereiche, in denen es um schwere Straftaten oder akute Gefahrenlagen geht. Eine Gewöhnung an den Einsatz im Alltag würde Freiheitsrechte schrittweise aushöhlen.

Regulierung spielt eine entscheidende Rolle. Der AI Act der Europäischen Union setzt klare Grenzen. Er verbietet die Echtzeit-Gesichtserkennung im öffentlichen Raum weitgehend. Ausnahmen gelten nur für spezielle Fälle wie die Suche nach vermissten Personen, die Abwehr einer unmittelbar drohenden Terrorgefahr oder die Identifizierung von Verdächtigen schwerer Straftaten. Die nachträgliche Auswertung von Aufnahmen ist unter strenger richterlicher Kontrolle möglich.

Oft wird Echtzeit-Erkennung als besonders invasiv betrachtet. Allerdings werden bei solchen Systemen nicht benötigte Daten sofort verworfen, während retrospektive Analysen auf gespeichertes Material zugreifen. Entscheidend ist deshalb nicht das Verfahren, sondern der Kontext und die Art des Einsatzes. Echtzeit-Systeme müssen auf eng begrenzte Fahndungslisten beschränkt bleiben.

Neben gesetzlichen Vorgaben braucht es klare interne Leitlinien. Organisationen sollten fest definieren, wer Entscheidungen



Organisationen sollten fest definieren, wer Entscheidungen trifft, wie Treffer geprüft werden und wie Daten gelöscht werden

trifft, wie Treffer geprüft werden und wie Daten gelöscht werden. Das Vier-Augen-Prinzip bietet sich an: Eine Zuordnung sollte stets von mindestens zwei Fachpersonen verifiziert werden. Protokollierungen und klare Aufbewahrungsfristen gehören ebenfalls dazu. Eine Speicherdauer von 30 Tagen erscheint angemessen, sofern kein laufendes Ermittlungsverfahren besteht.

Einheitliche Standards würden den verantwortungsvollen Einsatz in verschiedenen Ländern erleichtern. Gesichtserkennung ist ein Werkzeug zur Unterstützung schneller Entscheidungen. Sie ersetzt keine menschliche Prüfung.

Geteilte Verantwortung

Staatliche Stellen schaffen den rechtlichen Rahmen, doch Technologieunternehmen tragen ebenfalls Verantwortung. Sie sollten klare Verhaltenskodizes etablieren, offen über Grenzen ihrer Systeme informieren und ihre Kunden schulen. Außerdem müssen sie bereit sein, Geschäftsangebote abzulehnen, die nicht den eigenen ethischen Standards entsprechen, selbst wenn diese rechtlich zulässig wären.

Darüber hinaus ist es wichtig, dass Unternehmen aktiv mit politischen Entscheidungsträgern zusammenarbeiten. Nur so können Regelwerke entstehen, die sowohl die Chancen als auch die Risiken neuer Technologien realistisch abbilden.

Gesichtserkennung sollte ein sorgfältig reguliertes Instrument bleiben. Sie gehört in Situationen, in denen große Gefahren bestehen. Mit klaren Vorgaben und einer verantwortungsvollen Anwendung lässt sich ein Gleichgewicht zwischen technischer Entwicklung und dem Schutz der Privatsphäre erreichen. GIT

Milestone Systems
www.milestonesys.com

© Bilder: Milestone Systems

Die Hardwarekomponenten von Blue Evo sind besonders robust und widerstandsfähig

ZUTRITT

Ganzheitlicher Ansatz

Kritis: Lösung für physischen Schutz, IT-Sicherheit und Zutrittsverwaltung

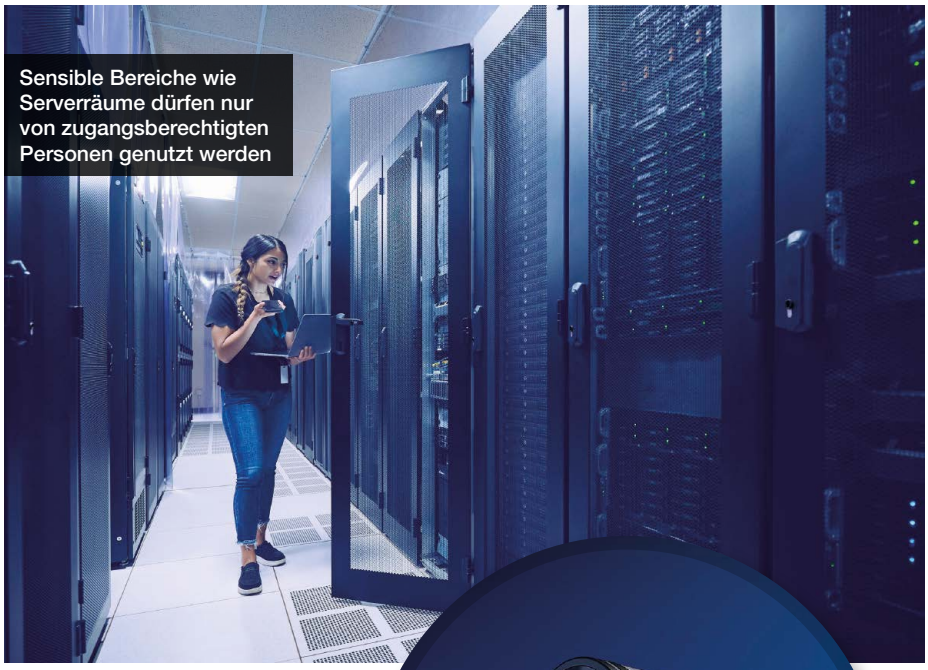
Ein mehrtägiger Stromausfall in Berlin hat Anfang des Jahres gezeigt, wie verwundbar die zentrale Energieversorgung in Deutschland ist. Verantwortlich dafür war ein gezielter Angriff auf Teile der kritischen Infrastruktur. Der physische Schutz sensibler Einrichtungen wird zunehmend zur konkreten Aufgabe für Betreiber, nicht nur im Bereich der IT, sondern auch bei der Zutrittsorganisation und der Gebäudesicherung. Eine Lösung bieten elektronische Schließsysteme wie Blue Evo von Winkhaus.

Geht es um die Sicherheit kritischer Infrastrukturen, steht häufig die Cyber-Sicherheit im Mittelpunkt. Doch auch unbefugter Zutritt zu Gebäuden, Immobilien und sensiblen Bereichen stellt ein erhebliches Risiko dar – mit potenziell weitreichenden Folgen für die Versorgungssicherheit und Betriebsabläufe. Vor diesem Hintergrund müssen Betreiber ihre Sicherheitskonzepte regelmäßig überprüfen und anpassen. Gerade bei wechselnden Dienstleistern, unterschiedlichen Nutzergruppen und hoher Personalfluktuation stoßen mechanische Systeme dabei oftmals an ihre Grenzen.

NIS-2-Richtlinie erhöht Sicherheitsanforderungen

Elektronische Schließsysteme wie Blue Evo von Winkhaus bieten hier Vorteile: Sie ermöglichen eine zentrale Verwaltung von Zutrittsrechten, schnelle Anpassungen bei Personalwechseln und eine transparente Dokumentation aller Zugangsereignisse. Mithilfe der Software BE Blue Control lassen sich Berechtigungen zeitlich und räumlich differenziert steuern. Bei Schlüsselverlust kann das Identmedium sofort gesperrt werden – ohne dass Hardware kostenintensiv ersetzt werden muss. Dank sogenannter Virtual Network Hubs werden Änderungen ohne manuellen Aufwand umgehend wirksam.

Zusätzlich erhöht die europäische NIS-2-Richtlinie die Anforderungen an die Sicherheit kritischer Einrichtungen.



Sensible Bereiche wie Serverräume dürfen nur von zugangsberechtigten Personen genutzt werden

Für Kritis ist es besonders wichtig, Zutrittsereignisse jederzeit nachverfolgen zu können. Dafür bietet Blue Evo unterschiedliche Möglichkeiten

Betreiber müssen nachweisen, dass sie geeignete Maßnahmen zum Schutz vor physischen und digitalen Sabotageakten ergreifen. Elektronische Zutrittsorganisationen können dabei unterstützen, diese Vorgaben effizient umzusetzen. Blue Evo überzeugt dabei sowohl softwareseitig als auch durch seine robuste Hardware: Zylinder, Beschläge und Zutrittsleser halten dank flächenbündiger Installation selbst hohen mechanischen Belastungen und Manipulationsversuchen stand.

Netzwerkausfälle können kompensiert werden

Auch im Ernstfall verbessert eine moderne Schließanlage die Betriebssicherheit. Die digitale Verwaltung funktioniert zeitweise ohne Netzwerkverfügbarkeit. In den Zutrittskontrollzentralen und Aufbuchlesern können Zutrittsberechtigungen vorsorglich gespeichert werden, sodass auch bei Netzwerkunterbrechungen der Zugang für bis zu 31 Tage gewährleistet bleibt. Sensible Daten werden darüber hinaus durch die eingesetzte Sicherheitsarchitektur zuverlässig geschützt. Sie verhindert unberechtigte Zutritte und bietet einen hohen Schutz vor Hackerangriffen.

„Mit Blue Evo verfolgen wir einen ganzheitlichen Ansatz für Anwendungen in sicherheitskritischen Bereichen“, so Dr.-Ing. Volker Brink, Leiter Produktmanagement Zutrittsorganisation bei Winkhaus. „Neben technischen Schutzmaßnahmen war es uns wichtig, eine Lösung zu entwickeln, die Betreiber bei der Erfüllung regulatorischer Anforderungen unterstützt. Gleichzeitig war unser Ziel, die Systeme möglichst automatisiert und einfach bedienbar zu gestalten.“

In der Praxis bewähren sich elektronische Schließsysteme unter anderem bereits bei Versorgungsunternehmen, kommunalen Institutionen und in der Logistikbranche. Die aktuellen Maßnahmen der Bundesregierung verdeutlichen, dass elektronische Zutrittslösungen künftig eine noch größere Rolle beim Schutz kritischer Infrastrukturen spielen werden. Für Betreiber werden moderne Schließanlagen somit zu einem zentralen Bestandteil ganzheitlicher Sicherheitskonzepte. GIT

Winkhaus
www.winkhaus.com

VIDEO

Nichts verpassen

13MP AI-Panoramakamera für eine Überwachung ohne tote Winkel

Hanwha Vision hat seine PNM-A13022RV vorgestellt, die neueste Ergänzung zu der Multi-Sensor-Kamera-Reihe. Mit einem horizontalen Sichtfeld von 194° und einer vertikalen Abdeckung von 93° erfasst die AI-Panoramakamera weitläufige Szenen mit weniger toten Winkeln, wodurch sie sich insbesondere für große offene Bereiche, komplexe Einrichtungen oder Außenumgebungen eignet. Diese weite Abdeckung reduziert den Bedarf an mehreren Kameras, senkt die Systemkosten und vereinfacht das gesamte Überwachungsmanagement.

Die PNM-A13022RV ergänzt die Multi-Sensor-Kamera-Reihe von Hanwha

Die PNM-A13022RV verwendet drei Bildsensoren, um ein Panoramabild zu erstellen, was zu weniger Nahtlinien führt als Panoramabilder, die aus vier Bildern bestehen. Bildverzerrungen werden in Echtzeit automatisch an den Nahtlinien angepasst, was ein durchgehend nahtloses Bild gewährleistet.

Die Kamera verfügt auch über eine horizontale Verzerrungskorrektur. Aufgrund der optischen Eigenschaften des Weitwinkel-Sichtfelds in Panoramakameras tritt oft eine Bildverzerrung auf, die den Horizont gekrümmt erscheinen lässt. Die PNM-A13022RV unterstützt die horizontale Verzerrungskorrektur, so dass Benutzer eine Referenzlinie festlegen können, um diesen Effekt zu korrigieren.

Die WiseIR-Technologie ermöglicht klare Bilder unter schlechten Lichtverhältnissen auf einer sichtbaren Länge von bis zu 20m über vier individuelle Zonen mit automatischer und manueller Pegelanpassung.

Flüssige, detailreiche Videobilder

Im Kern der Leistung der PNM-A13022RV steht ihre hochauflösende 13MP-Kamera, die mit 30 FPS arbeitet und so ein flüssiges, detailliertes Video liefert, das schnell bewegte Objekte und kritische Ereignisse mit Klarheit erfasst. Integrierte KI-Funktionen ermöglichen die Objektklassifizierung, Bewegungserkennung und erweiterte Analysen in voller 30fps, einschließlich Personen-, Fahrzeug- und Kennzeichenerkennung. Geschäftsintelligenz – einschließlich Personen-, Fahrzeug- und Menschenzählung, Warteschlangenmanagement und Heatmap – wird von der KI-Engine angetrieben. Metadatenattribute wie Geschlecht, Alter, Gesichtsmaske, Brille, Fahrzeugtypen und -farben und Kleidungsfarben werden direkt an Ihr Videomanagementsystem übertragen, was die forensische Suche vereinfacht und es Sicherheitsteams ermöglicht, schnell auf Vorfälle zu reagieren.

Datenschutz und Cybersicherheit

Die Kamera enthält auch Datenschutz- und Cybersicherheitsmaßnahmen zum Schutz sensibler Daten, mit FIPS 140-3 Level 3 Zertifizierung, sicherem Booten und verschlüsselter Speicherung, um eine robuste Geräteintegrität zu gewährleisten. Organisationen können die Kamera mit Zuversicht in sensiblen oder regulierten Umgebungen einsetzen, in dem Wissen, dass betriebliche Effizienz und Compliance gewahrt bleiben.

Die Konnektivität und Verwaltung werden durch integrierte Cloud-Unterstützung, Wi-Fi-Direktinstallation und Kompatibilität mit großen VMS-Plattformen vereinfacht, was eine Fernüberwachung, Konfiguration und nahtlose Integration in bestehende Sicherheitssysteme ermöglicht. Das robuste, wetterfeste Gehäuse der Kamera mit IK10-Schlagfestigkeit und IP66-Eindringungsschutz gewährleistet einen zuverlässigen Betrieb auch unter harten Außenbedingungen. GIT

Hanwha Vision
www.hanwhavision.eu

© Eizo

Eizo bringt IP-Decoder-Monitor auf den Markt

Eizo stellt mit dem DuraVision FDF2731 W-IP die neueste Generation seiner IP-Decoder-Bildschirme für Sicherheit und Überwachung vor. Bereits seit 2014 bietet das Unternehmen innovative Videoüberwachungsprodukte an, die zum effektiven Schutz von Personen, Unternehmen und Infrastruktur eingesetzt werden können. Ein umfassender Ansatz zu einer notwendigen, physischen Sicherheit geht meist mit Komplexität von Systeminstallation, Cybersicherheit und Wartungsanforderungen einher. Rasante technologische Fortschritte können dabei für Nutzer, Integratoren und Berater eine Herausforderung darstellen. Computerlos zeigt der DuraVision FDF2731 W-IP per Netzwerk übertragene Videostreams an. Weder Software noch andere Hardware sind für den Full-HD-Decoder-Monitor erforderlich. Das bedeutet eine leichte Installation, wenig Pflege sowie wenig Zeit- und Arbeitsaufwand.

www.eizo.de

S-ToP 2026: Security Team of Professionals Netzwerkveranstaltung

Das Security Team of Professionals hat mit einer exklusiven Netzwerkveranstaltungsreihe zum Thema „Vernetzt! Vorausschauend! Sicher!“ erneut Fachleute der Sicherheitsbranche zusammengebracht, das teilt Dallmeier mit. Sicherheitsverantwortliche, Systemintegratoren, Planer und Entscheider erhielten an drei Standorten in Deutschland die Gelegenheit, sich mit führenden Herstellern über aktuelle Entwicklungen moderner Sicherheitslösungen auszutauschen. Führende Hersteller – AG Neovo, Dallmeier electronic, Milestone Systems, Raytec, Vomatec, G&D und VuWall – bündelten innerhalb von S-ToP ihr Know-how. Die S-ToP Veranstaltungsreihe stand dieses Jahr unter dem Motto „Vernetzt! Vorausschauend! Sicher!“.

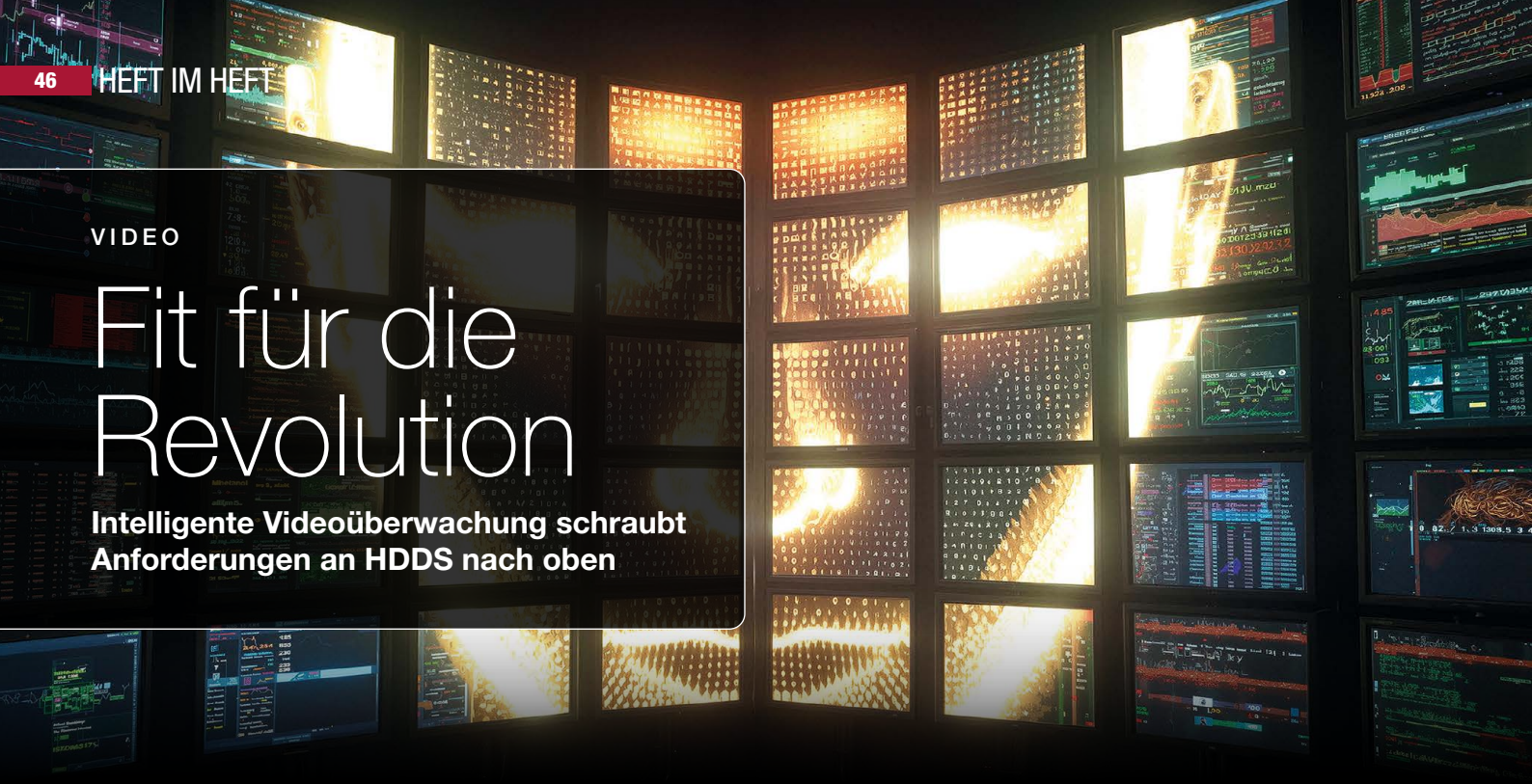
www.dallmeier.com

Cloud-basierte Appliance Cloudlink 2210

Die cloud-basierte Appliance Cloudlink 2210 von Genetec wurde für komplexe unternehmensweite Implementierungen entwickelt und adressiert die praktischen Herausforderungen, denen Unternehmen bei der Einführung eines cloud-basierten Modells in großem Maßstab gegenüberstehen: Dazu zählen etwa Speicherkosten, die Kompatibilität mit bestehenden Geräten, die keine direkte Cloud-Konnektivität ermöglichen sowie die Notwendigkeit, den lokalen Betrieb bei Verbindungsunterbrechungen aufrechtzuerhalten. Dank seines stapelbaren 2U-Rack-Designs erlaubt Cloudlink 2210 großen Organisationen, cloud-basierte Sicherheit auch in stark ausgelasteten, geschäftskritischen Umgebungen auszubauen, ohne bestehende Infrastrukturen grundlegend zu verändern. Wie die übrigen Produkte der Genetec Cloudlink-Reihe unterstützt das Modell 2210 multiple Workloads, darunter Videomanagement, Zutrittskontrolle und Einbruchserkennung, in einer einzigen Appliance.

© Genetec

www.genetec.de



VIDEO

Fit für die Revolution

Intelligente Videoüberwachung schraubt Anforderungen an HDDS nach oben

Künstliche Intelligenz verändert die Videoüberwachung grundlegend. Ob in der Fertigung, im Handel oder in anderen Branchen – KI-basierte Analysen machen Prozesse effizienter, erkennen Muster in Echtzeit und unterstützen bei wichtigen Entscheidungen. Gleichzeitig wächst die Datenmenge rasant, wodurch moderne Überwachungssysteme vor neue technische Anforderungen gestellt werden. Ein Kommentar von Rainer W. Kaese, Senior Manager, HDD Business Development bei Toshiba Electronics Europe.

© Toshiba

Künstliche Intelligenz revolutioniert gerade die Videoüberwachung und erschließt ihr ganz neue Anwendungsbereiche. In der Fertigung lassen sich KI-basierte Videoanalysen beispielsweise nutzen, um automatisiert Beschädigungen an Produkten zu erkennen, Teile zu tracken oder analoge Anzeigen abzulesen. Im Handel wiederum erlaubt die Auswertung von Videomaterial mit KI unter anderem, vergriffene und falsch platzierte Waren im Regal in Echtzeit aufzuspüren oder Mitarbeiter zu benachrichtigen, wenn sich Kunden im Kassenbereich stauen.

Die Flut an neuen Anwendungsfällen geht jedoch mit einer Flut an Daten einher und stellt Überwachungssysteme vor ganz neue Herausforderungen. Zum einen zeichnen Unternehmen mehr und mehr Daten auf und speichern diese – zumindest teilweise – auch länger als bisher, um ihre KI-Modelle regelmäßig mit neuen Situationen nachtrainieren zu können. Angesichts hochauflösender Kameras mit bis zu 8 K, die 100 Mbit/s und mehr liefern, müssen größere Datenmengen als je zuvor zuverlässig aufgefangen werden. Zum anderen kommen zu den hohen sequentiellen Schreiblasten nun auch viele zufällige Lesezugriffe, wenn Videos für KI-Analysen oder KI-Trainings abgerufen werden.

Wirtschaftlich speichern mit HDDs

Was sich im ersten Moment nach einem Szenario für SSDs anhört, ist nach wie vor ein typischer Anwendungsfall für HDDs. Nur sie sind in der Lage, die riesige Datenflut wirtschaftlich zu speichern – zumal das Schreiben sequentieller Datenströme ohnehin eine ihrer Stärken ist und ihnen auch das regelmäßige Überschreiben des Videomaterials nichts ausmacht. Unternehmen sollten allerdings darauf achten, zu den für den KI-Einsatz entwickelten Surveillance-Modellen zu greifen, da diese für die speziellen Anforderungen des KI-Zeitalters optimiert sind. Sie bieten Kapazitäten von über 20 TB und kommen mit bis zu 64 Videostreams sowie bis zu 32 KI-Streams zurecht.

Dafür sorgen etwa Verbesserungen am Vibrationsschutz, durch den die Geschwindigkeit in Systemen mit mehreren Laufwerken seltener aufgrund unerwünschter Schwingungen gedrosselt werden muss, sowie spezielle Mechanismen zur Fehlerkorrektur, die Frame-Verluste bei hohen KI-Arbeitslasten verhindern.

Darüber hinaus sind Surveillance-HDDs äußerst robust und zuverlässig, sodass sie sich für geschäftskritische Anwendungen eignen, zu denen viele der neuen KI-Use-Cases zählen. Unternehmen können sich darauf verlassen, dass ihre wertvollen Videodaten korrekt aufgefangen werden und jederzeit für die unterschiedlichsten Auswertungen abrufbar sind. GIT

Toshiba Electronics Europe GmbH (TEE)
www.toshiba-storage.com

Schneider Electric modernisiert Videoüberwachung mit Genetec

Schneider Electric hat seine Videoüberwachung mit der Plattform Genetec Security Center modernisiert und vereinheitlicht. Als global führendes Unternehmen im Bereich Energie und Automatisierung beschäftigt Schneider Electric fast 160.000 Mitarbeiter, davon 15.000 in Frankreich, verteilt auf über 100 sehr unterschiedliche Standorte. Dazu zählen Vertriebsniederlassungen, Bürogebäude sowie Industrieanlagen mit erhöhtem Schutzbedarf. Diese Vielfalt erfordert flexible Sicherheitskonzepte, die standortspezifische Risiken berücksichtigen und gleichzeitig einen reibungslosen Betrieb gewährleisten.

Vor der Einführung der neuen Plattform nutzte Schneider Electric ein proprietäres Videosystem, das mit der Zeit den wachsenden Anforderungen an eine moderne Sicherheitsinfrastruktur nicht mehr genügte. Um die physische Sicherheit zu vereinheitlichen und gleichzeitig die betrieblichen Besonderheiten einzelner Standorte zu berücksichtigen, entschied sich das Unternehmen für eine grundlegende Überarbeitung der Strategie.

Schneider Electric, auf der Suche nach einem neuen Technologiepartner, setzte auf die Beratung durch Fiducial, das die Lösungen von Genetec für die Standorte in Frankreich vorschlug. Ausschlaggebend waren insbesondere die offene Architektur von Genetec Security Center in Verbindung mit dem IP-basierten Videomanagementsystem Omnicast. Beide ermöglichen es, bestehende

© Genetec | architecture Groupe-6 | image Laurent Perreau

Kamerasysteme weiter zu nutzen und neue Komponenten schrittweise zu integrieren.

Für die Überwachung setzt Schneider Electric eine mehrstufige Strategie um. Kleine Standorte werden aus der Ferne überwacht, an mittleren Standorten ergänzen Sicherheitskräfte vor Ort die Überwachung, während kritische Standorte rund um die Uhr betreut werden. Die Systeme aller Standorte werden über eine zentrale Leitstelle überwacht.

Dabei kommt die Federation Technologie von Genetec zum Einsatz, mit der Sicherheitssysteme über eine gemeinsame Benutzeroberfläche zusammengeführt werden. Diese zentrale Sicht vereinfacht die Koordination, die Analyse von Vorfällen und die Reaktion auf Sicherheitsereignisse.

www.genetec.de

Ajax präsentierte auf seinem jüngsten „Special Event“ u.a. zwei neue Produktlinien für Videoüberwachung

KOMPLETTSYSTEME

„Dare to be first“

Ajax Special Event 2025

Im November 2025 stellte Ajax Systems einem internationalen Fachpublikum seine neuesten Entwicklungen vor. Das Event brachte live und online Fachleute aus 35 Ländern zusammen. Im Mittelpunkt standen Lösungen für drahtlosen Hochsicherheits-Einbruchschutz, skalierbare Videoüberwachung und neue Hub-Zentralen für Projekte unterschiedlicher Größenordnung.

Ein zentrales Highlight war die Vorstellung des nach Angaben des Herstellers weltweit ersten drahtlosen Grade 3-Einbruchschutzsystems. Damit soll die drahtlose Technologie den strengsten Sicherheitsstandards entsprechen und sich für Hochrisikostandorte eignen. Das System umfasst Bewegungs- und Öffnungsmelder, Bedienteile, Sirenen, Paniktasten, Signalverstärker, Integrationsmodule sowie die Hub-Zentrale Superior Hub G3 Jeweller. Die Kommunikation erfolgt über die neue Funktechnologie Superior Jeweller, die Reichweite, Stabilität und Sabotageschutz verbessern soll.

Videoüberwachung: Baseline und Superior

Ajax präsentierte zwei Produktlinien für Videoüberwachung. Die „Baseline“ kommt mit HLVF-Kameras mit motorisiertem Varifokalobjektiv und Autofokus für flexibles Zoomen. Ergänzt wird das Portfolio durch die NVR H2D-Serie mit zwei Festplatten, redundanten Aufzeichnungsoptionen und PoE-Modellen für bis zu 16 Kameras.

Die „Superior“-Reihe besteht aus Kameras mit Hybridbeleuchtung, verbessertem CMOS-Sensor und motorisiertem P-Iris-Objektiv – sie sollen detailreiche Aufnahmen bei allen Lichtverhältnissen liefern. Zwei-Wege-Audio und integrierte Lautsprecher ermöglichen aktive Abschreckung. Die neuen Superior NVRs verfügen über KI-Funktionen, unterstützen bis zu 32 Kanäle und bieten Speicherkapazitäten von bis zu 24 TB.

Mit dem Superior MegaHub stellte Ajax seine bislang leistungsfähigste Hub-Zentrale vor. Sie unterstützt bis zu 999 Geräte, bietet zertifizierten Sabotageschutz und ist für große Projekte wie Einkaufszentren oder Industrieanlagen konzipiert. Neben 100 Gruppen und 100 Automatisierungsszenarien können bis zu 1000 Benutzer verwaltet werden.

Für mittelgroße und große Projekte wurde der Superior Hub Hybrid 2 vorgestellt. Er unterstützt bis zu 250 Geräte, 25 Gruppen und 64 Automatisierungsszenarien. Damit verdoppelt sich die Kapazität gegenüber dem Vorgängermodell. Auch dieses Gerät ist nach Grade 3 zertifiziert.

Mit der EN54 Line führt Ajax eine vollständig drahtlose kommerzielle Brandwarnanlage vor

Der „Superior Megahub“ ist die bislang leistungsfähigste Hub-Zentrale von Ajax

Perimeterschutz mit Vorhangbewegungsmeldern

Das Baseline-Portfolio für den Außenbereich wurde um zwei neue Vorhangbewegungsmelder erweitert: Curtain Outdoor Mini Jeweller für schmale Bereiche wie Fenster oder Türen, mit präziser Erkennung und Haustiermodus. Dazu kommt der CurtainCam Outdoor HighMount (PhOD) Jeweller, der erste Ajax-Melder mit integrierter Fotokamera zur Alarmverifizierung. PIR- und K-Band-Sensoren ermöglichen eine Voralarmfunktion.

Die ausschließlich akkubetriebene Hub-Zentrale Hub BP Jeweller erhielt ein Upgrade. Im Energiesparmodus kann sie bis zu vier Jahre mit einem Akku betrieben werden und eignet sich für Standorte ohne Stromversorgung oder Personal.

Brandwarnanlage

Mit der EN54 Line stellte Ajax eine vollständig drahtlose Brandwarnanlage vor, die für kommerzielle Projekte konzipiert ist. Laut Unternehmensangaben ermöglicht sie eine schnelle Installation ohne Programmierung und lässt sich über Apps lokal oder aus der Ferne steuern.

Weiterentwicklung der Services

Ajax Services wurden erweitert, um Installationen durch Abonnements in wiederkehrende Einnahmen zu verwandeln. Neu sind unter anderem: Ajax SIM für stabile Konnektivität, Ajax Ultra DP für bidirektionale Signalübertragung, Ajax Cloud Storage für sichere Archivierung und Ajax Photo Mode für Fotoalarmverifizierung.

Die Aktivierung kann nun direkt über Kartenzahlung in der Ajax PRO-App erfolgen. Endnutzer sollen künftig ebenfalls die Möglichkeit erhalten, Services eigenständig zu bezahlen. GIT

Ajax Systems Germany GmbH
www.ajax.systems

SERVER-SICHERHEIT

„Wir digitalisieren den Serverraum“

Assa Abloy übernimmt Kentix – Geschäftsführer Joachim Mahlstedt im Interview mit GIT SICHERHEIT

Mit der Übernahme des IoT-Security-Spezialisten Kentix durch Assa Abloy beginnt für das Unternehmen eine entscheidende Wachstumsphase. Im Gespräch erläutert Joachim Mahlstedt, Geschäftsführer der Kentix GmbH, welche strategischen Beweggründe hinter dem Zusammenschluss stehen und wie sich dadurch neue Marktchancen, technologische Skalierungspotenziale sowie internationale Vertriebswege eröffnen. Das Interview beleuchtet zudem aktuelle Entwicklungen im Bereich physische Sicherheit, Monitoring kritischer Infrastrukturen und regulatorische Anforderungen.

Joachim Mahlstedt (l.), Managing Director, und Thomas Fritz, General Manager bei Kentix

GIT SICHERHEIT: Herr Mahlstedt, mit der Übernahme von Kentix durch Assa Abloy ergeben sich viele Veränderungen und neue Perspektiven. Was waren aus Ihrer Sicht die strategischen Beweggründe für diesen Schritt – und welche Chancen ergeben sich daraus für Kentix?

Joachim Mahlstedt: Der Zusammenschluss mit Assa Abloy ist für Kentix ein strategischer Schritt, um die nächste Wachstumsphase zu ermöglichen. Unsere Technologien stoßen international auf großes Interesse, gleichzeitig erfordert der globale Markt eine entsprechend starke Präsenz. Assa Abloy bringt genau diese Reichweite mit und ergänzt die Innovations- und IoT-Kompetenz von Kentix sehr gut.

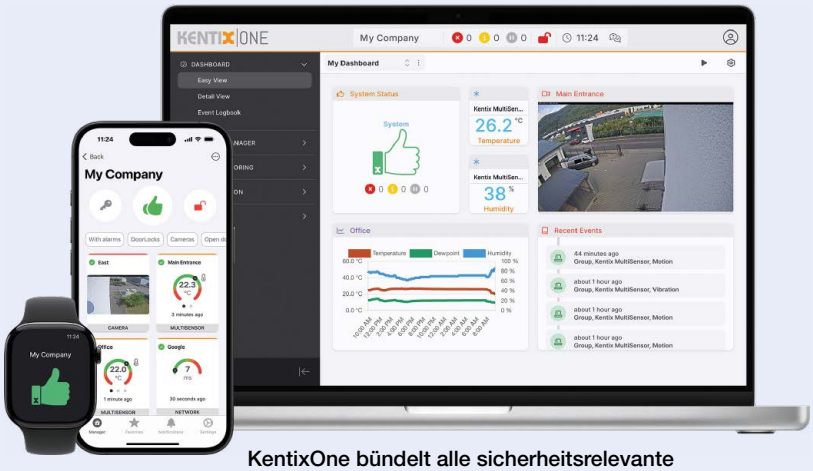
Wie verändert sich die Positionierung von Kentix im Markt durch die Zugehörigkeit zum globalen Player Assa Abloy?

Joachim Mahlstedt: Besonderen Wert legen wir darauf, die technologische Kompetenz und Agilität von Kentix beizubehalten. Technologisch eröffnen sich neue Möglichkeiten, insbesondere im Hinblick auf die Skalierung bestehender Lösungen. Themen wie Data Center, verteilte Infrastrukturen und kritische Umgebungen lassen sich durch die globale Ausrichtung von Assa Abloy schneller und breiter adressieren. Ziel ist es, die vorhandenen Technologien in international einsetzbare Sicherheits- und Infrastrukturlösungen einzubringen. Durch die Zugehörigkeit zur global agierenden Assa Abloy Gruppe stärkt Kentix seine Marktposition nachhaltig. Die Integration eröffnet Kentix den Zugang zu neuen Märkten sowie zusätzlichen internationalen Vertriebswegen und ermöglicht es, die Stärken beider Unternehmen gezielt zu bündeln. Als Teil der Assa Abloy Gruppe kann Kentix Kunden künftig noch gezielter und umfassender bedienen und seine Wachstumsstrategie auf internationaler Ebene weiter ausbauen.

Welche Entwicklungen beobachten Sie derzeit im Markt für physische Sicherheit und Monitoring kritischer Infrastrukturen, und welche Rolle spielen regulatorische Rahmenbedingungen wie der Cyber Resilience Act dabei?

Joachim Mahlstedt: Aktuell beobachten wir eine klare Verschiebung von isolierten Sicherheitslösungen hin zu integrierten Systemen, die die Bereiche physische Sicherheit, IT und Betrieb zusammenführen. Betreiber kritischer Infrastrukturen

Der steigende Bedarf an Rechenkapazitäten führt zu einer höheren Nachfrage nach hochverfügbaren, skalierbaren und gleichzeitig resilienten IT-Infrastrukturen



KentixOne bündelt alle sicherheitsrelevante Funktionen in einer durchgängigen Plattform

wollen nicht mehr nur Alarme, sondern echte Resilienz, das heißt frühzeitige Detektion, lokale Handlungsfähigkeit und nachvollziehbare Prozesse.

Regulatorische Rahmenbedingungen wie NIS2, die CER-Richtlinie und insbesondere der Cyber Resilience Act wirken dabei als starke Beschleuniger. Der CRA schreibt Security-by-Design, Update-Fähigkeit und ein professionelles Schwachstellenmanagement für vernetzte Produkte vor. Für Hersteller bedeutet das zwar höhere Anforderungen, für Betreiber jedoch mehr Transparenz, Planungssicherheit und Vertrauen in die eingesetzten Systeme. Physische Sicherheit wird damit endgültig zu einem festen Bestandteil der ganzheitlichen Sicherheitsarchitektur.

Der wachsende Bedarf an Rechenkapazitäten stellt neue Anforderungen an Rechenzentren und IT-Infrastrukturen. Welche Trends beobachten Sie im deutschen Markt, und wie bewerten Sie diese im Vergleich zu internationalen Märkten?

Joachim Mahlstedt: Auf dem deutschen Markt beobachten wir, dass der steigende Bedarf an Rechenkapazitäten vor allem zu einer höheren Nachfrage nach hochverfügbaren, skalierbaren und gleichzeitig resilienten IT-Infrastrukturen führt. Betreiber investieren verstärkt in modulare und energieeffiziente Konzepte, Edge-Rechenzentren für die lokale Verarbeitung sowie in ganzheitliche Überwachungslösungen, die physische und digitale Risiken zusammenführen. International ist der Trend ähnlich, doch Länder mit schnell wachsenden Hyperscaler-Märkten setzen noch stärker auf Automatisierung, KI-gestützte Betriebsoptimierung und cloudnahe Architekturen. Deutschland hebt sich durch seinen Fokus auf Sicherheit, Normierung und regulatorische Anforderungen ab, was zu robusteren, jedoch planungsintensiveren Lösungen führt. Betreiber profitieren letztlich von höherer Resilienz sowie von klaren Compliance- und Sicherheitsstandards.

Kommen wir mal auf das Produktportfolio von Kentix selbst zu sprechen: Welche Lösungen oder Produkte führt Kentix aktuell im Portfolio, die besonders für den White Space in Rechenzentren relevant sind?

Joachim Mahlstedt: Im White-Space-Bereich adressiert Kentix die physische Sicherheit und das Monitoring der kritischen Infrastruktur rund um Racks und technische Zonen im Rechenzentrum. Dazu zählen Lösungen zur physischen Zutrittskontrolle auf Rack- und Cage-Ebene sowie Systeme zur Überwachung von Umgebungsparametern wie Temperatur, Luftfeuchtigkeit und Luftstrom in Kalt- und Warmzonen.

Ergänzend umfasst das Portfolio Funktionen zur Leckage- und Feuchtigkeitserkennung im Rack-Umfeld sowie zur Energie- und Stromüberwachung. Alle Komponenten werden zentral über unsere IoT-Plattform KentixOne gebündelt und ermöglichen eine durchgängige Transparenz über Sicherheits-, Betriebs- und Verfügbarkeitszustände.

Welche Rolle spielen Skalierbarkeit und Systemintegration bei der Umsetzung Ihrer Lösungen?

Joachim Mahlstedt: Skalierbarkeit und Systemintegration sind zentrale Anforderungen bei der Umsetzung unserer Lösungen. Unsere Kunden betreiben in der Regel komplexe IT- und OT-Umgebungen, in die sich Sicherheits- und Monitoringlösungen nahtlos einfügen müssen.

KentixOne ist daher von Grund auf so konzipiert, dass sie sich flexibel in bestehende Infrastrukturen integrieren lässt – sei es durch offene Schnittstellen, standardisierte Protokolle oder unterschiedliche On-Premise-Betriebsmodelle wie Hardware-Appliance (SiteManager) oder containerbasierte Umgebungen (Docker). Die softwaredefinierte Architektur ermöglicht es zudem, Lösungen schrittweise zu erweitern und an wachsende oder verteilte Infrastrukturen anzupassen. Auch bei Störungen einzelner Netzwerksegmente bleiben zentrale Sicherheitsfunktionen erhalten, was insbesondere für kritische Infrastrukturen entscheidend ist.

Nicht selten stehen sich Sicherheitsanforderungen und die damit verbundenen Kosten unversöhnlich gegenüber. Welche Auswirkungen haben Ihre Lösungen auf die Kostenstruktur, den Betrieb und die Effizienz im Alltag der Anwender?

Joachim Mahlstedt: Gerade für KRITIS- und Data-Center-Betreiber ist es entscheidend, Sicherheit effizient und wirtschaftlich zu betreiben. KentixOne setzt genau hier an, indem sicherheitsrelevante Funktionen in einer durchgängigen Plattform gebündelt werden. Das reduziert Komplexität und senkt die laufenden Kosten spürbar.

Im täglichen Betrieb profitieren Anwender von klaren Prozessen und einer zentralen Steuerung aller sicherheitsrelevanten Ereignisse. Risiken lassen sich schneller bewerten, Maßnahmen gezielt auslösen und vermeidbare Einsätze reduzieren. Gleichzeitig vereinfacht ein einheitliches System den Betrieb verteilter Standorte und beschleunigt Erweiterungen.

Darüber hinaus unterstützt KentixOne die strukturierte Erfüllung von Compliance- und Audit-Anforderungen, da relevante Sicherheitsinformationen zentral verfügbar und nachvollziehbar dokumentiert sind. GIT

Kentix GmbH
https://kentix.com

PHYSISCHE SICHERHEIT

Wenn das rote Team für helle Aufregung sorgt

Fehlende Balance: „Fokus auf Cybersecurity verkennt physische Sicherheit“

„Viele Unternehmen und Behörden konzentrieren ihre Sicherheitsmaßnahmen zu einseitig auf Cybersecurity und vernachlässigen die physische Sicherheit“, sagt Kevin Heneka, Inhaber der Sicherheitsfirma Hensec. Bei Gefährdungsprüfungen, die sein Unternehmen regelmäßig durchführt, falle die ungleiche Balance immer wieder auf. „Die IT-Abteilungen haben manchmal 20 oder noch mehr Tools zur Cyberabwehr in Betrieb, aber die Sicherung des Firmengeländes lässt oftmals arg zu wünschen übrig“, berichtet der Sicherheitsfachmann aus der Betriebspraxis.

Unternehmen und Behörden sollten nach Ansicht von Kevin Heneka digitale und analoge Sicherheit zusammendenken und implementieren. Da die Gegner ganzheitlich operieren, sei auch eine 360-Grad-Abwehr notwendig, um sich vor hybriden Angriffen zu schützen. Als Beispiel nennt er die Absicherung von IT-Systemen vor physischer Sabotage. „Jede Cyberabwehr ist hinfällig, wenn der Serverraum Mängel bei den Zugangskontrollen aufweist, wie es nicht selten der Fall ist.“

Cyberkriminelle, die Sicherheitskontrollen überlisten, wollen zusehends nicht nur an digitale Daten gelangen oder diese manipulieren, sondern bereiten physische Angriffe vor, sagt Heneka. Als Beispiel nennt er „einfache Videokameras aus Fernost zur Überwachung des Firmengeländes, die leicht auszuschalten sind, um anschließend die vernachlässigte Umzäunung zu überwinden.“

Drohnen und Smart Buildings als Sicherheitsrisiken

Der Sicherheitsexperte verweist sowohl auf eine steigende Spionagetätigkeit ausländischer Geheimdienste als auch auf neue Angriffsformen etwa durch Aktivisten oder Terroristen, vor denen sich Unternehmen und Behörden schützen müssten. So seien die wenigsten Firmen auf Drohnenangriffe ausreichend vorbereitet. Dabei gebe es längst gut funktionierende, in Deutschland gefertigte Drohnen-Detektions-Systeme auf dem Markt, die ohne weiteres in ein umfassendes Sicherheitskonzept eingebunden werden können und sollten.

Als weiteren Schwachpunkt, der häufig vernachlässigt werde, benennt der Sicherheitsfachmann die Entwicklung bei den Smart Buildings. Moderne Gebäude seien ohne ein Maß an Automatisierung gar nicht mehr denkbar – dies berge jedoch auch neue Gefahrenpotenziale insbesondere für hybride Angriffsformen. So könnten Unbefugte beispielsweise durch digitale Manipulation der Zugangskontrollen wie Türschlösser, Aufzüge und andere Zugangssysteme physische Sicherheitslücken schaffen, um Gebäude zu betreten. „Unternehmen wie Behörden verlassen sich allzu häufig blind auf reine Cyberabwehr und ziehen den Fall, dass sich aus digitalen Angriffsszenarien auch oftmals gravierende Konsequenzen für die analoge Welt ergeben, gar nicht ernsthaft ins Kalkül“, so der Hensec-Chef.

Abhilfe Red Teaming

Kevin Heneka empfiehlt Firmen und Verwaltungen, sich regelmäßig einem Red-Teaming-Test zu unterziehen. Dabei agiert eine Gruppe (das „Red Team“) als hypothetischer Angreifer, um die Robustheit im Ernstfall zu prüfen und dabei Schwächen und Sicherheitslücken aufzudecken. Red Teams nutzen – in Absprache mit dem Auftraggeber – eine Vielzahl von Techniken, die von Social Engineering über physische Eindringversuche bis hin zu komplexen Cyberangriffen reichen, um Schwachstellen in der Software, in den Prozessen, in der physischen Sicherheit oder im menschlichen Verhalten aufzudecken.

Kevin Heneka: „Viele Führungskräfte sind geschockt über die gravierenden Sicherheitsmängel in ihren Organisationen, die beim Red Teaming zutage treten. Das Problem der Cybersicherheit haben praktisch alle auf dem Radar, aber die Erkenntnis, wie leicht der physische Zutritt zum Firmengelände, zur IT-Zentrale oder gar zu den Chefbüros möglich ist, sorgt regelmäßig für helle Aufregung.“ GIT

Hensec Secure Solutions
www.hensec.com

Barox Kommunikation führt KI-gestützten Produktberater ein

Mit der Einführung eines KI-basierten Produktberaters auf der Unternehmenswebsite baut Barox Kommunikation sein digitales Beratungsangebot gezielt aus. Die dialogbasierte Lösung ist rund um die Uhr verfügbar und unterstützt Geschäftskunden dabei, komplexe Produktauswahlen schneller und fundierter zu treffen. In Kürze wird sie zudem Geräte-Konfigurationsvorschläge bereitstellen, die die Inbetriebnahme effizienter gestalten. Der KI-Produktberater erfasst individuelle Anforderungen und leitet daraus präzise Produktempfehlungen ab. Der digitale Beratungsprozess auf der Website kann aufgrund der konversationsbasierten Nutzerführung im Vergleich zur klassischen Nutzung von Filterlogiken oder manuellen Recherchen deutlich vereinfacht und beschleunigt werden.

„Die beste digitale Produktberatung ist die, die zuhört", sagt Rudolf Rohr, Geschäftsführer bei Barox Kommunikation. „Unser Produktberater verbindet moderne KI-Technologie mit tiefem Produkt- und Sortimentswissen. So schaffen wir für unsere Kunden eine effizientere Entscheidungsfindung. Wir verstehen die Lösung als Ergänzung zu unserem Serviceangebot und möchten dadurch die persönliche Beratung keinesfalls ersetzen." Die Experten stünden selbstverständlich weiterhin für individuelle Fragen und Wünsche zur Verfügung, so Rudolf Rohr. Der KI-Produktberater wird laufend weiterentwickelt, kennt stets das aktuelle Sortiment und wird an Nutzerfeedback angepasst. Die Lösung ist auf den Produktseiten der Website des Unternehmens zu finden. **www.barox.de**

Markus Noga, Chief Technology Officer von Ionos, und Claudia Plattner, BSI-Präsidentin

BSI und Ionos schließen Kooperation

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und Ionos, einer der größten europäischen Anbieter von Hosting-Dienstleistungen und Cloud-Infrastrukturen mit Sitz in Montabaur, schließen eine strategische Kooperation. Ziel ist, die Sicherheit und Souveränität der digitalen Infrastruktur in Deutschland zu erhöhen. Unter anderem unterstützt Ionos in Abstimmung mit dem BSI die Bundesverwaltung beim Aufbau einer Private-Enterprise-Cloud-Umgebung. Ein weiterer Fokus der Zusammenarbeit liegt auf der Zukunftsfähigkeit kryptografischer Verfahren mit dem Ziel, sensible Daten der öffentlichen Verwaltung schon heute so zu schützen, dass sie auch gegenüber künftigen Entschlüsselungstechnologien resilient bleiben. Kooperationsvereinbarungen bieten einen verbindlichen Rechtsrahmen, um hoch vertrauliche Informationen auszutauschen und weitreichende technische Analysen durchzuführen. **www.bsi.bund.de**

TEST-REIHE

Zwischen Norm und Praxis

GIT SICHERHEIT und EPS Vertriebs GmbH untersuchen im Kundentest die Ajax Fire EN54 Brandwarnanlage

Brandwarnanlagen nach EN54 nehmen im anlagentechnischen Brandschutz eine zunehmend zentrale Rolle ein. Sie schließen die Lücke zwischen einfachen Rauchwarnmeldern und komplexen, aufgeschalteten Brandmeldeanlagen und ermöglichen eine normkonforme, strukturierte Alarmierung in zahlreichen Gebäudetypen. Insbesondere in Bildungs- und Betreuungseinrichtungen, Pflegeeinrichtungen, kleineren Sonderbauten sowie gewerblich genutzten Bestandsgebäuden bieten sie eine technisch überwachte Lösung zur frühzeitigen Branderkennung. Vor diesem Hintergrund kündigen die EPS Vertriebs GmbH und GIT SICHERHEIT einen gemeinsamen Kundentest der Ajax Fire EN54 Brandwarnanlage an, bei dem reale Anwendererfahrungen systematisch ausgewertet werden.

Die Ajax Fire EN54 Brandwarnanlage ist als vollständig funkbasiertes Brandwarnsystem konzipiert. Zentrales Element ist eine Brandwarnzentrale mit integriertem Touchdisplay, über die bis zu 200 Komponenten verwaltet werden können. Neben der lokalen Anzeige in Klartext unterstützt die Zentrale LAN , WLAN und Mobilfunkkommunikation, wodurch eine Cloud Anbindung mit kostenloser APP möglich ist.

Zum Systemportfolio gehören optische Rauchmelder mit Dual Spektral Analyse, Wärmemelder in verschiedenen Ausprägungen, manuelle Druckknopfmelder, akustische und optische Signalgeber sowie Ein und Ausgangsmodule zur Integration externer Systeme. Alle Funkkomponenten sind gemäß EN 54 25 zertifiziert, sämtliche Geräte entsprechen den jeweiligen Teilen der europäischen Normenreihe EN54.

Die Energieversorgung der Melder erfolgt batteriebetrieben. Die Auslegung ist auf mehrjährige Betriebszeiten ausgelegt, wobei der Systemstatus kontinuierlich überwacht und Störungen aktiv gemeldet werden.

Installation, Inbetriebnahme und Bedienung

Ein zentrales Merkmal des Systems ist der Verzicht auf klassische Verkabelung zwischen den Komponenten. Dadurch reduziert sich der Montageaufwand insbesondere in bestehenden Gebäuden erheblich. Die Inbetriebnahme erfolgt softwaregestützt über die bekannten Ajax Anwendungen, die sowohl für Errichter als auch für Betreiber konzipiert sind.

Die Bedienoberfläche der Zentrale setzt auf eine klare Darstellung in verständlicher Sprache. Alarm und Störmeldungen werden eindeutig zugeordnet, was insbesondere in Stresssituationen eine schnelle Orientierung ermöglichen soll. Ergänzend können berechtigte Nutzer über mobile Endgeräte informiert werden, wenn sie sich nicht im Objekt befinden.

Anwendungsbereiche und Abgrenzung

Normativ ist die Ajax-Fire EN54 als Brandwarnanlage einzuordnen und damit klar von einfachen Rauchwarnmeldern nach EN 14604 sowie von aufgeschalteten Brandmeldeanlagen abzugrenzen. Die Anwendung erfolgt gemäß DIN VDE V 0826 2 in Objekten, in denen eine frühzeitige Branddetek-


Ajax Brandwarnzentrale mit großem und intuitiv zu bedienendem Touch-Display


Produktübersicht der Ajax EN54 Brand Brandwarnanlagen

tion und strukturierte Alarmierung erforderlich ist, jedoch keine direkte Feuerwehr Aufschaltung vorgesehen ist.

Typische Einsatzbereiche sind unter anderem Kindergärten, Schulen, Pflege und Betreuungseinrichtungen, kleinere Hotels, Bürogebäude oder kommunale Einrichtungen. Gerade hier spielen Nachrüstbarkeit, geringe Eingriffe in die Bausubstanz und eine klare Alarmorganisation eine zentrale Rolle.

Alleinstellungsmerkmale im Wettbewerbsumfeld

Im Vergleich zu klassischen, drahtgebundenen Brandwarnanlagen verfolgt das Ajax System einen konsequent funkbasierten Ansatz mit vollständiger EN54 Zertifizierung – einschließlich der Funkübertragung. Die Integration weiterer sicherheitstechnischer Funktionen über kompatible Module sowie die zentrale Verwaltung über eine gemeinsame Systemplattform unterscheiden das System von vielen Insellösungen.

Hinzu kommt die Kombination aus normgerechter Technik und einer vergleichsweise kompakten Produktpalette, die auf standardisierte Anwendungsfälle ausgelegt ist und Planungs wie Installationsprozesse vereinfachen soll.

Ausblick auf den Kundentest

Der von GIT SICHERHEIT und EPS angekündigte Kundentest setzt genau an diesem Punkt an: Im Fokus stehen nicht Laborwerte oder Herstellerangaben, sondern reale Erfahrungen aus dem Betrieb. Die befragten Anwender bewerten unter anderem Installation, Alltagstauglichkeit, Bedienbarkeit, Alarmorganisation und wahrgenommene Betriebssicherheit.

Die Ergebnisse werden redaktionell ausgewertet und in einer späteren Ausgabe der Fachzeitschrift veröffentlicht. Der Vorbericht markiert damit den Auftakt zu einer praxisnahen Betrachtung moderner, funkbasierter Brandwarntechnik nach EN54.

Schulungen und Qualifizierung als ergänzender Baustein

Begleitend zur Systemtechnik bietet die EPS Vertriebs GmbH ein strukturiertes Schulungs- und Trainingsprogramm an, das sich an Facherrichter, Planer und Betreiber richtet. In der EPS-Akademie werden sowohl grundlegende als auch systemspezifische Inhalte rund um moderne Brandwarn- und Sicherheitstechnik vermittelt. Einen besonderen Schwerpunkt bilden dabei die Ajax-Brandschutz-Kompaktschulungen, in denen die normgerechte Planung, Installation, Inbetriebnahme und Bedienung der Ajax Fire EN54 Brandwarnanlage praxisnah behandelt werden. Die kompakten Präsenzformate richten sich an Anwender, die ihr Fachwissen gezielt vertiefen und sicher im Projektalltag anwenden möchten. Aktuelle Termine und Anmeldemöglichkeiten zur Ajax-Brandschutz-Kompaktschulung sind verfügbar unter:

EPS Vertriebs GmbH
www.eps-vertrieb.de

© Bilder: EPS / Ajax

Brandschutzlösungen für Sortiertechnik

In ihrem neuen Whitepaper geht die d&d Brandschutzsysteme GmbH auf die frühzeitige Detektion von Bränden in den Bereichen Sortiertechnik, Schredder und Zerkleinerungsanlagen in der Kreislaufwirtschaft ein. In Recyclingbetrieben wird täglich tonnenweise Material verarbeitet. Betreiber stehen dabei vor der Herausforderung, hochautomatisierte Prozesse unter hohem Zeitdruck sicher zu gestalten und zugleich den Brandgefahren zu begegnen, die durch die unsachgemäße Entsorgung von Lithium-Ionen-Akkus, brennbaren Materialien und mechanischer Reibung ausgehen. Das Whitepaper „Hochpräzise Flammendetektion in Recycling- und Abfallbetrieben“ zeigt auf, wie Betreiber durch den gezielten Einsatz moderner Sensortechnologie Brände frühzeitig erkennen und effektiv verhindern können. Mit den Lösungen von Det-Tronics bietet der Brandschutzspezialist die passenden Detektionslösungen für die besonderen Anforderungen der Recyclingwirtschaft. **www.dd-brandschutzsysteme.de**

© d&d Brandschutzsystem

LITHIUM-IONEN-BATTERIEN

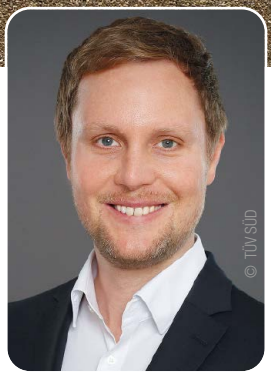
Von Fertigung bis Finishing

Risikobasierte Brandschutzstrategien in der Batterieproduktion

In den meisten Batteriespeichern sind LIB-Zellen verbaut. Risikobasierte Brandschutzkonzepte in der Herstellung schützen auch vor den Folgen thermischen Durchgehens

© Braillegrenade/Shutterstock

Die Elektrifizierung zahlreicher Prozesse hat zu einem rasanten Anstieg des Bedarfs an Speichertechnologien geführt. Besonders stark ist die Nachfrage nach Lithium-Ionen-Batterien (LIB) aufgrund ihrer technischen Überlegenheit im Vergleich zu anderen Speichertechnologien, insbesondere für mobile und dezentrale Anwendungen. In der Produktion ebenso wie später im Einsatz bestehen für diese Zellen allerdings nicht zu vernachlässigende Brandrisiken, denen Hersteller, Betreiber und Anwender am besten mit einer ganzheitlichen, risikobasierten Brandschutzstrategie begegnen. Ein Beitrag von Manuel Obert, Senior Projekt und Business Development Manager bei TÜV Süd Industrie Service.



© TÜV SÜD

Manuel Obert, Senior Projekt und Business Development Manager bei TÜV Süd Industrie Service

Die weltweite Nachfrage nach Lithium-Ionen-Batterien (LIB) wächst kontinuierlich, denn sie bieten aktuell das beste Gesamtpaket aus Energiedichte, Effizienz, Lebensdauer, Leistungsfähigkeit und Kosten. Industrielle Anwendungsgebiete dieser Technologie sind beispielsweise Batteriespeichersysteme (BESS), E-Mobilität und Unterhaltungselektronik. Schätzungen zufolge wird eine weltweite Nachfrage für Batterien von 4,2 TWh im Jahr 2030 bis zu 6,8 TWh im Jahr 2035 erwartet, wobei mehr als 85 Prozent dieser Nachfrage durch LIB gedeckt werden soll – hauptsächlich aufgrund der starken Nachfrage nach batterieelektrischen Fahrzeugen (EVs) und BESS.

Produktionsprozess und prozessspezifische Risiken

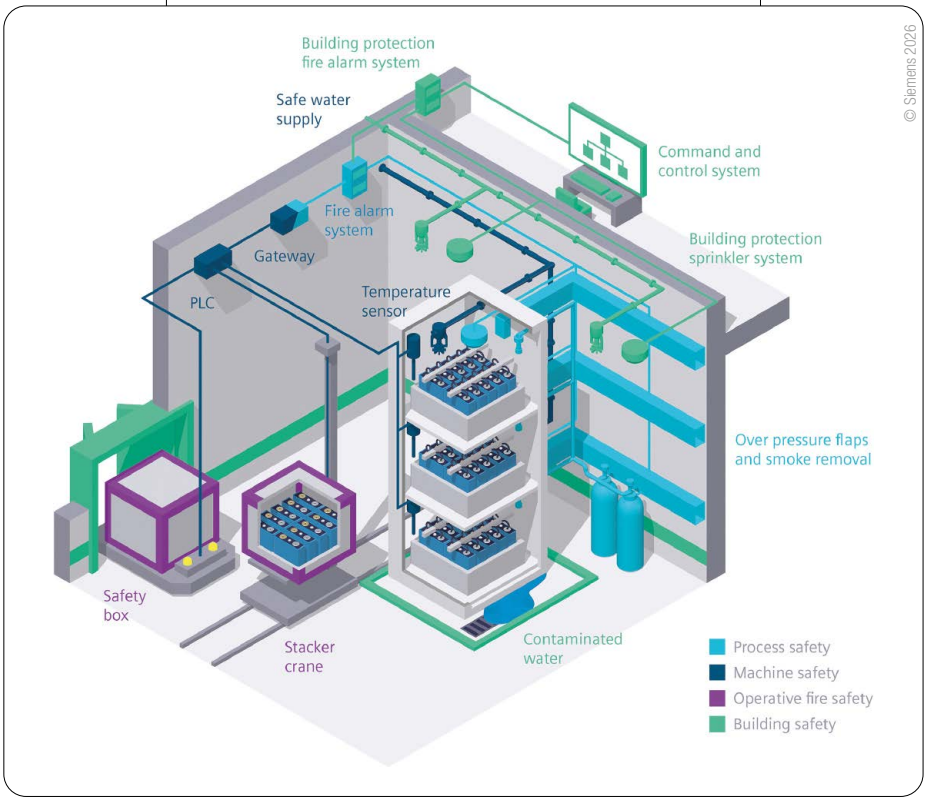
Die Produktion von LIB-Zellen umfasst die drei Hauptprozessschritte Elektrodenfertigung, Zell-Assemblierung und Zell-Finishing. Jeder birgt spezifische Brandrisiken, die einer gesonderten Analyse bedürfen. In der Elektrodenfertigung entstehen Brandrisiken insbesondere durch leicht entzündliche organische Lösungsmittel oder mechanische Funken, statische Entladungen, Staubexplosionen und Materialfehler.

Bei der Zell Assemblierung, die das Vereinzeln, Stapeln, Verpacken und insbesondere die Elektrolytbefüllung umfasst, bestehen Brandrisiken vor allem aufgrund des Einsatzes hochentzündlicher organischer Elektrolyte sowie aufgrund technischer Defekte, die zu Funkenflug oder Beschädigungen führen. Die Elektrolytbefüllung birgt ein besonders hohes Risiko, da der Elektrolyt leicht entflammbar ist und Wärmeeinträge – etwa beim Schweißen oder Kontaktieren – eine Zündung begünstigen können.

Das größte Risikopotenzial liegt im Zell Finishing, insbesondere in den Prozessschritten Formierung und Reifung (Aging). In diesen Phasen ist die Gefahr eines thermischen Durchgehens („Thermal Runaway“) am höchsten. Thermisches Durchgehen bezeichnet eine unkontrollierte, selbstverstärkende Erhitzungsreaktion innerhalb einer Zelle, die zu Feuer oder Explosion und zur Freisetzung hochgiftiger Rauchgase führen kann und in der Folge auch auf benachbarte Zellen propagieren kann. Dieser Prozess ist irreversibel, weshalb Schutzkonzepte auf Früherkennung, räumliche Trennung und Beschränkung ausgerichtet sein müssen. Jede Fehlbelastung einer Zelle – thermisch, mechanisch oder elektrisch – kann ein thermisches Durchgehen auslösen.

Die Formierung stellt den gefährlichsten Prozessschritt dar, da die Zellen hier erstmals geladen werden und Produktionsfehler aus vorhergehenden Prozessen (z. B. Separatorbeschädigungen oder eine fehlerhafte Elektrolytbefüllung) das Risiko weiter erhöhen. Während des Agings lagern viele geladene Zellen über längere Zeit ohne permanente Überwachung durch z. B. ein Batteriemanagementsystem (BMS), wodurch ein zusätzliches Brandrisiko entsteht, das gezielt adressiert werden muss.

Um den risikoreichen Formierungsprozess abzusichern, sind abgestimmte Maßnahmen aus den Bereichen Gebäude-, Prozess- und Maschinensicherheit sowie dem operativen Brandschutz erforderlich



Besonderheiten von LIB berücksichtigen

Angesichts der erheblichen Risiken, die LIB in der Produktion bergen, ist es notwendig, geeignete risikobasierte Schutzkonzepte zu entwickeln. Zwar werden alternative und innovative Batterietechnologien wie z. B. Festkörperbatterien und Natrium Ionen Batterien erprobt, doch konventionelle LIB bleiben aufgrund ihres hohen Marktanteils weiterhin vorherrschend. Hersteller müssen die spezifischen Gefährdungen der einzelnen Fertigungsschritte kennen und ihnen vorbeugen, da bereits geringfügige Defekte schwerwiegende Brandereignisse auslösen können. Anwender wiederum sollten die besonderen Risiken im Betrieb berücksichtigen, denn ein Großteil der Brände entsteht während Lade oder Nutzungsphasen.

Brandschutzkonzept und Schutzmaßnahmen

Die Risikoanalyse betrachtet deshalb die einzelnen Prozessschritte der LIB-Zellproduktion und identifiziert kritische Bereiche. Für diese werden gezielte Sicherheitsstrategien zur Vermeidung von Brandgefahren entwickelt. Die drei Bereiche des vorbeugenden Brandschutzes (baulich, anlagentechnisch und organisatorisch) müssen um Prozesssicherheit und operativen Brandschutz (z. B. prozessbedingte Notfallmaßnahmen) erweitert werden. Entscheidend für die Sicherheit ist es, kritische Prozesse baulich abzutrennen. Wenn Gefahren dank der risikobasierten Strategie frühzeitig erkannt werden, lassen sich auch die besonders kritischen Prozessschritte Zellformierung und Aging beherrschen. Hier sind zusätzliche spezifische Maßnahmen erforderlich: neben der baulichen Trennung (z. B. mit Hilfe von feuerbeständigen Trennwänden) ist der Einsatz von Lösch- beziehungsweise Sprinkleranlagen sinnvoll. Lagerung und Verpackung sollten räumlich ebenfalls von anderen Produktionsprozessen getrennt sein und über geeignete Löschvorrichtungen verfügen.

Rechtlicher Rahmen und normative Lücken

Zu den wichtigsten deutschen baurechtlichen Vorschriften für das Gebäude einer Produktionsanlage für LIB gehören die Musterbauordnung (MBO) / Landesbauordnungen, die Muster-Verwaltungsvorschrift Technische Baubestimmungen (MVV TB), Sonderbauvorschriften wie z. B. die Muster-Industriebaurichtlinie sowie über die MVV TB verbindlich anzuwendenden DIN-Normen und technische Regelwerke.

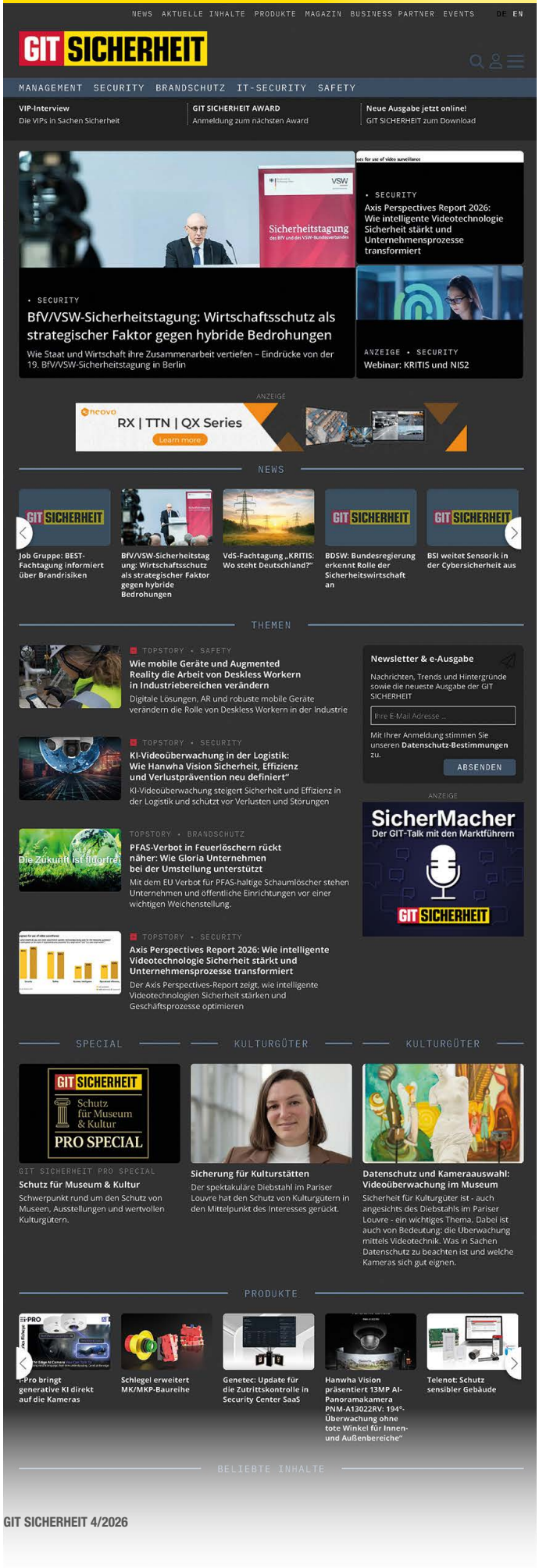
Da auf Prozess- und Maschinenebene weder die baurechtlichen Vorschriften noch nationale und internationale Regelwerke die spezifischen Brandrisiken in Verbindung mit LIB-Zellen hinreichend betrachten, beziehungsweise entsprechende Regelwerke überhaupt nicht existieren, ist ein risikobasierter Ansatz zwingend erforderlich. Eine solche Risikoanalyse nach EN ISO 19353:2019 und DIN EN ISO 12100:2011 berücksichtigt das Zusammenspiel aus Schadensausmaß, Eintrittswahrscheinlichkeit und der Möglichkeit, eine Propagation zu vermeiden.

Eine integrative, risikobasierte Brandschutzstrategie verzahnt die Gebäude-, Maschinen- sowie Prozesssicherheit eng mit dem baulichen, anlagentechnischen und organisatorischen Brandschutz. Sie ergänzt das bauordnungsrechtliche Brandschutzkonzept, das eine verpflichtende Genehmigungsunterlage ist, die sich allerdings rein auf das Gebäude bezieht.

TÜV SÜD unterstützt Hersteller von LIB sowie Planer und Betreiber von Produktionsanlagen. Gleichermaßen findet die risikobasierte Brandschutzstrategie Anwendung beim Betrieb von BESS. Das Ziel ist hierbei Risiken zu minimieren, Mitarbeitende, Investitionen und die Umwelt zu schützen und die Anforderungen aus den internationalen und nationalen Regelwerken hinsichtlich der Batteriesicherheit ganzheitlich zu erfüllen. GIT

TÜV Süd Industrie Service GmbH
www.tuvsud.com/de-is

Diesen Monat auf GIT-SICHERHEIT.de



IMPRESSUM

Herausgeber
Wiley-VCH GmbH

Geschäftsführer
Dr. Guido F. Herrmann

Senior Director, Publishing and Content Services
Dr. Katja Habermüller

Publishing Director
Dipl.-Betriebswirt Steffen Ebert

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

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

Anzeigenleitung
Miryam Reubold
+49 6201 606 127

Sales Director
Jörg Wüllner
+49 6201 606 748

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

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

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@vuservice.de
Unser Service ist für Sie da von Montag - Freitag zwischen 8:00 und 17:00 Uhr

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

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

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

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

Abonnement 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, vfdb, 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.

Druck
westermann DRUCK | pva

Printed in Germany, ISSN 2751-4536

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

WILEY

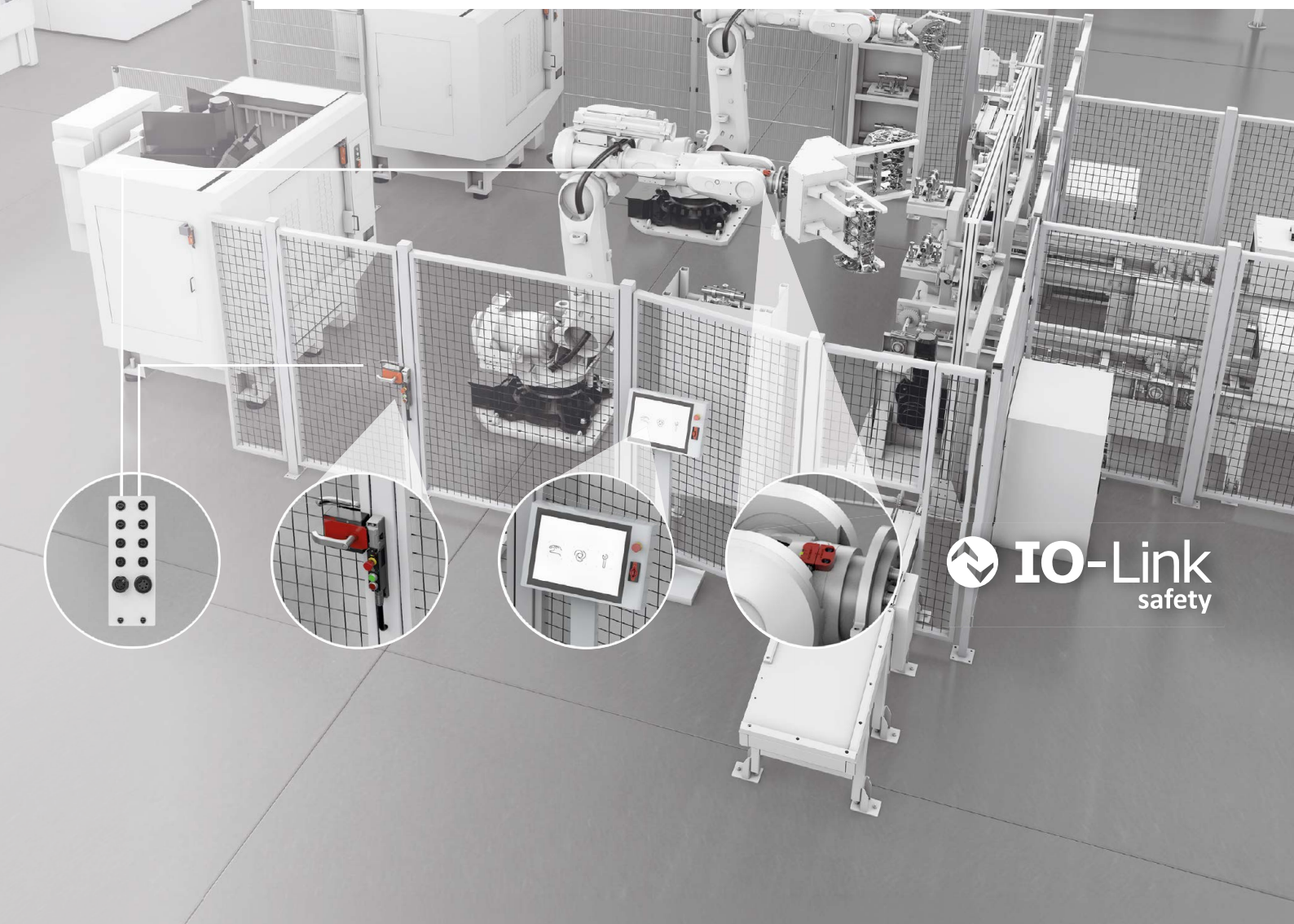
GIT SICHERHEIT

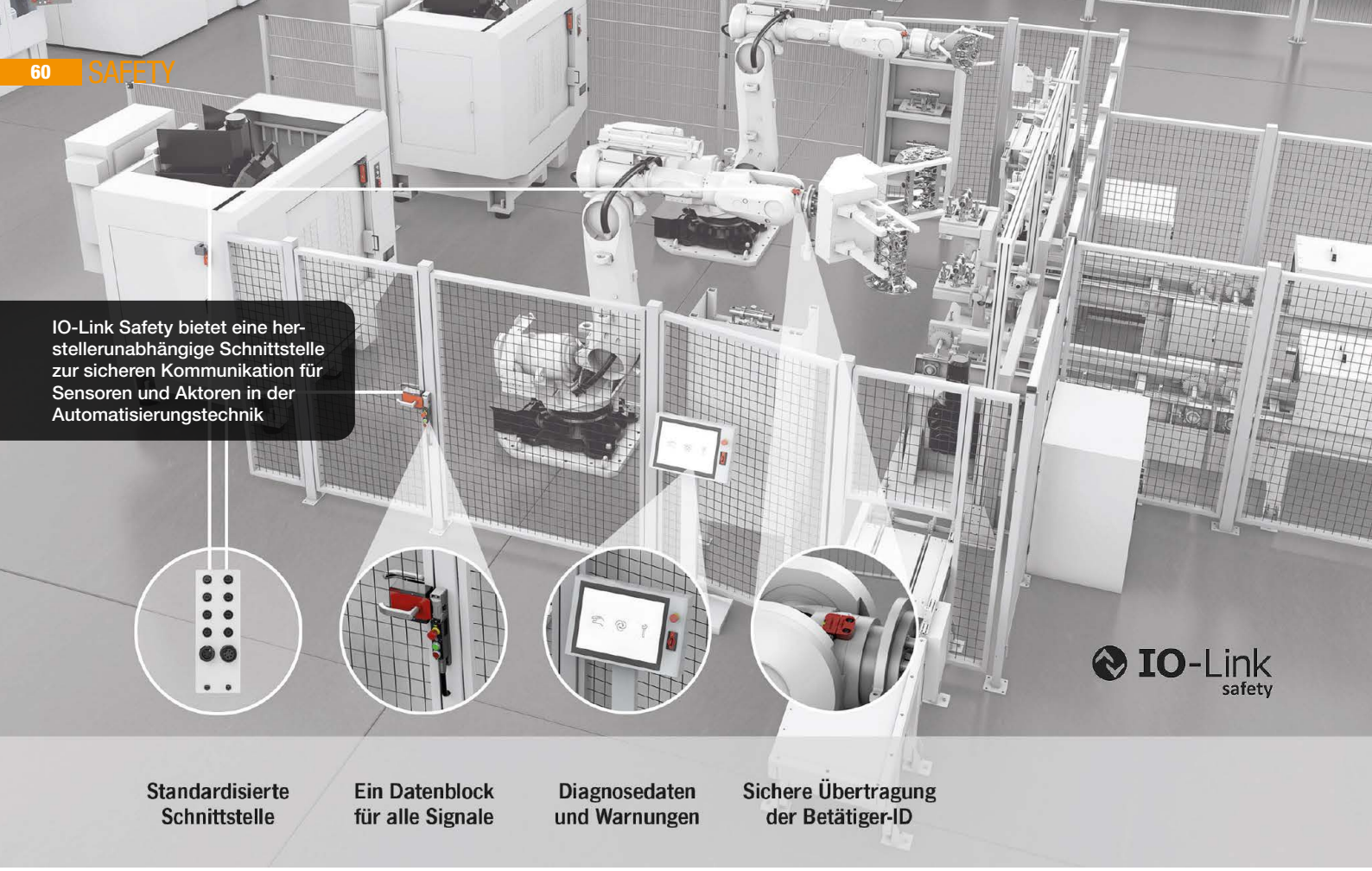
INNENTITEL – MASCHINENSICHERHEIT

EUCHNER
More than safety.

SICHER VERBUNDEN –

SICHERHEITSSCHALTER MIT IO-LINK SAFETY





IO-LINK SAFETY

Euchner geht die letzten Meter der Automatisierung

IO-Link Safety: Sicherheit mit Daten

Bildlich gesprochen, waren die letzten 20 Meter in der Automatisierung lange ein Nadelöhr: Sensoren und Aktoren mussten einzeln verdrahtet werden – je mehr Sicherheitssignale und Diagnosedaten übertragen werden sollten, desto komplexer die Verdrahtung. Euchner adressiert dieses Problem mit IO-Link Safety. Statt vieler Adern ist nur noch eine einzige Leitung notwendig, die alle relevanten Daten überträgt. Gleichzeitig entstehen zusätzliche Funktionen und mehr Kontextinformationen.

Mit IO-Link Safety vereinfacht Euchner die Kommunikation auf den letzten 20 Metern deutlich. Statt Informationen über viele einzelne Leitungen zu übertragen, kommt nun eine einzige Plug-and-Play Verbindung zum Einsatz. Das vermeidet Einzelverdrahtungen und ist insbesondere bei Sicherheitszuhaltungen an Maschinen vorteilhaft, wo viele Leitungen zusammenlaufen. Klassische Konzepte übermitteln meist nur ein digitales Signal – sicher oder unsicher, Schutztür geöffnet oder geschlossen.

Eine Leitung, mehr Informationen

IO-Link Safety ist eine Erweiterung des IO Link Protokolls. Sicherheits- und Zusatzdaten werden gemeinsam über eine Punkt zu Punkt Verbindung an einen IO-Link-Safety Master übertragen (bis SIL3 / PL e; SIL = Safety Integrity Level, PL = Performance Level).

Der Unterschied liegt nicht nur in der reduzierten Verdrahtung, sondern in einer erweiterten Funktionsebene: Statt nur sicher/unsicher zu signalisieren, liefern die Geräte zusätzliche Kontextinformationen.

Beispiele: Welcher Betätiger hat ausgelöst? Warum wurde eine Tür geöffnet? Ist die Türmechanik in Ordnung? „Mit IO-Link Safety übertragen wir Sicherheitsinformationen inklusive Kontext. Dadurch werden Funktionen möglich, die vorher technisch nicht umsetzbar waren“, erklärt Xabier Antolin, Head of Product Management bei Euchner.

Diese zusätzliche Informationsebene ermöglicht neue Maschinenkonzepte und bietet gleichzeitig umfangreiche Diagnosedaten in Echtzeit.

Gründe für IO-Link Safety

IO-Link Safety nutzt dieselbe Verbindungstechnik wie Standard IO Link. Anwender benötigen lediglich einen geeigneten IO-Link Safety Master. Damit entsteht ein durchgängiger Standard für unterschiedlichste Geräte – von einfachen Sensoren bis zu komplexen Sicherheitszuhaltungen.

Neue Funktionen wie die sichere Übertragung von Betätiger ID, Schlüsseldaten oder Mechanik Status liefern Informationen, die mit klassischer Verdrahtung nicht verfügbar waren. Der Planungs- und Installationsaufwand sinkt: Eine Leitung ersetzt viele Einzeladern. Geräteparameter lassen sich per IO-Link Safety übertragen, sodass der Austausch von Komponenten ohne lange Stillstandszeiten möglich ist.

Zusätzlich stehen umfangreiche Zustandsdaten und Diagnoselogs in Echtzeit bereit. Anwender erkennen nicht nur, dass Fehler auftreten, sondern auch deren Ursache. Das reduziert Stillstandszeiten und erleichtert gezielte Wartung.

Sichere Kommunikation über Standard Leitungen

Technisch basiert IO-Link Safety auf dem sogenannten Black Channel Ansatz. Dabei werden Sicherheitsdaten über einen physikalisch unsicheren Kanal übertragen, jedoch funktional abgesichert. Für Anwender bedeutet das, dass keine speziellen Leitungen oder zusätzliche Konfiguration erforderlich sind.

Im Vergleich zu klassischen Safety Bussystemen arbeitet IO-Link Safety mit kompakten Datenstrukturen und zyklischen Punkt zu Punkt Verbindungen. Die Reaktionszeiten fallen niedrig aus, und die Architektur bleibt übersichtlich. Euchner bietet aktuell zwei parallele Konzepte:

- Sicherheitsschalter der Baureihen BP/BR in Kombination mit einem Gateway (ESM-CB oder GWY): Nicht sichere Daten laufen über IO Link, Sicherheitssignale werden klassisch verdrahtet. Geeignet für Bestandsanlagen und Erweiterungen
- Integriertes IO-Link Safety: Sicherheits- und Zusatzdaten laufen gemeinsam über IO-Link Safety bis zum Master.

Warum jetzt damit beschäftigen?

Maschinen werden flexibler, Varianten zahlreicher und die Integrationsdichte höher. Klassische Verdrahtung begrenzt diese Entwicklung. IO-Link Safety ergänzt IO-Link um eine sichere Kommunikationsschicht und ermöglicht modulare Sicherheitskonzepte.

Maschinenbauer profitieren insbesondere bei Anlagen mit häufigen Formatwechseln, dezentralen Sicherheitsfunktionen oder hohem Diagnosebedarf – etwa im Sondermaschinenbau, in flexiblen Fertigungszellen oder der Montagetechnik. Eine standardisierte, skalierbare Sicherheitstechnik bietet Planungssicherheit und lässt sich in bestehende Steuerungslandschaften integrieren.

Know-how trifft Praxis

Euchner entwickelt seit 2008 busbasierte Sicherheitstechnik. IO-Link Safety macht transpondercodierte Sicherheitsschalter, Zuhaltungen und Schutztürsysteme kommunikationsfähig bis SIL3 / PL e. Der Fokus liegt nicht auf der Schnittstelle selbst, sondern auf der Frage, welche sicherheitsrelevanten Informationen aus den Geräten sinnvoll übertragen werden. Diese Erkenntnisse aus der Praxis fließen in die Geräteentwicklung ein.

Das erste vollständig integrierte Produkt ist der CES-C07, ein kompakter Sicherheitsschalter ohne Zuhaltung. Weitere Geräte – darunter die CTP Zuhaltungen mit IO-Link Safety – sind in Vorbereitung. „Wir bleiben nicht bei der Vereinfachung der letzten 20 Meter stehen. Wir gehen weiter bis zur sicheren, kontextreichen Kommunikation entlang der gesamten Sicherheitskette“, betont Xabier Antolin. GIT

Das erste vollständig integrierte Produkt ist der CES-C07: ein IO-Link Safety Switch, der Sicherheits- und Diagnosedaten gemeinsam überträgt und SIL3 / PL e erreicht

Euchner GmbH + Co. KG
www.euchner.com

Viele Probleme entstehen oft lange vor der eigentlichen Begehung – häufig durch Nachlässigkeit, Zeitdruck, Unwissenheit oder begrenzte Budgets

TITELTHEMA

Sieben Schritte zur reibungslosen Betriebsbegehung

Wie Anlagenbetreiber Sicherheitslücken systematisch schließen

Frank Bauder, Head of Safety Services bei Leuze

Was, wenn die nächste Betriebsbegehung morgen ansteht? Wer als Anlagenbetreiber bei diesem Gedanken nervös wird, sollte die internen Prozesse kritisch prüfen. Die gute Nachricht: Mit der richtigen Vorgehensweise lassen sich Risiken in der industriellen Automatisierung rechtzeitig vor dem nächsten Prüftermin zuverlässig erkennen und beheben – wie, erklärt Frank Bauder, Head of Safety Services bei Leuze. Außerdem im Interview mit GIT SICHERHEIT zu diesem Thema: Matthias Bristle, Produktmanager Safety Solutions bei Leuze.

Lückenlose Sicherheit an Maschinen und Anlagen ist die Grundlage für einen störungsfreien und effizienten Betrieb in der industriellen Automatisierung. Regelmäßige Gefährdungsbeurteilungen spielen dabei eine Schlüsselrolle: Sie decken Schwachstellen im sicheren Betrieb von Maschinen auf. Die Erfahrung zeigt, dass die meisten Probleme lange vor der eigentlichen Begehung entstehen – häufig durch Nachlässigkeit, Zeitdruck, Unwissenheit oder begrenzte Budgets. Leuze unterstützt Betreiber dabei, einen sicheren Betrieb mit Safety-Expertise und Safety Solutions zu erreichen. Die Unterstützung gliedert sich in sieben Schritte:

Schritt 1: Gefährdungen identifizieren

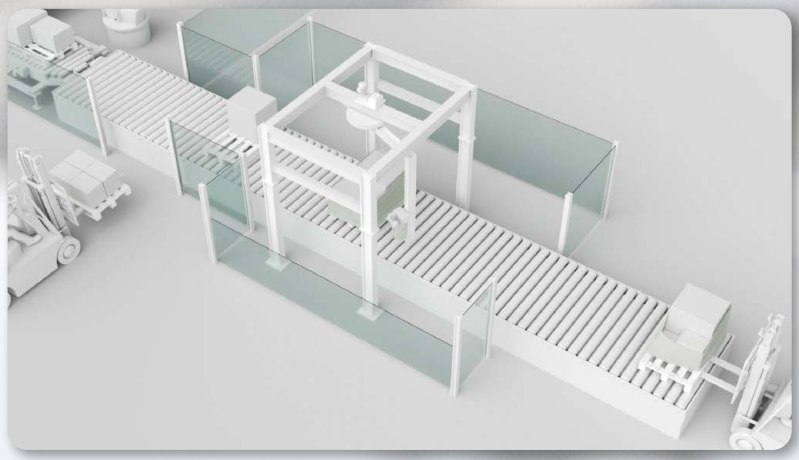
Sicherheit beginnt mit Transparenz: Alle relevanten Gefährdungen müssen identifiziert werden. Dazu gehört es, mindestens mechanische und elektrische Gefährdungen unter Berücksichtigung der Maschinengrenzen aufzunehmen. Weiterhin ist der Zustand der Schutzeinrichtungen (beispielsweise sichere Sensoren und Steuerungen) zu dokumentieren, um Manipulation und Verschleiß zu erkennen.

Ein Safety-Check von Leuze bringt hier die erforderliche Klarheit und fasst die Ergebnisse in Berichtsform zusammen.

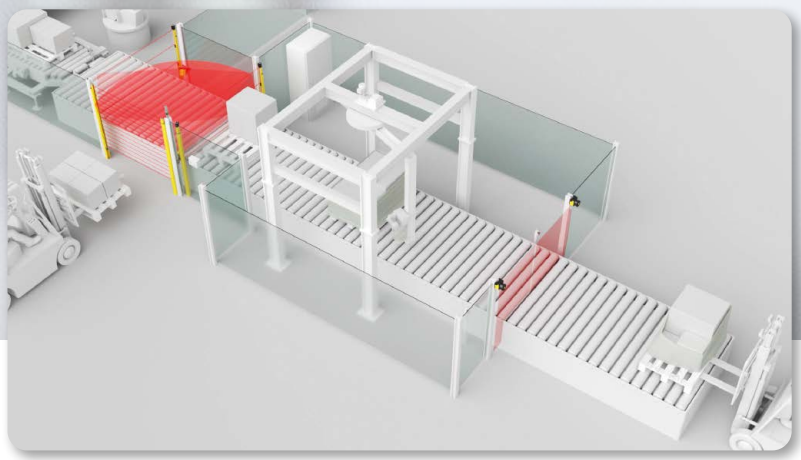
Schritt 2: Risiken beurteilen (EN ISO 12100)

Anschließend gilt es, die identifizierten Gefährdungen objektiv zu bewerten, normenkonform einzuordnen und daraus risikomindernde Maßnahmen abzuleiten. Die Risikoanalyse bildet somit die Grundlage für alle folgenden technischen Entscheidungen und Investitionen.

Die Safety-Experten von Leuze erstellen aussagekräftige Risikobeurteilungen inklusive der Entwicklung von Sicherheitsfunktionen, Empfehlung risikomindernder Maßnahmen und Beschreibung von verbleibenden Restrisiken.



▲ Schwachstellen für einen sicheren Betrieb von Maschinen und Anlagen sind nicht immer auf den ersten Blick ersichtlich. Leuze unterstützt Betreiber dabei, einen sicheren Betrieb mit Safety-Expertise und Safety Solutions zu erreichen ▶



▲ Regelmäßige Gefährdungsbeurteilungen spielen eine Schlüsselrolle für lückenlose Sicherheit an Maschinen und Anlagen

Schritt 3: Sicherheitskonzept erstellen

Das Sicherheitskonzept beschreibt die Umsetzung aller risikomindernden Maßnahmen. Es ist bestens geeignet, mit allen Beteiligten die Machbarkeit, Umsetzbarkeit und Benutzerfreundlichkeit zu diskutieren und festzulegen und somit Missverständnisse zu vermeiden.

Aus diesem gemeinsam verabschiedeten Sicherheitskonzept entwickeln die Safety-Spezialisten von Leuze die Umsetzung im Detail und die Planung von Verifikation und Validierung. Das Fundament bildet hier das umfassende Industrie- und Applikationswissen, das eine praxistaugliche und nachhaltige Umsetzung ermöglicht.

Schritt 4: Im Konzept auf Safety Solutions setzen

Klassisch wird nach dem Konzept die Umsetzung geplant und entwickelt. Alle Tätigkeiten, von der Idee über die Bauteileauswahl, die Realisierung und den Nachweis der Wirksamkeit sind pro Maschine oder Applikation komplett durchzuführen. Oft stoßen klassische Sicherheitskonzepte bei komplexen Applikationen an ihre Grenzen. So zum Beispiel durch sich ändernde Formate (wechselnde Palettenbeladungen) an Mutingstationen. In diesen Fällen sind weitergedachte Safety Solutions gefragt, die exakt auf die jeweilige Aufgabenstellung ausgerichtet sind.

Leuze bietet hierfür Lösungen, die sich gezielt an den Applikationsanforderungen orientieren – und den kompletten Prozess von der Analyse der Aufgabenstellung über die Sicherheitsarchitektur bis hin zur umfänglichen Dokumentation abdecken.

Schritt 5: Safety Solution umsetzen und in Betrieb nehmen

Entscheidend ist die Detailanalyse des gegebenen Anlagenlayouts der Applikation. Nur auf dieser Basis können die geeigneten Sicherheitskomponenten (zum Beispiel sichere Sensoren oder Schalter) bestimmt in die Applikation eindesignt und die entsprechende Geräte-Parametrierung definiert werden.

Zusätzlich sichern Inbetriebnahme und Unterweisung vor Ort durch die Safety-Experten und Produktspezialisten den Erfolg.

Schritt 6: Wirksamkeit nachweisen

Bei der Verifikation und Validierung (Proof of Concept) wird die korrekte Auslegung und Wirksamkeit aller sicherheitsrelevanten Komponenten und Funktionen durch Tests, Messungen und vollständig dokumentierte Prüfung unter Realbedingungen nachgewiesen.

Schritt 7: Dokumentieren und regelmäßig inspizieren

Alle erforderlichen Dokumente wie die Risikobeurteilung, Messberichte und CE-Konformitätserklärung werden bereitgestellt und bilden den neuen Ist-Zustand. Wiederkehrende Inspektionen der Schutzeinrichtungen und die regelmäßige Gefährdungsbeurteilung als Abgleich mit dem „Stand der Technik“ gewährleisten ein konstantes Sicherheitsniveau. Dies gewährleistet einerseits die Sicherheit für die Bediener und andererseits die Verfügbarkeit der Maschine für die Produktion über die gesamte Lebensdauer. GIT

?!

Interview

Lesen Sie auf der nächsten Seite das Interview mit Matthias Bristle, Product Manager Safety Solutions & Services, wie Betreiber Bestandsmaschinen zukunftsfähig machen

▶

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

Fit für neue Vorgaben

Wie Betreiber Bestandsmaschinen zukunftsfähig machen

Ab Mitte Januar 2027 gilt die neue Maschinenverordnung (EU) 2023/1230. Im Interview erklärt Matthias Bristle, Produktmanager Safety Solutions bei Leuze, wie Betreiber Bestandsmaschinen sicher und normkonform halten – und welche Rolle intelligente Safety Solutions dabei spielen.

GIT SICHERHEIT: Herr Bristle, was bedeutet die neue Maschinenverordnung für Betreiber von Bestandsmaschinen?

Matthias Bristle: Die gute Nachricht: Das übergeordnete Ziel bleibt unverändert – Maschinen müssen sicher betrieben werden. Neu ist jedoch, dass die Maschinenverordnung die Anforderungen an Risikobeurteilung, Nachweisführung und Dokumentation wesentlich präziser adressiert als die bisherige Maschinenrichtlinie. Genau hier kommen unsere Safety Dienstleistungen und Solutions ins Spiel: Sie sind individuell auf die jeweiligen Bedürfnisse und Applikationen zugeschnitten und sorgen für einen sicheren und rechtskonformen Betrieb. Uns ist wichtig, dass Unternehmen bei diesen Aufgaben nicht allein gelassen werden. Deshalb unterstützen wir mit umfassenden Services – von der Analyse über die Entwicklung und Integration bis zur Validierung und Dokumentation.

Wo liegen in der Praxis die größten Herausforderungen für Anlagenbetreiber, wenn Maschinen modernisiert werden müssen?

Matthias Bristle: Die Anpassung von Bestandsanlagen an neue Normen und Vorgaben ist oft eine echte Herausforderung. Häufig fehlt bereits die Transparenz darüber, welchen tatsächlichen Sicherheitsstatus der eigene Maschinenpark hat. Hinzu kommen komplexe Produktionsprozesse, Unsicherheiten über die Grenzen klassischer Sicherheitskonzepte und der ständige Zeitdruck im Tagesgeschäft. Deshalb empfehlen wir grundsätzlich einen strukturierten, methodischen Ansatz, der alle relevanten Aspekte berücksichtigt und die Umsetzung planbar macht. Entscheidend ist: Es reicht nicht aus, einfach eine Sicherheitseinrichtung zu kaufen. Man muss sie auch richtig auswählen, korrekt integrieren und ihre Wirksamkeit nachweislich validieren. Nur so entsteht am Ende eine wirklich sichere Lösung, die Mitarbeiter schützt.

Wie sieht das konkret aus, wenn Leuze bei der Nachrüstung und Validierung unterstützt?

Matthias Bristle: Wir bieten unseren Kunden einen ganzheitlichen Service – angefangen bei Safety Checks vor Ort, über normkonforme Risikobeurteilungen bis hin zu Engineering und Validierung. Unsere Expertinnen und Experten begleiten den Prozess von Anfang bis Ende: von der ersten Analyse über die Entwicklung individueller Sicherheitslösungen bis zur rechtssicheren Dokumentation und regelmäßigen Inspektionen. So entsteht ein durchgängiger Sicherheitsprozess, der alle Anforderungen abdeckt und Betreiber wirklich entlastet. Am Ende geht es darum, dass sich die Sicherheitskonzepte an die individuellen Gegebenheiten vor Ort anpassen und eben nicht umgekehrt.

Wie lässt sich denn sicherstellen, dass die getroffenen Sicherheitsmaßnahmen auch langfristig wirksam bleiben?

Matthias Bristle: Das ist ein ganz wichtiger Punkt, wenn nicht der wichtigste. Sicherheit endet nicht mit dem Projektabschluss – sie beginnt dort und muss im laufenden Betrieb aktiv gelebt werden. Stellen Sie sich vor, Sie verlassen mit Ihrem Auto das Werk oder die Werkstatt. In diesem Moment ist das Fahrzeug technisch einwandfrei, alles ist geprüft und korrekt eingestellt. Aber damit ist es nicht dauerhaft sicher. Schon nach wenigen Kilometern können sich Schrauben leicht lösen, Bremsen verschleißen oder der Reifendruck verändern.

© Asecos

Asecos zeigte Sicherheitslösungen auf der LogiMAT

Die Asecos GmbH zeigte auf der LogiMAT in Stuttgart auf seinem Messestand den Ion-Line Ultra Sicherheitsschrank für das Lagern und Laden von Lithium-Ionen-Batterien und informierte über Konzepte der normgerechten Gefahrstofflagerung im Logistikumfeld. Mit dem Ultra präsentierte der Hersteller seine Premiumlösung für das sichere Lagern und Laden von Lithium-Akkus. Der Ultra erfüllt die Vorgaben der GS-Prüfung und wurde zudem als erster Sicherheitsschrank seiner Art von der neutralen Zertifizierungsstelle ECB mit der Schutzklasse I/O90 zertifiziert – der höchsten Einstufung nach VDMA 24994:2024-08.

Der Schrank bietet 90-minütigen Brandschutz von außen nach innen und innen nach außen – getestet nach DIN EN 14470-1 sowie in Anlehnung an die DIN EN 1363-1. Er bietet außerdem Branddetektion und Alarmweiterleitung.

www.asecos.com

Matthias Bristle,
Product Manager
Safety Solutions
& Services

„Das übergeordnete Ziel bleibt unverändert – Maschinen müssen sicher betrieben werden.

Wenn man das nicht regelmäßig kontrolliert, steigt das Risiko mit jeder Fahrt – für einen selbst und für alle Verkehrsteilnehmer in der Umgebung. Genau deshalb sind regelmäßige Hauptuntersuchungen durch zertifizierte Stellen verpflichtend.

Genauso verhält es sich mit Maschinen: Auch, wenn sie zu Beginn perfekt eingerichtet und geprüft sind, ändern sich im Betrieb ständig die Rahmenbedingungen – Prozesse, Belastungen, Nutzungsverhalten oder Umgebungsfaktoren. Ohne regelmäßige Kontrolle, Anpassung und Wartung verliert selbst die beste Sicherheitslösung im Laufe der Zeit an Wirksamkeit. Sicherheit ist also kein einmaliger Zustand, sondern ein kontinuierlicher Prozess. Betreiber erhalten dazu klare Vorgaben für Prüfintervalle und können sich darauf verlassen, dass das Schutzniveau über den gesamten Lebenszyklus stabil bleibt. So erspart man sich unangenehme Überraschungen bei der nächsten Betriebsbegehung.

Anlagen werden immer komplexer. Wie beeinflusst das die Sicherheitskonzepte in der industriellen Automatisierung?

Matthias Bristle: Das stimmt, die Anforderungen steigen. Klassische Schutzkonzepte wie Muting stoßen mittlerweile bei vielen Applikationen an ihre Grenzen, zum Beispiel in Verpackungslinien mit häufig wechselnden Formaten oder bei der Absicherung von Roboterzellen an Übergabestationen mit fahrerlosen Transportsystemen: Wir setzen hier auf leistungsfähige Lösungen, die das Schutzfeld von Sicherheitslaserscannern softwaregestützt dynamisch anpassen, sodass auch bei veränderten Gegebenheiten eine lückenlose Überwachung ohne Materialflussunterbrechung erreicht wird. Solche Lösungen erfüllen höchste Sicherheitsanforderungen, ermöglichen einen produktiven, manipulationssicheren und normkonformen Betrieb und sind das Ergebnis aus jahrelanger Erfahrung in unterschiedlichen Bereichen der Maschinensicherheit.

Und welche Vorteile bringt die Zusammenarbeit mit einem externen Safety-Partner wie Leuze?

Matthias Bristle: Ich bin überzeugt, dass es in vielen Fällen effizienter ist, auf das Wissen von neutralen Safety-Experten zurückzugreifen, statt viel Zeit und Ressourcen aufzuwenden, um das erforderliche Fachwissen kontinuierlich auf dem Laufenden zu halten. Unsere Fachleute bringen umfassendes Know-how zur aktuellen Normenlage, gesetzlichen Vorgaben und branchenspezifischen Herausforderungen ein. Das lässt sich dann normensicher umsetzen und in einer rechtssicheren Dokumentation festhalten. Wer Projektrisiken reduzieren, Stillstände minimieren und nachhaltige Sicherheit möchte, ist mit einem erfahrenen Partner wie Leuze gut beraten. GIT

EIGENSICHERE TABLETS UND SMARTPHONES

Deskless Worker im Kontext der Digitalisierung

Wie mobile Geräte und Augmented Reality die Arbeit von Deskless Workern in Industriebereichen verändern

Ungeachtet der Branche stehen Unternehmen bei Digitalisierungsinitiativen immer vor großen Herausforderungen. Gerade in der Prozessindustrie herrschen oft Bedingungen vor, die notwendige zukunftsgerichtete Digitalisierungsprojekte zusätzlich erschweren können. So müssen neben technologischen Entwicklungen auch die IT-Sicherheit, der Explosionsschutz oder auch die speziellen Anforderungen der sogenannten „Deskless Worker“, die ihren Arbeitsplatz schwerpunktmäßig mobil und auf dem Industriegelände haben, mitgedacht werden. Daher ist es unerlässlich, eine umfassende Planung mit einem erfahrenen Partner durchzuführen.

Für Deskless Worker stellen eigensichere Smartphones und Tablets die zentrale Arbeits- und Kommunikationsplattform dar

Zur zuverlässigen Unterstützung von Deskless Workern bietet Pepperl+Fuchs Tablets und Smartphones nebst passenden Peripheriegeräten für explosionsgefährdete Bereiche sowie raue Umgebungen an, die auch den anspruchsvollen Einsatzbedingungen im Industriealltag trotzen. Die Tablets lassen sich dank Stift- und Handschuhunterstützung sowie dem operativen Temperaturbereich von -20° Celsius bis +50° Celsius auch in rauen Outdoor-Bereichen und in der industriellen Fertigung einsetzen. Das frontseitige NFC-Modul gestattet innovative, sichere Zugangs- und Identitätskontrollen für geschützte Bereiche und Anlagenteile. Für die notwendige Authentifizierung kommt ein Fingerprint-Sensor zum Einsatz.

Zahlreiche sogenannte SmartBacks – Aufsätze, die an der Rückseite angebracht werden – ergänzen die ruggedized Tablets und erweitern den Funktionsumfang um spezifische Leistungsmerkmale. Ein passender Scanner-Frame erweitert das Tablet beispielsweise um die Funktionalitäten zum performanten Scannen von Barcodes, Tracken von Transporten und Picken von Warenstücken in Lagern. Weiteres SmartBack-Zubehör umfasst unter anderem einen zusätzlichen Akku zur Verlängerung der Laufzeit oder spezielle Halterungen für weiterführende Anwendungen. Zusätzlich erlaubt die SmartBack-Technologie maßgeschneiderte, kundenspezifische Lösungen. Ebenso steht ein IO-Dock zum Anschluss an externe Geräte und Displays zur Verfügung, was das Tablet zu einer Alternative zu einem stationären Office-PC macht.

Augmented Reality für erweitertes Potenzial

Ein enormes Potenzial zur Digitalisierung von Prozessen auf Device-Level bietet Augmented Reality (AR). Echtzeitinformationen können so direkt ins Sichtfeld der Mitarbeitenden gebracht und räumlich sowie kontextsensitiv dargestellt werden. Dies geschieht etwa durch Markierungen an Kabeln oder Flanschen oder durch die Anzeige von Prozesswerten unmittelbar neben den entsprechenden Ventilen. So wird nicht nur die kognitive Belastung der Deskless Worker erheblich reduziert, es erlaubt diesen auch, situative Bedienentscheidungen schneller, sicherer und präziser zu treffen.

Eine ideale Ergänzung von Augmented Reality stellt der Mobilfunkstandard 5G dar. Neben der notwendigen Bandbreite liefert dieser vor allem eine äußerst geringe Latenz, um AR-Inhalte in Echtzeit zu übertragen und nahtlos einzubinden. Techniker vor Ort erhalten so kontextsensitive Anleitungen, Overlay-Markierungen auf Bauteilen sowie Live-Daten wie Sensorwerte oder Trends direkt in ihr Sichtfeld eingeblendet. Gleichzeitig können jederzeit und standortunabhängig Remote-Experten zugeschaltet werden, um bei Bedarf unterstützend und instruktiv einzugreifen.

Keine Digitalisierung ohne IT-Sicherheit

Bei allen Digitalisierungsinitiativen muss die IT-Sicherheit bereits von Beginn an mitgedacht werden. Die hohen Anforderungen, die heute an die IT-Sicherheit gestellt werden, schließen intuitive und effiziente

Dank 5G-Unterstützung eignet sich das Tab-Ex 05 ideal auch für anspruchsvolle Augmented-Reality-Anwendungen

Bedienung nicht aus. Im Gegenteil, durch den Einsatz moderner, explosionsgeschützter Smartphones und Tablets, wie sie Pepperl+Fuchs anbietet, lassen sich diese Aspekte auch in der Prozessindustrie problemlos vereinen. Diese Geräte verfügen über integrierte biometrische Authentifizierungsverfahren, beispielsweise Fingerabdrucksensoren, die einen schnellen, benutzerfreundlichen und gleichzeitig hochsicheren Zugang gewährleisten.

Kunden von Pepperl+Fuchs profitieren zudem davon, dass die mobilen Endgeräte problemlos in Mobile-Device-Management-Systeme (MDM) eingebunden werden können und Teil des Android Enterprise Recommended (AER) Programms von Google sind. So ist eine konsistente, einfache Bereitstellung und Verwaltung der mobilen Lösungen durch langfristigen Hardware- und Betriebssystem-Support ebenso garantiert wie regelmäßige Android-Upgrades und Sicherheitspatches.

Der Deskless Worker der Zukunft ist hochvernetzt

Bereits jetzt bilden eigensichere Tablets und Smartphones die zentrale Plattform für den Deskless Worker. Sie fungieren als Hub, ermöglichen die Authentifizierung, sammeln Sensordaten und bündeln die verschiedensten Kommunikationskanäle wie beispielsweise E-Mail oder Mobilfunk. Sie integrieren zudem nahtlos Geräte wie Kommunikations-Peripherals, mobile Scanner oder IoT-Gateways. Damit werden sie in explosionsgefährdeten Bereichen zum Dreh- und Angelpunkt für sichere, effiziente und vernetzte Arbeitsprozesse.

Künftig wird die Bedeutung dieser Rolle sogar noch weiter steigen. Zunehmend werden Mitarbeitende von persönlichen, KI-gestützten Assistenzsystemen begleitet, die als virtuelle Experten fungieren, die Anlagen bis ins kleinste Detail kennen und in Echtzeit bei den Aufgaben unterstützen. Tablets und Smartphones als zentrale Bedien- und Informationsplattform werden durch Wearables ergänzt. Beispielsweise dienen Audio-Headsets als primäre Kommunikationsschnittstelle für die Zusammenarbeit mit Kollegen sowie digitalen Experten.

Pepperl+Fuchs als Pionier arbeitet kontinuierlich an der Entwicklung intuitiver Lösungen, bei denen geeignete Peripheriegeräte und Wearables die Tablets und Smartphones ergänzen, um Menschen in industriellen Umgebungen optimal zu vernetzen, Arbeitsprozesse zu vereinfachen und die Effizienz nachhaltig zu steigern.

Der Deskless Worker entwickelt sich so nach und nach zu einem hochvernetzten, intelligent unterstützten Akteur, der jederzeit sicher, in Echtzeit und kontextsensitiv auf alle für seine Arbeit relevanten Informationen, Analysetools und weiterführendes Expertenwissen zugreifen kann. GIT

Pepperl+Fuchs SE
www.pepperl-fuchs.com/

INDUSTRIAL SECURITY

CRA: Mit der Ungewissheit umgehen

Wie Maschinenbauer ohne finale CRA-Vorgaben Risiken managen, Komponenten auswählen und OT Netzwerke absichern

Der CRA fordert den Maschinenbau maximal heraus. Denn erstens sind seine Details noch immer nicht final festgelegt, und zweitens enthält er Aspekte, die in der OT schwer umzusetzen sind. Erschwerend kommt hinzu, dass auch die entsprechenden europäischen Normen noch auf sich warten lassen. Was sollten Maschinenbauer nun tun?

Maschinenbau-Unternehmen stehen vor dem Dilemma, dass sie sich vorbereiten müssen, ohne exakt zu wissen, worauf. Dasselbe gilt auch für die Anbieter der Komponenten, die sie für die Umsetzung des CRA benötigen.

Fortgeschrittene Unternehmen haben bereits ein Risk-Assessment bezüglich CRA für alle Maschinenreihen durchgeführt und wissen, welche Risiken in welchem Ausmaß und mit welchen Auswirkungen auftreten können und wie sie diese Risiken mitigieren können.

Um ihre Maschinen und Anlagen sicherer zu machen, benötigen sie jedoch elektronische Produkte, z. B. SPS, HMIs, Switches oder Firewalls, die auch selbst der CRA entsprechen müssen. Bei der Auswahl besteht das Risiko, dass sie auf Produkte setzen, die künftig nicht mehr geliefert werden, weil sie nicht CRA-konform sind. Re-Designs sind daher zum aktuellen Zeitpunkt kritisch, da sie in der Regel komplex sind und einige Zeit dauern. Ebenso kann es bei Maschinen im Feld passieren, dass Ersatzteile aufgrund mangelnder CRA-Konformität nicht mehr verfügbar sind. Der Knackpunkt ist also: Wie starten, ohne das genaue Ziel zu kennen?

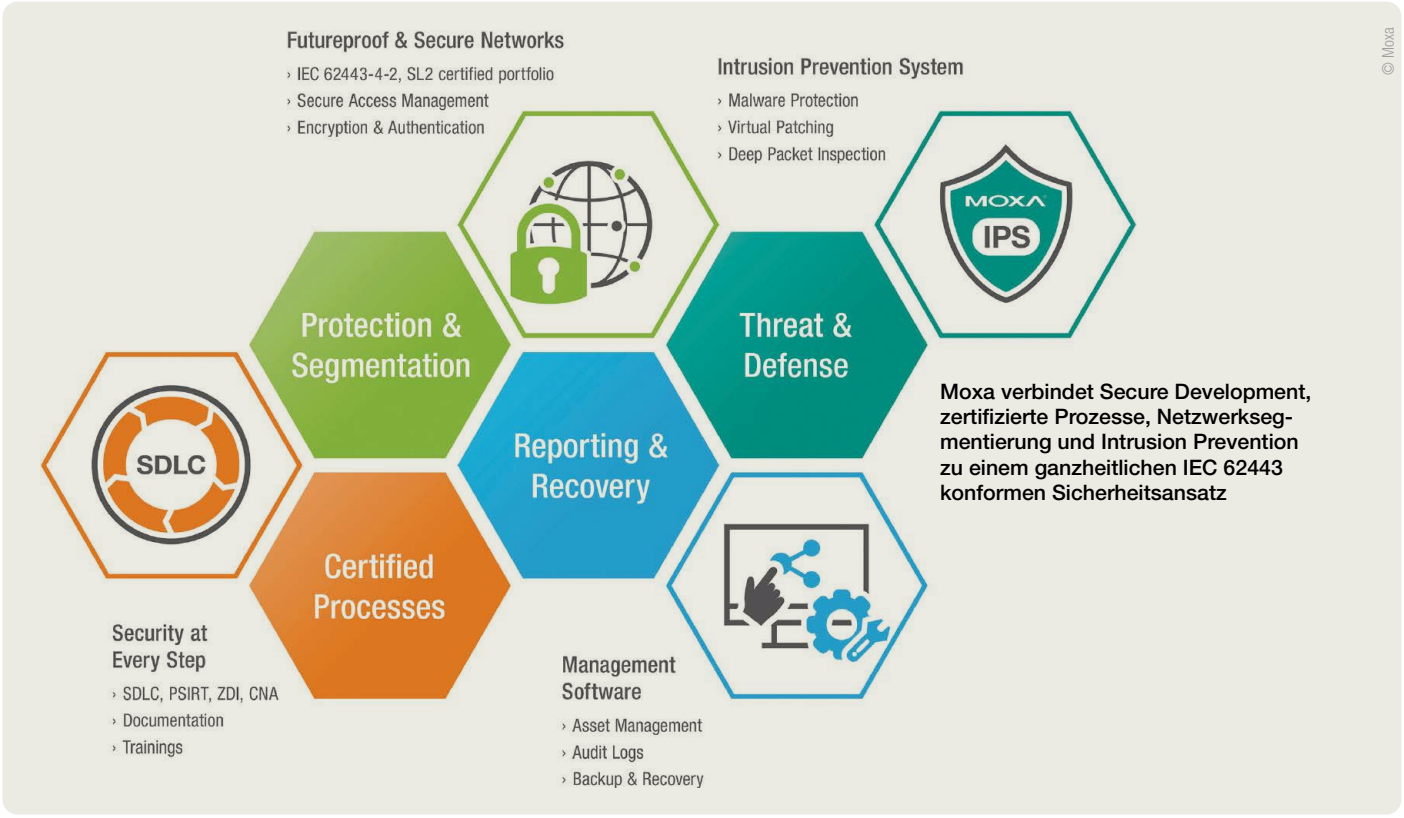
Pragmatisch vorgehen

Der CRA soll dafür sorgen, dass alle in die Pflicht genommen werden, sich dem Thema Cybersicherheit anzunehmen. Wer dies nicht tut, darf seine Produkte nicht mehr verkaufen. Nichts zu tun, ist keine Option. Wer hingegen pragmatisch startet und mit etwas Menschenverstand an die Sache herangeht, hat schon die größte Strecke hinter sich gebracht.

Zwei Aspekte spielen eine große Rolle:

- der Umgang mit erzeugten Daten (seien es Daten aus der Maschinensoftware, die IP des Unternehmens oder Produktionsdaten des Kunden)

Bitte umblättern ▶



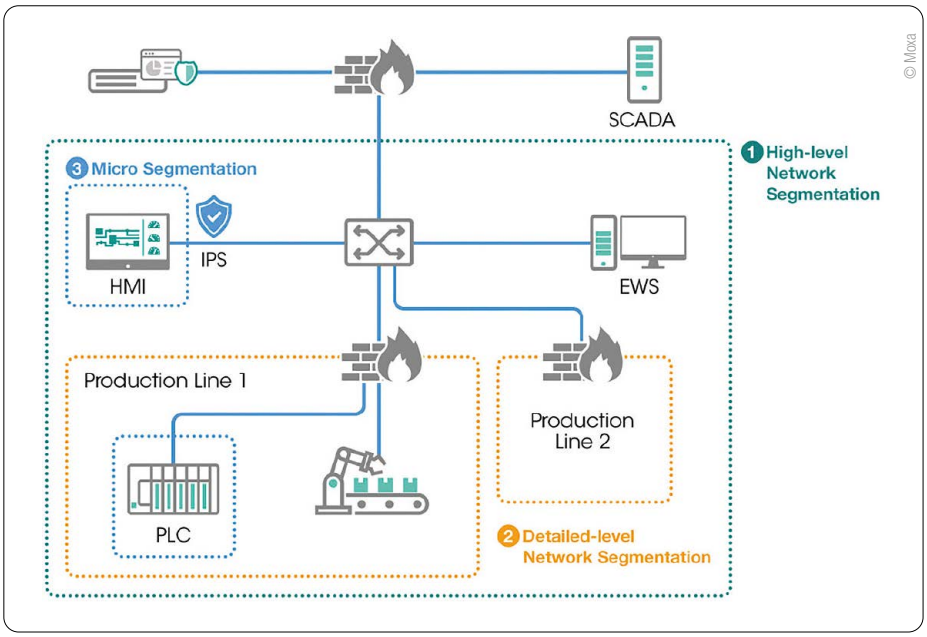
Moxa verbindet Secure Development, zertifizierte Prozesse, Netzwerksegmentierung und Intrusion Prevention zu einem ganzheitlichen IEC 62443 konformen Sicherheitsansatz

- physische und digitale Datenzugriffe

Umgang mit Daten

Folgendes Beispiel verdeutlicht den Umgang mit Daten: Ein Hersteller verkauft Abfüllmaschinen. In den Produktionen seiner Kunden haben die Mitarbeiter Zugriff auf die Produktionsdaten. Ein Mitarbeiter bei Getränkehersteller X weiß, dass Wettbewerber, die dieselbe Abfüllmaschine nutzen, auch dieselbe Remote-Lösung haben. Er könnte sich Zugriff auf die Remote-Lösung verschaffen und hätte damit auch Zugriff auf alle Produktionsdaten dieser Wettbewerber.

Der Hersteller der Abfüllmaschinen muss sich nun fragen: Ist es wahrscheinlich, dass dieser Fall eintritt? Wenn ja: Wie wahrscheinlich? Mit welchem Aufwand wäre dies verbunden? Wie hoch wäre der wirtschaftliche Schaden für ihn selbst und für seine Kunden? Mit derartigen Szenarien lassen sich potenzielle Risiken identifizieren, bewerten, mitigieren sowie dokumentieren.



Bei „Defense in Depth" handelt es sich ein mehrschichtiges Sicherheitskonzept, bei dem technische (z. B. Firewalls, IPS) und organisatorische Maßnahmen (z. B. Netzwerksegmentierung) kombiniert werden

Kriterien für die Komponentenauswahl

Bei der Auswahl von elektronischen und digitalen Produkten bietet die internationale Norm IEC 62443 Orientierung. Denn die Hauptforderung des CRA wird darin bestehen, dass die Produkte möglichst sicher sein müssen. Hersteller, die nach IEC 62443-4-1 zertifiziert sind und IEC 62443-4-2-konforme oder -zertifizierte Produkte anbieten, haben die höchste Wahrscheinlichkeit, dass ihre Produkte den CRA erfüllen.

Denn die Kernaspekte der IEC 62443 für den Maschinenbau sind:

- Zielsetzung: Schutz von Produktionsanlagen (OT-Bereich) vor Cyberangriffen, Steigerung der Anlagenverfügbarkeit und sichere Integration von Komponenten.
- Struktur: Die Norm gliedert sich in verschiedene Teile (allgemein, Richtlinien, Systemanforderungen, Komponentenanforderungen).
- Security Levels (SL): Die Norm definiert Sicherheitsstufen (SL 1 bis 4), die angeben, wie gut ein System gegen verschiedene Arten von Bedrohungen geschützt ist.
- Defense in Depth: Kernprinzip ist ein mehrschichtiges Sicherheitskonzept, bei dem technische und organisatorische Maßnahmen kombiniert werden.
- Rollen: Sie richtet sich an Betreiber, Systemintegratoren und Komponentenhersteller.

Je nach Risikobewertung der Maschine oder Anlage sollten Produkte mit einem entsprechenden Security Level eingesetzt werden. Diese lauten:

- SL 0: Keine besonderen Anforderungen oder Sicherheitsvorkehrungen erforderlich.
- SL 1: Schutz vor zufälligen oder unbeabsichtigten Verstößen (unbeabsichtigte Fehler).
- SL 2: Schutz vor vorsätzlichen Verstößen mit einfachen Mitteln (geringe Ressourcen, allgemeine Fähigkeiten).
- SL 3: Schutz vor vorsätzlichen Verstößen mit ausgeklügelten Mitteln (moderate Ressourcen, IACS-spezifische Fähigkeiten).
- SL 4: Schutz vor vorsätzlichen Verstößen mit ausgeklügelten Mitteln und umfangreichen Ressourcen (Nationalstaaten, fortgeschrittene persistente Bedrohungen).

OT-Netzwerk-Konzepte

Maschinen werden immer häufiger in ganzen Anlagen ausgeliefert oder beim Kunden in solche integriert. Damit spielen im Rahmen des CRA auch OT-Netzwerk-Konzepte eine Rolle. Ein sinnvolles Netzwerk-Konzept beginnt mit einem Risk-Assessment: Welches Riskio besteht, wenn eine Entität Zugriff erhält, sei es physisch direkt am Gerät im Schaltschrank, digital vor Ort oder aus der Ferne?

Ein physischer Zugriff lässt sich relativ einfach mit Schlüsseln, Türen und Toren, Sicherheitspersonal und Zugriffskarten einschränken. Aber auch der digitale Zugriff kann mit diversen Lösungen kontrolliert werden:

- Mit VLANs kann ein physischer Switch in mehrere logische Geräte geteilt werden. Dies verhindert, dass sich Geräte im gleichen Netz unbeabsichtigt stören.
- Im Rahmen eines Site-Zone-Cell-Konzepts wird definiert, welche Geräte in welchen Zonen „sprechen" dürfen und welche der Services erlaubt sind. Firewalls zwischen den Zonen sorgen dafür, dass diese Regeln eingehalten werden.
- Industrielle IPS (Intrusion Prevention System) bieten noch mehr Sicherheit. Hierfür analysieren IPS die Datenpakete und blockieren diese gegebenenfalls. Große Stärke von IPS ist es, Muster zu erkennen. Bei einem wiederkehrenden Muster kann das System bereits einzelne Elemente blockieren.

Fazit

Solange die Details des CRA noch nicht festgelegt sind, eignet sich die Norm IEC-62443 als Leitfaden, sowohl für die Auswahl von Komponenten als auch für die Entwicklung von Maschinen, die dem CRA entsprechen sollen. Ein empfehlenswerter Ausgangspunkt ist eine Risikobewertung mit allen wichtigen Abteilungen im Unternehmen bezüglich Cybersicherheit und möglichem Missbrauch eigener sowie erzeugter Kundendaten. Es gilt, jetzt anzufangen, um das Delta, das sich mit Finalisierung des CRA und den daraus folgenden europäischen Normen zeigen wird, zu verkleinern und schnell zu schließen. GIT

Autor:
Philipp Jauch
Industry Market Manager
Industrial Automation
bei Moxa Europe

Moxa Inc.
www.moxa.com

DISTRIBUTION

First Call-Partner für Ingenieure und Integratoren

Im Gespräch mit Connor Doherty: Schnelle Teile, klare Daten, starke Systeme – wie DigiKey Automatisierung ganzheitlich und sicherheitsorientiert gestaltet

DigiKey entwickelt sich vom reinen Komponentenlieferanten zum sicherheitsorientierten Automatisierungspartner. Transparente Daten, schnelle Verfügbarkeit, ein systemorientiertes Portfolio und gezielte Unterstützung bei Sicherheitsstandards und zertifizierten Komponenten machen das Unternehmen zum „First Call“ für Ingenieure in zunehmend komplexen und sicherheitskritischen Automationsumgebungen. Das Gespräch mit Connor Doherty, Director of Industrial Automation bei DigiKey, führte Anke Grytzka-Weinhold, Chefredakteurin unserer Automatisierungs-Fachzeitschrift messtec drives Automation.

Was bedeutet „Automatisierungspartner“ für DigiKey – über die reine Komponentenverfügbarkeit hinaus? Worin unterscheidet sich dieses Verständnis vom traditionellen Distributorenmodell in Bezug auf den Mehrwert für OEMs, Systemintegratoren und Endanwender?

Connor Doherty: Für DigiKey bedeutet es, ein Automatisierungspartner zu sein, Kunden entlang des gesamten Automatisierungslebenszyklus zu unterstützen – von der Konzeptphase über Design und Implementierung bis hin zu Wartung, Reparatur und Betrieb (MRO = Maintenance, Repair and Operations). Traditionelle Distributoren konzentrieren sich häufig auf Verfügbarkeit und eine transaktionsbasierte Auftragsabwicklung. DigiKey hingegen legt großen Wert darauf, Designs über ihren gesamten Lebenszyklus hinweg zu begleiten. Unser Automation Resource Center bietet umfassende Online-Ressourcen und Unterstützung zu Themen wie Protokollen, Programmierung, SPS, Robotik und vielem mehr. Darüber hinaus stellen wir durch schnelle Fulfillment-Prozesse, die Bereitstellung von Kleinmengen, transparente Lieferzeiten und ein breites Produktspektrum eine hohe operative Resilienz sicher.

Welche Kundenwünsche in der Automatisierung haben für Sie in den kommenden drei Jahren Priorität?

Connor Doherty: Der Automatisierungsmarkt entwickelt sich rasant – getrieben durch neue Technologien und regional variierende Investitionsschwerpunkte. Für uns stehen drei Herausforderungen im Mittelpunkt:

1. Zeitdruck bei der Implementierung:
Kunden müssen zunehmend komplexere Automatisierungslösungen schneller umsetzen – bei gleichzeitig knapper werdenden Engineering-Ressourcen. Wir möchten sicherstellen, dass sie die passenden Produkte kennen und sie schnell erhalten.

2. Steigende Systemkomplexität:
Automatisierungssysteme bestehen heute aus mehr Steuerungen, höheren Leistungsanforderungen, zusätzlicher Sensorik, mehr Signalen und stärker vernetzter Kommunikation. DigiKey bietet systemorientierten Support, um die benötigten zusätzlichen Komponenten zu identifizieren.

3. Lebenszyklusresilienz:
Während viele Lösungen noch auf Legacy-Systemen basieren, entstehen gleichzeitig zahlreiche Innovationen. Wir möchten beide Welten bedienen und ein ausgewogenes Portfolio für neue und bestehende Systeme bereitstellen.

Wie entwickelt sich Ihr Portfolio von Komponenten hin zu kompletten Lösungen?

WILEY

35 Jahre

Git Sicherheit

Nächstes Heft: die Jubiläumsausgabe

Mit VIP-Statements, Standortbestimmungen, Trend-Reports – und einer Zeitreise durch 35 Jahre Sicherheit

Kontakt: GIT-GS@Wiley.com

Connor Doherty: DigiKey erweitert sein Portfolio bewusst und systemorientiert. Anstatt ausschließlich weitere SKUs (SKU = Stock Keeping Unit) hinzuzufügen, konzentrieren wir uns auf den gezielten Ausbau grundlegender Komponenten und der dazugehörigen Hersteller. Wir analysieren permanent, welche Lösungstechnologien fehlen und welche Lieferanten sich strategisch eignen. Besonders im Fokus stehen Industrie-Controller, I/Os, Sensoren, Motoren und Antriebe sowie Relais. Zudem investieren wir verstärkt in Konnektivität, Edge Computing und Stromversorgungslösungen – essenzielle Bausteine für zentrale vertikale Segmente der Automatisierung. Unser Ziel ist ein leistungsstarkes, umfassendes Angebot, das die Anforderungen unserer Kunden vollständig abdeckt.

Was sind DigiKeys mittelfristige Ziele für die kommenden drei Jahre?

Connor Doherty: Wir investieren intensiv in das Wachstum unseres Automatisierungsgeschäfts – es wird weiterhin unser am schnellsten wachsendes Segment bleiben. Wir wollen Umsatz und Kundenbasis steigern, die Vielfalt der pro Kunde bezogenen Produkte erhöhen und unser Lieferanten- und Technologieportfolio erweitern. Langfristig möchten wir der „First Call"-Partner für Automatisierungsingenieure und Systemintegratoren sein.

Wie wirkt sich das geopolitische Umfeld auf DigiKeys Automatisierungsgeschäft aus?

Connor Doherty
ganz persönlich

Welcher Superheld wären Sie gerne? Ironman – viele Ingenieure teilen seine Faszination für Hightech.

Mit wem würden Sie gerne für einen Tag Ihr Leben tauschen? Mit meiner Frau – um mehr Zeit mit unserem neun Mnate alten Baby zu verbringen.

Was würden Sie erfinden? Teleportation – um Reisen zu ersetzen und mehr persönliche Begegnungen zu ermöglichen.

Ich wollte schon immer … einen eigenen Garten anlegen, um meine Familie mit frischen Kräutern, Gemüse und Obst zu versorgen.

Connor Doherty: Geopolitische Entwicklungen verstärken die Bedeutung diversifizierter Beschaffungsstrategien. Wir stellen detaillierte Produktinformationen bereit – einschließlich Herkunftsland und alternativer Optionen. Ein US-spezifischer Filter ermöglicht die Suche nach verzollten respektive unverzollten Produkten. Über unser Foreign Trade Zone (FTZ)-Programm reduzieren wir zudem die direkten Auswirkungen von Zöllen. Parallel dazu verbessern wir kontinuierlich unsere Export-Compliance-Prozesse, um schnell und regelkonform liefern zu können.

Wie begegnet DigiKey der wachsenden Nachfrage nach sicherheitszertifizierten Komponenten?

Connor Doherty: Sicherheit gewinnt immer mehr an Bedeutung. Daher haben wir auf unserer Website eine eigene Kategorie für sicherheitsrelevante Produkte eingeführt. Sie umfasst PSA-Ausrüstung, Maschinensicherheitskomponenten wie Lichtvorhänge, Relais und Steuerungen sowie Hard- und Software für Sicherheitsprotokolle – darunter Not-Aus-Schalter, Türverriegelungen, Laserscanner und vieles mehr. Wir erweitern unser Angebot kontinuierlich und erleichtern gleichzeitig die Auffindbarkeit dieser Komponenten auf DigiKey.com.

Welche Rolle spielt Ihr Portfolio bei sicheren IoT- und Edge-Hardwarelösungen?

Connor Doherty: Mit dem Aufstieg von IoT und Edge Computing ist die Sicherheit auf Hardware-Ebene stärker in den Mittelpunkt gerückt. Viele Cybersicherheitsfunktionen entstehen unmittelbar in den Komponenten, die unsere Lieferanten entwickeln – häufig integriert in Modulen, die wir vertreiben. Wir entwickeln diese Sicherheitstechnologien nicht selbst, stellen jedoch sicher, dass sie für unsere Kunden zugänglich und zuverlässig verfügbar sind.

Unsere Aufgaben sind zweigeteilt:
1. Auffindbarkeit sicherer Bausteine:
Wir integrieren sicherheitsrelevante Merkmale klar in die Produktdefinitionen und durchsuchbaren Attribute, damit Kunden schnell geeignete Komponenten identifizieren können.
2. Sicherstellung der Echtheit:
Wir arbeiten eng mit Lieferanten zusammen, um Konformitäts- und Echtheitszertifikate zu verifizieren. Die Integrität der Lieferkette zu schützen, ist eine der wirkungsvollsten Maßnahmen zur Minimierung von Cybersicherheitsrisiken auf Geräteebene.

> „Es geht nicht nur darum, die Teile auf Lager zu haben, sondern darum, Kunden dabei zu helfen, schnell und sicher die richtigen Teile zu finden.

So tragen wir dazu bei, dass Kunden zuverlässig sichere, vernetzte Geräte am Edge entwickeln können.

Wie unterstützt DigiKey Ingenieure bei der Umsetzung globaler Sicherheitsstandards wie IEC 61508, ISO 13849 und IEC 62443?

Connor Doherty: DigiKey hilft Konstrukteuren, sich in der Welt globaler Sicherheitsstandards zurechtzufinden. Wir machen Zertifizierungen transparenter und erleichtern ihre Berücksichtigung bereits in frühen Entwicklungsphasen. Die Einhaltung der Normen wird zwar von den Herstellern durch umfassende Zertifizierungen gewährleistet – wir stellen jedoch sicher, dass diese Informationen während des Auswahlprozesses verfügbar, klar formuliert und nutzbar sind. Zukünftig möchten wir die Nutzbarkeit und den Umfang dieser Daten weiter ausbauen, um Konstrukteuren zu ermöglichen, von Beginn an sichere und normkonforme Entscheidungen zu treffen.

Was macht DigiKey im Automationsmarkt besonders?

Connor Doherty: Wir verfolgen nach wie vor die gleiche Philosophie wie vor über 50 Jahren: Produkte schnell zum Kunden zu bringen. Wir nutzen unsere jahrzehntelange Erfahrung im Bereich elektronischer Bauteile und übertragen bewährte Verfahren konsequent auf die Automatisierungsbranche. Die Fähigkeiten, die uns zum größten ECommerceDistributor für elektronische Komponenten gemacht haben, setzen wir nun gezielt im Bereich der Automatisierungsprodukte ein. GIT

DigiKey Electronic Germany GmbH
www.digikey.de

Stefan Schönegger

B&R ernennt Stefan Schönegger als CTO

Stefan Schönegger ist von ABB Machine Automation (B&R) zum Chief Technology Officer (CTO) ernannt worden. Er ist seit 2006 in verschiedenen Positionen bei der Machine Automation tätig und begann seine Laufbahn als Projektleiter für SPS- und Steuerungssysteme. In den folgenden Jahren hatte er verschiedene Führungsfunktionen inne, unter anderem als Leiter Produktmanagement. Seit 2022 leitet er die globale Produktgruppe Controls. Er hat langjährige und umfassende Erfahrung mit B&R-Technologien, ein tiefes Verständnis der Kundenanforderungen sowie enge Verbindungen zu Industriepartnern. Seine Fähigkeit, starke und innovative Organisationen aufzubauen und zu leiten, bildet eine solide Grundlage für seine Aufgaben als CTO. „Ich freue mich auf die neue Aufgabe bei B&R. Gemeinsam mit unseren Teams werden wir unsere technologische Ausrichtung in den Bereichen Automatisierung, Software und autonome industrielle Lösungen weiterentwickeln“, so Stefan Schönegger. **www.br-automation.com**

Martin Kunz, CEO Steute Technologies

Neuer CEO bei Steute Technologies

Martin Kunz hat die Position des Chief Executive Officer (CEO) der Steute Technologies mit Hauptsitz in Löhne übernommen. Er hat mehr als 20 Jahre internationale Führungserfahrung in Industrie- und Prozesstechnologieunternehmen und wird die weitere strategische Entwicklung sowie das profitable Wachstum der Steute Gruppe verantworten. Nach dem Studium des Wirtschaftsingenieurwesens an der Rheinland-Pfälzischen Technischen Universität Kaiserslautern-Landau (RPTU) bekleidete Martin Kunz zahlreiche internationale Führungspositionen in europäischen und US-amerikanischen Industrieunternehmen. Dazu zählen unter anderem leitende Funktionen bei Xylem Inc., einem weltweit führenden Anbieter von Wassertechnologie, und zuletzt als CEO von Concentric AB, einem führenden Anbieter von Motorpumpen, Hydrauliklösungen und Kühlsystemen.

www.steute.com

SicherMacher

Der GIT-Talk mit den Marktführern

GIT SICHERHEIT

Kontakt:
Miryam.Reubold@Wiley.com

WILEY

GIT SICHERHEIT

INNENTITEL – ARBEITSSICHERHEIT

Sicherheit trifft Umweltbilanz

Wie Multinorm Green Sicherheit, Langlebigkeit und eine transparente Umweltbilanz verbindet

FRISTADS®

INNENTITEL

Sicherheit trifft Umweltbilanz

Wie Multinorm Green Sicherheit, Langlebigkeit und eine transparente Umweltbilanz verbindet

In vielen industriellen Arbeitsumgebungen gehört umfassender Schutz zum Alltag. Gleichzeitig wachsen die Anforderungen an Komfort, Langlebigkeit und Nachhaltigkeit stetig. Lange Zeit galt es als schwierig, all diese Faktoren in einer einzigen Schutzkleidungslösung zu vereinen – insbesondere im Bereich der Multinorm-Bekleidung. Genau hier setzt Multinorm Green an: eine Schutzkleidung, die Sicherheit, Tragekomfort, Haltbarkeit und messbare Nachhaltigkeit in einem ganzheitlichen Konzept verbindet.

Der Schutz von Menschen steht seit jeher im Mittelpunkt moderner Arbeitskleidung. Sicherheit umfasst heute jedoch auch ökologische Transparenz, verantwortungsvolle Materialwahl und langlebige Produkte, die Ressourcen schonen. Multinorm Green berücksichtigt diese Entwicklung und erweitert den Begriff der Sicherheit um die Dimension des Umwelt- und Ressourcenschutzes.

Ein zentraler Schritt dieser Entwicklung ist eine Multinorm-Kollektion mit Umweltproduktdeklaration, EPD. Das Kürzel steht für „Environmental Product Declaration". Dabei handelt es sich um einen anerkannten, international normierten Standard, der die Umweltauswirkungen eines konkreten Produkts über seinen gesamten Lebenszyklus transparent darstellt. Die EPD liefert nachvollziehbare Daten zu CO_2-Emissionen und Wasserverbrauch über den gesamten Lebenszyklus hinweg – einschließlich relevanter Scope 3 Emissionen – also indirekte Emissionen außerhalb der eigenen Produktion, z. B. aus Lieferketten. Damit erhalten Unternehmen eine transparente Grundlage, um den ökologischen Fußabdruck ihrer Schutzkleidung realistisch zu bewerten.

Die Multinorm Green Kollektion von Fristads ist u. a. zertifiziert nach EN ISO 11612 (Hitze & Flammschutz), IEC 61482 2 (Störlichtbogen), EN ISO 11611 (Schweißerschutz), EN 1149 5 (Elektrostatischen Eigenschaften), EN 13034 Typ 6 (begrenzter Chemikalienschutz) und EN ISO 20471 (Warnschutz)

Schutzkleidung für den realen Arbeitsalltag

Multinorm Green wurde für tägliche Belastungen in anspruchsvollen Einsatzbereichen entwickelt. Jede Faser ist auf Langlebigkeit ausgelegt. Das Material erreicht eine Abriebfestigkeit von 100.000 Scheuertouren im Martindale Test. Zum Vergleich: typischerweise hält moderne Multinorm-Schutzkleidung 50.000–80.000 Scheuertouren aus. Zudem ist Multinorm Green für mindestens 100 industrielle Waschzyklen geprüft und zugelassen, wobei der Schnitt bei Multinorm-Schutzkleidung bei 50 industriellen Waschzyklen liegt. Verstärkungen aus Aramid sowie Ripstop Strukturen stabilisieren zudembesonders beanspruchte Bereiche und reduzieren Verschleiß. Diese Haltbarkeit führt zu längerer Nutzungsdauer, geringerem Ersatzbedarf, niedrigeren Gesamtbetriebskosten und einem reduzierten Ressourcenverbrauch über den gesamten Produktlebenszyklus.

Die Kollektion ist PFAS frei und Oeko Tex zertifiziert. Der Verzicht auf PFAS reduziert die Umweltbelastung, während die Zertifizierung sicherstellt, dass keine gesundheitsschädlichen Chemikalien in direkten Hautkontakt gelangen.

Ein weiterer entscheidender Sicherheitsfaktor liegt im inhärenten Flammschutz. Die flammhemmenden Eigenschaften sind fest in die Fasern integriert und nicht lediglich durch chemische Ausrüstung aufgebracht. Der Flammschutz bleibt also über die gesamte Lebensdauer der Kleidung erhalten, da die flammhemmenden Eigenschaften nicht ausgewaschen werden können.

Jedes Kleidungsstück der Multinorm Green wird mit einer Umweltproduktdeklaration (EPD) geliefert ist PFAS frei und nach Oeko Tex zertifiziert

Nachhaltigkeit messbar machen

Transparenz ist ein wesentlicher Bestandteil moderner Nachhaltigkeitsstrategien. Deshalb wird jedes Kleidungsstück mit einer individuellen Umweltproduktdeklaration ausgeliefert. Diese macht den Ressourcenverbrauch sichtbar und ermöglicht objektive Bewertungen sowie Vergleiche. Unternehmen erhalten damit eine verlässliche Entscheidungsgrundlage für ihre Nachhaltigkeitsziele.

Auch die Materialzusammensetzung folgt einem ressourcenbewussten, nachhaltigem Ansatz. Zum Einsatz kommt eine Fasermischung aus Modacryl, rückverfolgbar gewonnenem Lyocell, Polyamid, Bio-Baumwolle, Elasthan und antistatischer Faser. Verantwortungsbewusst beschaffte Rohstoffe, kombiniert mit langlebiger Konstruktion, sorgen für einen effektiven Schutz bei gleichzeitig reduzierter Umweltbelastung.

Bewegungsfreiheit als Sicherheitsfaktor

Schutzkleidung muss sowohl schützen als auch funktional sein. Vollständig dehnbare Stoffe passen sich jeder Bewegung an und ermöglichen maximale Flexibilität im Arbeitsalltag. Segmentierte Reflexelemente erhöhen die Sichtbarkeit, ohne die Beweglichkeit einzuschränken.

Die Kollektion Multinorm Green erfüllt umfassende Multinorm-Anforderungen und ist für Arbeitsumgebungen konzipiert, in denen mehrere Gefährdungen gleichzeitig auftreten können: Flammen, Hitze, Lichtbögen, Schweißarbeiten, elektrostatische Entladungen, flüssige Chemikalien und hohe Sichtbarkeit. Ergänzt wird dies durch ein breites Größenspektrum (XS bis 6XL) einschließlich speziell entwickelter Damenmodelle.

Funktionale Lösungen für unterschiedliche Anforderungen

Die Hosenmodelle sind in zwei Varianten erhältlich, die beide auf denselben Grundelementen basieren: Vollstretchmaterial, segmentierte Reflexelemente, Ripstop Stretchverstärkungen und Multinorm Zertifizierungen. Inhärenter Flammschutz und funktionale Taschenlösungen sind Teil der Grundausstattung.

Die Premium Version richtet sich an Anwender mit hohen Anforderungen an Belastbarkeit und Anpassungsfähigkeit. Zusätzliche elastische Bundbereiche erhöhen den Tragekomfort und Aramidverstärkungen schützen besonders beanspruchte Zonen. Verstellbare Beinabschlüsse, Stiefelhaken und flexible Beinlängenanpassungen unterstützen eine präzise Passform. Die reguläre Version bietet denselben Schutz, konzentriert sich jedoch auf wesentliche Funktionen und den Komfort ohne zusätzliche Ausstattungsmerkmale zu benötigen – eine wirtschaftliche Lösung ohne Kompromisse beim Schutz.

Für risikoreiche Arbeitsbereiche stehen außerdem Latzhosen, Handwerker Latzhosen und Overalls zur Verfügung. Sie bieten vollständige Körperabdeckung und kombinieren die Stretch Technologie mit Schutz für Tätigkeiten in beengten Räumen oder bei Hitze.

Ein neuer Ansatz für die Branche

Multinorm Green zeigt, dass Schutzkleidung verschiedene Anforderungen miteinander verbinden kann: technische Leistungsfähigkeit, messbare Nachhaltigkeit, ergonomischen Komfort und Haltbarkeit. Damit entsteht ein neues Konzept für eine Branche, die sich zunehmend an ganzheitlichen Sicherheitskonzepten orientiert.

Was früher als schwer vereinbar galt, wird hier greifbar: Multinorm Schutz, der sowohl Menschen schützt als auch Umweltaspekte berücksichtigt und den Anforderungen des Arbeitsalltags entspricht. GIT

Für einen hohen Tragekomfort und hohe Beweglichkeit sorgen Vollstretchmaterial, segmentierte Reflexelemente sowie Ripstop-Stretchverstärkungen

Fristads AB
www.fristads.com

TEST-REIHE

Der GIT Lesertest: Sicherheitsschuhe

Atlas und GIT SICHERHEIT suchen Tester – Maximum Protection im harten Arbeitsalltag

Sicherheitsschuhe gehören zu den am stärksten beanspruchten Bestandteilen der persönlichen Schutzausrüstung. Gerade in anspruchsvollen Arbeitsumgebungen müssen sie nicht nur schützen, sondern auch dauerhaft Komfort, Stabilität und Passform bieten. Gemeinsam mit Atlas möchte GIT SICHERHEIT deshalb herausfinden, wie sich die neue Max Series im echten Arbeitseinsatz bewährt – und öffnet die Redaktion erneut für das ehrliche Feedback aus der Praxis.

Im Mittelpunkt dieses Lesertests steht die neue Atlas Max Series – ein S3 Sicherheitsschuh, der speziell für die anspruchsvolle Arbeitsweltentwickelt wurde und maximale Sicherheit mit moderner Ergonomie und Technologie verbinden soll.

Zum Testprodukt: Atlas Max Series (S3)

Mit der Max Series führt Atlas eine neue Sicherheitsschuh Generation ein, die für Tätigkeiten mit hoher mechanischer Beanspruchung konzipiert wurde. Ein zentrales Merkmal der Serie ist das neu entwickelte lederfreie Obermaterial ProTraX, das gezielt auf typische Belastungen im Arbeitsalltag ausgelegt ist.

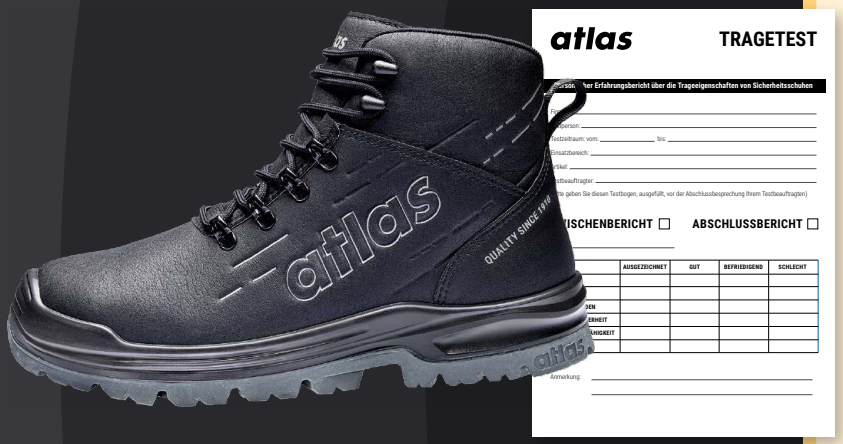
ProTraX wurde für Einsatzbereiche entwickelt, in denen Sicherheitsschuhe regelmäßig Abrieb, Kontakt mit rauen Oberflächen sowie wechselnden Umgebungsbedingungen ausgesetzt sind. Im Vergleich zu klassischen Leder oder textilen Obermaterialien verfolgt ProTraX einen materialtechnischen Ansatz, der auf Widerstandsfähigkeit, Formstabilität und Pflegeeigenschaften abzielt.

- Form- und Strukturstabilität: Während textile Materialien unter Dauerbelastung an Stabilität verlieren können und Leder je nach Pflegezustand nachgibt, zielt ProTraX auf eine gleichbleibende Materialstruktur über die gesamte Nutzungsdauer ab.
- Feuchtigkeits- und Schmutzverhalten: ProtraX ist so ausgelegt, dass es (auch bei Standwasser), verglichen zu Leder, kaum Feuchtigkeit aufnimmt. Auf diese Art kommt es bei Nässe weder zu einer Gewichtszunahme durch Feuchtigkeitseinlagerung, noch zu Kältebrücken oder Nässegefühl im Schuh.
- Gewicht: Durch die Nutzung von ProTraX als Obermaterial und der Lightweight-Schaftkonstruktion, ist der Schuh extrem leicht und bleibt es auch unter allen Witterungsbedingungen.
- Pflege: Sicherheitsschuhe der Max-Series benötigen keine spezielle Pflege und lassen sich aufgrund des neuen Obermaterials einfach reinigen

Warum ist das für den Test relevant?

Gerade das Obermaterial entscheidet im Arbeitsalltag maßgeblich über Lebensdauer, Schutzwirkung und Akzeptanz eines Sicherheitsschuhs. Mit dem Lesertest soll überprüft werden, wie sich ProTraX unter realen Einsatzbedingungen bewährt – insbesondere im Vergleich zu bislang eingesetzten Sicherheitsschuhen mit anderen Obermaterialien.

Gesucht ist eine praxisnahe, ehrliche Bewertung, die nicht auf theoretischen Kennwerten, sondern auf tatsächlichen Erfahrungen im täglichen Einsatz basiert.



Wir suchen TESTER!

Melde Dich bei uns bis 08.05.2026 unter

GIT-GS@WILEY.COM

unter unter der Betreff „Lesertest Atlas Max-Series“ oder scanne einfach den QR-Code am Ende des Beitrags

Wen wir suchen

Dieser Lesertest richtet sich ausdrücklich an Unternehmen:

- Aufruf an Betriebe, in denen Sicherheitsschuhe verpflichtend getragen werden
- Pro Unternehmen ca. fünf Testpersonen
- Voraussetzung: Pflicht zum Tragen von S3 Sicherheitsschuhen im beruflichen Alltag
- Idealerweise Mitarbeiterinnen und Mitarbeiter, die Sicherheitsschuhe täglich und unter anspruchsvollen Bedingungen nutzen

Was habt Ihr davon? – Eure Vorteile als Tester

Die teilnehmenden Unternehmen und Tester profitieren von einem besonderen Mehrwert:

- 3D Fußscan und professionelle Fußvermessung vor Ort durch Produktexperten von Atlas (exakte Bestimmung von Größe, Weite und Fußtyp)
- Direkte Ausgabe der Sicherheitsschuhe vor Ort
- Individuelle, fachkundige Beratung durch Atlas Experten
- Die getesteten Schuhe dürfen behalten werden

Ablauf des Lesertests – was wir von Euch erwarten

- Atlas kommt zu Euch (Vor Ort Termin) mit 3D Scan und direkter Schuhausgabe
- Tragetest über vier Wochen im regulären Arbeitsalltag
- Ausfüllen eines kurzen strukturierten Testberichts
- Bewertung der Schuhe inklusive Fotomaterial aus dem Arbeitseinsatz
- Rücksendung der Unterlagen an die Redaktion GIT SICHERHEIT

Im Anschluss erfolgt die redaktionelle Auswertung des Lesertests. Die Ergebnisse werden online sowie im Print in einer der kommenden Ausgaben von GIT SICHERHEIT veröffentlicht.

Interesse geweckt?

Unternehmen, die an diesem exklusiven Lesertest teilnehmen möchten, können sich mit einer kurzen Beschreibung ihres Einsatzbereichs und der vorgesehenen Testpersonen bei der Redaktion melden.

Wir suchen Tester – macht mit und sagt uns ehrlich, was die neue Atlas Max Series im Arbeitsalltag leistet!

Jetzt per Mail anmelden!

Sonnen- und Hitzeschutz sind bei Arbeiten ein Freien ein absolutes Muss, ebenso wie ein ausreichendes Maß an Wasser, um Dehydrierung, Hitzeschlag oder Hitzekrämpfen vorzubeugen

ARBEITSSCHUTZ

Umweltschutz und Arbeitsschutz im Klimawandel

Herausforderungen und Lösungen in vier Punkten

Der Klimawandel bringt eine Vielzahl neuer Herausforderungen mit sich, die sich nicht nur auf unsere Umwelt, sondern auch auf die Arbeitswelt auswirken. Arbeitnehmer, die unter freiem Himmel oder in nicht klimatisierten Innenräumen tätig sind, sehen sich zunehmend extremen Wetterbedingungen, neuen Insektenarten und einer veränderten Pflanzenwelt ausgesetzt.

In diesem Zusammenhang wird deutlich, dass Umweltschutz und Arbeitsschutz enger miteinander verknüpft werden müssen. Umweltschutz zielt darauf ab, die negativen Auswirkungen menschlicher Aktivitäten auf die Natur zu minimieren, während der Arbeitsschutz darauf abzielt, die Sicherheit und Gesundheit der Arbeitnehmer zu gewährleisten. Beide Bereiche beeinflussen sich gegenseitig: Ein intaktes Umweltmanagement kann die Risiken für Arbeitnehmer senken, während ein umfassender Arbeitsschutz dazu beitragen kann, die Belastungen für die Umwelt zu reduzieren.

1. Hitze als Gefährdungsfaktor für Arbeitnehmer

Mit der Erhöhung der Durchschnittstemperaturen und der Zunahme von Hitzewellen wächst die Gefahr für Arbeitnehmer, die im Freien oder in schlecht belüfteten Innenräumen arbeiten. Hohe Temperaturen führen zu einer verminderten Leistungsfähigkeit und erhöhen das Risiko von Arbeitsunfällen. Die körperliche Belastung bei hohen Temperaturen kann zu Dehydrierung, Hitzeschlag oder Hitzekrämpfen führen, insbesondere für Menschen, die körperlich anstrengende Arbeiten verrichten.

Schutzmaßnahmen gegen Hitze

Die Gefährdung durch Hitze erfordert eine Kombination aus organisatorischen, technischen und persönlichen Maßnahmen. Organisatorisch sollten Arbeitszeiten an kühlere Tageszeiten angepasst und häufigere Pausen eingelegt werden. Technische Lösungen wie Schattenspender und Ventilationssysteme tragen zur Reduzierung der Hitze am Arbeitsplatz bei. Schließlich müssen Arbeitnehmer durch geeignete Kleidung und den richtigen Umgang mit Hitze geschult werden.

2. Insekten als Vektoren für Krankheiten

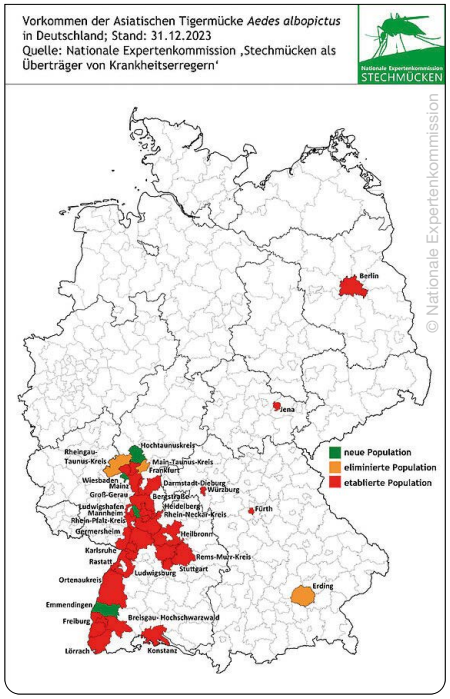
Der Klimawandel begünstigt auch die Verbreitung von Insektenarten, die als Vektoren für verschiedene Krankheiten fungieren. Arten wie die Asiatische Tigermücke, die Krankheiten wie Dengue-Fieber, Zika-Virus und Chikungunya übertragen kann, breiten sich durch die wärmeren Temperaturen in neuen Regionen aus. Auch Zecken, die Krankheiten wie Borreliose und Frühsommer-Meningoenzephalitis (FSME) übertragen, profitieren von milderen Wintern und verlängerten Aktivitätsperioden.

Präventive Maßnahmen zum Schutz vor Insekten

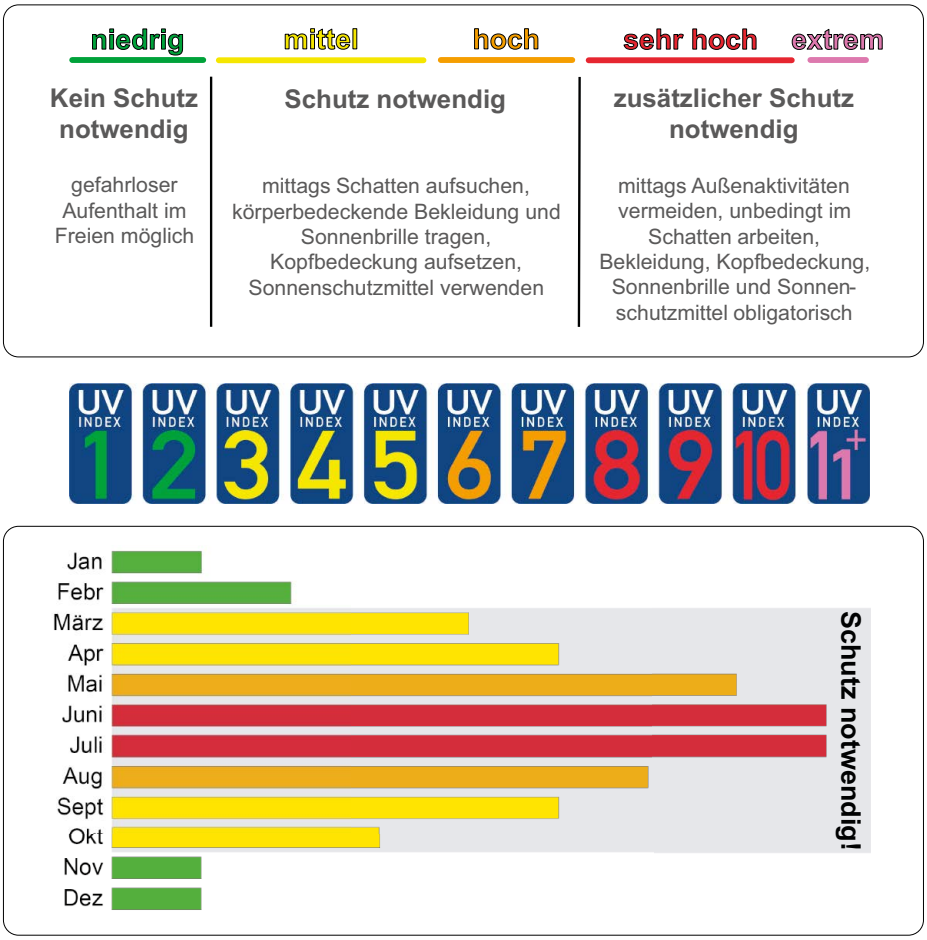
Schutzmaßnahmen gegen die gesundheitlichen Risiken durch Insekten umfassen das Tragen von Schutzkleidung, die Verwendung von Insektenschutzmitteln (Repellentien) und die Sensibilisierung der Arbeitnehmer. In Risikogebieten sollten Arbeitgeber sicherstellen, dass ihre Mitarbeiter geimpft sind, sofern eine Impfung gegen die betreffenden Krankheiten verfügbar ist. Die Schulung der Arbeitnehmer über die Risiken und den Umgang mit Insektenstichen ist ebenso entscheidend.

3. Pflanzen und Allergien: Neue Herausforderungen im Arbeitsschutz

Durch den Klimawandel verändern sich auch die Flora und ihre Auswirkungen auf die Gesundheit. Längere Blütezeiten und eine höhere Pollenproduktion erhöhen die Pollenbelastung in der Luft, was insbesondere für Allergiker problematisch ist. Neue, allergene Pflanzenarten wie die Beifuß-Ambrosie breiten sich in Regionen aus, in denen sie bisher nicht heimisch waren, und stellen eine zusätzliche Gefahr dar.



Die aus Asien stammende Tigermücke breitet sich gegenwärtig immer weiter nach Norden aus. In Deutschland sind insbesondere die Gebiete am Oberrheinlauf betroffen



Der UV-Index Jahreskalender gibt an, in welche UV-Index-Werte im langjährigen Mittel in den einzelnen Monaten typsicherweise maximal erreicht werden

Strategien zur Reduzierung von Allergie-Risiken

Um das Risiko von Allergien zu mindern, sollten Arbeitszeiten an pollenarme Zeiten angepasst werden. Arbeitnehmer sollten über den Umgang mit Allergien geschult und über Schutzmaßnahmen wie das Tragen von Nasenfiltern oder speziellen Atemmasken informiert werden. Diese Maßnahmen tragen dazu bei, die Gesundheit und Produktivität der Arbeitnehmer trotz erhöhter Pollenbelastung zu erhalten.

4. Integration von Umweltschutz in den Arbeitsschutz

Die fortschreitenden Auswirkungen des Klimawandels machen deutlich, dass Umwelt- und Arbeitsschutz nicht mehr getrennt voneinander betrachtet werden können. Eine Integration beider Bereiche ist notwendig, um sowohl die Umwelt zu schützen als auch die Gesundheit und Sicherheit der Arbeitnehmer zu gewährleisten. Ein ganzheitlicher Ansatz, der umweltfreundliche Arbeitspraktiken fördert, kann zur Reduktion des ökologischen Fußabdrucks und zur Schaffung gesünderer Arbeitsplätze beitragen.

Die Notwendigkeit eines ganzheitlichen Ansatzes

Ein ganzheitlicher Ansatz im Arbeitsschutz umfasst die Nutzung erneuerbarer Energien, den Einsatz nachhaltiger Materialien und eine effiziente Abfallwirtschaft. Diese Maßnahmen tragen nicht nur zum Umweltschutz bei, sondern verbessern auch die Arbeitsbedingungen und verringern die Gesundheitsrisiken für die Arbeitnehmer.

Gesetzliche und regulatorische Entwicklungen

Auch auf gesetzlicher Ebene wird die Verbindung von Umwelt- und Arbeitsschutz zunehmend gefordert. Das Lieferkettengesetz in Deutschland und internationale Initiativen wie die Agenda 2030 der Vereinten Nationen für nachhaltige Entwicklung setzen Standards für gesunde Arbeitsbedingungen und Umweltschutz. Diese Entwicklungen zeigen, dass es ohne verbindliche Vorgaben nicht möglich ist, beide Bereiche wirksam zu gestalten. Unternehmen sind daher gefordert, sich an diese neuen Standards anzupassen und nachhaltige, sichere Arbeitsweisen zu etablieren.

Fazit

Der Klimawandel stellt neue Herausforderungen an den Umwelt- und Arbeitsschutz, die nur durch eine enge Verzahnung beider Bereiche bewältigt werden können. Hitze, neue Insektenarten und allergene Pflanzen erfordern gezielte Schutzmaßnahmen und Anpassungen. Durch einen ganzheitlichen Ansatz, der Umwelt- und Arbeitsschutz vereint, können Unternehmen die Gesundheit ihrer Mitarbeiter schützen und gleichzeitig zu einer nachhaltigeren Wirtschaft beitragen. Ein solcher Ansatz ist nicht nur im Interesse der Arbeitnehmer, sondern auch der Unternehmen und der Gesellschaft als Ganzes. GIT

Autor:
Donato Muro
Inhabe und Leitender Sichereits- und Brandschutzingenieur von Sicherheitsingenieur.NRW

Sicherheitsingenieur.NRW
https://sicherheitsingenieur.nrw/

SCHUTZKLEIDUNG

„Moderne PSA muss deutlich mehr können…“

Kübler-PSA-Experte Sven Traub erklärt, wie Schutz, Tragekomfort und Wirtschaftlichkeit in modernen PSA-Konzepten zusammenspielen

In der Persönlichen Schutzausrüstung steigen die Anforderungen stetig: Neben normgerechtem Schutz erwarten Unternehmen heute langlebige, komfortable und wirtschaftlich sinnvolle Lösungen. Im Interview erläutert Sven Traub, Leiter Key Account Management bei Paul H. Kübler Bekleidungswerk GmbH & Co. KG, wie moderne PSA diese Erwartungen erfüllt, welche Rolle Beratung und Service einnehmen und welche Position die neue Multinorm-Kollektion Safety X Compact im Portfolio einnimmt.

GIT SICHERHEIT: Herr Traub, aus Ihrer Erfahrung als Leiter des Key Account Managements bei Paul H. Kübler, was wird von Persönlicher Schutzausrüstung heute erwartet?

Sven Traub: Moderne Persönliche Schutzausrüstung (PSA) muss deutlich mehr können als „nur“ schützen. Selbstverständlich steht die zuverlässige Erfüllung aktueller Normen – etwa in den Bereichen Hitze- und Flammschutz, Lichtbogenschutz, Chemikalienschutz oder Warnschutz – weiterhin im Mittelpunkt. Gleichzeitig gilt es bei der Produktentwicklung, den Spagat zu schaffen zwischen optimalem

Safety X Compact vereint zertifizierten Multinorm-Schutz mit robuster Verarbeitung und langlebigen Materialien

Schutz und höchstmöglichem tragphysiologischem Komfort. Darüber hinaus erwarten Anwender und Unternehmen eine dauerhaft hohe Schutzwirkung, die auch für die industrielle Wäsche ausgelegt ist und über die gesamte Lebensdauer hinweg bestehen bleibt. Hinzu kommen Aspekte wie Langlebigkeit und die Berücksichtigung einer einfachen Reparierbarkeit bereits in der Produktentwicklung – wodurch die Kleidung lange im Kreislauf gehalten wird und höchste Wirtschaftlichkeit bietet. Von ebenso großer Bedeutung ist die Akzeptanz der Mitarbeitenden. Diese wird maßgeblich von den tragphysiologischen und ergonomischen Eigenschaften bestimmt. Gefordert wird eine atmungsaktive, hautfreundliche und möglichst leichte PSA. Ergonomische Schnitte, intelligente Materialkombinationen, die maximale Bewegungsfreiheit bieten, ein differenzierter Größenspiegel, der auch Damengrößen beinhaltet, und natürlich auch eine moderne Linienführung sind weitere entscheidende Voraussetzungen, dass Schutzkleidung im Arbeitsalltag angenommen und konsequent getragen wird.

Unternehmen stehen in der Verantwortung, die Vorgaben der PSA-Verordnung (EU) 2016/425 zu erfüllen. Welche Informationen und Dokumente fordern Kunden für den Nachweis, dass sie ihren Sorgfaltspflichten nachkommen und zugleich wirtschaftlich handeln?

Sven Traub: Arbeitgeber müssen PSA der Schutzklassen 2 und 3 den Beschäftigten nicht nur kostenlos zur Verfügung stellen, sondern auch gewährleisten, dass diese hygienisch einwandfrei aufbereitet wird. Parallel dazu steigen die Erwartungen an Serviceleistungen. Dazu zählen verlässliche Lieferfähigkeit, langfristige Nachlieferbarkeit über viele Jahre hinweg, digitale Produktinformationen sowie Wasch- und Leasingkonzepte, die reibungslos in bestehende Prozesse integriert werden können. Verstärkt achten Unternehmen aus Industrie, Handwerk und Energieversorgung zudem auf nachhaltige Materialien, Transparenz in den Lieferketten und eine wirtschaftlich sinnvolle Gesamtkostenbetrachtung über den kompletten Produktlebenszyklus. Darüber hinaus beobachten wir, dass Individualisierungsmöglichkeiten, etwa durch Logos oder Farbakzente, deutlich an Relevanz gewonnen haben. PSA wird somit zunehmend Bestandteil eines ganzheitlichen Sicherheits- und Markenkonzepts.

Sven Traub, Leiter Key Account Management bei Paul H. Kübler Bekleidungswerk GmbH & Co. KG

In welcher Rolle sieht sich Kübler angesichts der immer komplexeren Erwartungen an PSA?

Sven Traub: Getreu unseres Mottos „von Profis für Profis“ setzen wir bei der Entwicklung und Konfektion technisch leistungsfähiger PSA schon immer auf den engen Austausch mit Anwendern. Angesichts der wachsenden Komplexität der PSA- bzw. Multinorm-Konzepte, Materialkombinationen und branchenspezifischer Schutzanforderungen sehen wir die Aufgabe zunehmend auch in der fundierten Beratung unserer Kunden. Die Qualität der Beratung und Tragetests im direkten Arbeitsplatzumfeld sind entscheidende Faktoren, damit ein hochentwickeltes Schutzkonzept in der Praxis tatsächlich funktioniert.

Wie gestaltet sich die Zusammenarbeit mit Kunden konkret?

Sven Traub: Unser Ziel ist es, gemeinsam mit unseren Partnern und den Endkunden die optimale Balance zwischen Schutzwirkung, Tragekomfort und Wirtschaftlichkeit für den jeweiligen Einsatzbereich zu finden. Die Grundlage für eine Produktempfehlung unsererseits bilden die normativen Anforderungen respektive die Gefährdungsanalysen. Gerne bringen wir auch unsere Expertise in der Anwendung von PSA bei Arbeitsplatzbegehungen ein. Des Weiteren unterstützen wir die Kunden bei der Durchführung von Tragetests. In der Einführungsphase von PSA schulen wir auf Wunsch die Sicherheitsfachkräfte zu Normen, Pflege- und Waschzyklen, Reparatur sowie Austauschintervallen und unterweisen die Träger im korrekten Tragen von PSA. Unser Rundum-Service zur Erhöhung der Sicherheit von PSA im Arbeitsalltag beinhaltet auch, dass wir Sondergrößen in kurzer Zeit individuell fertigen und den Kunden eine Reparaturmatrix sowie Originalmaterialien zur Verfügung stellen.

Kübler hat gerade mit Safety X Compact eine neue Schutzkleidungs-Kollektion auf den Markt gebracht – welche Lücke schließen Sie damit im Hinblick auf die bereits bestehende Kollektion Kübler Protectiq?

Sven Traub: Safety X Compact ist die neue Einstiegskollektion von Kübler im Multinorm-Bereich. Wir entsprechen damit dem Wunsch von Kunden nach einer preisgünstigeren Alternative zu Kübler Protectiq speziell für Einsatzbereiche, in denen die PSA aufgrund hoher Schmutzkontamination und starker mechanischer Belastung in kürzeren Intervallen ersetzt werden muss.

Welche Gefahren deckt Safety X Compact durch seine Multinorm-Zertifizierungen ab?

Sven Traub: Sie vereint Schweißerschutz (EN ISO 11611), Schutz gegen Hitze und Flammen (EN ISO 11612), Elektrostatische Eigenschaften (EN 1149-5) und Schutz gegen thermische Auswirkungen eines Störlichtbogens (EN ISO 61482-1-2) sowie leichten Chemikalienschutz (EN 13034 Typ 6).

Wo und ab wann ist die neue Kollektion erhältlich?

Sven Traub: Safety X Compact ist ab sofort im Fachhandel und Technischen Handel erhältlich. GIT

Paul H. Kübler Bekleidungswerk GmbH & Co. KG
www.kuebler.eu

STÖRLICHTBOGENSCHUTZ

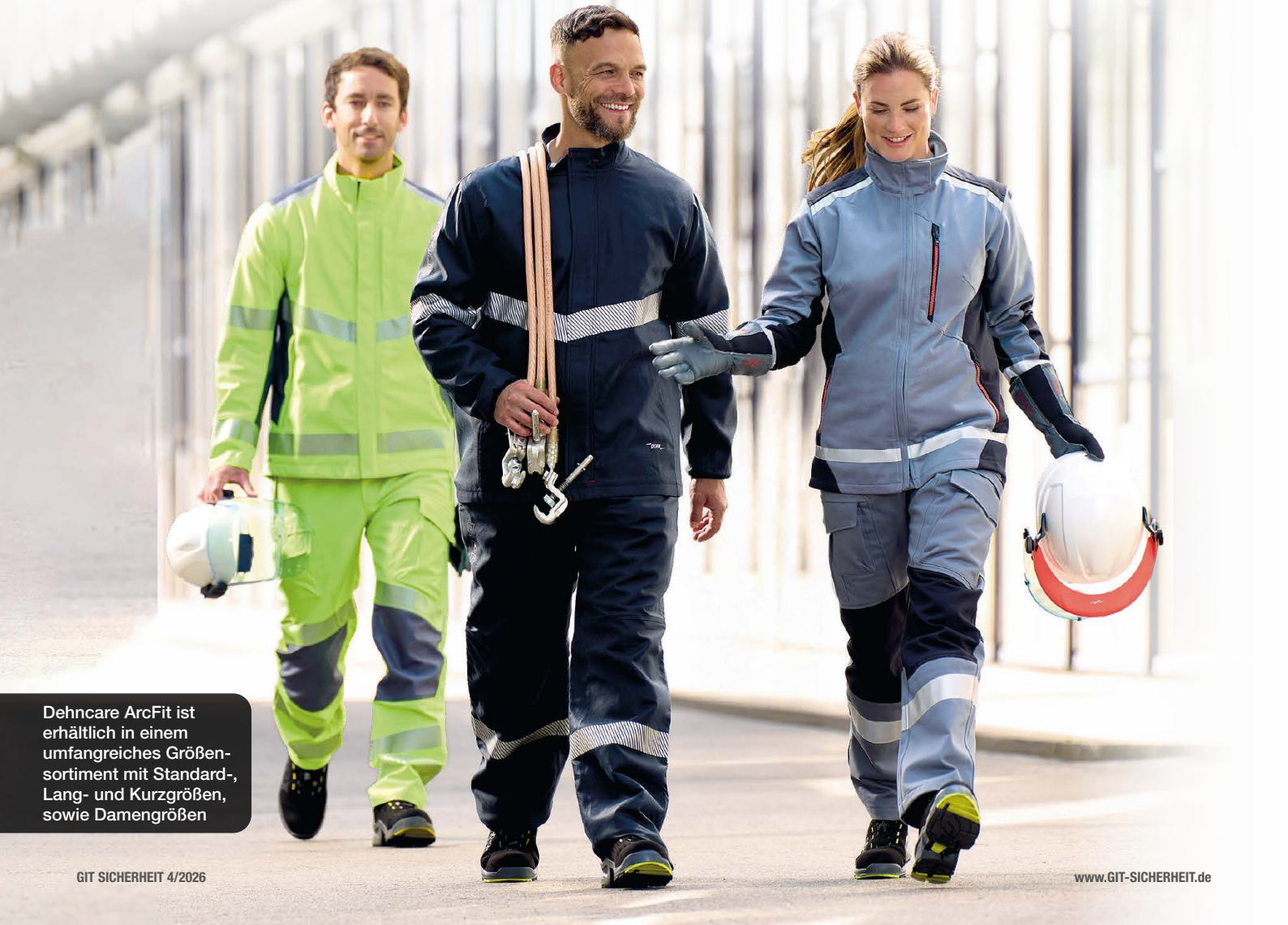
Praxisgerechter Störlicht-bogenschutz im Arbeitsalltag

Effektiver Störlichtbogenschutz für Arbeiten an elektrischen Anlagen

Personen, die an oder in der Nähe von unter Spannung stehenden Teilen elektrischer Anlagen arbeiten, sind grundsätzlich den Gefährdungen durch Störlichtbögen ausgesetzt. Störlichtbögen sind selten, aber beim Arbeiten an elektrischen Anlagen und Systemen nicht vollständig ausschließbare Ereignisse. Sie fordern daher einen zuverlässigen Schutz.

Um das Verletzungs- und Unfallrisiko zu minimieren, sind umfangreiche und sichere Lösungen essentiell. Schutzkleidung gegen Störlichtbögen (PSAgS) schützt Mitarbeitende zuverlässig und sollte zudem angenehm zu tragen sein. Dehncare ArcFit ist widerstandsfähig und erfüllt die erforderlichen Normen für das Arbeiten an elektrischen Anlagen. Die Multinorm-Schutzkleidung wurde entwickelt, um ihren Trägern zusammen mit dem abgestimmten Zubehör den nötigen Schutz vor den thermischen Auswirkungen eines Störlichtbogens zu bieten. Für das Arbeiten an Anlagen mit höheren Energien kommt Dehncare ArcFit HLP 63 (High Level Protection) zum Einsatz.

Dehncare ArcFit ist eine Multinorm-schutzkleidung, die Anwender schützt, an verschiedenste Arbeitsbedingungen angepasst ist und so unter anderem Störlichtbogenschutz, Hitze und Flammenschutz sowie Schutz gegen elektrostatische Aufladung bietet. Sie ist eine komfortable, sportliche und individualisierbare Schutzkleidung und Teil der Persönlichen Schutzausrüstung gegen Störlichtbögen. Die Outdoor-Variante erreicht durch die Jacken-



Dehncare ArcFit ist erhältlich in einem umfangreiches Größensortiment mit Standard-, Lang- und Kurzgrößen, sowie Damengrößen

Hosen-Kombination die Warnschutzklasse 3 nach EN ISO 20471. Diese garantiert eine hohe Sichtbarkeit bei Tag und Nacht und muss bei „erhöhter Gefährdung“, z.B. im Straßenverkehr mit einer durchschnittlichen Verkehrsgeschwindigkeit von mehr als 60 km/h, getragen werden.

Neben der schmutz- und wasserabweisenden Oberfläche ist der Schutz (Typ 6) gegen flüssige Chemikalien nach EN 13034 für die Auswahl der richtigen PSAgS erforderlich. Komfort ist eine weitere wichtige Eigenschaft der Schutzkleidung.

Einen hohen Schutz mit Störlichtbogen-Schutzklasse APC 2 – PPE 4 gemäß NFPA 70E (US-Norm für elektrische Sicherheit am Arbeitsplatz) bietet die Schutzkleidung Dehncare ArcFit HLP 63. Insbesondere bei, temporären Schalthandlungen oder bei Arbeiten an Anlagen mit höheren Energien, beispielsweise in Niederspannungs-haupt- und Mittelspannungsschaltanlagen, kommt sie zum Einsatz. Die dazugehörige störlichtbogen-geprüfte Latzhose kann über der normalen Kleidung getragen werden. Durch die seitlichen Öffnungen an den Hosenbeinen ist ein Überziehen mit Schuhen möglich. Die PSAgS Dehncare ArcFit HLP 63 bestehend aus Jacke und Latzhose entspricht der Kat. III gem. PSA-Verordnung (EU) 2016/425 und erfüllt alle notwendigen normativen Anforderungen, die an Schutzkleidung dieser Art gestellt werden.

Für eine vollständige PSAgS wird neben der Schutzkleidung zudem Kopf-, Gesichts-, Hand- und Fußschutz benötigt. Halbschuhe und Schnürstiefel mit einer isolierenden Laufsohle bis 1000 V komplettieren die Ausrüstung.

Hände als primäre Gefährdungszone

Häufig wird das Gefährdungspotential in Bezug auf die Hände in der Praxis unterschätzt. In einschlägigen Normen, wie der EN 61482-2, wird den praktischen Anforderungen im Arbeitsalltag nicht ausreichend Aufmerksamkeit geschenkt. Daher ist der nötige Schutz für die Hände gesondert zu bewerten.

Der Dehn APG XT bietet Schutz auch unter 300 mm Abstand zum Störlichtbogen

Die Berufsgenossenschaft hat einen Prüfgrundsatz entwickelt, der praxisnahe Bedingungen bei der Störlichtbogenprüfung anwendet und insbesondere einen verkürzten Arbeitsabstand der Hände berücksichtigt. Daraus resultieren zwei neue Schutzklassen (APC1_150 / APC2_150), die speziell den Schutzbedarf der Hände in realen Situationen abdecken. Der Prüfgrundsatz GS-ET-42-2 der DGUV beschreibt zusätzliche Anforderungen für Handschuhe und passt die Prüfung an die täglichen Arbeitsbedingungen an. Die Prüfung bei reduziertem Abstand,150 mm statt 300 mm Entfernung vom Störlichtbogen, stellt hohe Anforderungen an Material und Hersteller. Der Handschuh APG XT von Dehn hat diese Zertifizierung erfolgreich bestanden und bietet Schutz bei gleichzeitigem Tragekomfort. Des Weiteren wurde er ebenso mit erhöhtem Prüfpegel von 630 kJ getestet.

Beim Schalten von Sicherungslasttrennschaltern, beim Ziehen von NH-Sicherungen, beim Prüfen der Spannungsfreiheit oder beim Erden- und Kurzschließen ist man durch die Nähe zur Anlage erhöhten Risiken ausgesetzt. Der APG XT ist exakt für diese Tätigkeiten entwickelt worden und bietet Schutz, wenn der Arbeitsabstand von 300 mm unterschritten wird.

Die PSAgS ist ein wichtiger Teil des ganzheitlichen Störlichtbogenschutzes. Nur so lässt sich ein zuverlässiger Schutz von Personen und eine bestmögliche Anlagenverfügbarkeit erreichen. Grundsätzlich sollten technische, organisatorische und persönliche Maßnahmen (TOP-Prinzip) zum Schutz vor Verletzungen durch Störlichtbögen immer als System betrachtet werden. GIT

Dehn SE
www.dehn.de

© Bilder: Dehn SE

EHS

Arbeitsschutz in Zeiten des Generationenwandels

Zielgruppengerechter Arbeitsschutz zwischen analogem Lernen und KI-gestützten Tools

„Was Hänschen nicht lernt, lernt Hans nimmermehr!“ – so lautet ein altbekanntes Sprichwort. Es soll besagen, dass im jungen Alter Informationen zumeist leichter aufgenommen werden als in späteren Jahren. Tatsächlich bleibt unser Gehirn ein Leben lang lernfähig und genau diese Fähigkeit ist im modernen Berufsleben auch zunehmend gefordert. In puncto sicheres Arbeiten bedeutet dies, jederzeit und in jedem Alter genau zu wissen, was man wie tut und wo wann welche Gefährdungen bestehen können. Um diese zu vermeiden oder sich angemessen vor ihnen zu schützen, genau dafür gibt es entsprechende Betriebsanweisungen, Gefährdungsbeurteilungen und Unterweisungen. Aber berücksichtigen diese auch, dass Hänschen vielleicht doch anders „lernt“ als Hans?

Der demographische Wandel in unserer Gesellschaft schreitet weiter voran, die geburtenstarken Jahrgänge nähern sich zunehmend dem Rentenalter, weniger Jüngere müssen nachrücken und mit den mittleren Jahrgängen irgendwie die Lücken schließen. Inzwischen sprechen wir nicht mehr nur von „alt“ und „jung“, sondern von den einzelnen Generationen. Ob Babyboomer (1956-66), Gen X (1966-80), Millennials (1981-95) oder Gen Z (1996-2012) – jede Generation hat ihre Besonderheiten, gerade auch geprägt durch den jeweiligen technologischen und gesellschaftlichen Entwicklungsstand während ihres Heranwachsens. Die Unterschiede sind besonders prägnant bei der unterschiedlichen Mediennutzung für Informationsaufnahme und -verarbeitung. Die Spanne reicht von den „klassischen“ über digitale und soziale Medien bis zu KI-gestützten oder -generierten Formen.

Arbeitsschutz zwischen Dokumentation, Verständnis und Wirksamkeit

Unabhängig vom Alter besteht die allgemeine Herausforderung beim Arbeitsschutz aus diesen beiden Punkten:

- Wie erreichen wir alle Mitarbeitenden?
- Wie verstehen sie uns?

Ein Blick auf die Entwicklung zeigt, dass nach wie vor der Arbeitsschutz „schwarz auf weiß“, also auf Papier beginnt: All die zahlreich zu beachtenden Gesetze, Regeln und Verordnungen sind digital höchstens als pdf-Dateien zu finden. Durch die in den 90er Jahren aufgekommenen Angebote wie etwa Powerpoint, Word, Excel oder SAP-Lösungen sollte dann alles sauber in den vorhandenen digitalen Formaten und Datenbanken dokumentiert werden. Der Hauptfokus bestand jedoch zumeist erstmal in der rechtlichen Absicherung („wir haben alles getan, bei Behördenbesuch kann ich alles nachweisen…“).

Bloße Schulungs-Durchführung und (digitale) Dokumentation allein können jedoch nicht schon ausreichendes Ziel im Arbeitsschutz sein. Ohne effektive Wirksamkeitskontrolle fehlt der Nachweis, ob auch wirklich alles verstanden wurde. Letztlich geht es aber darum, neben dem Wissen auch ein echtes Verständnis bei allen Mitarbeitenden für sicheres Arbeiten zu schaffen. Dazu muss die Kernfrage nach dem „wie“ gelöst werden (Wie bekomme ich all das nötige Wissen tatsächlich in die Köpfe der Menschen?).

Ein Blick auf die Entwicklungsstufen der unterschiedlichen Generationen offenbart, dass es die eine Lösung hierfür nicht gibt. Innerhalb von vier Generationen erfolgte der Wechsel vom analogen über das digitale hin zum virtuellen Zeitalter – und in rasendem Tempo verändern nun die scheinbar unendlichen Möglichkeiten der Künstlichen Intelligenz unseren Alltag.

Technologie, Kultur und Haltung als Schlüssel für zielgruppengerechten Arbeitsschutz

Als EHS-Softwareanbieter unterstützt Secova seit 2008 Unternehmen dabei, ihre zahlreichen Aufgaben und Pflichten bei Arbeitsschutz und Arbeitssicherheit leichter zu meistern. Gestartet mit online-Unterweisungen (UWS), die Mitarbeitende orts- und zeitunabhängig durchführen können, bietet sam zahlreiche Funktionsmodule für unterschiedlichste Anforderungen und auch mobilen Einsatz. Mit sam-VR werden Simulationen möglich ohne echte Gefahr für die Anwendenden. Und AI-

sam ist die Plattform für erste KI-gestützte Lösungen – etwa für Begehungen, LMRAs (Last Minute Risk Assessments) oder digitale Sicherheitsdatenblätter.

Ganz neu ist „Operation Risk" – dieser Ansatz verbindet die praktische Erfahrung des Stuntman und „RiskBuster" Holger Schumacher mit wissenschaftlich fundierter Risikokompetenz und digitalem Knowhow der Secova. Das Ziel: Risikobewusstsein und Selbstverantwortung bei Mitarbeitenden nachhaltig stärken.

Klar ist: Software allein wird nie reichen! – Wie auch in ganz anderen Bereichen des Lebens geht es primär nicht so sehr um das pure „Wissen", sondern ebenfalls um „Akzeptanz" und die dahinterliegende „Kultur". Erst in dieser Verbindung lassen sich die Möglichkeiten von Software (im Allgemeinen) auch tatsächlich ausnutzen und „die PS auf die Straße bringen". Daher ist für Secova das Match aus einfach bedienbarer Software (sam) und entsprechender Kulturarbeit (Operation Risk) ein idealer Lösungsansatz, der Hand in Hand gehen muss, um das volle Potenzial auszuschöpfen.

Übergeordnetes Ziel ist es, zu einem sicheren Verhalten zu gelangen. Doch wie auch in ganz anderen Bereichen des Lebens führt unser „Wissen" nicht automatisch zu entsprechendem „Handeln". So zeigt etwa das Beispiel „Klimawandel" deutlich: Wir wissen, wir können so nicht weiter machen, tun es aber trotzdem. Was also zählt? Es dreht sich neben dem Wissen eben auch immer um das Verstehen und dann in der Folge um das Verinnerlichen – also um eine Haltung, die wir idealerweise erzeugen. Eine Haltung ähnlich wie ein tiefliegendes Wertegerüst, was die Menschen in ihrem Handeln prägt und unterstützt.

Von Babyboomer bis GenZ – für sicheres und risikobewusstes Arbeiten gilt es, generationsübergreifend alle zu erreichen

Wohin geht die Reise, wie kann zielgruppengerechter Arbeitsschutz aussehen? Klar ist: Es gibt nicht die eine Lösung, Die Mischung macht's! Für Secova sieht diese Mischungsempfehlung aktuell so aus:

- Persönliche Unterweisungen mit Wirksamkeitskontrolle (WK)
- UWS, GBUs (Gefährdungsbeurteilungen) und weitere Anwendungen per E-Learnings mit integrierten WK-Tests, ergänzt durch
- sam 3D und sam 360 ° = EHS Gamification
- Kurz-Videos = z. B. Hygieneregeln per App für Smartphone oder Tablet
- sam-VR = Gefahren gefahrlos „wie in echt" erleben – auch als „Game" verfügbar
- sam AR = im Live-Umfeld virtuelle Gefahren simulieren
- LMRA = Beteiligung der Mitarbeitenden an der GBU und Sensibilisierung vor Tätigkeitsantritt
- KI mit AI-sam = künstliche Intelligenz liefert echten Mehrwert, unterstützt und vereinfacht verschiedene Prozesse
- Operation Risk = gezieltes Training z. B. von Risikokultur für verbesserte Risikokompetenz GIT

Interview

Lesen Sie auf der nächsten Seite das Gespräch mit Johannes Türk-König und Holger Schumacher

Secova GmbH & Co. KG
www.secova.de

BG Bau: Verbände einigen sich auf Sicherheitsanforderungen

Der Fachbereich Bauwesen im Spitzenverband Deutsche Gesetzliche Unfallversicherung (DGUV) hat gemeinsam mit Verbänden aus Handwerk, Handel und Industrie verbindliche Anforderungen für keilgezinkte Dachlatten festgelegt. Diese wurden während der Messe Dach+Holz als Anhang zur Dachlattenvereinbarung unterzeichnet und veröffentlicht. Ziel ist es, die Arbeitssicherheit auf Dächern weiter zu verbessern und Durchsturzunfälle wirksam zu vermeiden.

Dachlatten, die als Standplatz genutzt werden sollen, müssen durchbruchsicher sein. Die dafür maßgeblichen Anforderungen sind in der „Vereinbarung über Dachlatten mit CE-Kennzeichnung aus Nadelholz" (Dachlattenvereinbarung) aus dem Jahr 2022 geregelt. Neben den Produkteigenschaften enthält sie Vorgaben zur Sortierung, Beschreibung, Kennzeichnung und Markierung von Dachlatten als Standplatz für Bauarbeiten. Gemeinsames Ziel der unterzeichnenden Organisationen ist es, die Sicherheit von Personen, die auf Dächern arbeiten, zu gewährleisten und Arbeitsunfälle nachhaltig zu verhindern.

Der nun in Köln unterzeichnete Anhang zur Dachlattenvereinbarung definiert die Produkt- und Produktionsanforderungen für Dachlatten mit Keilzinkenverbindung. Die Regelung gilt für visuell oder maschinell nach der Festigkeit sortierte keilgezinkte Dachlatten für tragende Zwecke. Sie stellt sicher, dass sowohl das verwendete Holz als auch die Keilzinkenverbindung der Dachlatten ausreichend tragfähig sind, um den Sicherheitsanforderungen bei Arbeiten auf Dächern zu entsprechen. Gleichzeitig schafft sie Rechtssicherheit für Hersteller sowie Anwender.

Der neue Anhang ergänzt die „Vereinbarung über Dachlatten mit CE-Kennzeichnung aus Nadelholz" vom 8. Juli 2022 und tritt am 25. Februar 2026 in Kraft. Er wird vom Fachbereich Bauwesen der DGUV sowie den unterzeichnenden Verbänden Zentralverband des Deutschen Dachdeckerhandwerks (ZVDH), Holzbau Deutschland – Bund Deutscher Zimmermeister im Zentralverband des Deutschen Baugewerbes (ZDB), Gesamtverband Deutscher Holzhandel (GD Holz), Hauptverband der Deutschen Holzindustrie (HDH), Bundesverband Deutscher Fertigbau (BDF) sowie Deutsche Säge- und Holzindustrie Bundesverband (DeSH) getragen. **www.bgbau.de**

Operation Risk

Wie Unternehmen Risikokompetenz neu denken

Wie gelingt echte Risikokompetenz in einer Arbeitswelt, in der vier Generationen unterschiedlich lernen und arbeiten? Holger Schumacher, Experte & Berater für Risikokultur – Business Stuntman, und Johannes Türk-König, Head of Customer Success bei Secova – System Engineer OR, zeigen, warum Risikokultur im Kopf beginnt – und wie digitale Lösungen sie im Alltag sichtbar und wirksam machen.

Das Team für mehr Risikokompetenz: Johannes Türk-König und Holger Schumacher (v. l.n.r.)

GIT SICHERHEIT: Herr Schumacher, viele Unternehmen tun sich schwer damit, ihre Mitarbeitenden wirklich für Risiken zu sensibilisieren. Was genau ist der Kern von „Operation Risk“ – und warum beginnt Risikokompetenz Ihrer Meinung nach im Kopf?

Holger Schumacher: Ich glaube es liegt daran, dass bisher der Fokus auf „Safety“ oder „Regeln“ liegt und die Analyse der Risiken für die Mitarbeitenden schwer ist. Sie haben es auch nie wirklich gelernt. Es braucht einfach eine Betrachtung durch eine andere „Linse“ mit dem Fokus auf das Risiko und dazu die Kompetenz, es zu erkennen. Genau das tun wir, ganz bewusst, mit Operation Risk! Risikokompetenz beginnt im Kopf, weil Menschen Risiken zuerst sehen müssen, um Situationen richtig zu interpretieren. Wir helfen mit „Mission: Risikokultur“ den Blick auf und den Dialog über Risiken in der Kultur zu verankern.

Sie kommen aus der Stuntwelt, wo Risiken zum Alltag gehören. Was hat Sie motiviert, dieses Wissen in den Arbeitsschutz zu übertragen – und was steckt für Sie persönlich hinter „Operation Risk“?

Holger Schumacher: Mich hat ein eigener Unfall geprägt: Du merkst in Sekunden, dass Risiko nicht theoretisch ist – es wird sofort real. In der Stuntwelt ist Safety kein Poster oder eine Kampagne, sondern gelebte Kultur. Genau diese möchte ich in den Arbeitsschutz übertragen, weil sie wirkt – auch unter Druck. Mein Konzept entstand ursprünglich für Stuntteams – aber es war zu gut, um es nur dort einzusetzen. „Operation Risk“ ist für uns die Chance, wirklich etwas zu bewegen: Impulse wirken kurz, aber was bleibt? Mit Operation Risk bekommt das Ganze ein System und damit Nachhaltigkeit. So wird Risikokompetenz ein echter Hebel.

Herr Türk-König, Secova betont, dass Software allein nicht reicht. Warum ist die Verbindung aus digitalen Tools und gelebter Sicherheitskultur für modernen Arbeitsschutz entscheidend?

Johannes Türk-König: Moderne Sicherheitskultur braucht vor allem eines: Beteiligung. Aber Beteiligung entsteht nur durch Erreichbarkeit. Genau hier ist Software der entscheidende Hebel. Ich kann damit nicht nur Informationen an alle senden, sondern jeden Einzelnen aktiv einbinden. Mitarbeitende können frühzeitig Beinaheunfälle melden oder Verbesserungsvorschläge einreichen. So werden alle zu aktiven Gestaltern von Sicherheit – und das ist die Basis für eine

gelebte Kultur, die weit über den reinen Arbeitsschutz hinausgeht.

Bei Operation Risk ist viel von „Beteiligung“ die Rede. Warum verändert sich eine Risikokultur erst dann wirklich, wenn Mitarbeitende aktiv in Beurteilungen, Entscheidungen und Verbesserungen eingebunden werden?

Holger Schumacher: Weil Risikokultur nicht durch Ansagen entsteht, sondern durch Dialog. Erst wenn Mitarbeitende aktiv mit beurteilen, entscheiden und verbessern, wird Risiko konkret. Man baut gemeinsamen Kontext auf. Dieser Kontext wirkt stärker als noch mehr Regeln oder diese immer wieder zu predigen. Denn Menschen verstehen, warum etwas kritisch ist und worauf es ankommt. Gleichzeitig entsteht Ownership: Wer beteiligt ist, übernimmt Verantwortung und stoppt eher, wenn etwas nicht passt. Beteiligung macht Risikokompetenz alltagstauglich.

Unternehmen stehen heute vor sehr unterschiedlichen Belegschaften – Babyboomer, Generation X, Millennials und Gen Z. Wie gelingt es, Arbeitsschutz so aufzubereiten, dass alle Generationen abgeholt werden?

Johannes Türk-König: Der Schlüssel liegt in der Flexibilität, die uns Software bietet. Statt starrer Einheitslösungen können wir damit gezielt auf die unterschiedlichen Gewohnheiten und Bedürfnisse verschiedener Mitarbeitergruppen eingehen. Es geht darum, Erreichbarkeit und Beteiligung passgenau zu gestalten. Je flexibler ein digitales System ist, desto höher ist die Wahrscheinlichkeit, dass wir wirklich jeden Einzelnen abholen und zur aktiven Teilnahme motivieren. Das ist der entscheidende Punkt.

Mit Tools wie UWS, VR, AR, LMRA und Alsam bietet secova viele Wege, Risiken sichtbar zu machen. Wie finden Unternehmen heraus, welche Bausteine sie wirklich brauchen – und wo ein sinnvoller Startpunkt liegt?

Johannes Türk-König: Der Start hat zwei Dimensionen: Einen schnellen Hebel und eine langfristige Strategie. Der größte Hebel ist die digitale Unterweisung. Da unterweisen Pflicht ist, muss jeder Mitarbeiter die Software nutzen. Das schafft drei positive Effekte: Die Unterweisungspflicht wird ressourcenschonend erfüllt, die Dokumentation ist rechtskonform und – am wichtigsten – wir schaffen eine garantierte Erreichbarkeit. Das ist die Basis. Darauf aufbauend folgt die Frage nach dem Gesamtziel: Wie geht man mit dem Thema Arbeitssicherheit im Unternehmen bisher um und wie soll es künftig sein? Genau hier setzen wir mit Operation Risk an. Wir verbinden die Ziele der Risikokultur mit den Möglichkeiten der Digitalisierung. GIT

Secova GmbH & Co. KG
www.secova.de

STÖRLICHTBOGENSCHUTZ

Klarer sehen und freier atmen

Die neue Störlichtbogenhaube von HB Protective für Schaltinstallateure sowie Netz- und Anlagentechniker

HB Protective Wear präsentierte auf der A+A 2025 seine neue Störlichtbogenhaube HB-ArcPro 12,5 kA für Schaltinstallateure sowie Netz- und Anlagentechniker. Sie wurde in Zusammenarbeit mit Mitgliedern des VIK-Verbands der Industriellen Energie- und Kraftwirtschaft speziell für den Einsatz bei Energieversorgern, Anlagenbau und Wartung sowie Stadtwerken und energieintensiven Branchen entwickelt.

Die Störlichtbogenhaube HB-ArcPro 12,5 kA bietet zuverlässigen Schutz und komfortables Arbeiten bei anspruchsvollen Einsätzen: Dank moderner Pure-View- und ArcVent Technologie kann der Träger klarer sehen und freier atmen

Das klappbare Flip-Visier bietet ein besonders großes Sichtfeld mit Pure View Technologie und eine beschlagfreie und kratzfeste Beschichtung. Als Frontschild wird die hochklappbare Ausführung „3P75-H: 3Phase 75 Cal“ des renommierten Herstellers Paulson Manufacturing verwendet. Der spezielle mehrlagige Materialaufbau hält in Kombination mit dem Gesichtsvisier den Lichtbogenenergien von bis zu 12,5 kA stand.

Ein extralanges Brustteil schützt den Träger zusätzlich im oftmals stark beanspruchten Brustbereich. Um ein Hochschlagen des Brustlatzes zu verhindern, ist dieser innen verstärkt und doppelt gearbeitet. Das bietet auch bei schwierigen und langwierigen Einsätzen Halt und Sicherheit. Das integrierte ArcVent-Belüftungssystem sorgt dabei für ein angenehmes Trageklima. Die Haube ist zudem so konzipiert, dass sie sich jedem darunter getragenen Helm anpasst.

Die von HB hergestellte Störlichtbogenhaube mit integriertem Gesichtsschutz hat die Lichtbogentests gemäß IEC 62819:2022 auf Basis der DIN EN 61482-1-2:2015-08 mit höheren Lichtbogenenergien bestanden. Derzeit existiert kein vergleichbares Produkt europäischer Herkunft auf dem Markt. GIT

HB Protective Wear
www.hb-online.com/de

Monika Hofmann (l.), Product Designer, und Dr. Florian Kühnlein, Director Produktgruppenmanagement Eyewear/Head

Schutzbrille mit German Design Award prämiert

Tolle Auszeichnung für die Uvex Safety Group: Für ihre neu entwickelte Schutzbrille Uvex pheos nxt guard durfte der deutsche Hersteller persönlicher Schutzausrüstung den German Design Award entgegennehmen. Die Brille überzeugt vor allem durch ihren direkt angespritzten Rahmen. Die Auszeichnung als „Winner“ rühmt „hervorragende Gestaltungsleistungen, die in ihrer jeweiligen Kategorie als wegweisend gelten“, wie es vonseiten des Rats für Formgebung heißt, der den Award vergibt. Entsprechend groß war die Freude bei Monika Hofmann, Product Designer, und Dr. Florian Kühnlein, Director Produktgruppenmanagement Eyewear/Head, als sie stellvertretend für das gesamte Uvex Team den Preis in Frankfurt in Empfang nehmen durften. Die Uvex pheos nxt guard vereint klassisch-sportliches Design, angenehme Leichtigkeit und innovativen Schutz. Ihr Highlight ist der Guard-Rahmen, der direkt an die Scheibe angespritzt wird, was die Schutzbrille enorm langlebig macht. **www.uvex-safety.de**

Blåkläder wird Mehrheitseigner bei WaschMal

Der schwedische Workwear-Hersteller Blåkläder beteiligt sich mehrheitlich an der WaschMal GmbH, einem deutschlandweit tätigen Wäscheservice für Geschäftskunden. Mit dem Einstieg Ende Dezember 2025 stärkt Blåkläder seine Servicekompetenz entlang des gesamten Lebenszyklus von Arbeitskleidung, von der Auswahl hochwertiger Workwear bis hin zu Reinigung, Pflege und Wiederverwendung im laufenden Betrieb. WaschMal mit Sitz in Köln wurde 2016 gegründet und ist auf die effektive Lohnwäsche von Berufsbekleidung spezialisiert. Das Unternehmen betreut aktuell rund 1.000 Geschäftskunden aus ganz Deutschland und arbeitet mit einem Netzwerk von etwa 400 regionalen, mittelständischen Wäschereien und Textilreinigungen zusammen. Mit seinem deutschlandweiten Abhol- und Lieferservice ermöglicht WaschMal Unternehmen, unabhängig von Hersteller oder Kollektion, eine flexible, bedarfsorientierte Komplettlösung. **www.blaklader.de**

Sicherheitsschuh Puma Safety Motion WNS

PIP EMEA hat einen modernen, komfortorientierten und ästhetisch anspruchsvollen Sicherheitsschuh für Frauen auf den Markt gebracht, die Puma Safety Motion WNS Linie. Die Motion WNS Modelle verbinden ein sportlich-dynamisches Design, angelehnt an aktuelle Trainingsschuhe, mit innovativer Sicherheitstechnologie, entwickelt speziell für den weiblichen Fuß. Frauen erwarten von einem Sicherheitsschuh heute mehr als Schutz: Er muss leicht, bequem und optimal an die natürliche Anatomie des weiblichen Fußes angepasst sein. Genau hier setzt die Motion WNS Linie an. Dank eines ergonomischen Leistens, der exakt auf die spezifischen Proportionen weiblicher Füße abgestimmt ist, bietet der Schuh nicht nur hervorragenden Halt, sondern auch einen guten Tragekomfort, vom ersten Anprobieren bis zum langen Arbeitstag. **www.ism-europa.de**

Jalas E Sport Sicherheitsschuhe

Die nachhaltige Jalas-E-Sport-Kollektion richtet sich an Unternehmen, die zuverlässigen Schutz, hohen Tragekomfort und ein modernes, sportliches Design in ihrem Sicherheitsschuh-Sortiment vereinen wollen. Die leichten, luftdurchlässigen Modelle wurden mit dem ergonomischen Know-how von Jalas entwickelt und bieten langlebige Sicherheit für typische Einsatzfelder wie Lager, Logistik, Montage und andere berufsalltägliche Umgebungen.

Viele Kunden suchten nach einem innovativen und komfortablen Sicherheitsschuh, der im harten Arbeitsalltag überzeugt und mit einem guten Preis-Leistungs-Verhältnis punktet – genau hier setze die E-Sport-Serie an, so Veronika Seliger, Distribution Relationship Managerin DACH bei Ejendals.

Die Jalas E Sport Sicherheitsschuhe sind konsequent auf ganztägigen Tragekomfort ausgelegt, insbesondere in warmen Arbeitsumgebungen oder in Innenbereichen. Luftdurchlässiges Mesh-Gewebe, atmungsaktive Lederdetails und eine ventilierende Einlegesohle sorgen für eine effiziente Luftzirkulation und verhindern Wärme- und Feuchtigkeitsstau im Schuh. Die mehrlagige FX2 Classic Einlegesohle gewährleistet dauerhafte Dämpfung und Stoßabsorption, während das ausgewogene, leichte Design Ermüdungserscheinungen reduziert.

Neben dem Komfort steht die sichere Performance im Mittelpunkt der E-Sport-Linie. Eine Zehenschutzkappe aus Aluminium bietet normgerechten Schutz, ohne unnötiges Gewicht hinzuzufügen, und die Jalas-Eco-Flex-Nageldurchtrittschutz-Einlage aus teilweise recyceltem Polyester erhöht die Sicherheit bei Tätigkeiten auf potenziell gefährlichen Untergründen.

Dank des zertifizierten Leitergrip-Systems (LG), das durch einen definierten Absatz einen sicheren Stand auf Leitern gewährleistet und ein Abrutschen verhindert, ist zuverlässiger Halt bzw. gute Rutschfestigkeit gegeben. Die wasserabweisenden Materialien schützen im Arbeitsalltag und machen die Modelle für eine Vielzahl typischer Industrie- und Handwerksanwendungen geeignet. **www.ejendals.com**

Liebe Leserinnen und Leser,

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

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

SICHERHEITS MANAGEMENT

Sicherheitsmanagement

barox
Switche für Video

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

Sicherheitsmanagement

GU BKS SERVICE

GU BKS SERVICE GmbH
Heidestr. 71 · 42549 Velbert
Tel. 0800/2051001
office@gu-bks.de · www.gu-bks.de
Service mit System GU BKS

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

hensec
secure solutions

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

ABUS
Security Tech Germany

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

Sicherheitsmanagement

DAITEM

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

Sicherheitsmanagement

idware
Identity • Access • Control

ID-ware Deutschland GmbH
Walther-von-Cronberg-Platz 2-18, Haus 6
60594 Frankfurt am Main
Tel. 069-210 855 60
info@id-ware.com, www.id-ware.com
Physical Identity & Access Management (PIAM)-Lösungen für große Organisationen, Software sowie Dienstleistungen für smarte Identifikations- und Authentifizierungsprozesse: PIAM-Suite, Credential Management, Access Management, Visitor Management, Contractor Management, SDK zur Kartenpersonalisierung, Photo Capture Tool, Hardware, Secure Credential Consultancy, Credentials as a Service

Sicherheitsmanagement

ASSA ABLOY
Opening Solutions

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

Sicherheitsmanagement

deister electronic

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

Sicherheitsmanagement

NSC
Sicherheitstechnik GmbH

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

Sicherheitsmanagement

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

Gebäudesicherheit

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

PERIMETER SCHUTZ

Sicherheitsmanagement

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

Gebäudesicherheit

SimonsVoss Technologies GmbH
Münchner Str. 16 · 85774 Unterföhring
Tel.: 089 992280
marketing-simonsvoss@allegion.com
www.simons-voss.com
Digitale Schließanlagen mit Zutrittskontrolle, kabellose und bohrungsfreie Montage, batteriebetrieben, keine Probleme bei Schlüsselverlust.
Digital Schließen ist neu für Sie? Rufen Sie an: 089 99228-555

Perimeterschutz

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

GEBÄUDE SICHERHEIT

VIDEO ÜBERWACHUNG

Gebäudesicherheit

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

Gebäudesicherheit

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

Videoüberwachung

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

Gebäudesicherheit

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

Gebäudesicherheit

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

Videoüberwachung

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

Gebäudesicherheit

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

Gebäudesicherheit

Uhlmann & Zacher GmbH
Gutenbergstraße 2-4 · 97297 Waldbüttelbrunn
Tel.: +49(0)931/40672-0 · Fax: +49(0)931/40672-99
contact.uz@assaabloy.com · www.uhlmannzacher.com
Elektronische Schließsysteme, modular aufgebaut und individuell erweiterbar.
Seit 2025 gehört das Unternehmen zur Assa Abloy-Firmengruppe.

Videoüberwachung

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

Videoüberwachung

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

Zeit + Zutritt

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

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

Videoüberwachung

Zeit + Zutritt

CES
C.Ed. Schulte GmbH Zylinderschlossfabrik
Friedrichstraße 243 · D-42551 Velbert
Objektabteilung@ces.eu · www.ces.eu
Mechanische, mechatronische und elektronische Schließsysteme, Zutrittskontrolle

Zeit + Zutritt

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

Zeit + Zutritt

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

Zeit + Zutritt

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

Zeit + Zutritt

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

Zeit + Zutritt

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

Zeit + Zutritt

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-Karusselltüren und -Portale für die Sicherheits-Zutrittskontrolle und Personenvereinzelung.

Zeit + Zutritt

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

Zeit + Zutritt

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

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

Zeit + Zutritt

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

Zeit + Zutritt

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

NOTRUF SERVICE LEITSTELLE

Notruf- und Service-Leitstelle

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

Notruf- und Service-Leitstelle

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

BRAND SCHUTZ

Brandschutz

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

Brandschutz

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

ARBEITS SICHERHEIT

Brandschutz

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

Brandschutz

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

Arbeitssicherheit

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

Arbeitssicherheit

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

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

GEFAHRSTOFF MANAGEMENT

Gefahrstoffmanagement

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

Gefahrstoffmanagement

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

Gefahrstoffmanagement

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

Gefahrstoffmanagement

SÄBU Morsbach GmbH
Zum Systembau 1 · 51597 Morsbach
Tel.: 02294 694-24 · Fax: 02294 694-38
safe@saebu.de · www.saebu.de
Gefahrstofflagerung, Gefahrstoffcontainer, Auffangwannen, Bodenschutzsysteme, Gasflaschenlagerung, Gasflaschencontainer, Gasflaschenbox, Kleingebinderegale
Unser Online-Shop: www.fladafi.de

GASMESS TECHNIK

Gasmesstechnik

smart GasDetection Technologies

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

MASCHINEN ANLAGEN SICHERHEIT

Maschinen + Anlagen

EUCHNER
More than safety.

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

Maschinen + Anlagen

IBF

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

Maschinen + Anlagen

SCHMERSAL
THE DNA OF SAFETY

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

Maschinen + Anlagen

PEPPERL+FUCHS

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

Maschinen + Anlagen

pizzato

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.

WILEY

35 Jahre

Git Sicherheit

Nächstes Heft: die Jubiläumsausgabe

Mit VIP-Statements, Standortbestimmungen, Trend-Reports – und einer Zeitreise durch 35 Jahre Sicherheit

Kontakt: GIT-GS@Wiley.com

DIE VIP LOUNGE

Sven Dawson

Head of Corporate Security, Airbus Defence and Space

Ihr Berufswunsch mit 20 war: Da ich damals bereits bei der Bundeswehr verpflichtet war, hatte ich den Drang, etwas Interessantes und Erfüllendes zu machen – dies hat sich bis heute nicht geändert.

Was hat Sie dazu bewogen, eine Aufgabe im Bereich Sicherheit zu übernehmen? Neugierde und die Vision, dass das Thema zunehmend wichtiger wird. So ist es auch gekommen.

Welche sicherheitspolitische Entscheidung oder welches Projekt sollte Ihrer Meinung nach schon längst umgesetzt sein? Die europäischen Staaten sollten viel mehr Zusammenarbeit wagen, als weiterhin zu versuchen, nationale Egoismen durchzusetzen. Auf diesen vulnerablen Punkt werden wir verstärkt von außen hingewiesen.

Was ist die Ihrer Meinung nach die beste Erfindung im Bereich Sicherheit? Die wirkungsmächtigsten Erfindungen im Bereich Sicherheit folgen meiner Meinung nach drei grundlegenden Prinzipien: Schutz von Informationen, Kontrolle von Zugang und frühzeitige Erkennung von Bedrohungen. Kryptographie bildet heute das Fundament der digitalen Sicherheit; mechanische und elektronische Zugangssysteme sichern physische Räume und kritische Infrastrukturen, während Technologien wie Radar erstmals eine Frühwarnfähigkeit gegenüber Bedrohungen geschaffen haben. Zusammen bilden diese Prinzipien die Grundarchitektur moderner Sicherheits- und Resilienzsysteme in Staat, Industrie und Verteidigung.

Ein Erfolg, den Sie kürzlich errungen haben, war: Wir haben erfolgreich Mitarbeiter aus einer kritischen Situation unversehrt evakuieren und gesund nach Hause bringen können. Diesen Lagen begegnen wir zunehmend leider öfter.

Wer hat Ihrer Meinung nach eine Auszeichnung verdient? Mein Podcast-Favorit Paul Ronzheimer. Er schafft es mit seinem Engagement nicht nur, Themen sehr gut und professionell zu beleuchten, sondern auch alle spannenden Themen tagespolitisch aktuell zu halten.

Wobei entspannen Sie? Handwerken, Gartenarbeit und generell Outdooraktivitäten

Welchen Urlaubsort können Sie empfehlen? Städte: Singapur, New York, Boston. Länder: USA.

Welche Zeitschriften lesen Sie regelmäßig? Der Spiegel

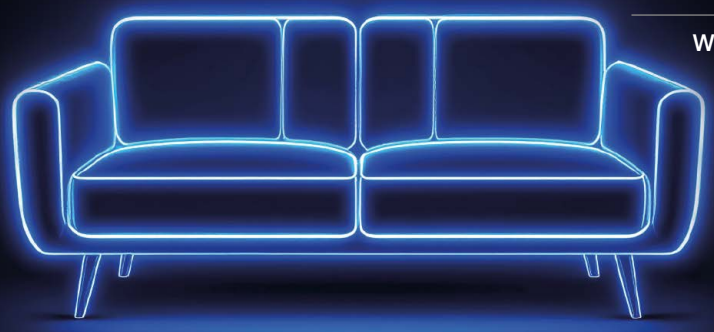
Die GIT SICHERHEIT ist für mich wichtig, weil sie eine Plattform darstellt, in dem die wichtigen Security-Entscheidungsträger aus der Industrie regelmäßig zu Wort kommen.

Welches Buch haben Sie zuletzt gelesen? „Shitbürgertum“ von Ulf Poschardt und davor „Wenn Russland gewinnt: Ein Szenario“ von Carlo Masala.

Welche Musik hören Sie am liebsten? Ich bin hier nicht wirklich festgelegt und gehe hier eher nach Laune, was ich gerade hören mag.

Was motiviert Sie? Dinge mit einem engagierten und motivierten Team zu bewegen und im Sinne der Sache voranzubringen. In der heutigen Welt ist Sicherheit nicht mehr nur ein Kostenfaktor für Unternehmen, sondern eine Grundvoraussetzung dafür, überhaupt Geschäfte tätigen zu können.

Worüber machen Sie sich Sorgen – und was stimmt Sie zuversichtlich? Wir haben als Land noch immer nicht wirklich verstanden, wie sehr wir uns transformieren und neu erfinden müssen. Wir sind zu langsam und schwerfällig, unser öffentlicher Dienst ist zu groß und teuer. Wir müssen mehr wagen und uns selbstbewusster in der Welt darstellen. Mich stimmt es zuversichtlich, dieses Thema immer öfter diskutieren zu können, denn dadurch stoßen wir den Wandel hoffentlich schneller an.



SicherMacher

Der GIT-Talk mit den Marktführern

GIT SICHERHEIT

Kontakt:
Miryam.Reubold@Wiley.com

WILEY

Smart messen mit X-meas

Im Turnaround, während der Revision und im Tagesgeschäft: Mit X-meas effizient und präzise freimessen, automatisch dokumentieren und digital freigeben. Der smarte Messassistent koordiniert Aufgaben via App und speichert Messprotokolle sicher in der Cloudsoftware.

Dräger

Technik für das Leben