34. JAHRGANG | November 2025 | AUSGABE 11

JVA Special
ab Seite 20

GIT SICHERHEIT

MAGAZIN FÜR SAFETY UND SECURITY

30 926

Ausgabe ONLINE lesen:

Titelthema Seite 66:

Made in Europe, gedacht für Deutschland

Interview mit Matthias Höhl, Country Sales Manager bei Pizzato

HEFT IM HEFT

MASCHINEN-SICHERHEIT
ab S. 64

WILEY

EUCHNER

More than safety.

SAFETY SERVICES

CONSULTING – ENGINEERING – TRAINING

UNSER TEAM BEGLEITET SIE – IN ALLEN LEBENSPHASEN IHRER MASCHINE

- Rechtssichere Beratung zur Maschinensicherheit – von der CE-Kennzeichnung bis zum sicheren Betrieb
- Unterstützung bei Konstruktion, Programmierung und Inbetriebnahme
- Praxisorientierte Schulungen
- Internationales Experten-Team

Kommen Sie vorbei!

> **SPS Nürnberg**
> Halle 7 / Stand 280

KI & Co. in der Maschinensicherheit

Resilienz ist das Wort der Stunde – nicht nur für uns Menschen, sondern auch für Maschinen und Anlagen. Gerade im Licht neuer regulatorischer Anforderungen gewinnt sie an Bedeutung. Die aktuelle Ausgabe der GIT SICHERHEIT setzt deshalb auf Innovation und tatkräftigen Optimismus – Werte, die unsere Branche in allen Facetten prägen.

Ein besonderes Highlight in diesem Sinne ist unser Titelthema ab Seite 66: Unter dem programmatischen Motto „Made in Europe, gedacht für Deutschland" zeigen Giuseppe Pizzato und Matthias Höhl, wie europäische Hersteller mit Flexibilität und Innovationskraft auf die Anforderungen des deutschen Marktes reagieren – und warum „Made in Europe" zunehmend als Qualitätsversprechen gilt.

Pünktlich zur Messe SPS – Smart Production Solutions 2025 in Nürnberg präsentieren wir Ihnen unser „Heft im Heft" zur Maschinensicherheit (ab Seite 64). Die Messe bleibt auch in wirtschaftlich herausfordernden Zeiten ein starkes Signal für die Branche. Im Interview mit Sylke Schulz-Metzner (ab Seite 72), erfahren Sie, wie die Veranstaltung die zentralen Trends der Automatisierung abbildet und welche Fokusthemen – von Industrial AI über digitale Zwillinge bis hin zu Cyber- und IT-Security – dieses Jahr im Mittelpunkt stehen.

Im Innentitel unseres Hefts im Heft stellt Bernstein sein neues „Gänseblümchen" vor – eine elektronische Zuhaltung, die das Smart Safety System um eine entscheidende Funktion ergänzt (ab Seite 64). Ebenfalls im Rahmen unseres Schwerpunktthemas schließen wir unsere Reihe „Maschinensicherheit im Kontext von KI und Security" in Kooperation mit VDMA und ZVEI ab. Diesmal geht es um den Cyber Resilience Act und die Maschinenverordnung: Welche Herausforderungen und Chancen bringen die neuen EU-Regularien? Die Antworten liefern wir Ihnen ab Seite 84.

Ein weiteres Fokusthema ist der Brandschutz im Vorfeld der VdS-Brandschutztage. Unsere Innentitel-Story über die Wagner Group (ab Seite 46) zeigt, wie Sauerstoffreduzierung und innovative Technologien die Betriebsfähigkeit kritischer Infrastrukturen sichern – und präventive Lösungen zum Standard machen.

Noch vor den VdS-Brandschutztagen, wie diese im schönen Köln, findet die PMRExpo statt (25.-27. November), zu der wir letzte News für Sie auf Seite 12 zusammengestellt haben. Sichere Kommunikation ist hier das Thema.

Abgerundet wird die Ausgabe durch unser JVA-Special (ab Seite 20), das praxisnahe Einblicke in die Sicherheit im Justizvollzug bietet – von KI-gestützter Suizidprävention über nachhaltiges Bauen bis hin zu aktuellen rechtlichen und technischen Entwicklungen.

Unser Team wünscht Ihnen eine inspirierende Lektüre, viele neue Impulse und einen erfolgreichen Austausch auf den Messen dieser Tage – ob auf der SPS, den VdS-Brandschutztagen oder der PMRExpo. GIT

Herzlichst,
Ihr

T. Gimbel

Dr. Timo Gimbel
für das Team GIT SICHERHEIT

TITELTHEMA

Made in Europe - Sicherheit für die deutsche Industrie

Interview mit Matthias Höhl und Giuseppe Pizzato

Seite 66

Carsten Baeck

Thomas Dallmeier

Thomas Kress

Ulrich Höfer

MANAGEMENT

JVA-SPECIAL

HEFT IM HEFT | MASCHINENSICHERHEIT

Sylke Schulz-Metzner

Alexander Aust

Carsten Gregorius und Frank Bauder

SECURITY

CYBER-SECURITY

RUBRIKEN

BRANDSCHUTZ

SAFETY

INDEX

QUICK-FINDER

ORGANISATIONEN, INSTITUTIONEN UND UNTERNEHMEN IM HEFT

NEWS

Erfolgreiche Premiere der SicherheitsExpo Berlin

Die SicherheitsExpo Berlin feierte Mitte September in der Veranstaltungslocation Station Berlin Premiere. Aussteller und Besucher zeigten sich sehr zufrieden mit der neuen Veranstaltung. Eine Fortsetzung der SicherheitsExpo Berlin ist geplant: am 22. und 23. September 2027 in der Station Berlin. Die Geschäftsführer des Messeveranstalters AFAG, Henning und Thilo Könicke, zeigen sich mit der ersten Ausgabe der SicherheitsExpo Berlin sehr zufrieden: „Die Premiere in Berlin war ein voller Erfolg. Mit der SicherheitsExpo Berlin hat die Hauptstadt nun eine spezialisierte Fachmesse rund um das wichtige Thema Sicherheit. Das Feedback der Aussteller ist sehr positiv: Wir konnten die richtigen Besucher für die Messe gewinnen. Gleichzeitig sehen wir, dass die Veranstaltung noch Entwicklungspotenzial hat, das wir gemeinsam mit der Branche schöpfen möchten." Das Angebot der rund 70 Aussteller umfasste wichtige Bereiche der Sicherheitstechnik, wie Zutrittskontrolle, Videoüberwachung, Brandschutz, Perimeter Protection und IT-Security. **www.afag.de**

Generationenwechsel beim Verband für Sicherheitstechnik

Wilfried Joswig

Wilfried Joswig hat die Geschäftsführung des Verbandes für Sicherheitstechnik (VfS) sowie der VfS Forum Sicherheit GmbH an seinen Nachfolger Dipl.-Ing. Carsten Feddern übergeben. Nach über 15 engagierten Jahren hat sich Wilfried Joswig gemeinsam mit seinem Co-Geschäftsführer Prof. Dr. Clemens Gause bereits in den letzten beiden Jahren intensiv Gedanken über eine mögliche Nachfolge gemacht, um gerade in Zeiten zunehmender Anforderungen an die Sicherheitstechnik auch zukünftig den Verband mit einer hohen Kontinuität weiterzuführen. Carsten Feddern bringt über 25 Jahre Führungserfahrung aus der Sicherheits- und Gebäudetechnik bei Siemens mit und ist auch bereits seit über 20 Jahre im VfS aktiv. Auch Wilfried Joswig bleibt dem VfS weiterhin verbunden und wird sein anerkanntes Know-how insbesondere in laufenden und zukünftigen Forschungsprojekten einbringen. **www.vfs-hh.de**

Assa Abloy akquiriert Kentix GmbH

Assa Abloy hat die Kentix GmbH, ein führendes Unternehmen von digitalen und IoT Zugangs- und Überwachungslösungen für Rechenzentren, übernommen. Das Unternehmen mit Sitz in Idar-Oberstein hat rund 50 Mitarbeiter.

Mit der Übernahme von Kentix stärkt Assa Abloy seine Position als führender Anbieter von Zutrittslösungen und ergänzt sein Portfolio gezielt um digitale Sicherheitslösungen für Data Center-Applikationen. „Ich freue mich sehr, Kentix in unserem Team willkommen zu heißen. Kentix steht für technologische Exzellenz, Agilität und herausragende Kundenlösungen – genau diese Stärken wollen wir bewahren und gezielt skalieren", so Achim Haberstock, SVP & Head of Central Europe bei Assa Abloy Opening Solutions EMEIA.

„Mit der Akquisition von Kentix stärkt Assa Abloy sein Produktportfolio im Bereich digitaler Sicherheitslösungen für Data Center-Anwendungen – sowohl in Deutschland als auch in der gesamten EMEIA-Region", erklärt David Moser SVP & Head of Digital and Access Solutions bei Assa Abloy Opening Solutions EMEIA.

Die Geschäftsführung von Kentix sieht die Integration in die weltweit agierende Assa Abloy Gruppe als einen positiven Schritt in Richtung Zukunft und nachhaltigem Wachstum. „Schon heute bestehen starke Gemeinsamkeiten zwischen Kentix und Assa Abloy. Durch die Integration eröffnen sich für Kentix neue Märkte und zusätzliche Vertriebsmöglichkeiten innerhalb der globalen Assa Abloy Gruppe", so Geschäftsführer Thomas Fritz. „Als Teil der Assa Abloy Gruppe haben wir die Chance, die Stärken beider Unternehmen zu bündeln und unsere Kunden künftig noch gezielter und umfassender zu bedienen. Gleichzeitig schaffen wir langfristig zusätzliche Ressourcen und Entwicklungsmöglichkeiten für unsere Mitarbeitenden", ergänzt Thomas Fritz.

Mit einer erweiterten Führungsstruktur und dem bestehenden Team bleibt Kentix auf Wachstumskurs und stärkt seine Marktposition nachhaltig. Für die Mitarbeiter ändert sich nichts, der Standort in Idar-Oberstein bleibt erhalten. **www.assaabloy.com/de**

25-Jahr-Feier Priorit (v. l. n. r): Landrat Patrick Puhlmann, Vorstand Priorit AG Tobias Väthjunker, Bürgermeister Stadt Osterburg Nico Schulz

25 Jahre Priorit AG – Jubiläumsfeier mit Blick in die Zukunft

Mit einer festlichen Veranstaltung hat die Priorit AG ihr 25-jähriges Firmenjubiläum begangen. Zahlreiche Gäste, darunter Geschäftspartner, Bürgermeister und Landrat sowie die Belegschaft aus Hanau und Osterburg, nahmen an den Feierlichkeiten teil und machten das Jubiläum zu einem besonderen Ereignis. In seiner Ansprache erinnerte der Vorstand Tobias Väthjunker zunächst an den kürzlich verstorbenen Firmengründer Reuter, dessen Visionen und Innovationskraft das Fundament des Unternehmens legten. „Viele unserer Produkte tragen noch heute seine Handschrift und prägen unseren wirtschaftlichen Erfolg“, betonte er.

Ein Rückblick verdeutlichte die Entwicklung der Priorit AG seit der Gründung im Jahr 2000. Von den ersten Produkten im Brandschutzbereich über den Meilenstein Priodek H bis hin zu heutigen Lösungen für eine sichere Lagerung von Lithium-Ionen-Akkus hat sich das Unternehmen kontinuierlich weiterentwickelt. **www.priorit.de**

TeleTrusT auf IT-Sicherheitsmesse und Kongress it-sa

Der Bundesverband IT-Sicherheit e. V. (TeleTrusT) beteiligte sich aktiv an der nationalen Leitmesse für IT-Sicherheit it-sa in Nürnberg. TeleTrusT ist Premium Partner und unterstützt die it-sa seit ihrer Etablierung. Die it-sa versteht sich als nationale und internationale IT-Sicherheitsmesse und Kongress, die ein breites Spektrum an Produkten und Dienstleistungen abbildet. Die NürnbergMesse als Trägergesellschaft ist TeleTrusT-Mitglied. Auf der it-sa 2025 präsentierte sich TeleTrusT mit einem erneut erweiterten Messeauftritt mit einigen Verbandsmitgliedern sowie mit einem Begleitprogramm. **www.teletrust.de**

Hekatron stattet SOS-Kinderdorf Schwarzwald mit Rauchwarnmeldern aus

Mehr Raum, mehr Sicherheit: Auch in den Kellergeschossen können sich die Kinder und Jugendlichen dank funkvernetzter Rauchwarnmelder nun behütet aufhalten

Damit Kinder spielen, träumen und sich gesund entwickeln können, brauchen sie Geborgenheit. Um dieses Gefühl im SOS-Kinderdorf Schwarzwald zu stärken, hat Hekatron Brandschutz der Einrichtung zusätzliche Rauchwarnmelder gespendet. Ziel ist es, die Sicherheit auch in den Kellerbereichen zu erhöhen – und damit neue Räume für Spiel und Begegnung zu erschließen. Die unscheinbaren Lebensbeschützer sind per Funk mit den Rauchwarnmeldern auf anderen Etagen vernetzt. Sollte es tatsächlich irgendwo im Haus brennen, alarmieren sämtliche Rauchwarnmelder – stockwerkeübergreifend. So werden auch Kinder, die sich zum Spielen in den Kellerräumen aufhalten, rechtzeitig gewarnt. „Hekatron unterstützt uns seit vielen Jahren dabei, unsere Häuser mit modernen Rauchwarnmeldern auszustatten. Mit den zusätzlichen Geräten können wir künftig auch die ausgebauten Kellerräume in einigen unserer Wohngruppen und Kinderdorffamilien als weitere sichere Spielfläche für die Kinder und Jugendlichen nutzen“, erklärt Ulrike Ebbing, Einrichtungsleitung im SOS-Kinderdorf Schwarzwald. **www.hekatron.de**

Langfristige Problemlöser

Im Gespräch mit Carsten Baeck, Geschäftsführender Gesellschafter, DRB Deutsche Risikoberatung

© DRB

Carsten Baeck hat als Polizeibeamter begonnen. Nach seiner Weiterqualifizierung als Betriebswirt war er mehr als ein Jahrzehnt lang in leitenden Positionen großer deutscher Sicherheitsdienstleister tätig – immer mit dem Fokus auf Schutz, Risikomanagement und Krisenbewältigung. 2005 hat er zusammen mit Robert Kilian die Deutsche Risikoberatung, DRB gegründet.

GIT SICHERHEIT: Herr Baeck, Sie sind geschäftsführender Gesellschafter der DRB Deutsche Risikoberatung und zusammen mit Robert Kilian deren Mitgründer. Wie kam es zu dieser Gründung und wie haben Sie die Aufgaben untereinander verteilt?

Carsten Baeck: Wir haben uns mit Gründung der DRB 2005 vor allem das Ziel gesetzt, Unternehmen bei der Minimierung von Risiken zu unterstützen. Dabei ging es aber von Anfang an auch darum, ihnen aufzuzeigen, wie sich Risiken in strategische Chancen verwandeln lassen. Was die Aufgabenverteilung betrifft: Meine Aufgaben bei der DRB umfassen neben der Geschäftsführung weiterhin die persönliche Beratung einiger unserer wichtigsten Kunden und mein Partner Robert Kilian leitet unser Büro in Frankfurt.

Sie sind daneben auch politisch aktiv?

Carsten Baeck: Das bin ich in der Tat schon seit rund 25 Jahren und ich engagiere mich in den Verbänden für Sicherheit in der Wirtschaft (ASW/VSWn) als Vorstandsmitglied. Privat liebe ich das Meer und halte mich gerne in meiner Heimat Fehmarn an der Ostsee sowie in Portugal auf, dessen herzliche Kultur ich sehr schätze. Ich bin zudem leidenschaftlicher Beachvolleyball-Spieler und genieße die Zeit mit meiner Familie und meinen Kindern.

Sprechen wir gleich einmal etwas näher speziell über Ihre Leidenschaft für das Thema Sicherheit. Das ist, wie wir alle wissen, ein weiter Begriff. Was umfasst das für Sie im Zusammenhang mit der DRB?

Carsten Baeck: Unser Fokus liegt klar auf dem Bereich „Operationale Risiken". Dabei unterstützen wir Unternehmen in den Feldern Spionage- und Sabotageabwehr, Informationsschutz, Krisen- und Notfallmanagement sowie im Bereich internationaler Ermittlungen. Über die Jahre hinweg haben wir uns den Ruf eines zuverlässigen Problemlösers erworben. Das bedeutet, dass wir

uns nicht nur um die reine Gefahrenabwehr kümmern, sondern auch strategisch beraten und Handlungsempfehlungen für den Ernstfall geben – und zwar immer individuell auf das jeweilige Unternehmen zugeschnitten. Ergänzend dazu setzen wir auf ein robustes Risiko- und Business Continuity Management (BCM), um Unternehmen nicht nur als unmittelbarer „Problemlöser" zur Seite zu stehen, sondern sie auch langfristig auf die sich ständig ändernde Risikolage vorzubereiten und zu betreuen.

Wie kann man sich Ihre Kundenstruktur vorstellen – und in welchen Bereichen haben Sie die größten Erfahrungen?

Carsten Baeck: Wir arbeiten vorwiegend für international tätige deutsche Unternehmen. Die Mehrzahl der DAX-Unternehmen gehört zu unseren Kunden, aber auch eigentümergeführte Unternehmen und exponierte Familien. Die größten Erfahrungen haben wir in der Spionage- u. Sabotageabwehr, im Informationsschutz und im Krisen- und Notfallmanagement. Wir sind aber auch Vertrauenspartner für internationale Ermittlungen.

Herr Baeck, lassen Sie uns einmal generell über die Gefährdungslage sprechen, mit denen es Unternehmen in Deutschland und international heute zu tun haben. Von Cyberangriffen bis zu Drohnenattacken kann alles dabei sein. Wo liegen aus Ihrer Wahrnehmung in der Beratung von Kunden die drängendsten Gefährdungen von außen, vor denen sich ein Unternehmen wappnen muss?

Carsten Baeck: Deutschland als führender Wirtschaftsstandort mit vielen innovativen Unternehmen ist leider auch ein attraktives Ziel für Spionage und Sabotage. Die hybride Kriegsführung – also die Vermischung digitaler und physischer Angriffe – nimmt zudem zu und stellt Unternehmen wie auch staatliche Strukturen vor große Herausforderungen. Insbesondere im Bereich der Kritischen Infrastruktur sehen wir einen enormen Schutzbedarf. Unsere Aufgabe ist es, Unternehmen zu sensibilisieren und sie konkret bei der Identifikation sowie Abwehr dieser Bedrohungen zu unterstützen.

Auch von politischer Seite her versucht man, diesen Gefahren zu begegnen. Hier ist etwa die nationale Wirtschaftsschutzstrategie des Bundesministeriums des Inneren und für Heimat zu nennen. Ziel ist es, die Resilienz u.a. unserer Wirtschaft vor illegitimer Einflussnahme von außen zu stärken. Wie nehmen Sie das wahr, welchen Stellenwert messen Sie diesen Maßnahmen bei?

Carsten Baeck: Der Wirtschaftsschutz muss tatsächlich oberste Priorität genießen, und zwar sowohl bei Unternehmen als auch in der Politik. Die bestehenden staatlichen Initiativen sind ein wichtiger Schritt, reichen aber meines Erachtens noch nicht aus. Eine deutlich engere und ressourcenstärkere Zusammenarbeit von Staat und Wirtschaft wäre notwendig, um effektiv auf die wachsenden Bedrohungen reagieren zu können. Hier sehe ich noch viel Luft nach oben.

> „Risiken lassen sich in strategische Chancen verwandeln

Betrachten wir einmal den Beratungsprozess: Sie vermitteln ja unter anderem auch Know-how darüber, wie Wirtschaftsspionage überhaupt funktioniert?

Carsten Baeck: Neben jeder Beratungsleistung, die wir durchführen ist es natürlich auch wichtig bei den Unternehmen ein Verständnis dafür zu entwickeln wie Spionage und Sabotage funktionieren. Dazu bieten wir individuell zugeschnittene Workshops und Trainings an, in denen potenzielle Angriffsszenarien durchgespielt und Präventionsmaßnahmen erarbeitet werden. Nur wenn man die Methoden der Täter kennt, kann man sich erfolgreich schützen.

Wie individuell verschieden sind Sicherheitsrisiken eigentlich, wenn man verschiedene Unternehmen vergleicht? Die Gefährdungslage dürfte sich bei vergleichbaren Unternehmen vermutlich kaum unterscheiden?

Carsten Baeck: Jedes Unternehmen hat ein eigenes individuelles Risikoprofil. Dieses gilt es zu erheben und zumindest jährlich fortzuschreiben. Natürlich ähneln sich Risiken z.B. in der gleichen Branche, daher ist der Erfahrungsaustausch untereinander hilfreich und wichtig. Hier sind z.B. die ASW-Allianz für Sicherheit in der Wirtschaft bzw. die VSWn wichtige Plattformen.

Lassen Sie uns das weitere Vorgehen in der Zusammenarbeit mit einem Kunden einmal durchdeklinieren. Es könnte ja beispielsweise mit einem Audit beginnen...?

Carsten Baeck: Genau. In der Regel starten wir mit einem vertraulichen Gespräch mit den Sicherheitsverantwortlichen und idealerweise der Geschäftsführung, um ein Grundverständnis von Zielen, Sorgen und Handlungsfeldern zu bekommen. Darauf folgt ein Kick-off-Workshop, in dem wir gemeinsam die bestehenden Sicherheitsstrukturen, aber auch eventuelle Schwachstellen beleuchten. Anschließend führen wir ein strukturiertes Audit durch, das auf die jeweilige Branche und das Geschäftsmodell zugeschnitten ist. Dieses umfasst Risikoanalysen, Risk Assessments und Schutzbedarfsanalysen. Wichtig ist dabei ein offener Austausch, denn nur auf Basis eines fundierten und ehrlichen Bildes lassen sich passgenaue Maßnahmen entwickeln. Selbstverständlich sichern wir dem Kunden hierbei absolute Vertraulichkeit zu.

Sie entwickeln daraufhin umfassende Schutzkonzepte. Könnten Sie das einmal anhand des einen oder anderen Beispiels anschaulich machen?

Carsten Baeck: Nehmen wir zum Beispiel eine Großveranstaltung: Am Anfang steht ein ausführliches Risk Assessment, das wir gemeinsam mit allen relevanten Stakeholdern durchführen, um ein Risikoinventar zu erstellen und die spezifische Bedrohungslage detailliert zu erfassen. Daraus leiten wir gemeinsam mit dem Kunden einen individuellen Schutzbedarf ab. Der kontinuierliche Austausch mit staatlichen Sicherheitsbehörden ist dabei essenziell, um jederzeit auf neue Entwicklungen reagieren zu können.

Je nach Komplexität benötigt man oft mehrere Monate, gelegentlich sogar ein Jahr, um ein solches Konzept passgenau umzusetzen. Durch regelmäßige Jour-fixe-Termine mit dem Projektteam bleiben alle Beteiligten eng eingebunden und auf dem aktuellen Stand. Dabei achten wir besonders auf eine kontinuierliche Risikobewertung, weil sich Bedrohungslagen dynamisch verändern können. Unser Ansatz ist stets persönlich und partnerschaftlich: Wir stimmen uns eng mit unseren Kunden ab, damit das Schutzkonzept laufend überprüft und bei Bedarf weiterentwickelt werden kann.

Wie kommt dabei Ihr Netzwerk von Partnern und Experten ins Spiel?

Carsten Baeck: Wir sind eine kleine Firma und das ist richtig so. Für jedes Projekt brauchen wir den richtigen Partner, gerade weltweit. Unsere Partner sind Vertraute,

Experten auf ihrem Gebiet. Insbesondere mein Partner Robert Kilian hat da als ehemaliger Group Risk Manager bei Ikea über 15 Jahre ein weltweites Netzwerk aufgebaut. Es gibt kaum ein Land auf dieser Welt in dem wir keine zuverlässigen und erfahrenen Partner haben.

Sie sind Partner des Zertifizierungssystems „Shore". Hier geht es ja vor allem um Standards für Immobilien, insbesondere in den Bereichen Retail, Hotels und Events?

Carsten Baeck: Shore steht für „Safe, Hospitality, Office, Retail und Entertainment" und ist das weltweit einzige unabhängige und international anerkannte Zertifizierungssystem, das sich konkret auf operationelle Risiken, Resilienz und Governance in Immobilien fokussiert. Es findet Anwendung in über 30 Ländern und wird insbesondere für Shoppingcenter, Einzelhandelsflächen, Büros, Hotels, Messen und Veranstaltungsorte genutzt.

Das Besondere an Shore ist die Harmonisierung von ESG-Zielen (Environment, Social, Governance) mit der Sicherheitsperspektive. So werden nicht nur Umweltschutz und Nachhaltigkeit berücksichtigt, sondern auch Sicherheitsaspekte, Governance-Strukturen und das Wohlbefinden der Menschen vor Ort. Damit bietet Shore eine hervorragende Ergänzung zu unserem eigenen Sicherheitsansatz, weil es eine ganzheitliche Bewertung von Assets ermöglicht und dabei gezielt auf den Schutz von Mitarbeitern, Besuchern und Investoren eingeht.

Welche Vorteile hat diese Zertifizierung?

Carsten Baeck: Zum einen schafft eine Shore-Zertifizierung Transparenz über den aktuellen Sicherheitsstatus einer Immobilie. Schwachstellen werden klar benannt, Handlungsfelder werden eindeutig aufgezeigt. Darüber hinaus ergeben sich handfeste Vorteile in Bezug auf ESG-Richtlinien, die zusehends von Investoren, Banken und Versicherern eingefordert werden. Nicht zuletzt steigert die Zertifizierung den Wert eines Assets, indem sie die Bereiche Sicherheit, Nachhaltigkeit und soziale Verantwortung glaubwürdig dokumentiert. Gerade im Kontext der EU-Taxonomie und den UN-Nachhaltigkeitszielen gewinnen ESG-Aspekte rasant an Bedeutung. Shore liefert hier einen Branchenmaßstab, an dem sich Betreiber und Investoren orientieren können.

Wie sieht so ein Zertifizierungsprozess aus?

Carsten Baeck: Hier kommt Robert Kilian ins Spiel. Er ist der Experte bei uns für dieses Thema und hat diesen international anerkannten Standard mit entwickelt. Der Prozess beginnt mit der Erhebung relevanter Daten – hierbei werden alle wichtigen Unterlagen und Informationen zur Immobilie zusammengetragen. In vielen Fällen erfolgt das teils über Online-Fragebögen, um ein möglichst umfassendes Bild zu erhalten. Ein von Shore akkreditierter Gutachter prüft anschließend die Unterlagen, bewertet das operationelle Risikomanagement und legt damit den Ausgangspunkt für die Zertifizierung fest.

Danach findet je nach gewünschtem Zertifizierungsniveau eine Vor-Ort- oder Online-Prüfung statt. Dabei wird detailliert analysiert, welche Maßnahmen bereits greifen, wo Verbesserungspotenzial besteht und inwiefern ESG-Kriterien erfüllt werden. Bei erfolgreicher Prüfung erhält das Asset eine von drei Zertifizierungsstufen: Zertifiziert, Gold oder Platin.

Die Zertifizierung ist drei Jahre gültig, wird aber durch zwei jährliche Compliance-Checks begleitet, um sicherzustellen, dass die Shore-Kriterien laufend erfüllt werden und der Betreiber weiterhin ein hohes Niveau an Sicherheit und Governance aufrechterhält. Für die Berichterstattung im Rahmen der EU-CSR Directive oder andere ESG-Regelwerke ist dieser standardisierte Nachweis ein großer Vorteil.

Insgesamt stellt Shore aus unserer Sicht eine ideale Ergänzung zur klassischen Sicherheitsberatung dar, weil es die Themen Betriebssicherheit, ESG und Governance auf einen gemeinsamen Nenner bringt – und damit nicht nur das Asset selbst, sondern auch das Vertrauen aller Stakeholder stärkt. Diese strukturierte Vorgehensweise ist für Investoren, finanzierende Banken und Versicherer von großem Vorteil.

Lassen Sie uns abschließend noch einen Blick auf das Lieferkettensorgfaltspflichtengesetz werfen. Neu seit 2024 ist ja, dass es schon für Unternehmen mit mehr als 1.000 Mitarbeitern gilt. Verstöße können teuer werden. Wie hoch ist hier der Beratungsbedarf, wo liegen die wesentlichen Schwachstellen bei den Unternehmen und wie können Sie hier unterstützen?

Carsten Baeck: Mir ist wichtig, dass das Verfahren entbürokratisiert wird und nicht zum reinen Papiermonster mutiert. Eine klare Aufgabenverteilung und ein schlanker Prozess können hier Wunder wirken. Wir setzen dabei auf Risikoanalysen und praxisnahe Maßnahmen, die sich eng an den betrieblichen Realitäten orientieren. Am Ende soll ein Unternehmen nicht nur die gesetzlichen Anforderungen erfüllen, sondern auch einen echten Mehrwert aus der Transparenz in seiner Lieferkette ziehen – im Sinne eines verantwortungsvollen, aber zugleich wirtschaftlich tragbaren Handelns. GIT

DRB Deutsche Risikoberatung GmbH
www.deutsche-risikoberatung.de

Securitas nutzt intelligente Screening-Lösung von Rohde & Schwarz

Durch eine strategische Partnerschaft mit Rohde & Schwarz stärkt Securitas seine Position im Bereich physische Sicherheit für den schnell wachsenden Rechenzentrumssektor. Das Unternehmen setzt dabei auf Personen-Screening mit Millimeterwellen-Technologie, um Bedrohungen zu erkennen. Mit der steigenden Nachfrage nach einer stets verfügbaren digitalen Infrastruktur steigen auch die Anforderungen an robuste physische Sicherheitssysteme, um besser vor Insider-Bedrohungen, Datendiebstahl, Sabotage und anderen Risiken zu schützen. Diese langfristige Zusammenarbeit fördert die Sicherheit von Rechenzentren und bietet den kritischsten und risikoreichsten Umgebungen der Welt mehr Präzision, Datenschutz und Agilität. Im Mittelpunkt der Partnerschaft steht die Integration der Screening-Technologie von Rohde & Schwarz in das mehrschichtige Sicherheitsangebot für Rechenzentren von Securitas, wodurch ein berührungsloser, sicherer und präziser Screening-Prozess eingeführt wird.

www.rohde-schwarz.com

BVSW Wintertagung: Grenzen der Sicherheit oder Sicherheit ohne Grenzen

Der Bayerische Verband für Sicherheit in der Wirtschaft (BVSW) veranstaltet vom 11. bis 13. März 2026 im Arabella Alpenhotel am bayerischen Spitzingsee seine Wintertagung. Experten aus Wissenschaft, Unternehmen und Behörden sind eingeladen, sich über die aktuellen Herausforderungen in der Sicherheit zu informieren. Gleichzeitig bietet die hochkarätige Veranstaltung die Gelegenheit, sich auszutauschen und sein Netzwerk zu erweitern.

Sicherheit brauche Zusammenarbeit, insbesondere in dieser komplexen Sicherheitslage, wie wir sie aktuell erleben, so BVSW-Geschäftsführerin Caroline Eder. „Mit der BVSW Wintertagung haben wir eine Plattform etabliert, auf der Wissen geteilt, Lösungen diskutiert und Netzwerke gestärkt werden. Wir freuen uns schon sehr darauf, die Sicherheitsbranche wieder willkommen zu heißen."

Die BVSW Wintertagung 2026 spannt den Bogen von der Cybersicherheit über die Innere Sicherheit bis hin zu den großen geopolitischen Herausforderungen, die Einfluss auf die Sicherheitslage in Deutschland und Europa haben. Ein zentrales Thema auf der BVSW Wintertagung 2026 ist die digitale Souveränität Deutschlands. Dazu wird es am zweiten Kongresstag eine Paneldiskussion geben. Zu dieser Gesprächsrunde eingeladen sind Experten des Bundesamts für Sicherheit in der Informationstechnik (BSI), der zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZiTis) sowie der Cybersecurity-Experte Timo Kob.

Direkt im Anschluss richtet sich der Blick auf die Verteidigungsfähigkeit Deutschlands. In seinem Vortrag zum Operationsplan Deutschland (OPLAN) zeigt Generalleutnant André Bodemann, wie militärische und zivile Strukturen ineinandergreifen sollen, um die Verteidigungsfähigkeit des Landes zu sichern. Über die Arbeit des neu gegründeten Nationalen Sicherheitsrats informiert die Politikwissenschaftlerin Christina Moritz.

Widerstandskraft ergibt sich jedoch nicht nur durch digitale und physische Abwehrstärke. Auch der gesellschaftliche Zusammenhalt ist ein wichtiger Faktor, um langfristig die wirtschaftliche und politische Stabilität zu sichern. Prof. Dr. Nils Goldschmidt, Direktor des Walter Eucken-Instituts an der Universität Tübingen, wird dazu einen Vortrag halten.

Die BVSW Wintertagung bietet zudem viele bewährte Programmpunkte, die mittlerweile fest zum Event gehören: Den Auftakt der Veranstaltung bildet eine hochkarätig besetzte Gesprächsrunde zur Inneren Sicherheit mit Landespolizeipräsident Michael Schwald, dem Präsidenten des Bayerischen Landesamts für Verfassungsschutz Manfred Hauser sowie dem BVSW-Vorstandsvorsitzenden Markus Klaedtke und der Geschäftsführerin Caroline Eder.

Zum Einstieg in den zweiten Kongresstag gibt Prof. Dr. Günther Schmid den Teilnehmern einen spannenden 360°-Einblick in die aktuelle geopolitische Großwetterlage. Den krönenden Abschluss bildet auch 2026 ein Vortrag von Dr. Benedikt Franke, dem CEO der Münchner Sicherheitskonferenz. Er nimmt die Teilnehmer mit auf einen abwechslungsreichen Rundgang durch die verschiedenen Gespräche, Konferenzen und Foren der MSC 2026, inklusive einiger Highlights jenseits des offiziellen Protokolls. Anmeldungen sind möglich über die BVSW-Website. **www.bvsw.de**

Hier finden Sie alle Gewinner

Wagner gewinnt GIT SICHERHEIT AWARD 2026

Die Wagner Group GmbH wurde mit dem GIT SICHERHEIT AWARD 2026 in der Kategorie „Brandschutz" ausgezeichnet. Prämiert wurde das innovative Sauerstoffreduzierungssystem OxyReduct F-Line, das unter definierten Bedingungen die Entstehung eines offenen Brandes aktiv vermeidet. Das System erweitert das bewährte Verfahren der Sauerstoffreduzierung um eine wasserstoffbasierte Brennstoffzellentechnologie, die gleichzeitig eine emissionsfreie Energieversorgung ermöglicht. Der zentrale Fortschritt liegt in der Verbindung von Schutzatmosphäre und autarker Energieversorgung. So gewährleistet die OxyReduct F-Line eine kontinuierliche Brandvermeidung bei CO_2-neutralem Betrieb – ein Meilenstein für den vorbeugenden Brandschutz. **www.wagnergroup.com**

PMRExpo 2025

Europas Leitmesse für sichere Kommunikation

Topmesse für sichere Kommunikation, 5G-Innovationen und Leitstellentechnologien – Impressionen von der PMRExpo 24

Vom 25. bis 27. November 2025 wird die Koelnmesse erneut zum Treffpunkt der europäischen Sicherheits- und Kommunikationsbranche. Die PMRExpo 2025 gilt als führende Fachmesse für Professionellen Mobilfunk (PMR) und Leitstellenlösungen und bringt Entscheider, Anwender und Anbieter aus sicherheitskritischen Bereichen zusammen. Vertreten sind Behörden und Organisationen mit Sicherheitsaufgaben (BOS), Betreiber kritischer Infrastrukturen (KRITIS) sowie Unternehmen aus Industrie, Energie, Verkehr und öffentlicher Verwaltung.

Im Mittelpunkt der diesjährigen PMRExpo steht die digitale Transformation sicherheitsrelevanter Kommunikation. Dabei werden aktuelle Entwicklungen und Technologien vorgestellt, die den Wandel von klassischen Schmalbandlösungen hin zu modernen Breitbandanwendungen prägen. Zu den Schwerpunkten zählen insbesondere 5G und 5G-Campusnetze, die neue Möglichkeiten für private, hochsichere Netzwerke eröffnen, sowie die Interoperabilität zwischen Schmal- und Breitbandnetzen. Auch private Breitbandnetze auf Basis von LTE und 5G gewinnen zunehmend an Bedeutung, da sie Nutzern mehr Kontrolle und Sicherheit bieten.

Ergänzend dazu präsentieren zahlreiche Aussteller neueste Leitstellen- und Sicherheitstechnologien, etwa moderne Dispatch-Systeme, integrierte Sicherheitsplattformen sowie Geräte- und Infrastrukturkomponenten – von Antennen und Repeatern bis zu Softwarelösungen und Headsets. Diese Vielfalt verdeutlicht, unter welchem Innovationsdruck sicherheitskritische Kommunikation heute steht.

PMRExpo Summit

Ein besonderes Highlight der Messe ist der PMRExpo Summit, auf dem internationale Experten aktuelle Trends, Technologien und Herausforderungen beleuchten. In Vorträgen und Podiumsdiskussionen werden Themen wie Cybersicherheit in Kommunikationsnetzen, die Zukunft der Leitstellenarchitektur, der Einsatz von Künstlicher Intelligenz in der Notfallkommunikation sowie Strategien für resiliente Infrastrukturen behandelt. Ergänzt wird das Programm durch praxisorientierte Formate wie Live-Demonstrationen, Workshops und Networking-Lounges, die den direkten Austausch zwischen Anwendern, Herstellern und Dienstleistern fördern.

Mit über 250 internationalen Ausstellern und rund 10.000 Fachbesuchern bietet die PMRExpo einen umfassenden Marktüberblick. Zu den namhaften Teilnehmern zählen unter anderem Airbus Secure Land Communications (Lösungen für BOS und militärische Kommunikation), Advancis Software & Services (Leitstellen- und Sicherheitsmanagement), 450connect GmbH (bundesweites LTE-Netz für KRITIS) und Alamos (Alarmierungs- und Einsatzmanagement für Feuerwehren und Rettungsdienste). Darüber hinaus sind führende Unternehmen wie Motorola Solutions, Frequentis, Rohill, Hytera Mobilfunk, Sepura, Telent, Atlas Elektronik und Drägervertreten, die ihre neuesten Produkte und Systemlösungen vorstellen. Das Spektrum reicht von moderner Funktechnik (TETRA, DMR, LTE, PoC) über Netzwerkinfrastruktur bis hin zu intelligenten Softwarelösungen für Leitstellen und Einsatzkräfte. GIT

Koelnmesse GmbH
www.pmrexpo.com

Hackathon auf der letztjährigen PMRExpo

VfS: Fachtagung und Workshop Zutritts- und Berechtigungsmanagement

Der Verband für Sicherheitswirtschaft (VfS) veranstaltet am 27./28. November 2025 beim DRK Landesverband Rheinland-Pfalz in Mainz die Fachtagung und Workshop „Zutritts- und Berechtigungsmanagement“. In einer bewegten Welt gibt es viele Themen, die auch das Zutritts- und Berechtigungsmanagement maßgeblich beeinflussen. Beispiele wie das KRITIS-Umsetzungsgesetz, Cloud, BIM (Building Information Modelling), 3D, Biometrie, NIS-2, sind nur einige davon. All dies erfordert erweiterte Maßnahmen bzw. bringt das Zutritts- und Berechtigungsmanagement in eine neue Dimension. Die damit verbundenen Anforderungen möchte der VfS in seiner Veranstaltung aufzeigen bzw. gemeinsam mit den Teilnehmern erarbeiten. Die Veranstaltung ist eine Mischung aus Fachvorträgen, Erfahrungsberichten, Stand der Wissenschaften, konstruktiven Dialogen und Podiumsdiskussionen. **www.vfs-hh.de**

VSW: Neuer Name – starke Mission

Aus der bisherigen Vereinigung für die Sicherheit der Wirtschaft e. V. wird Verband für Sicherheit in der Wirtschaft Hessen – Rheinland-Pfalz – Saarland e. V. (VSW-Mainz). Mit dieser Umbenennung ziehe man mit dem VSW-Bundesverband (ehemals ASW Bundesverband) gleich und schaffe damit eine klare Einheitlichkeit in Namen, Logo und Außenauftritt. Der Verband positioniere sich zukunftsorientiert und zeige seine gewachsene Bedeutung für die Unternehmen in der Region – gerade in einem zunehmend komplexen und dynamischen Sicherheitsumfeld. Der neue Name bringt die Rolle des Verbands als zentrale Stimme der Wirtschaftssicherheit in der Region klar und verständlich zum Ausdruck. **www.vsw.de**

Genetec bleibt Marktführer bei VMS

Genetec bleibt nach aktuellen Marktanalysen weiterhin der weltweit führende Anbieter im Bereich Videomanagement-Software. Zu diesem Ergebnis kommen die unabhängigen Analystenhäuser Omdia und Novaira Insights in ihren aktuellen Studien. Demnach verteidigt Genetec im „Video Surveillance & Analytics Database Report 2025“ von Omdia den ersten Platz im globalen Markt für Videomanagement-Software (VMS). Auch in der kombinierten Kategorie aus VMS und Videoüberwachung-as-a-Service (VSaaS) führt das Unternehmen das weltweite Ranking an. Wachstumstreiber ist unter anderem die steigende Nachfrage nach cloudbasierten, skalierbaren Sicherheitslösungen. Die Mitte 2024 eingeführte Plattform Security Center SaaS konnte in kurzer Zeit signifikante Marktanteile im VSaaS-Segment gewinnen. In der Region Amerika, dem aktuell größten und dynamischsten VSaaS-Markt, belegt Genetec Rang 4. Weltweit zählt das Unternehmen nun zu den Top 10 der VSaaS-Anbieter. **www.genetec.de**

Erfolgreich: Wagner setzt auf Innovation und Internationalisierung

Torsten Wagner

Die Wagner Group GmbH blickt auch in diesem Jahr auf ein erfolgreiches Geschäftsjahr zurück. Trotz des anhaltend herausfordernden Marktumfelds, schwacher Weltwirtschaft und steigender Lohn-, Rohstoff- und Transportkosten hat das Unternehmen mit einer konsolidierten Gesamtleistung von 152 Mio. EUR im Geschäftsjahr 2024/25 sein Wachstumsziel von 10 % erneut erreicht. Mit diesem Ergebnis setzt das Unternehmen seinen strategischen Wachstumspfad WAGNER.2026 konsequent fort. Umfangreiche Investitionen im vergangenen Geschäftsjahr, zum einen in den Auf- und Ausbau neuer Standorte in Europa und Middle East, zum anderen in digitale Prozesse sowie eine neue Online-Präsenz, zahlen auf die strategische Internationalisierung sowie die Zukunftsfähigkeit der Unternehmensgruppe ein. Das Unternehmen stärkt damit seine Marktposition nachhaltig. Die Exportquote beträgt derzeit rund 51 %, Tendenz weiterhin steigend.

www.wagnergroup.com

Strategische Partnerschaft mit Zukunft

Assa Abloy über die Integration von Uhlmann & Zacher

Im Januar 2025 hat Assa Abloy die Firma Uhlmann & Zacher übernommen, einen der führenden Anbieter im Bereich elektronischer Schließtechnik (GIT SICHERHEIT berichtete). Nun wollten wir genauer wissen, wie sich die Zusammenarbeit nach den ersten Monaten gestaltet. Im Doppelinterview geben Achim Haberstock, Senior Vice President Central Europe Assa Abloy Opening Solutions, und Dr. Ingo Dietz von Bayer, Senior Operation Development Manager Central Europe, Einblicke in den Integrationsprozess und ziehen eine erste Zwischenbilanz.

Achim Haberstock, Senior Vice President Central Europe Assa Abloy Opening Solutions

Dr. Ingo Dietz von Bayer, Senior Operation Development Manager Central Europe

Herr Haberstock, Herr Dr. Dietz von Bayer, welche strategischen Überlegungen standen hinter dieser Akquisition?

Achim Haberstock: Die Übernahme von Uhlmann & Zacher ist ein logischer Schritt in unserer Strategie: Wir erweitern unser Portfolio gezielt um innovative und komplementäre Lösungen. U&Z bringt über 30 Jahre Erfahrung in elektronischer Zutrittskontrolle mit und ist bekannt für technologische Innovationskraft. Dieses Know-how ergänzt unser Angebot ideal und stärkt unsere Position in Deutschland und international. Wichtig war uns außerdem, Kontinuität für Kunden und Mitarbeitende zu sichern. Wir nutzen Synergien, ohne die Identität von U&Z zu verwässern. Das ist nicht nur ein strategischer Zugewinn, sondern auch ein klares Bekenntnis zum Standort Waldbüttelbrunn.

Wie gestaltet sich die Integration des Unternehmens mit seinen mehr als 110 Mitarbeitern in die Strukturen von Assa Abloy?

Dr. Ingo Dietz von Bayer: Uhlmann & Zacher bleibt als eigenständige Tochtergesellschaft erhalten, die Arbeitsplätze in Waldbüttelbrunn sind gesichert. Wir verfolgen eine Integration, die bewusst behutsam und zugleich zielgerichtet ist. Als Integrationsmanager koordiniere ich alle Funktionsbereiche – von Operations über Finance und IT bis hin zu Prozessoptimierungen. Neben technischen Fragen spielen kulturelle Themen eine große Rolle. Wir führen gemeinsame Tools und Plattformen ein, die den Mitarbeitenden Zugang zu Informationen und Schulungen erleichtern. Gleichzeitig arbeiten wir eng mit den Führungsteams zusammen, um Effizienzpotenziale zu heben und nachhaltige Ergebnisse zu erzielen.

Das erste Dreivierteljahr seit der Akquisition ist nun vergangen. Können Sie eine erste Bilanz ziehen?

Achim Haberstock: Unsere Zwischenbilanz ist sehr positiv. Die Integration läuft planmäßig, und erste gemeinsame Projekte sind erfolgreich gestartet. Besonders freut mich die enge Zusammenarbeit der Kolleginnen und Kollegen von U&Z mit den Teams der Assa Abloy Sicherheitstechnik. Der Know-how-Transfer zeigt schon jetzt klare Fortschritte.

Dr. Ingo Dietz von Bayer: Auch aus Sicht des Integrationsmanagements sind wir auf einem sehr guten Weg. Wir haben früh Strukturen geschaffen, die Transparenz und Kommunikation fördern. Kunden profitieren heute schon von einem erweiterten Portfolio und einer stärkeren Marktpräsenz. In den kommenden Monaten geht es um Prozessoptimierungen und die Entwicklung neuer, gemeinsamer Lösungen. Ziel bleibt, die Stärken beider Unternehmen zu verbinden und so langfristig Mehrwert für Kunden und Mitarbeitende zu schaffen. GIT

Assa Abloy Sicherheitstechnik
www.assaabloy.com/de

Asecos nimmt neues Logistikzentrum in Betrieb

Die Asecos GmbH hat ihr neues Logistikzentrum in Betrieb genommen. Das Gebäude in unmittelbarer Umgebung des Firmensitzes in Gründau-Lieblos bündelt künftig sämtliche Logistikprozesse des Unternehmens und schafft zusätzliche Flächen für die Produktion am Hauptstandort. Damit reagiert Asecos auf die steigende Nachfrage und stärkt seine Position auf internationalen Märkten.

Für den Neubau hat das Unternehmen ein über 11.000 Quadratmeter großes Grundstück erworben und darauf ein nachhaltiges, energieeffizientes Logistikgebäude errichtet. Von hier aus wird die weltweite Belieferung realisiert. Das Logistikzentrum ist zudem so konzipiert, dass es bei Bedarf erweitert werden kann.

In der neuen Halle können bis zu 1.900 Sicherheitsschränke zeitgleich gelagert werden. Die Aufbewahrung erfolgt in hochmodernen Verschiebeanlagen, die eine effiziente Nutzung der Fläche ermöglichen. Für den Versand werden Lkws bereits am Haupttor registriert und direkt zu den passenden Laderampen geleitet. Ein bodengleicher, wettergeschützter Zugang erleichtert die Verladung der Produkte. Überdachte Flächen ermöglichen die seitliche Beladung, sodass bis zu neun Fahrzeuge gleichzeitig abgefertigt werden können.

In Deutschland, Österreich und der Schweiz übernehmen eigene Fahrerteams die Auslieferung. Sie sind mit den Produkten vertraut und gewährleisten eine fachgerechte Handhabung vor Ort. Auch externe Speditionen holen die Sicherheitsschränke künftig im neuen Logistikzentrum ab und liefern sie von dort an die Kunden.

Durch die Bündelung der Logistik an einem zentralen Standort sind am nur 900 Meter entfernten Hauptsitz Lagerflächen frei geworden, die nun für eine Ausweitung der Produktion genutzt werden. So kann das Unternehmen besser auf die steigende Nachfrage reagieren und den wachsenden internationalen Markt bedienen.

Bei der Konstruktion des neuen Logistikgebäudes spielte das Thema Nachhaltigkeit eine entscheidende Rolle: Die Halle wurde in Holzbauweise errichtet, großzügige Tageslichtfenster in der Decke sorgen für natürliche Beleuchtung, und moderne Gebäudetechnik trägt zu einem geringen Energieverbrauch bei. Zudem erzeugt eine Photovoltaikanlage auf dem begrünten Dach den Großteil des benötigten Stroms. Ergänzt wird das nachhaltige Konzept durch eine Blühwiese neben der Halle, die dank spezieller Saatmischung Lebensraum für zahlreiche Insekten schafft und so die Artenvielfalt fördert. **www.asecos.com**

Gerhard Ameis erneut in den Vorstand der VBW gewählt

Gerhard Ameis, Vizepräsident des BDSW sowie langjähriger Vorsitzender und seit 2022 stellvertretender Vorsitzender der BDSW-Landesgruppe wurde erneut in den Vorstand der VBW – Vereinigung der Bayerischen Wirtschaft e. V. gewählt. Er ist bereits seit 2013 Mitglied des VBW-Vorstands. Mit der Wiederwahl unterstreicht die VBW das Engagement und die Kompetenz von Gerhard Ameis, der sich seit vielen Jahren erfolgreich für die Belange der Sicherheitswirtschaft in Bayern einsetzt. Der BDSW ist langjähriges Mitglied der VBW. Die Landesgruppe Bayern im BDSW pflegt intensive Kontakte zur VBW. Die VBW ist die freiwillige, zentrale und branchenübergreifende Interessenvertretung der bayerischen Wirtschaft. Sie vereint 164 Arbeitgeber- und Wirtschaftsverbände sowie 52 Fördermitglieder. In den Unternehmen ihrer Mitgliedsverbände arbeiten rund 4,8 Millionen sozialversicherungspflichtig Beschäftigte – das entspricht fast 90 Prozent aller Arbeitnehmer im Freistaat. **www.bdsw.de**

Grenzen der Sicherheit – Sicherheit ohne Grenzen

BVSW lädt zur Wintertagung 2026

Vom 11. bis 13. März 2026 verwandelt sich das Arabella Alpenhotel am bayerischen Spitzingsee zum Treffpunkt für die Sicherheitsbranche: Expertinnen und Experten aus Wissenschaft, Unternehmen und Behörden sind eingeladen, sich über die aktuellen Herausforderungen in der Sicherheit zu informieren. Gleichzeitig bietet die hochkarätige Veranstaltung die Gelegenheit, sich auszutauschen und sein Netzwerk zu erweitern.

„Sicherheit braucht Zusammenarbeit, insbesondere in dieser komplexen Sicherheitslage, wie wir sie aktuell erleben", sagt BVSW-Geschäftsführerin Caroline Eder. „Mit der BVSW-Wintertagung haben wir eine Plattform etabliert, auf der Wissen geteilt, Lösungen diskutiert und Netzwerke gestärkt werden."

Die Tagung spannt den Bogen von der Cybersicherheit über die innere Sicherheit bis hin zu den großen geopolitischen Herausforderungen, die Einfluss auf die Sicherheitslage in Deutschland und Europa haben.

Die digitale Souveränität Deutschlands ist ein zentrales Thema der Veranstaltung. Dazu wird es am zweiten Kongresstag eine Paneldiskussion geben. Zu dieser Gesprächsrunde eingeladen sind Expertinnen und Experten des Bundesamts für Sicherheit in der Informationstechnik (BSI), der zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZiTis) sowie der Cybersecurity-Experte Timo Kob.

Direkt im Anschluss richtet sich der Blick auf die Verteidigungsfähigkeit Deutschlands. In seinem Vortrag zum Operationsplan Deutschland (OPLAN) zeigt André Bodemann, stellvertretender Befehlshaber des operativen Führungskommandos der Bundeswehr, wie militärische und zivile Strukturen ineinandergreifen sollen, um die Wehrhaftigkeit des Landes zu sichern. Über die Arbeit des neu gegründeten Nationalen Sicherheitsrats informiert die Politikwissenschaftlerin Christina Moritz.

Widerstandskraft ergibt sich jedoch nicht nur durch digitale und physische Abwehrstärke. Auch der gesellschaftliche Zusammenhalt ist ein wichtiger Faktor, um langfristig die wirtschaftliche und politische Stabilität zu sichern. Prof. Dr. Nils Goldschmidt, Direktor des Weltethos-Instituts an der Universität Tübingen, wird dazu einen Vortrag halten.

Die BVSW-Wintertagung 2026 findet vom 11. bis 13. März 2026 im Arabella Alpenhotel statt. Im Bild die Veranstaltung 2025

Boris Bärmichl, Vorstand der BVSW-Digitalsparte spricht über KI (Veranstaltung 2025)

Umfassendes Programm

Die BVSW-Wintertagung bietet zudem viele bewährte Programmpunkte, die mittlerweile fest zum Event gehören: Den Auftakt der Veranstaltung bildet eine hochkarätig besetzte Gesprächsrunde zur Inneren Sicherheit mit Landespolizeipräsident Michael Schwald, dem Präsidenten des Bayerischen Landesamtes für Verfassungsschutz Manfred Hauser sowie dem BVSW-Vorstandsvorsitzenden Markus Klaedtke und der Geschäftsführerin Caroline Eder.

Zum Einstieg in den zweiten Kongresstag gibt Prof. Dr. Günther Schmid den Teilnehmenden einen spannenden 360°-Einblick in die aktuelle geopolitische Großwetterlage. Den krönenden Abschluss bildet auch 2026 wieder der Vortrag von Dr. Benedikt Franke, dem CEO der Münchner Sicherheitskonferenz. Er nimmt die Teilnehmenden mit auf einen abwechslungsreichen Rundgang durch die verschiedenen Gespräche, Konferenzen und Foren der MSC 2026, inklusive einiger Highlights jenseits des offiziellen Protokolls. Noch gibt es freie Plätze für die Wintertagung 2026. Anmeldungen sind möglich auf der Website des Verbandes. GIT

BVSW
www.bvsw.de

i-Pro feiert sechsjähriges Jubiläum

i-Pro Co., Ltd feierte sein sechsjähriges Jubiläum als unabhängiges Unternehmen. Das Unternehmen unterstreicht seine starke Marktposition und sein Engagement für Innovation und vermeldet mehrere wichtige Meilensteine, darunter die Eröffnung einer neuen Fabrik in Japan, die branchenweit erste ISO/IEC 42001-Zertifizierung für KI-Management, die Einführung von Active Guard 3.0 mit generativen KI-Funktionen und die Erweiterung seines globalen Führungsteams.

Seit seiner Gründung verzeichnet i-Pro ein kontinuierliches zweistelliges Wachstum und eine solide Rentabilität, angetrieben durch die starke Nachfrage nach seinen Edge-Processing-KI-Kameras für Sicherheits-, Schutz- und medizinische Anwendungen sowie seinen Ruf für hochwertige Technik und Cyber-Resilienz. Der Jahresumsatz des Unternehmens liegt heute um mehr als 70 Prozent über dem Wert vor der Unabhängigkeit.

Ab dem 1. Oktober 2025 wird das neue Werk des Unternehmens in Saga (Tosu City, Präfektur Saga, Japan) als i-Pro-Produktionsstätte voll in Betrieb sein, wodurch die globale Widerstandsfähigkeit der Fertigung gestärkt und die langfristige Lieferstabilität für Partner und Kunden sichergestellt wird. Durch die Verlagerung der Produktion nach Japan plant i-Pro, Design- und Fertigungsteams unter einem Dach zusammenzuführen, um die Zusammenarbeit zu verbessern und Tests und Produktion zu beschleunigen.

Der Standort zielt auch darauf ab, eine agile, hochflexible Fertigung in kleinen Stückzahlen einzuführen, bei der standardisierte Kernmodule mit kundenspezifischen Konfigurationen kombiniert werden. Dieser Ansatz soll die Produktionszeit verkürzen, die Effizienz steigern und eine schnellere weltweite Lieferung einer größeren Vielfalt an Produkten ermöglichen, die auf die individuellen Bedürfnisse der Kunden zugeschnitten sind.

Entsprechend seinem Wachstum als globales Unternehmen hat i-Pro seinen Vorstand und sein Führungsteam um erfahrene Führungskräfte und angesehene Branchenführer mit vielfältigem und internationalem Hintergrund erweitert, darunter Gerard Figols (Direktor, Chief Operating Officer), Hiroo Okamoto (Direktor, Unternehmensleiter und Chief Financial Officer), James Rothstein (nicht geschäftsführender Direktor, Global Executive Advisor), Kaori Yagi (Direktorin, Mitglied des Prüfungs- und Aufsichtsausschusses), Bill Brennan (Vorsitzender des Vorstands für Amerika) und Dayanna Nunez (Chief Human Resources Officer).

„Mit einer wachsenden globalen Präsenz, einem erweiterten Führungsteam und kontinuierlichen Investitionen in KI und innovative Technologien startet i-Pro in sein siebtes Jahr als zuverlässiger, langfristiger Partner für Unternehmen und Endnutzer, die nach Technologien suchen, die sowohl sofortigen Mehrwert bieten als auch zukunftssicher sind“, so Masato Nakao, CEO von i-Pro Co. **www.i-pro.com**

Primion feiert 30-jähriges Bestehen mit sozialem Engagement

Giving back at 30 – unter diesem Motto unterstützt die Primion Technology GmbH im Jubiläumsjahr 2025 ausgewählte soziale Initiativen. Den Auftakt macht die Beschäftigungseinrichtung St. Franziskus der Caritas in Sigmaringen. Die Einrichtung bietet rund 70 Menschen mit psychischen Beeinträchtigungen eine sinnstiftende Tätigkeit, individuelle Förderung sowie die Chance auf Wiedereingliederung in den ersten Arbeitsmarkt oder eine langfristige Beschäftigung in einem geschützten Rahmen. Seit 2019 setzt die Einrichtung auf ein Zeiterfassungssystem von Primion. Das bisher genutzte Terminal wurde im Rahmen des Jubiläums nun durch ein modernes Modell ersetzt und vor Ort durch einen eigenen Servicetechniker installiert und eingerichtet – sehr zur Freude des gesamten Teams. **www.primion.io**

Bei der Übergabe des neuen Zeiterfassungsterminals (v. l.): Elke Selg, Sascha Dienstknecht, Birgitt Siegert (alle Caritas), Primion-Techniker Benjamin Oßwald und Klaus Rauser (Werkstattleitung)

Peter Bachus, Präsident des VSW-Mainz, eröffnet den VSW-Sicherheitstag 2025. Eines seiner Themen bei der Eröffnung: Umbenennung des VSW in „Verband für Sicherheit in der Wirtschaft Hessen – Rheinland-Pfalz – Saarland e. V. – VSW Mainz“

Zwischen KI, Krisen und Cyberangriffen

Der VSW-Sicherheitstag 2025 als Weckruf für Unternehmen

Am 29. September 2025 versammelten sich im Hofgut Nonnenau bei Ginsheim-Gustavsburg Fach- und Führungskräfte aus Wirtschaft, Behörden und Wissenschaft zum VSW-Sicherheitstag. Unter dem Motto „Globale Bedrohungen – Nationale Antworten“ standen die strategischen Herausforderungen für Unternehmen in einer Welt zwischen Künstlicher Intelligenz, geopolitischen Krisen und hybriden Konflikten im Mittelpunkt.

Peter H. Bachus, Präsident des VSW-Mainz, eröffnete die Veranstaltung mit einem Appell zur Wachsamkeit und betonte die Rolle des VSW-Mainz als Brücke zwischen Wirtschaft und Sicherheitsbehörden. Prof. Dr. Roman Poseck, Hessischer Innenminister, analysierte die objektive Sicherheitslage in Hessen. Während die Kriminalitätsstatistiken eine leichte Entspannung zeigen, bleibt das subjektive Sicherheitsgefühl der Bevölkerung angespannt. Poseck warnte zudem vor einer „falschen Toleranz in der Gesellschaft“ gegenüber Extremismus und hob die Notwendigkeit hervor, Rechtsextremismus, Linksextremismus und Islamismus gleichermaßen zu bekämpfen. Ein zentrales Thema der Tagung war die zunehmende Bedrohung durch hybride Angriffe – auch durch staatliche Akteure. Bernd Neumann, Präsident des Landesamtes für Verfassungsschutz Hessen, verdeutlichte, wie gezielte Desinformationskampagnen und Sabotageakte das Vertrauen in demokratische Prozesse untergraben. Die Grenzen zwischen Cybercrime und hybrider Kriegsführung verschwimmen zunehmend.

Geopolitische Machtverschiebungen und ihre Folgen

Prof. em. Dr. Günther Schmid beleuchtete in seinem Vortrag die globale Machtverschiebung im Spannungsfeld China – USA – Russland. Die internationale Politik sei von einer neuen Risikobereitschaft und einer sinkenden Hemmschwelle zur Gewaltanwendung geprägt. Für Unternehmen bedeute dies, geopolitische Risiken stärker in die eigene Strategie zu integrieren und Sicherheitsverantwortung auf Führungsebene zu verankern.

Cyber-Security als Chefsache: Aktuelle Bedrohungen und strategische Antworten

Der Nachmittag stand ganz im Zeichen der Cyber-Security – ein Thema, das angesichts der aktuellen Studienlage dringlicher denn je ist. Hakan Özbek, Senior Managing Director bei Ankura, betonte: „Cybersicherheit ist mittlerweile Chefsache.“ Neben technologischen Herausforderungen wie Quantencomputern und KI seien geopolitische und regulatorische Faktoren entscheidend für eine ganzheitliche Sicherheitsstrategie. Besonders kritisch: Der Fachkräftemangel und die sinkende Versicherbarkeit von Cyberrisiken.

Mark T. Hofmann, Wirtschaftspsychologe und Crime-Analyst, zeigte eindrucksvoll, wie Hacker KI und Deepfakes für Angriffe nutzen. Ransomware-Attacken, Datenleaks und gezielte Erpressungen sind längst keine Einzelfälle mehr. KI-gestützte Angriffe sind heute als Service im Darknet verfügbar – die Eintrittshürden

In diesem Jahr lag der Fokus auf den Themenfeldern hybride Bedrohungen und Cyber-Security. Insbesondere die Vorträge von Hakan Özbek (links), Senior Director, Risk Advisory – Germany, Ankura GmbH, und Mark T. Hofmann (rechts), Kriminal- & Geheimdienstanalyst und Organisationspsychologe, befasste sich mit der aktuellen Bedrohungslage im Bereich Cyber-Security

für Cyberkriminalität sinken rapide. Hofmann warnte: „KI wird es in Zukunft jedem ermöglichen zu hacken."

Drohnenabwehr und die Psychologie der Angst

Markus Piendl, Sachverständiger für Sicherheitstechnik, präsentierte im Rahmen des Projekts DIANA aktuelle Ansätze zur Drohnendetektion und -abwehr. Die zunehmende Verbreitung von Drohnen – sowohl kommerziell als auch im Eigenbau – stellt Unternehmen und Behörden vor neue Herausforderungen. Wie akut diese sind, zeigen nicht zuletzt die Sichtung russischer Drohnen über Dänemark, Polen und Rumänien.

Abgerundet wurde der Tag durch einen Beitrag zur psychosozialen Dimension von Sicherheit. Prof. Dr. Borwin Bandelow von der Universität Göttingen erläuterte, wie sich die Wahrnehmung von Bedrohungen – etwa durch Cyberangriffe – auf das individuelle und kollektive Angstempfinden auswirkt. Die Menschen gewöhnen sich an abstrakte Bedrohungen, unterschätzen dadurch aber oft deren reale Gefahr. Ein Problem, dem sich die Sicherheitsbranche häufig gegenüber sieht.

Fazit und Ausblick

Der VSW-Sicherheitstag 2025 machte deutlich: Die Bedrohungslage für Unternehmen ist komplexer und dynamischer denn je. Cyber-Security muss als strategische Führungsaufgabe verstanden werden. Die aktuellen Studien zeigen, dass Unternehmen ihre Resilienz dringend stärken, in Prävention investieren und regulatorische Anforderungen ernst nehmen müssen. GIT

Der nächste VSW-Sicherheitstag findet am 30. September 2026 statt.

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

EVENT

Sicherheit im Justizvollzug

Fachtagung „Sicherheit in der JVA XVII“ am 2. und 3. Dezember 2025

Der Verband für Sicherheitstechnik (VfS) lädt erneut zur Fachtagung „Sicherheit in der JVA XVII“. Am 2. und 3. Dezember 2025 treffen sich Fachleute aus Justiz, Sicherheitsbehörden und Industrie im Berufsförderungswerk Nürnberg, um aktuelle Entwicklungen und Herausforderungen der Sicherheit im Justizvollzug zu diskutieren.

Auch dieses Jahr veranstaltet der VfS eine Fachtagung zum Thema „Sicherheit in der JVA“. Geboten wird ein vielseitiges Programm mit hochkarätigen Fachvorträgen und praxisnahen Einblicken. Zu den Themen zählen unter anderem der Einsatz künstlicher Intelligenz zur Suizidprävention und Verbesserung der Sicherheit in niedersächsischen Justizvollzugsanstalten, das Problem Sucht mit dem Blick auf den österreichischen Ansatz „Therapie statt Strafe“, sowie Brandschutz in Justizvollzugsanstalten. Weitere Schwerpunkte sind nachhaltiges und zirkuläres Bauen, Bauen im laufenden Betrieb am Beispiel der JVA Wuppertal-Vohwinkel und die Arbeit eines Gefängnisseelsorgers.

In einer Podiumsdiskussion werden außerdem aktuelle rechtliche und technische Entwicklungen beleuchtet – darunter das KRITIS-Dachgesetz, NIS2 und Building Information Modeling (BIM). Ergänzend widmen sich Fachbeiträge Themen wie Clankriminalität und ihre Auswirkungen auf Justizvollzug und Gerichtssicherheit sowie dem Tetra-Bos-Gebäudefunk als verlässlicher Kommunikationslösung für Einsatzkräfte.

Produkte und Systeme für den Justizbereich

Begleitet wird die Veranstaltung von einer Fachausstellung führender Unternehmen, die innovative Produkte und Systeme für den Justizbereich präsentieren. Der persönliche Austausch spielt wie immer eine große Rolle – sei es bei den Pausen, in der Ausstellung oder bereits am Vorabend der Veranstaltung.

Am ersten Abend rundet ein besonderes Rahmenprogramm die Tagung ab. Eine gemeinsame Fahrt zum Nürnberger Christkindlmarkt mit anschließendem Besuch in einem Restaurant bietet Gelegenheit, in entspannter Atmosphäre Kontakte zu pflegen.

Die Zahl der Präsentationsflächen ist begrenzt – interessierte Unternehmen sollten sich zeitnah anmelden, um sich einen Standplatz zu sichern. GIT

Verband für Sicherheitstechnik
VfS e.V.
www.vfs-hh.de

Themen auf der Fachtagung „Sicherheit in der JVA XVII“

Dienstag, 2. Dezember

- **Einsatz künstlicher Intelligenz zur Suizidprävention und Verbesserung der Sicherheit in niedersächsischen Justizvollzugsanstalten**
  Dirk Becker, Niedersächsisches Justizministerium, Hannover
  Oliver Wertheim, FZI Forschungszentrum Informatik, Karlsruhe
- **Problem Sucht: Therapie statt Strafe – der österreichische Weg**
  Dr. Martin Kitzberger, Verein Gründer Kreis, Wien
- **Brandschutz in Justizvollzugsanstalten**
  Matthias Otto, Prüfingenieur für Brandschutz, Leipzig
- **Podiumsdiskussion zu KRITIS-Dachgesetz/NIS-2/BIM**

Mittwoch, 3. Dezember

- **Tetra-Bos-Gebäudefunk – eine sichere Verbindung für alle Einsatzkräfte**
  Henning Müller, Planungsbüro Telmotion, Lübeck
- **Clankriminalität in Deutschland – Auswirkungen auf JVA- und Gerichtssicherheit**
  Thomas Ganz, Berater und Experte für Clankriminalität, Hannover
- **Nachhaltiges / Zirkuläres Bauen in der Justizvollzugsanstalt Mannheim**
  Manfred Döpke, Vermögen und Bau Baden-Württemberg, Mannheim

Das vollständige Programm finden Sie unter: www.vfs-hh.de

www.gu-bks.de

GU BKS SERVICE

IHR DIENSTLEISTUNGSPARTNER.

Von der Planung bis zur Instandhaltung.

Überzeugen Sie sich selbst:

- 27. - 28.11.25 VfS-Fachtagung „Zutritts- und Berechtigungsmanagemen“ Mainz
- 02. - 03.12.25 VfS-Fachtagung „Sicherheit in der JVA“ Nürnberg
- 03. - 04.12.25 VdS-BrandSchutzTage Köln

Service mit System

Von JVA bis Besucherkommunikation am Empfang: Die Einsatzmöglichkeiten des integrierten KI-Dolmetschers sind vielfältig

Funkwerk Security Solutions stellt ein neues Add-on für ihr Gefahrenmanagementsystem Vipro GMS 5 KRITIS vor: den KI Live-Reader. Mit dieser Funktion für automatische Transkription, Übersetzung und Dokumentation wird KI-Technologie direkt in das Gefahrenmanagementsystem integriert. Damit ermöglicht Funkwerk eine Verbesserung der Kommunikation in multikulturellen Umgebungen.

GEFAHRENMANAGEMENT

Sprachbarrieren überwinden

Ins Gefahrenmanagementsystem integrierter KI-Dolmetscher

Es ist Alltag in der Justizvollzugsanstalt: Ein Insasse spricht eine Fremdsprache, das Personal überwiegend Deutsch. Mit Vipro GMS und dem integrierten KI-Dolmetscher können beide z.B. über die Sprechstelle direkt in ihrer Muttersprache kommunizieren. Die KI erkennt die Sprache und übersetzt das Gespräch in Echtzeit, erstellt automatisch eine schriftliche Zusammenfassung und protokolliert das Gespräch revisionssicher. Das Personal kann klare Anweisungen geben und Missverständnisse werden vermieden. Gleichzeitig spart das System Zeit, da kein externer Dolmetscher benötigt wird und Protokolle automatisch erstellt werden. Routinegespräche lassen sich effizienter gestalten und durch die automatisierte, nachvollziehbare Dokumentation wird die interne Berichterstattung erheblich erleichtert.

Integration ins Gefahrenmanagementsystem

Vipro GMS 5 KRITIS bietet eine dezentrale Systemarchitektur und umfassende KRITIS-Konformität, um höchste Sicherheitsstandards zu erfüllen. Das System nutzt TLS 1.3 und AES256-Verschlüsselung und bietet eine nahtlose Integration von SIP-basierten Endgeräten für effiziente Kommunikation und Prävention in sicherheitskritischen Umgebungen. Der KI Live-Reader baut durch das Add-on eine zuverlässige Echtzeit-Umwandlung gesprochener Sprache in geschriebenen Text, mehrsprachig und sicherheitsrelevant auf. Ob in Justizvollzugsanstalten, Krankenhäusern, Industriebetrieben oder kritischen Infrastrukturen, Sprachbarrieren in der Kommunikation zu Leitstellen gehören damit der Vergangenheit an.

- Das Ergebnis besteht in mehr Sicherheit und Effizienz durch klare Verständigung:
- Verbesserte Kommunikation: Zuverlässige Verständigung in sicherheitsrelevanten Situationen.
- Mehrsprachige Übersetzung: Unterstützung von über 26 Sprachen (99,3 % aller Sprachbarrieren in Deutschland), mit Cloud-Anbindung erweiterbar auf 42.
- Zeitersparnis: Automatische Protokollierung und Dokumentation von Gesprächen ohne Zusatzaufwand.
- Revisionssichere Ablage: Alle Gespräche werden gespeichert und sind jederzeit nachvollziehbar.
- Nahtlose Integration: Einfache Einbindung in bestehende Vipro GMS-Umgebungen für langfristige Investitionssicherheit.

Das System ist insbesondere für multikulturelle Umgebungen entwickelt:

- Justiz & Behörden: Kommunikation zwischen Personal und Insassen ohne Dolmetscher.
- Gesundheitswesen: Verständigung mit Patienten und Angehörigen.
- Industrie & Logistik: Klare Kommunikation mit Lieferanten und Fremdfirmen.
- Empfang & Zutrittskontrolle: Besucherkommunikation ohne Sprachhürden.

Vom Gespräch zum Protokoll

Die Bedienung des Systems erfolgt intuitiv: Gespräche starten wie gewohnt über eine Sprechstelle oder ein Telefon. Die KI erkennt automatisch die Sprache der Teilnehmer, übersetzt in Echtzeit und stellt sowohl Originaltext als auch Übersetzung klar dar. Beide Gesprächspartner können in ihrer Muttersprache sprechen, während das System simultan übersetzt als Audio und Text. Am Ende erstellt der KI Live-Reader automatisch eine zusammenfassende Gesprächsdokumentation, die sicher in der Datenbank gespeichert und mit dem Ereignis verknüpft wird. GIT

Funkwerk
www.funkwerk-security.de/jva

PMR Expo: Accellence zeigt mit Partnern Videoanalyse in Leitstellen

Wie profitieren Sicherheitsbehörden und KRITIS-Betreiber von modernem Videomanagement? Diese Frage steht im Mittelpunkt des Messeauftritts von Accellence Technologies auf der PMR Expo 2025 in Köln. Gemeinsam mit Mauell, Anbieter von Kontrollraum- und Leitstellenausstattungen und Adder, Spezialisten für KVM-Lösungen, präsentiert der Softwarehersteller in einem realistischen Leitstellen-Szenario effiziente Videoanalyse.

Die PMR Expo in Köln gilt als die führende europäische Fachmesse für sichere Kommunikation, Leitstellen und kritische Infrastrukturen. Sie richtet sich an Fach- und Führungskräfte aus Behörden (BOS), Energieversorgern, Verkehrsbetrieben und der Industrie, die Kommunikations- und Sicherheitsprozesse effizient gestalten wollen bzw. müssen. Accellence Technologies demonstriert gemeinsam mit den Partnern Mauell und Adder, wie moderne Leitstellen Videodaten, Ereignisse und Systemmeldungen intelligent verarbeiten können.

Vom Videobild zur Entscheidung: Mehrwert durch Integration

Über die KVM-Technologie von Adder lassen sich unterschiedliche Anwendungen und Systeme sicher und latenzfrei ansteuern, während Mauell mit professionellen Monitoren und Möbelsystemen für Leitstellen die physische Arbeitsumgebung bereitstellt.

Accellence zeigt in dieser Umgebung anschaulich, wie sich Videomanagement und Ereignisverarbeitung in Leitstellenprozesse integrieren lassen. Zentral dabei sind das Videomanagement-System Vimacc, das sich durch seine flexible Architektur und Skalierbarkeit auszeichnet, sowie die Videomanagementlösung Ebüs, mit der Videosysteme unterschiedlicher Hersteller unter einer einheitlichen Oberfläche aufgeschaltet und bedient werden können.

PMRExpo: Halle 7, Stand A032 **www.accellence.de**

GIT SICHERHEIT

Die GIT SICHERHEIT ist für mich wichtig, weil sie vor allem das Bewusstsein dafür schärft, dass jeder selbst etwas für seine eigene und die Sicherheit seines Unternehmens tun kann und sollte.

Falk Schnabel,
Präsident der Polizei Hamburg

Sicherheitskonzepte gegen hybride Bedrohungen

Auf der diesjährigen Protekt in der Kongresshalle am Zoo Leipzig präsentiert LivEye die für den dauerhaften Gebrauch konzipierte Überwachungslösung NSTR.security. Die kompakte Mietlösung schützt kritische Infrastruktur mit einer Kombination aus Überwachungskameras, KI-gestützter Analysesoftware und 24/7-Leitstelle vor ungewolltem Zugriff und Sabotage. Am Messestand freut sich Andreas Schmitz, Resilienzmanager KRITIS, auf regen Austausch. Er hält zudem einen Vortrag zum Thema „Mobile Sicherheit als Lösung zum Schutz gegen hybride Bedrohungen“. Für Prävention und Aufklärung sorgt NSTR.security. Die Überwachungslösung identifiziert und stoppt Eindringlinge mit einer Kombination aus Überwachungskamera, KI und dauerhaft besetzter Leitstelle: Fünf integrierte Kameras eines Systems liefern gestochen scharfe Bilder über eine Fläche von rund 4.300 m². Mit einem Überwachungsradius von 200° spähen sie bis in kleinste Ecken.

Protekt: Richard-Wagner-Saal, Stand RWS4 **www.liveye.com**

MOBILIAR

Funktional und menschlich

Möbel von Pineapple für Gemeinschaftsräume im Strafvollzug

Gemeinschaftsbereiche in Haftanstalten stellen besondere Anforderungen an Planung und Gestaltung. Sie sollen soziale Begegnung ermöglichen, Tagesstruktur schaffen und ein Mindestmaß an Alltagsnähe bieten – ohne dabei auf notwendige Schutzmaßnahmen zu verzichten. Das Spannungsfeld zwischen Kontrolle und Lebensqualität lässt sich nur durch ein sorgfältiges Zusammenspiel von Gestaltung, Materialwahl und baulicher Umsetzung ausbalancieren. So entstehen Räume, die strukturiert wirken und dennoch eine menschliche Atmosphäre bewahren.

Für Inhaftierte sind Gemeinschaftsräume essenzielle Treffpunkte. Hier finden Gespräche, Spiele, Lernangebote und gemeinsames Verweilen statt – Momente, die zur sozialen Stabilisierung und psychischen Gesundheit beitragen. Damit dies gelingt, müssen diese Räume so konzipiert sein, dass sie zuverlässig funktionieren, gleichzeitig aber Offenheit und Vertrauen ermöglichen.

Ein durchdachtes Raumkonzept spielt dabei eine zentrale Rolle: Vom Mobiliar bis zur Wandgestaltung muss alles so ausgelegt sein, dass es funktional bleibt und zugleich eine einladende Wirkung entfaltet. Natürliche Farben, ergonomisches Design und widerstandsfähige Materialien helfen, eine Umgebung zu schaffen, die nicht abschreckend wirkt, sondern Orientierung und Ruhe vermittelt.

Schwachstellen vermeiden – durch kluge Gestaltung

Ein typisches Problem in solchen Einrichtungen besteht im potenziellen Missbrauch von Gegenständen und Möbeln. Ungesicherte Spalten, Nähte oder Hohlräume bieten Möglichkeiten

Gemeinschaftsbereiche in Haftanstalten stellen besondere Anforderungen an Planung und Gestaltung

© Xsquared Architects | Photography by Natasha Mulhall

Wenn Gestaltung und Funktion harmonieren, entstehen Orte, die weit mehr leisten als reine Überwachung

zur Verbergung unerlaubter Objekte – eine Herausforderung für den reibungslosen Betrieb.

Moderne Möbelentwicklungen von Pineapple setzen hier an: Mit fugenlosen Oberflächen, verdeckten Konstruktionen und besonders widerstandsfähigen Materialien wird potenziellem Missbrauch effektiv vorgebeugt. Gleichzeitig erleichtert dies die Reinigung und Wartung – ein praktischer Vorteil im anspruchsvollen Alltag des Strafvollzugs.

Fortschrittliche Designs gehen noch einen Schritt weiter: Möbel mit verstärkten Strukturen, abgedeckten Unterseiten und glatten Übergängen lassen keine unnötigen Zwischenräume zu. Dadurch wird das Risiko unerwünschter Nutzung minimiert – ganz ohne auf Ästhetik oder Komfort zu verzichten.

Sicheres Design ohne Abschreckung

Schutzmaßnahmen müssen heute kein Widerspruch zu wohnlichem Design sein. Im Gegenteil: Sie werden zunehmend als integraler Bestandteil ästhetischer und funktionaler Konzepte verstanden. Glatte Formen, angenehme Materialien und intelligente Details ermöglichen eine angenehme Umgebung, die den Überblick bewahrt und zugleich respektvoll wirkt.

Ein Blick nach Nordeuropa oder Australien zeigt, wie solche Konzepte bereits umgesetzt werden: Gemeinschaftsbereiche sind dort so gestaltet, dass sie Kommunikation fördern, Spannungen abbauen und gleichzeitig klare Grenzen setzen. Das Ergebnis sind Räume, die sowohl alltagstauglich als auch strukturiert wirken – im besten Sinne funktional und menschlich.

Fazit

Die Gestaltung von Gemeinschaftsräumen in Haftumgebungen verlangt ein feines Gespür für das richtige Maß an Kontrolle, Alltagstauglichkeit und Menschlichkeit. Moderne Einrichtungskonzepte zeigen, dass es möglich ist, belastbare und zugleich lebensnahe Räume zu schaffen, die zur Stabilisierung des Alltags und zur positiven Entwicklung beitragen.

Wenn Gestaltung und Funktion harmonieren, entstehen Orte, die weit mehr leisten als reine Überwachung: Sie fördern Struktur, Gemeinschaft und ein respektvolles Miteinander – ein wichtiger Baustein für einen zeitgemäßen und verantwortungsvollen Umgang mit Menschen in geschlossenen Einrichtungen. GIT

Pineapple
www.pineapplecontracts.com

Glatte Formen, angenehme Materialien und intelligente Details ermöglichen eine angenehme Umgebung

Ralf Kötting (l.) und Martin Willers, beide Projektverantwortliche für die JVA Münster beim BLB NRW

JVA-NEUBAU

Zum Neubau der JVA Münster

„Die bauliche Struktur einer JVA ist zentraler Faktor für die Umsetzung eines modernen Justizvollzugs“

Der Bau und Liegenschaftsbetrieb NRW (BLB NRW) ist das Immobilienunternehmen des Landes Nordrhein-Westfalen. Als solches errichtet es im Auftrag des NRW-Justizministeriums derzeit eine neue Justizvollzugsanstalt in Münster, wo es den 180 Jahre alten Vorgängerbau ersetzt. GIT SICHERHEIT sprach mit den Projektverantwortlichen Ralf Kötting und Martin Willers.

Herr Kötting, Herr Willers, Sie sind Projektverantwortliche beim Bau- und Liegenschaftsbetrieb des Landes Nordrhein-Westfalen (BLB NRW). Könnten Sie zum Einstieg etwas über Ihr Haus und seine Aufgaben sagen?

Ralf Kötting: Der BLB NRW ist Eigentümer und Vermieter fast aller Immobilien des Landes Nordrhein-Westfalen. Mit rund 4.000 Gebäuden und einer Mietfläche von etwa 10,3 Millionen Quadratmetern verantwortet er eines der größten Immobilienportfolios Europas. Er befasst sich u. a. mit Entwicklung und Planung, Bau und Modernisierung sowie Bewirtschaftung und Verkauf von technisch und architektonisch komplexen Immobilien. Darüber hinaus plant und realisiert der BLB NRW mit seinem Bereich Bundesbau die zivilen und militärischen Baumaßnahmen der Bundesrepublik Deutschland in Nordrhein-Westfalen. Der BLB NRW beschäftigt mehr als 3.000 Mitarbeiterinnen und Mitarbeiter an acht Standorten.

In Ihrem Verantwortungsbereich entsteht derzeit die komplett neue Justizvollzugsanstalt Münster. Geben Sie uns ein paar Eckdaten?

Martin Willers: Wir realisieren eine neue Justizvollzugsanstalt mit 640 Haftplätzen für den geschlossenen Männervollzug. Neben den Haftgebäuden gehören dazu alle für den Betrieb notwendigen Einrichtungen wie Werkstätten, Pädagogisches Zentrum, Küchen, Begegnungszentrum, Sportstätten, Garagen, Kammer und die Verwaltung. Insgesamt sind es 14 Gebäude mit einer Bruttogeschossfläche von rund 63.000 m².

Mit welchen Zeiträumen wurde dieses Projekt geplant – und wann soll die JVA eröffnet werden?

Ralf Kötting: Dem Start der Rohbauarbeiten Ende 2023 waren umfangreiche Planungen sowie vorbereitende Maßnahmen vorausgegangen, angefangen mit einer gesamträumlichen Standortanalyse. Dabei wurde mit externen Partnern in einem mehrstufigen Verfahren der am besten geeignete Standort ermittelt. Danach haben wir im Bereich des Grundstückes umfassende Ausgleichsmaßnahmen nach dem Bundesnaturschutzgesetzt realisiert. Zudem haben wir vor Start der Rohbauarbeiten die rund einen Kilometer lange Haftmauer errichtet. Dadurch hatten wir

gleichzeitig schon die Sicherung für die spätere Baustelle und benötigten in weiten Teilen keinen Bauzaun. Die eigentliche Planung der Gebäude hat Ende 2019 begonnen. Die Arbeiten kommen gut voran, werden aber aufgrund ihres Umfangs und ihrer Komplexität noch einen längeren Zeitraum in Anspruch nehmen. Gerade in diesem sensiblen Bereich geht Sicherheit und Qualität vor Schnelligkeit.

Anlass für die Entscheidung für einen Neubau war ja vor allem, dass die bisherige Anstalt im Zentrum von Münster den Ansprüchen des modernen Strafvollzugs nicht mehr genügt?

Martin Willers: Mitte 2016 wurden Teile der alten JVA als einsturzgefährdet eingestuft, woraufhin die entsprechenden Hafthäuser umgehend geräumt wurden. Die Sanierung einer Haftanstalt im laufenden Betrieb ist äußerst schwierig und oftmals unverhältnismäßig aufwendig. Im Fall der JVA Münster kamen die statischen Probleme dazu, die eine Sanierung unmöglich machten.

Visualisierung der in Bau befindlichen neuen JVA Münster

Darüber hinaus genügten die zum Teil fast 180 Jahre alten Gebäude nicht mehr den heutigen Anforderungen an einen modernen Justizvollzug.

Welche Anforderungen stellt der moderne Justizvollzug an die bauliche Struktur einer JVA?

Ralf Kötting: Die bauliche Struktur einer JVA ist ein zentraler Faktor für die Umsetzung der Ziele des modernen Justizvollzugs. Gemäß § 2 Strafvollzugsgesetz (StVollzG) besteht der Zweck des Vollzugs darin, „den Gefangenen zu befähigen, künftig in sozialer Verantwortung ein Leben ohne Straftaten zu führen". Damit rückt die Resozialisierung in den Mittelpunkt des Vollzugskonzepts. Dies verlangt von einer JVA-Struktur ein ausgewogenes Verhältnis zwischen Sicherheit, Resozialisierung und Humanität.

Können Sie ein paar Beispiele dafür nennen, wie dies in Münster umgesetzt wird?

Martin Willers: Zunächst einmal gibt es ein mehrstufiges Sicherheitskonzept, nämlich eine Kombination aus baulichen, technischen und organisatorischen Maßnahmen wie Zäune, Schleusen und Überwachungssysteme. Wir haben differenzierte Sicherheitsbereiche, bei denen die Haftarten getrennt werden: Untersuchungshaft, Strafhaft und ein verstärkt gesicherter Haftbereich. Es gibt moderne Arbeitsumgebungen für Bedienstete mit guten Sichtachsen und kurzen Wegen zu den Arbeitsplätzen. Außerdem haben wir Werkstätten, Schulungsräume und IT-Lernräume für die beruflichen Qualifikationen sowie Therapie- und Beratungsräume für Sozialarbeit, Psychotherapie, Suchtberatung und seelsorgerische Betreuung. Auch Freizeit- und Sportangebote zur Förderung von Gesundheit und sozialem Verhalten gehören dazu. Ebenfalls wichtig ist die interdisziplinäre Zusammenarbeit: Sozialdienst, psychologischer Dienst, medizinischer Dienst und Vollzugsbeamte arbeiten räumlich und organisatorisch eng zusammen.

Mauer und Zäune rund um die JVA waren auch Gegenstand von Fragen von Anwohnern am neuen Standort. Können Sie etwas dazu sowie zur Sicherheitstechnik im Allgemeinen sagen?

Ralf Kötting: Im Hinblick auf die Mauer- und Zaunanlagen der JVA Münster bestehen keine spezifischen gesetzlichen Vorgaben aus bauordnungsrechtlicher Sicht. Die detaillierten technischen Vorgaben für die Haftmauer und die Sicherungszaunanlage kommen vom Ministerium der Justiz des Landes Nordrhein-Westfalen. Die sicherheitstechnischen Einrichtungen in der neuen JVA sind natürlich sehr umfangreich. Dazu gehören zum Beispiel eine Personennotsignalanlage, ein digitales Videosystem, Zaundetektion sowie eine Schlüsselfachanlage mit Schlüsselmanagement. Auf Details können wir aus Sicherheitsgründen nicht eingehen.

Es gibt in Münster auch ein umfassendes Brandschutzkonzept. Welche Besonderheiten hat es?

Martin Willers: Brandschutz ist auch im Justizvollzug ein zentrales Thema. Der Schutz der Gefangenen sowie der Justizvollzugsbeamtinnen und -beamten hat dabei höchste Priorität. Für die JVA Münster wurde ein umfassendes Brandschutzkonzept durch einen unabhängigen Brandschutzsachverständigen erstellt. Dieses wurde in enger Abstimmung mit der Feuerwehr Münster sowie dem BLB NRW-internen Servicecenter für bauaufsichtliche Angelegenheiten entwickelt. Eine Besonderheit der Einrichtung liegt darin, dass neben den hohen Anforderungen an den Brandschutz auch die Manipulationssicherheit gewährleistet sein muss. Erwähnenswert ist zudem, dass das Brandschutzkonzept kein starres, einmalig erstelltes Dokument darstellt. Es wird während der fortlaufenden Planung und dem Baufortschritt regelmäßig überprüft, ergänzt und aktualisiert.

Bei der Grundsteinlegung kamen ein altes Haftraumtürschloss und ein ausrangiertes Personennotrufgerät in eine eingemauerte Zeitkapsel...

Ralf Kötting: Bei der technischen Entwicklung der Personennotrufgeräte haben wir sicherlich einen Quantensprung erlebt. Auch die heutigen Haftraumschlösser sind in puncto Sicherheit nicht mit den früheren zu vergleichen. Insofern bieten die Zugaben der JVA Münster für die Zeitkapsel einen spannenden Blick auf die analoge Sicherheitstechnik der Vergangenheit. GIT

Bau- und Liegenschaftsbetrieb NRW
www.blb.nrw.de

ROBOTIK

Robotik wird Sicherheits-strategie

Warum die Software der wahre Gamechanger ist

Die Anforderungen an Sicherheitssysteme steigen. Vor allem Kritische Infrastrukturen (KRITIS), weitläufige Industrieareale oder schwer zugängliche Einsatzgebiete sind besonders schutzbedürftig. Herkömmliche Maßnahmen geraten dabei schnell an ihre operativen und wirtschaftlichen Grenzen. Vor diesem Hintergrund rücken robotergestützte Sicherheitslösungen immer stärker in den Fokus innovativer Sicherheitsstrategien. Securiton hat dafür die Softwareplattform „SecuriBotic Central“ als Steuer- und Einsatzinstanz entwickelt.

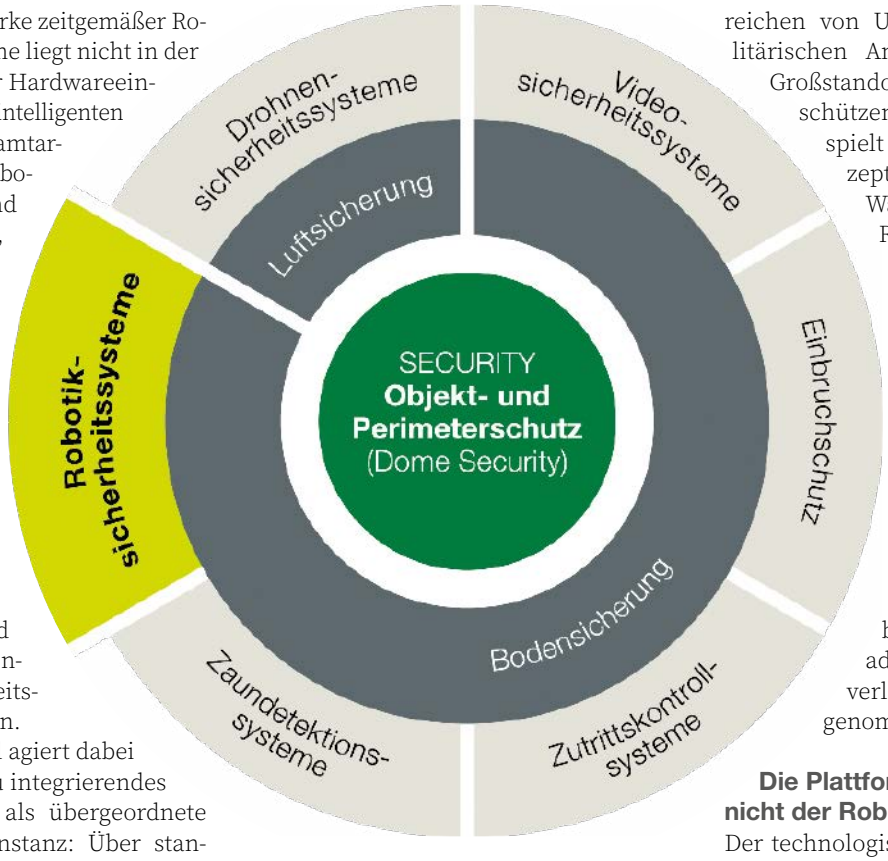
Die eigentliche Stärke zeitgemäßer Robotiksicherheitssysteme liegt nicht in der Anwendung einzelner Hardwareeinheiten, sondern in der intelligenten softwarebasierten Gesamtarchitektur: Roboter, ob bodengebunden, fliegend oder schwimmend, werden zu vollintegrierten Bestandteilen eines umfassenden Sicherheitsmanagementsystems. Die „SecuriBotic Central“ ist eine Softwareplattform mit der Fähigkeit, verschiedene Robotereinheiten zentral zu koordinieren, automatisch zu steuern und damit zum jederzeit einsatzbereiten Sicherheitsagenten zu verwandeln.

SecuriBotic Central agiert dabei nicht als zusätzlich zu integrierendes Subsystem, sondern als übergeordnete Steuer- und Einsatzinstanz: Über standardisierte Schnittstellen bindet sie vorhandene Sicherheitslösungen wie etwa Zaundetektion oder Videoanalyse an und nutzt deren Ereignisse als Trigger für robotische Interventionen. So können autonome „First Responder“ gezielt und regelbasiert in Alarmzonen entsendet werden, um verdächtige Situationen vor Ort zu verifizieren und sicherheitsrelevante Daten in Echtzeit an die Leitstelle zu übermitteln. Das Resultat ist eine durchgängige, skalierbare und hochautomatisierte Sicherheitsarchitektur mit minimalem Integrationsaufwand.

Zentral gesteuert, flexibel kombiniert

Je nach Einsatzszenario lässt sich der jeweils passende, kompatible „Agent“ auswählen. Alle Einheiten werden dann über dasselbe Bedien- und Steuerinterface geführt. So entsteht ein Ökosystem, das eine große Auswahl verschiedener Systeme ermöglicht, gleichzeitig aber eine einheitliche Bedienlogik bietet.

Ein weiterer Vorteil liegt in der Modularität der Sensorik (Pay Loads): Die Agents lassen sich je nach Bedarf individuell mit Wärmebildkameras, optischen PTZ-Kameras, Gasdetektoren, Laserscannern oder akustischen Sensoren ausstatten, um konkrete Situationsdaten zu erfassen, zu analysieren und Interventionsvorschläge zu übermitteln. Typische Einsatzfelder reichen von Umspannwerken und militärischen Anlagen über industrielle Großstandorte bis hin zu kompakten, schützenswerten Objekten. Dabei spielt das Fortbewegungskonzept der Agenten (Land, Luft, Wasser) eine untergeordnete Rolle: Für jedes Terrain und jede Gefährdungslage lässt sich SecuriBotic Central entsprechend konfigurieren. Darüber hinaus sind die Systeme nicht nur für dauerhafte Installationen geeignet, sondern auch taktisch mobil einsetzbar und „mobile-deploy“-fähig. So können sie für temporäre Sicherheitsaufgaben, Veranstaltungen oder ad-hoc-Operationen schnell verlegt und sofort in Betrieb genommen werden.



Verlässliche Hightech-Securitylösungen aus einer Hand, intelligent miteinander verzahnt

Die Plattform entscheidet – nicht der Roboter

Der technologische Fortschritt in der Sicherheitsrobotik verschiebt den Fokus: Nicht der Roboter als Einzelprodukt steht im Mittelpunkt, sondern die Plattform, die ihn steuert, vernetzt und in bestehende Systeme integriert. Anwender entscheiden sich somit nicht für ein Gerät, sondern für ein skalierbares, zukunftssicheres System, das sich nahtlos in vorhandene Sicherheitsarchitekturen einfügt. Mit SecuriBotic Central setzt die intelligente Synergie aus Hardware und Software neue Standards für Sicherheit, Effizienz und Verfügbarkeit. GIT

Securiton Deutschland
www.securiton.de/robotics

GIT SICHERHEIT AWARD 2026 WINNER

PLUS X AWARD
ABUS
HÖCHSTE KUNDENZUFRIEDENHEIT 2025
Schließsysteme
www.plusxaward.de

TECTIQ VON ABUS

DIGITAL, SICHER & EINFACH ZUTRITTE MANAGEN

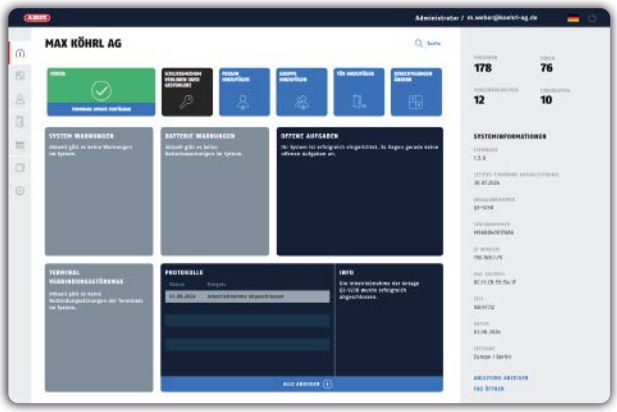
Das digitale Schließsystem TECTIQ von ABUS bietet maßgeschneiderte Sicherheit, die perfekt auf die Bedürfnisse der Kunden zugeschnitten ist. Anwender profitieren von der einfachen Bedienung und der zuverlässigen Funktionalität im täglichen Einsatz.

Die Auszeichnungen mit dem GIT Sicherheit Award 2026 und dem Plus X Award 2025 für höchste Kundenzufriedenheit bestätigen die vielen Vorteile des TECTIQ Systems.

TECTIQ von ABUS – die Software macht den Unterschied!

Modern, übersichtlich, intuitiv:
Mit der digitalen Schließanlage TECTIQ und seiner Bedien-Software Access Manager setzen wir neue Maßstäbe in Sachen nutzerfreundlicher Schließanlagen-Software. Selbst Anwender ohne Vorkenntnisse finden sich schnell zurecht und haben das System stets effizient & sicher im Griff.

Über die besonders übersichtliche Bedienoberfläche lassen sich mit wenigen Klicks



- **Nutzer anlegen oder entfernen**
- **Nutzergruppen erstellen oder bearbeiten**
- **Berechtigungen erteilen oder entziehen**
- **Zeitpläne definieren oder flexibel anpassen**

und das von überall aus und über verschiedene Gebäude und Standorte hinweg!

Zusätzliche Funktionen wie der Datenschutz- und Betriebsratsmodus sowie die Definition individueller Feier- und Sperrtage machen die Software noch leistungsfähiger – und gleichzeitig leicht bedienbar.

TECTIQ von ABUS – digitale Zutrittskontrolle, die einfach funktioniert.

Jetzt QR-Code scannen und unverbindlich anfragen!

VIDEOSICHERHEIT

Volle Kontrolle

Ein Versprechen für Sicherheit: Thomas Dallmeier über das Gütesiegel „made in Germany“

Thomas Dallmeier, CEO von Dallmeier

Das Unternehmen Dallmeier ist seit Jahrzehnten ein führender Anbieter von Videoüberwachungs- und Videoinformationstechnologie. Im Gespräch mit GIT SICHERHEIT erklärt CEO Thomas Dallmeier, warum das Gütesiegel „Made in Germany“ für sein Unternehmen mehr als ein Marketingversprechen ist – und weshalb internationale Kunden gezielt nach Produkten aus Deutschland verlangen.

Herr Dallmeier, Ihr Unternehmen entwickelt und produziert seit jeher in Deutschland. Warum halten Sie so konsequent am Standort fest?

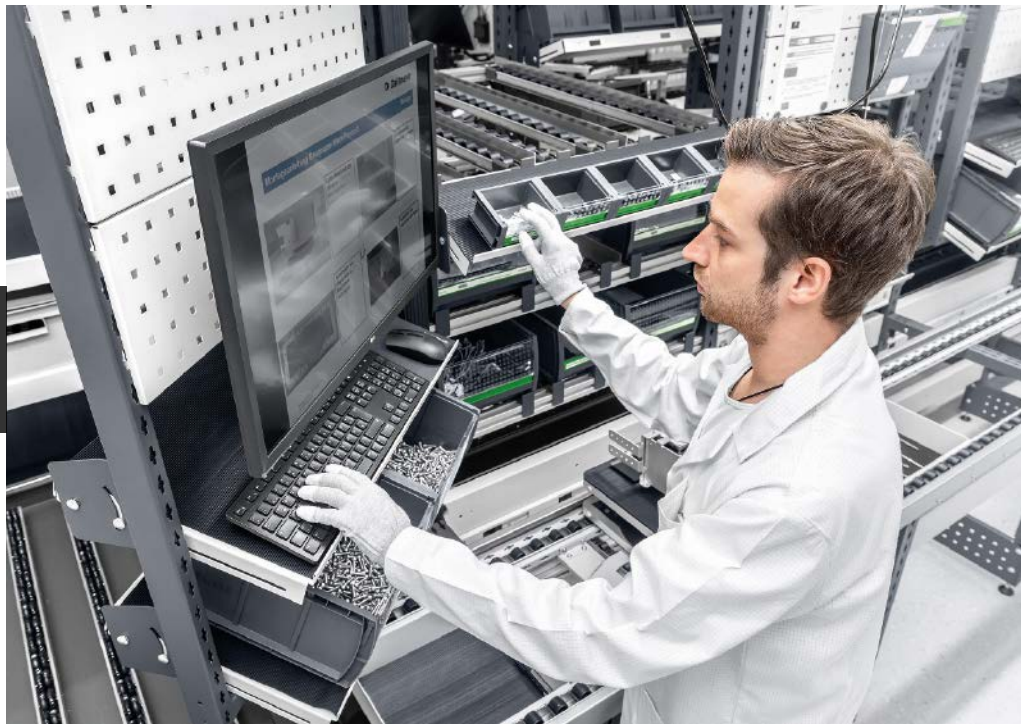
Thomas Dallmeier: Für uns ist „Made in Germany“ seit jeher eine Verpflichtung, keine Werbefloskel. Unsere Kunden verlangen Qualität, und sie sind auch bereit, dafür zu zahlen. Gerade in der Sicherheitstechnik geht es nicht nur um Funktionalität, sondern vor allem um Vertrauen.

Viele asiatische Anbieter locken mit günstigen Preisen. Was unterscheidet Dallmeier davon?

Thomas Dallmeier: Preis ist nicht alles. Bei sicherheitsrelevanten Produkten kann ein vermeintlich günstiger Einkaufspreis sehr teuer werden – zum Beispiel, wenn Daten unbemerkt ins Ausland abfließen oder versteckte Hintertüren im System existieren. Solche Fälle sind bekannt. Unsere Kunden – von Flughäfen über Stadien bis hin zu Industrieanlagen – wissen: Mit Dallmeier haben sie die volle Kontrolle über Hard- und Software.

Was bedeutet „volle Kontrolle“ konkret?

Thomas Dallmeier: Wir entwickeln und produzieren sämtliche Kernkomponenten selbst – von der Kamera über die Aufzeichnungssoftware bis zur intelligenten Auswertung. Rund 50 % unserer Entwicklungsressourcen fließen allein in Sicherheitsaspekte. Damit machen wir die Sicherheitstechnik selbst sicher – Stichwort Cybersecurity und „Secure by Design“. Nur so können wir garantieren, dass unsere Produkte frei von Manipulationen sind.



Dallmeier entwickelt und produziert sämtliche Kernkomponenten selbst – von der Kamera über die Aufzeichnungssoftware bis zur intelligenten Auswertung

Wie sieht ein echter „Secure by Design"-Ansatz in der Praxis aus?

Thomas Dallmeier: Ein echter „Secure by Design"-Ansatz beginnt bei Dallmeier wie gesagt bereits bei der Produktentwicklung: Durch eigene Softwareentwicklung und Fertigung in Deutschland gewährleisten wir eine vollständige Transparenz in der Lieferkette und minimieren das Risiko von Hintertüren. Technisch setzen wir auf mehrere Schutzebenen: sichere Datenübertragung, strenge Zugriffskontrollen, abgeschottete Betriebssysteme und integrierte Sicherheitsvorkehrungen gegen unbefugten Zugriff. Regelmäßige Updates sowie Penetrationstests ergänzen das Konzept und sorgen dauerhaft dafür, dass unsere Kunden maximale Sicherheit bei minimalem Administrationsaufwand erhalten.

Sind Datenschutzvorgaben eher Herausforderung oder Chance für die Entwicklung von Sicherheitstechnologie?

Thomas Dallmeier: Beides – aber vor allem eine Chance. Vorschriften wie die DSGVO bringen zweifellos technische und organisatorische Herausforderungen mit sich. Gleichzeitig fördern sie aber Transparenz, Qualität und Verantwortungsbewusstsein. Wer Datenschutz nicht als Hürde, sondern als festen Bestandteil der Systemarchitektur versteht, schafft Vertrauen – insbesondere im Umfeld von Behörden, kritischer Infrastruktur oder international agierenden Unternehmen. Am Ende ist Compliance keine Last – sie ist eine Stärke, die Vertrauen und Differenzierung schafft.

Andere Unternehmen verlagern aus Kostengründen ins Ausland. Warum kommt das für Sie nicht infrage?

Thomas Dallmeier: Weil man damit Vertrauen verspielt. Wenn ich nicht mehr weiß, was in einer Komponente steckt, kann ich meinen Kunden keine hundertprozentige Sicherheit versprechen. Made in Germany bedeutet für uns: Jeder Entwicklungsschritt ist nachvollziehbar, überprüfbar und transparent.

Gerade im Bereich der Hochtechnologie ist in der Vergangenheit bereits viel wertvolles Know-how aus Deutschland abgewandert – etwa im Bereich der Kameraoptik. Wir sehen darin eine Verpflichtung: Dallmeier investiert gezielt in die Entwicklungstiefe am Standort Regensburg, um genau dieses Wissen zu sichern und weiter auszubauen. Unser Anspruch ist es, nicht nur fertige Komponenten zu integrieren, sondern Schlüsseltechnologien selbst zu beherrschen – für mehr Transparenz, Qualität und langfristige Innovationsfähigkeit.

Welche Rolle spielt dabei die Nachfrage der Kunden?

Thomas Dallmeier: Eine entscheidende. Unsere Kunden fragen gezielt nach Made in Germany, weil es für Qualität, Datenschutz und Compliance steht. In internationalen Ausschreibungen ist es häufig sogar das ausschlaggebende Kriterium.

Wird das Gütesiegel künftig noch wichtiger werden?

Thomas Dallmeier: Ganz klar: ja. Cyberangriffe, Industriespionage und geopolitische Unsicherheiten nehmen zu. Vertrauen in Herkunft und Integrität von Produkten wird immer wichtiger. Wer Made in Germany kauft, investiert nicht nur in Technik, sondern in Zukunftssicherheit.

Wie relevant ist das Thema KI in Ihren Entwicklungen – und wie stellen Sie hier Qualität und Transparenz sicher?

Thomas Dallmeier: Künstliche Intelligenz ist für uns kein Trend, sondern ein zentraler Baustein unserer Entwicklungen. Um Qualität und Transparenz sicherzustellen, gehen wir bewusst unseren eigenen Weg: Wir trainieren unsere neuronalen Netze auf unserem firmeneigenen, speziell dafür ausgestatteten Testgelände – und das unter realen Einsatzbedingungen.

Der Vorteil liegt auf der Hand: Bei vielen am Markt verfügbaren Netzen ist unklar, mit welchen Daten sie trainiert wurden. Genau hier lauern Risiken – von Verzerrungen in den Ergebnissen bis hin zu nicht nachvollziehbaren Fehlerquellen. Wir dagegen schaffen unsere Trainingsdaten selbst, exakt abgestimmt auf die Anforderungen unserer Kunden. So behalten wir die volle Kontrolle über den Input und können garantieren, dass unsere Netze praxisnah, zuverlässig und transparent arbeiten. Dieser Ansatz steigert nicht nur die Präzision und Verlässlichkeit, sondern schafft eine klare Grundlage für Vertrauen in die Technologie. Kurz gesagt: Wir setzen auf „AI made in Germany".

Bitte umblättern ▶

Nicht nur die Hardware, auch die Software von Dallmeier entsteht in Deutschland

Andere Hersteller werben auch mit „Made in Germany“. Wo liegt der Unterschied zu Dallmeier?

Thomas Dallmeier: Leider ist es in unserer Branche oft so, dass „Made in Germany“ oft nur die Endmontage in Deutschland umfasst. Dabei werden Komponenten teilweise aus sensiblen oder sicherheitskritischen Regionen eingekauft. Das mag formaljuristisch reichen, hat mit echtem „Made in Germany“ aber wenig zu tun.

Noch kritischer ist allerdings der Software-Bereich: Bei vielen Herstellern stammen die zentralen Software-Komponenten nicht aus Deutschland. Kunden können daher kaum nachvollziehen, wer tatsächlich Zugriff auf ihre sensiblen Videodaten hat – oder ob im schlimmsten Fall Hintertüren eingebaut sind.

Bei Dallmeier ist das anders: Wir entwickeln und produzieren unsere Hardware in Deutschland, und genauso entsteht unsere Software hier – inklusive aller Themen rund um Datenschutz und Datensicherheit. Das heißt: Von der ersten Schraube bis zur letzten Codezeile unterliegt alles deutschen Qualitäts- und Rechtsstandards. Das ist für unsere Kunden nicht nur ein Qualitätsversprechen, sondern vor allem ein entscheidender Faktor für Vertrauen.

Sie haben Rechtsstandards erwähnt… Wie können Organisationen die DSGVO einhalten, ohne die Effizienz ihrer Systeme zu gefährden?

Thomas Dallmeier: Datenschutz und Effizienz schließen sich nicht aus – im Gegenteil: Unsere Systeme sind so konzipiert, dass sie beides vereinen. Ein integriertes Rechtemanagement sorgt beispielsweise für eine präzise Steuerung von Benutzergruppen und Zugriffsrechten. Funktionen wie Privacy Zones ermöglichen es, sensible Bereiche dauerhaft oder ereignisbasiert zu verpixeln. Ein besonders praxisnahes Beispiel ist das Panomera Privacy Shield: Die fernsteuerbare Abdeckung für unsere Multifocal-Sensorkameras unterstützt nicht nur die Einhaltung von Datenschutzvorgaben, sondern erhöht durch die Remote-Bedienung gleichzeitig die Effizienz.

Ihr Fazit, Herr Dallmeier?

Thomas Dallmeier: Made in Germany ist für uns kein Label, sondern ein Versprechen – an unsere Kunden, an unsere Mitarbeiter und an den Standort Deutschland. In der Sicherheitstechnik darf es keine Kompromisse geben. Und genau dafür stehen wir. GIT

Dallmeier electronic
www.dallmeier.com

Wisniowski investiert in Polen und Deutschland

Wisniowski setzt zwei strategische Investitionsprojekte um, die seine Position auf dem europäischen Markt weiter stärken. Das Unternehmen hat sowohl den Ausbau seines Produktionswerks innerhalb der polnischen Investitionszone als auch den Kauf eines Grundstücks in Deutschland für den Bau eines modernen Büro- und Schulungskomplexes bekannt gegeben.

Auf einem 8.316 m² großen Grundstück im nordrhein-westfälischen Unna/Kamen entsteht ein moderner Büro- und Schulungskomplex mit Ausstellung, Konferenzbereich und Best-Seller-Schulungszentrum. Der neue Standort soll Kunden nicht nur Zugang zum gesamten Produktsortiment der Marke ermöglichen, sondern auch bis zu 30 neue Arbeitsplätze in der Region schaffen.

Die günstige Lage in der Nähe des Verkehrsknotenpunkts Kamener Kreuz erlaube dem Unternehmen eine schnelle und effiziente Kundenbetreuung in Deutschland und Westeuropa. Das sei ein strategischer Schritt für die weitere Expansion, so Marcin Burek, Vertriebsleiter für die DACH-Region bei Wisniowski.

Der Komplex wird im Einklang mit der Green-Light-Initiative realisiert – einer Strategie zur Reduzierung des CO_2-Fußabdrucks durch den Einsatz von Wärmepumpen, Photovoltaikanlagen und Ladestationen für Elektrofahrzeuge. „Dies ist ein wichtiges Signal für die lokale Wirtschaft – die Investition schafft Arbeitsplätze und unterstützt die Weiterentwicklung von Fachkompetenzen in der Region“, kommentiert Sascha Dorday, Geschäftsführer der WFG Kreis Unna.

Die Investition am polnischen Standort im Wert von fast 160 Mio. PLN (ca. 37 Mio. Euro) umfasst den Ausbau der technischen Infrastruktur, die Modernisierung des Maschinenparks sowie die Anschaffung innovativer Produktionslinien. Das Projekt soll die technologischen Prozesse optimieren, die operative Effizienz steigern und alle Produktgruppen weiterentwickeln – von Toren und Bauelementen bis hin zu Zaunsystemen. Darüber hinaus entstehen neue Beschäftigungsmöglichkeiten in modernen Produktions- und Technologiebereichen.

Wisniowski ist eine Marke mit polnischen Wurzeln und über 35 Jahren Geschichte. Sie begann 1989, als Firmengründer Andrzej Wisniowski das erste automatisierte Garagentor in Polen entwickelte. Seitdem hat sich das Unternehmen dynamisch entwickelt, in Innovationen und moderne Produktionslinien investiert. Heute beschäftigt es 2.200 Mitarbeiter und vertreibt seine Produkte in 35 Ländern weltweit. **www.wisniowski.de**

IP-DECODER

Die nächste Generation

IP-Decoder-Lösung für Videoüberwachungssysteme

Rasante technologische Fortschritte können für Endnutzer, Integratoren und Berater eine Herausforderung darstellen. Eizo stellt mit dem Duravision DX0231-IP die neueste Generation seiner IP-Decoder-Lösung für Sicherheit und Überwachung vor. Die Komplexität der Systeminstallationen, Cybersicherheit und Wartungsanforderungen unterstreichen die Notwendigkeit eines umfassenden Ansatzes für die physische Sicherheit. Seit der Einführung des ersten IP-Decoder-Monitors des Herstellers im Jahr 2014 bietet Eizo Lösungen, mit denen Nutzer visuelle Technologien zum Schutz von Personen, Unternehmen und Infrastruktur einsetzen können.

DX0231-IP: Leistungsstarke Decodierung sowie flexible Videowiedergabe

Mit dem DX0231-IP bietet Eizo eine eigenständige IP-Decoder-Lösung an, die in einer flexiblen Konfiguration an bis zu zwei 4K-Monitore angeschlossen werden kann, um IP-Kameras, bzw. Videostreams anzuzeigen. Die Lösung funktioniert ohne PC, Anwendungssoftware oder zusätzliche Hardware und bietet Anwendern einen einfachen Installationsprozess, der Zeit und Kosten für die Ersteinrichtung und Systemwartung spart. Dadurch werden potenzielle Fehlerquellen reduziert und Sicherheitslücken ausgeräumt, da nur eine Minimal-Ausrüstung für die Überwachung sensibler Bilddaten über das Netzwerk erforderlich ist.

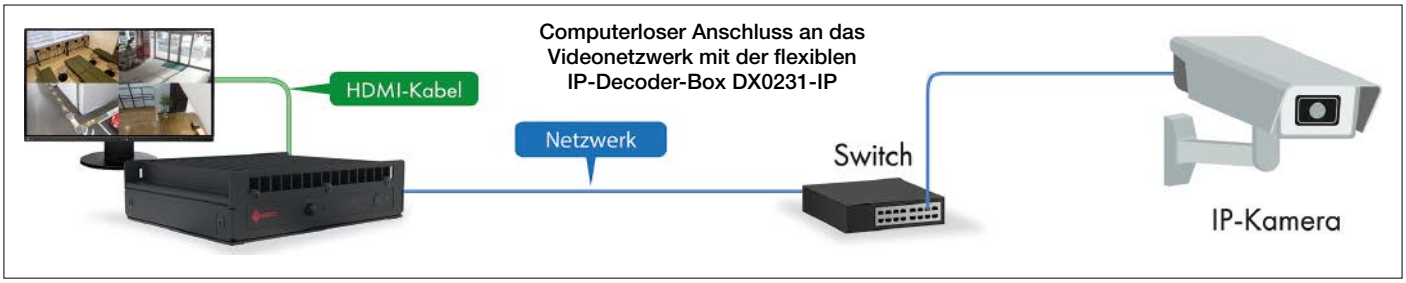
Das smarte Gerät ist mit über 300 Kameras kompatibel, darunter 4K-Kameras mit Onvif-Profil S, Axis-, Vapix-, Panasonic- und i-Pro-Protokollen. Anwender können bis zu 48 Kameras registrieren und bis zu 32 gleichzeitig anzeigen. Das Produkt verfügt erstmals über eine Audioausgabe von IP-Kameras für eine audio-visuelle Situationserkennung.

Der Decoder erweitert die Vielseitigkeit seines Vorgängers und unterstützt die Ultrawide-Bildauflösungen 3840 x 1600 und 3440 x 1440. Dies ermöglicht die Anzeige von Bildern aus Panoramakameras und erleichtert so die Überwachung großer Bereiche und die effektive Beseitigung von toten Winkeln. Der Hersteller hat sich verpflichtet, seine Umweltbelastung zu reduzieren, indem es bei der Produktverpackung des DX0231-IP auf Kunststoff verzichtet.

Zusätzliche Funktionen

- Ereignisreaktion durch Integration mit lokalen Sicherheitssystemen und -geräten (Alert-to-Action)
- Web-Benutzeroberfläche für intuitive Kameragruppierung, -platzierung und -layout
- Zwei HDMI-Ausgänge, jeder mit einer Auflösung von 3840 x 2160
- Optionale Lizenzen zur Freischaltung erweiterter Funktionen für spezielle Benutzeranforderungen wie bspw. VMS-Unterstützungen
- 24-Stunden-Betrieb, 2 Jahre Herstellergarantie für langfristige Zuverlässigkeit

Eizo
www.eizo.de/dx0231-ip



Computerloser Anschluss an das Videonetzwerk mit der flexiblen IP-Decoder-Box DX0231-IP

VIDEOSICHERHEIT

Auf dem Weg zu neuen Meilensteinen

60 Jahre Videosicherheitstechnik von IPS

Modernes Videomanagement und intelligente Videoanalysen vereinen die Marke IPS Intelligent Video Software zu einem hochstabilen Frühwarnsystem für die präventive Gefahrenerkennung. Seit 60 Jahren prägt IPS von Securiton die Videosicherheitstechnik in Deutschland und Europa. „Wir entwickeln unsere IPS-Technologie mit dem Anspruch weiter, auch in Zukunft Maßstäbe in der professionellen Sicherheitsüberwachung zu setzen“, sagt Peter Treutler, Leiter der Business Unit IPS von Securiton in München.

Peter Treutler, Leiter der Business Unit IPS von Securiton

Höchste Sicherheit für Leben und Sachwerte und auch eine spürbare Entlastung für die Anwender im Alltag – das sind die Ziele, die Peter Treutler und sein Entwicklungsteam zu Innovationen für IPS antreiben. In der Securiton-Softwareschmiede am Standort München finden sie Antworten auf Kundenanforderungen und die sich ständig verändernden Marktbedürfnisse: eine intelligente Videoanalyse, die sich den realen Bedingungen flexibel anpasst, benutzerfreundliche Systeme, automatisierte Wartungshilfen, eine leistungsfähigere und zugleich schlankere Hardware-Architektur sowie eine offene und dennoch cybersichere Systemstruktur.

Maßgeschneiderte neuronale Netze

In sicherheitskritischen Anwendungen, speziell bei der lückenlosen Überwachung großer Freigelände und kritischer Infrastruktur, werde Videotechnologie auch weiterhin das Mittel der Wahl bleiben, prognostiziert Peter Treutler. Denn die kontinuierliche und flächendeckende Präsenz und Tiefe einer fest installierten Videosicherheitsanlage könne weder mit Robotern noch mit Drohnen erreicht werden.

Die Weiterentwicklung der intelligenten Videoanalyse werde künftig maßgeblich durch Künstliche Intelligenz geprägt sein, so Peter Treutler. „Standard KI-Modelle stoßen jedoch im sicherheitskritischen Umfeld schnell an ihre Grenzen. Deshalb investieren wir gezielt in das Training maßgeschneiderter neuronaler Netze, die genau auf diese anspruchsvollen Einsatzszenarien zugeschnitten sind – insbesondere im Bereich der Hochsicherheit.“ In der Objektverifikation gelte es, mithilfe von KI unerwünschte Alarme weiter zu senken und die Zuverlässigkeit der Systeme zu steigern. Sie müssen auch unter schwierigen und ständig wechselnden Umgebungsbedingungen noch verlässlicher ein sicherheitsrelevantes Objekt von einer harmlosen Störgröße wie etwa einem Tier, einem Schatten oder einer Reflexion unterscheiden können.

Zudem sieht Treutler die Verlagerung hin zur Anomalie-Erkennung: Leistungsfähige neuronale Netze lernen, was in einer bestimmten Umgebung „normal“ ist, und schlagen Alarm, wenn sie Abweichungen feststellen. „Solche Ansätze sind in dynamischen Umgebungen sinnvoll, etwa auf der Straße zur Erkennung von Geisterfahrern oder in Bahnhöfen zur Detektion plötzlicher Panikbewegung in Menschenmengen.“ Für den Perimeterschutz bleibe jedoch die Herausforderung: Sobald das System eine Anomalie erkannt hat, muss es weiter detailliert klassifizieren und interpretieren können, worum genau es sich bei dem erkannten Objekt handelt.

Leistungsfähiger, effizienter, leichter zu bedienen

Die IPS Next Gen-Produktfamilie wird in den nächsten Jahren sukzessive die bisherige IPS-Systemgeneration ablösen. Mit einer Reihe bedeutender technologischer Weiterentwicklungen wird sie noch leistungsfähiger, effizienter und einfacher in der Handhabung sein. Der IPS NextGen Client bietet heute schon eine vollständig überarbeitete, klar strukturierte Benutzeroberfläche für die intuitive und schnellere Bedienung durch Anwender und Techniker.

Auf modularisierte, ergänzend KI-gestützte Analyseverfahren setzt die IPS Next Gen Video Analytics, die deutlich leistungsfähiger und gleichzeitig einfacher zu konfigurieren ist. Mit einer verbesserten Detektionsgenauigkeit und einer signifikanten Reduktion unerwünschter Alarme entlastet sie das Sicherheitspersonal spürbar.

Nächster Meilenstein

Aktuell ist mit dem IPS Next Gen Video Manager der nächste Meilenstein in der Entwicklung. Das System basiert auf einer komplett neuen Architektur und einem modernen Messaging-Konzept. Es wird Ressourcen noch effizienter nutzen und bei geringerem Hardware-Einsatz mehr Kameras und Analysen pro Server ermöglichen. Über die Cloud werden sich Wartung, Konfiguration und Patch-Management remote und teilweise auch automatisiert durchführen lassen.

Wichtig ist Peter Treutler die Verbesserung der technischen Unterstützung vor Ort. So werden neue Tools und Assistenzfunktionen die Installation und Wartung der IPS-Systeme weiter vereinfachen, um die Arbeit der Techniker zu beschleunigen und Ausfallzeiten zu minimieren. „Wir wollen mit der IPS-Technologie die Besten sein, weil wir glauben, dass Videosicherheit auf diesem Niveau einen echten Unterschied macht – für unsere Kunden, für die Sicherheit ihrer Anlagen und Umgebungen und letztlich für die Sicherheit von Menschen“, sagt der Leiter der Business Unit IPS. GIT

Securiton Deutschland
www.securiton.de

Nahbereich LiDAR Sensoren für hochsichere Innenbereiche

Optex hat Redscan Lite LiDAR Sensoren mit extrem präziser und schneller Nahbereichserkennung für hochsichere Innenbereichen vorgestellt. Die Redscan Lite RLS-1010L Sensoren sind die neueste Ergänzung des mehrfach ausgezeichneten Redscan LiDAR Sortiments von Optex.

Sie haben eine vollständige Abdeckung und bieten sicheren Schutz von Hochsicherheitszonen und besonders gefährdeten engen Innenbereichen, die nur schwer abgedeckt werden können. Selbst Eindringversuche über kleinste Lücken in Rechenzentren zwischen Server-Racks, Käfigen oder in Lüftungsschächten erkennen die RLS-1010L Sensoren zuverlässig.

Mithilfe ihrer Time-of-Flight-Technologie (Laufzeitmessung) erkennen die Sensoren Eindringlinge innerhalb eines 10 m x 10 m Bereichs präzise innerhalb von 100 ms. Unabhängig von Veränderungen in der Raumtemperatur oder den Lichtbedingungen zeigen die Sensoren gleichbleibend hohe Leistung in jedem Innenbereich – selbst bei absoluter Dunkelheit.

Bei horizontaler Installation erzeugen die Sensoren unsichtbare Ebenen, die bspw. Dachfenster und Raumdecken abdecken können. Werden sie hingegen vertikal angebracht, bilden sie unsichtbare Laserwände zum Schutz von Server-Racks, wertvollen Vermögensgegenständen, Personenschleusen und vielem mehr.

Dank einer Reihe von nutzerfreundlichen Eigenschaften ist die Installation und Konfiguration der Sensoren einfach und effizient. Ein optionales Laser-Alignment-Tool erleichtert während der Installation die Visualisierung der Detektionszone; die automatische Bereichskorrektur der Sensoren hilft, ein Übersprechen über den Überwachungsbereich hinaus zu vermeiden; und ein einfaches Drehen der Seitenknöpfe passt den LiDAR-Winkel an den gewünschten Zielbereich an.

„Moderne Umgebungen wie Rechenzentren werden häufig eng bebaut. Redscan Lite Sensoren sind unsere Antwort auf die wachsende Nachfrage nach schneller Detektion in engen, sicherheitskritischen Räumen. Seit wir 2009 die LiDAR Technologie für Sicherheitsanwendungen entwickelt haben, ist es unser fortwährender Anspruch, echte Lösungen für echte Probleme unserer Kunden zu entwickeln. Dafür ist Redscan Lite das neueste Beispiel“, so Mac Kokobo, Head of Global Security Business bei Optex.

Kundenfeedback habe gezeigt, wie groß der Bedarf nach verbessertem Schutz in kleinen, engen Bereichen und Räumen geworden ist. Deshalb wollte man, dass Redscan Lite auch in schmalen Lücken genutzt werden könne und schnelle, hochpräzise Ergebnisse in Innenbereichen biete. **www.optex-europe.com**

ZUTRITT

Mit Highspeed ins Gebäude

Effiziente Personenvereinzelung mit Speedgates

Speedgates für die Personenvereinzelung zeichnen sich durch einen hohen Personendurchsatz in Kombination mit Zutrittskontrollsystemen aus. Die Technik beruht neben schnell fahrenden Türen auf einer Sensorik die elektronisch „vereinzelt“, woher auch der ebenfalls geläufige Name Sensorschleuse herrührt. Speedgates sind heute state of the art bei der Absicherung von Eingangsbereichen. Was zeichnet diese Technik aus und was gibt es zu beachten? Ein Beitrag von Stephan Stephani, Business Development Manager Security Entrance Control DACH bei Assa Abloy Entrance Systems.

Schneller, länger, schmaler. So kann man die Effizienzanforderungen an Speedgates für die Personenvereinzelung kurz und bündig zusammenfassen. Ein Wettbewerb der Superlative ist damit nicht gemeint, sondern vielmehr die Faktoren, die das Sicherheitsniveau beeinflussen.

Je schneller eine Tür ist, desto eher kann sie bei unberechtigten Durchtrittsversuchen schließen. Entgegen der Vermutung beeinflusst die Türgeschwindigkeit den Personendurchsatz kaum. In Kombination mit der Gehäuselänge trägt die Geschwindigkeit zur Sicherheit bei. Je länger ein Gehäuse und somit die Detektionslänge und je höher die Geschwindigkeit, desto weiter können die Türen schließen, bevor die Person in den Unfallschutz gelangt und die Türen nicht weiter schließen.

Faktor Durchgangsbreite

Je breiter ein Sperrflügel, desto weiter ragt er in den Detektionsbereich und überdeckt somit die Erfassung von unberechtigten Durchtrittsversuchen mit der Unfallschutzzone. Die Gehäuselänge, bzw. Detektionslänge sollte daher immer länger sein als die Durchgangsbreite.

Zudem trägt die Durchgangsbreite erheblich zur Sicherheit bei, da die reduzierte Breite rein physikalisch verhindert, dass mehrere Personen nebeneinander passieren können. Ein klassisches Vereinzelungsmaß beträgt ca. 500-650 mm. Ein barrierefreier Durchgang von 900 mm ermöglicht schon eher zwei Personen einen Durchtritt. Ab 1.000 mm Durchgang ist keine mechanische Barriere mehr gegeben, um ein paralleles Passieren zu verhindern. Gehen zwei Personen im Gleichschritt durch eine Sensorschleuse mit waagerechter Detektion, so wird dies auch nicht elektronisch erkannt. Der unerkannte Durchtritt einer unberechtigten Person ist dann nicht zu verhindern.

Geschwindigkeit ist nicht alles

Einzeln betrachtet stellt daher die Geschwindigkeit der Türen keinen Vergleichswert verschiedener Typen dar. Zumal die Geschwindigkeit, bzw. die Schließkraft gem. DIN EN 17352 definiert ist und somit Grenzen aufweisen. Es gilt: je schneller die Tür, je länger das Gehäuse und die Detektionslänge und je schmaler der Durchgang, desto höher die Sicherheit gegen unberechtigte Zutritte.

Der hohe Personendurchsatz von bis zu 60 Personen pro Minute wird hingegen durch Speichern von Freigaben erreicht. Liegen mehrere Freigaben an, so bleibt der Durchgang so lange geöffnet, bis alle berechtigten Personen durchgetreten sind, oder die entsprechenden Timer abgelaufen sind. Ist z.B. der Ausgang frei begehbar, so können beliebig viele Personen passieren, ohne dass die Türen zwischendurch schließen. Der Personendurchsatz ist somit nur noch abhängig von der Durchgangsgeschwindigkeit der Personen.

Benutzerverhalten bei Zutrittskontrolle

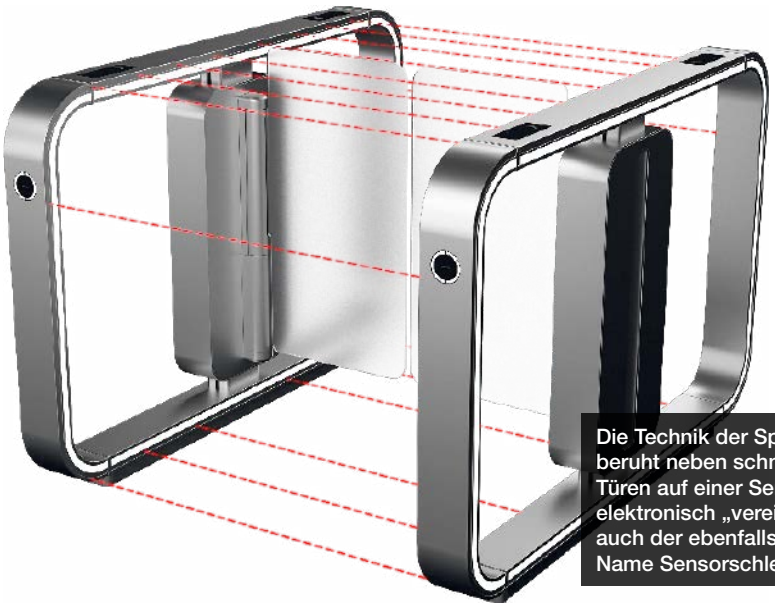
Wird eine Zutrittskontrolle verwendet, dann ist der Gesamtablauf entscheidend für den Personendurchsatz. Geübte Mitarbeiter bedienen die Anlagen schneller als Besucher, die diese Anlagen nur einmalig

nutzen. Bei der Planung der benötigten Anzahl an Durchgängen ist daher eher das Benutzerverhalten zu berücksichtigen, als verschiedene Anlagen miteinander zu vergleichen. Erfahrungsgemäß kann mit 35 bis 40 Personen bei geübten Mitarbeitern mit berührungslosen RFID- Karten kalkuliert werden. Bei Zutritten einmaliger Besucher mit verschiedenen Medien hingegen ist eher von 20 bis 25 Personen zu rechnen.

Für die richtige Planung ist es wichtig, auch den Einsatzzweck und den Standort zu betrachten. Es sind immer die Spitzenzeiten zu betrachten, an denen viele Personen in einem kurzen Zeitraum den Durchgang nutzen. Besonderes Augenmerk ist zu legen auf Eingänge in der Nähe von Haltestellen des ÖPNV, zu Kantinen oder Besuchergruppen.

Warum gibt es aber dann verschiedene Ausführungen in Länge und Breite? Dies ist ergibt sich zum einen durch bauliche Einschränkungen, als auch durch erweiterte Möglichkeiten der elektronischen Vereinzelung bei Sensorschleusen im Vergleich zu rein mechanischen Vereinzelungssystemen. Unter mechanischen Vereinzelungssystemen sind Anlagen wie Drehkreuz und Drehsperren zu verstehen, bei denen rein mechanisch eine Kammer gebildet wird, in denen nur eine Person Platz findet, auch wenn diese Anlagen elektronisch gesteuert werden.

Bauliche Einschränkungen betreffen zum einen die Gehäuselängen. Ist es aus Platzgründen nicht möglich lange Gehäuse einzusetzen, dann müssen ggf. Kompromisse bei der Sicherheit eigegangen werden.



Die Technik der Speedgates beruht neben schnell fahrenden Türen auf einer Sensorik die elektronisch „vereinzelt“, woher auch der ebenfalls geläufige Name Sensorschleuse herrührt

Barrierefreie Eingänge

Größere Durchgangsbreiten werden als barrierefreie Eingänge erforderlich. Diese können Teil einer Reihe von Schleusen sein, bei der mindestens einer der Anlagen einen breiten Durchgang aufweist. Für Rollstuhlfahrer, Rollatoren, Materialtransport oder ähnliches sind die Schleusen anders anzusteuern als für normale Benutzer, da ansonsten Alarme ausgelöst werden. Ein Rollator wird z.B. als unberechtigte Person gewertet.

Auch Brandschutzauflagen können breitere Durchgänge erfordern. Die Breiten und die Anzahl der breiten Durchgänge wird hierbei von dem Brandschutzverantwortlichen festgelegt und richtet sich unter anderem nach Anzahl der Personen und dem Nutzerkreis. Die Aufschaltung einer Brandmeldeanlage stellt eine Möglichkeit dar, die Türen zu öffnen. Befindet sich die Schleuse in einem Hauptfluchtweg, dann ist die Aufschaltung einer Brandmeldeanlage in der Regel nicht ausreichend, sondern es wird eine Fluchtweglösung gem. EltVtr oder DIN EN 13637 benötigt. Diese erfordern zwingend eine Auslösung in der Nähe der Tür und eine Entriegelung der Türen zum manuellen Öffnen.

Waren früher bei mechanischen Vereinzelungsanlagen Nebentüren für Materialtransporte und Fluchtwege erforderlich, so können diese in Speedgates integriert werden.

Die Anforderungen an eine Personenvereinzelung gelten aber auch bei Speedgates weiterhin. Es mag architektonisch verlockend und nutzerfreundlich erscheinen, möglichst breite Durchgänge mit möglichst kurzen Gehäusen einzusetzen, die nur langsam schließen. Dies muss aber immer gegenüber den Sicherheitsinteressen abgewogen werden. GIT

Je schneller die Tür, je länger das Gehäuse und die Detektionslänge und je schmaler der Durchgang, desto höher die Sicherheit gegen unberechtigte Zutritte

Assa Abloy Entrance Systems
www.assaabloyentrance.de

LARGE LANGUAGE MODELS (LLMS)

Ein Jahr der KI

Sprachmodelle in Security Operations Center

Das Cybersicherheitsunternehmen Advens sieht in der Nutzung von Large Language Models (LLMs) einen der wichtigsten Trends im Bereich Security Operations Center (SOC) im Jahr 2025. LLMs sind eine Art der künstlichen Intelligenz (KI), die durch Machine Learning in der Lage sind, Textinhalte zu verstehen und zu generieren. In Form von ChatGPT und ähnlichen Plattformen sind LLMs der breiten Öffentlichkeit vor allem in den vergangenen zwei Jahren bekannt geworden. Im modernen SOC kommt KI jedoch schon lange zum Einsatz, insbesondere wenn es um das Identifizieren von potenziellen Bedrohungen geht.

Die Aufgabe eines Security Operations Center (SOC) besteht darin, sicherheitsrelevante Vorfälle in einem Netzwerk oder System in Echtzeit zu identifizieren, zu analysieren und zu beheben. Für diesen Prozess muss eine gewisse Flexibilität gegeben sein – die Experten im SOC müssen sich dynamisch an verschiedene Fälle und Situationen anpassen. Gleichzeitig beginnt ein Wettlauf gegen die Zeit, wenn ein sicherheitsrelevanter Vorfall identifiziert wird. Es muss eine große Menge an Informationen verarbeitet und analysiert werden, um festzustellen, ob es sich um eine tatsächliche Bedrohung handelt oder nicht.

„LLMs sind die Scouts im SOC. Bei einem potenziellen Vorfall dienen sie dazu, alle möglichen Eventualitäten abzubilden und die ersten Schritte hin zu verschiedenen Erklärungsansätzen zu erarbeiten. Im nächsten Schritt entscheiden dann die menschlichen Experten, welcher dieser Ansätze verfolgt werden soll“, sagt Arthur Tondereau, Data Scientist bei Advens.

Die Vorteile von LLMs

Das Besondere an LLMs ist, dass sie natürliche Sprache verstehen und in Maschinensprache übersetzen können. Beispielsweise können die Experten im SOC die simple Frage „Was geschah eine Stunde vor dem Vorfall X?“ stellen, worauf ein LLM über Schnittstellen zu anderen SOC-Tools die gewünschten Informationen einholt und verständlich zusammenfasst. Die Reaktionszeit auf Vorfälle verkürzt sich auf diese Weise signifikant.

Dieser Effizienzgewinn fällt noch einmal größer aus, wenn die LLMs zu KI-agentenähnlichen Lösungen weiterentwickelt werden. Dabei handelt es sich um LLMs, die darauf trainiert werden, entsprechend den individuellen Anforderungen der Experten eine bestimmte Aufgabe zu erfüllen, zum Beispiel über eine Schnittstelle mit dem Log-Analyse-Tool oder der Wissensdatenbank des SOC. Das LLM bzw. der KI-Agent wird damit zu einem wichtigen Teil des SOC-Werkzeugkastens zum Identifizieren, Analysieren und Beheben von potenziellen Bedrohungen.

Halluzinationen vorbeugen

Gleichzeitig sind LLMs jedoch nach wie vor ein Werkzeug, das die menschliche Expertise nicht ersetzen sollte und nicht ersetzen kann, so das Unternehmen. Standardmäßig seien LLMs nämlich darauf ausgelegt, eine Antwort geben zu müssen, koste es, was es wolle. Deshalb werden sie im Zweifelsfall eine entsprechende Information erfinden – das „Halluzinieren“, das auch beispielsweise bei ChatGPT bekannt ist.

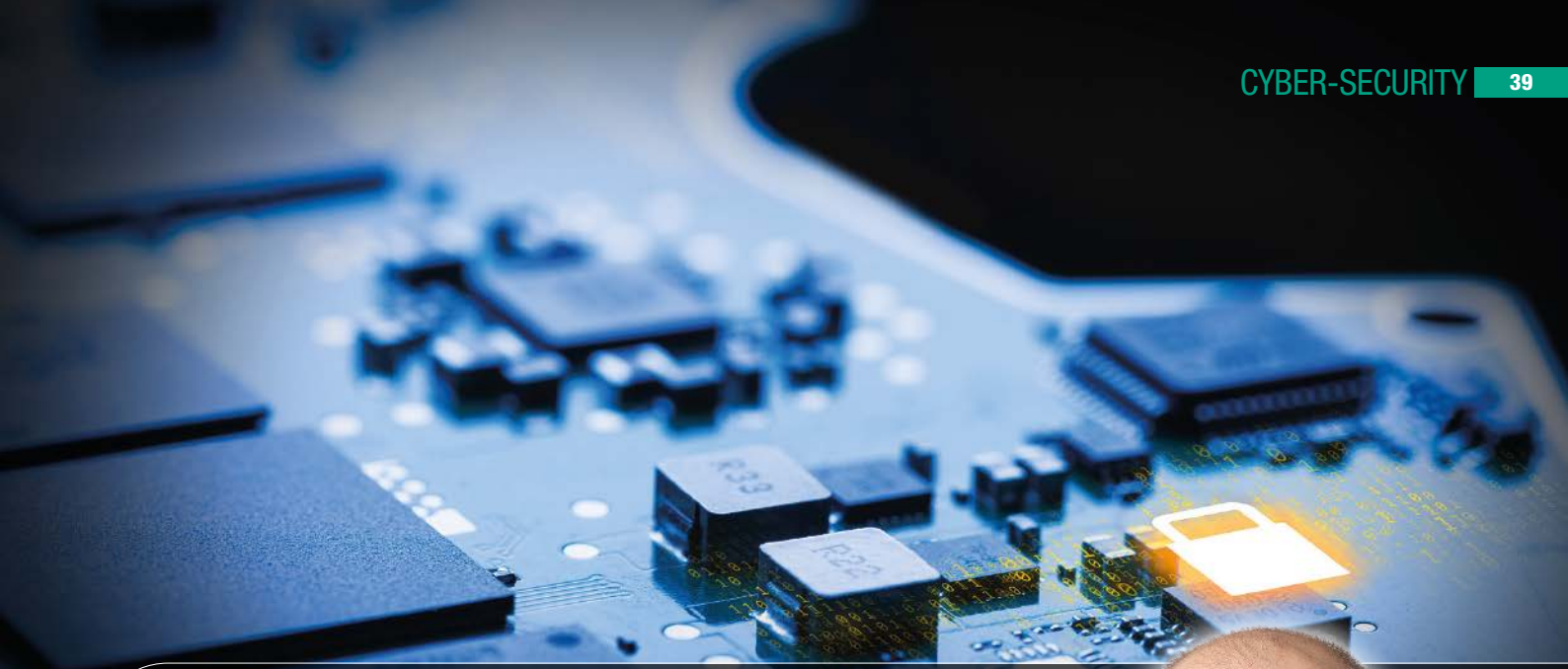
Um dies zu verhindern, brauche es einerseits Leitplanken: SOC-Teams können Sicherheitsschleifen in den Prozess integrieren, die sicherstellen, dass Informationen und Quellenangaben systematisch auf inhaltliche Korrektheit überprüft werden. Dafür müsse in jeder Phase des Prozesses Transparenz gewährleistet werden. Jede Anfrage müsse für die Experten einsehbar sein, genau wie die Argumentation und Herleitungen der LLMs. Und nicht zuletzt brauche es deshalb weiterhin menschliche SOC-Mitarbeiter, denn nur Teams mit der notwendigen Expertise können überprüfen, ob die vom LLM gelieferten Informationen korrekt sind.

Regulatorische und Sicherheitsaspekte mitdenken

Mit der zunehmenden Integration von LLMs in SOCs sind auch regulatorische Aspekte zu berücksichtigen. So werden mit dem AI Act der Europäischen Union in Zukunft SOCs, die kritische Infrastruktur überwachen, auch selbst als kritische Infrastrukturen gelten – und müssen damit entsprechend geschützt werden. Diese Sicherheitsanforderungen gelten dann auch für die im SOC genutzten LLMs, gerade auch weil LLMs wie jedes andere System Schwachstellen haben, die von Angreifern gezielt ins Visier genommen werden können. Ein Beispiel dafür wäre eine Prompt Injection, die das LLM dazu zwingt, verdächtige Aktivitäten zu ignorieren.

Auf lange Sicht wird die Nutzung von LLMs für SOC-Anbieter unabdinglich werden, um den Anforderungen ihrer Kunden zu entsprechen. Damit liegt es jedoch auch in der Verantwortung jedes einzelnen Anbieters, in ihren SOCs die notwendigen Rahmenbedingungen zu schaffen, um LLMs produktivitätssteigernd, sicher und allen relevanten Vorschriften entsprechend zu integrieren, sodass sie ihre Experten-Teams bestmöglich unterstützen können. GIT

aDvens
www.advens.com



CYBERSICHERHEIT

Angriffsfläche IoT

Cybersicherheit in der Videosicherheit

Cyberattacken öffnen den Weg zur Kontrolle über die Geräte, zu DDoS-Angriffen, Attacken gegen Behörden, Krankenhäuser und Schulen – und auch im Krieg gegen die Ukraine beobachten Russen Luftabwehrsysteme zur Planung ihrer Angriffe. Die Zahl der Angriffe nimmt nach Erhebungen jedes Jahr auf krasse Weise zu. GIT SICHERHEIT sprach mit Andre Bastert, Global Product Manager AXIS OS bei Axis Communications, über die Cybersicherheitsstrategie seines Unternehmens.

Andre Bastert, Global Product Manager Axis OS

Herr Bastert, Kameras sollten nach Möglichkeit cybersicherheitsmäßig keine Schwäche zeigen. Und doch werden IP-Kameras von allen Geräten wohl am häufigsten angegriffen. Wie ist die Lage aus Ihrer Sicht?

Andre Bastert: Die Lage ist tatsächlich besorgniserregend. Internationale Berichte zur Verwundbarkeit von IoT-Geräten zeigen dies deutlich. Die schiere Anzahl – wir sprechen von Billionen von vernetzten IoT-Geräten – und deren oft unzureichende Absicherung stellen alle am Geschehen Involvierten, darunter Hersteller, Betreiber oder Regulierungsbehörden, vor enorme Herausforderungen. Es überrascht daher nicht, dass der IoT-Markt zunehmend mit einer Flut von Gesetzesnovellen, Regularien und neuen Standards konfrontiert wird. Leider gelingt es vielen Herstellern bislang nicht, Cybersicherheit konsequent in ihre Produkte zu integrieren. Die daraus resultierende „Angriffsfläche IoT" ist ein wachsendes Risiko, dem wir dringend begegnen müssen.

Eine Cybersicherheitsstrategie ist für einen Hersteller wie Axis also unabdingbar, kann aber ohne den Anwender alleine nichts ausrichten. Könnten Sie einmal die Entwicklung Ihrer Strategie erläutern, seitdem Axis 2016 erstmals einen Schwachstellenreport veröffentlicht hat?

Andre Bastert: Seit 2016 haben wir einen langen Weg zurückgelegt und sind stolz auf die Fortschritte, die wir beim Schwachstellenmanagement erzielt haben. Damals haben wir uns intensiv mit Best Practices aus der IT-Branche beschäftigt und von führenden Unternehmen gelernt. Auf dieser Grundlage haben wir unsere eigene „Axis Vulnerability Management Policy" entwickelt. Sie legt transparent dar, wie wir mit Schwachstellen umgehen – von der Identifikation über das Patchen bis hin zu den Abläufen und der Kommunikation mit unseren Partnern und Kunden, sobald eine Schwachstelle identifiziert wurde.

Könnten Sie etwas näher auf die Zusammenarbeit mit externen Forschern eingehen – Stichwort Penetrationstests – und auf den Beitritt zum Common Vulnerabilities and Exposures (CVE)-Programm 2021?

Andre Bastert: Im Jahr 2021 sind wir dem MITRE CVE Program als CVE Numbering Authority (CNA) beigetreten. Jede identifizierte Schwachstelle erhält eine CVE-ID, also eine eindeutige Identifikationsnummer, zusammen mit einem ausführlichen Security Advisory mit weitergehenden Informationen. Durch die Einbindung ins CVE-Programm werden diese Informationen direkt extern verbreitet, sodass auch

Bitte umblättern ▶

unsere Kunden informiert werden, zeitnah reagieren und Patches installieren können. Die Informationsverbreitung und die damit verbundene Transparenz und Reichweite dieses Prozesses sind große Vorteile dieses Programms und ein echter Gewinn für uns und unsere Kunden, denn durch den dort stattfindenden „Knowledge Transfer" war es uns möglich, unser Schwachstellenmanagement weiterzuentwickeln und zu professionalisieren, indem wir unsere Prozesse und Abläufe nach dem Vorbild von IT-Größen wie Google, Microsoft oder Cisco angepasst haben.

Ein weiterer Schritt nach vorne war der Start unseres ersten Bug-Bounty-Programms in Zusammenarbeit mit Bugcrowd. Hier belohnen wir ethische Hacker finanziell für das verantwortungsvolle Melden von Schwachstellen. Allein auf diese Weise haben wir mittlerweile mehr als 30 Schwachstellen behoben. Hinzu kommen unzählige Penetrationstests, die Axis entweder jährlich in Auftrag gibt oder von unseren Kunden initiiert werden. Durch diese haben wir inzwischen mehr als 50 Schwachstellen identifiziert und gepatcht.

Einen weiteren Meilenstein beim Thema Schwachstellenmanagement stellt für uns die Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) dar. Inzwischen tragen mehr als 220 Netzwerkprodukte von Axis das IT-Sicherheitskennzeichen vom BSI. Eine zentrale Verpflichtung dabei ist, die BSI-Marktaufsicht proaktiv über entdeckte Schwachstellen zu informieren. So werden sicherheitsrelevante Informationen schnell verbreitet – ein wichtiger Schritt in Richtung des in Deutschland noch gesetzlich umzusetzenden Cybersecurity Resilience Acts (CRA) der Europäischen Union.

Bei unserer Strategie setzen wir also auf internationale Kooperation und ein mehrschichtiges Sicherheitskonzept mit einer Reihe von Maßnahmen, mit denen wir unsere Produkte schrittweise robuster machen – durch Penetrationstests, Bug-Bounty-Programme, transparente Kommunikation und regulatorische Zusammenarbeit. Cybersicherheit ist allerdings kein Einmalprojekt, sondern ein kontinuierlicher Prozess, der Engagement auf allen Ebenen erfordert. Erst eine Strategie, die auf gegenseitigem Austausch und professioneller Zusammenarbeit beruht, stärkt die Produktsicherheit.

Lassen Sie uns einen näheren Blick auf Ihre Sicherheitsplattform „Axis Edge Vault" werfen...

Andre Bastert: Das, was wir als „Axis Edge Vault" bezeichnen, umfasst im Grunde die Gesamtheit aller hardwarebasierten, fortschrittlichen Sicherheitstechnologien bei Axis – und bildet somit das Fundament der Cybersicherheit in unseren Netzwerkprodukten. Zum Beispiel erwarten unsere Kunden, dass ihr Axis-Produkt ausschließlich mit Axis-autorisierter Software startet – und nicht mit beliebigem Code. Ebenso erwarten sie, dass das Produkt auf dem Weg zu ihnen nicht manipuliert wurde und dass es sich zweifelsfrei als echtes Axis-Gerät ausweisen kann. Dafür sorgen Funktionen wie Secure Boot, Signed OS und die Axis Device ID.

Darüber hinaus müssen hochsensible Daten, beispielsweise Zertifikate, private Schlüssel für die Netzwerkkommunikation oder Zugangsinformationen für Türsteuerungen, sicher gespeichert werden, ohne dass sie extrahierbar sind. Daher verwenden wir in unseren Produkten ausschließlich TPM-Module und Secure Elements, die nach Common Criteria und FIPS 140 zertifiziert sind. Die international geprüften TPM-Module und Secure Elements, die wir in unseren Produkten verwenden, kommen unter anderem auch in Smartphones oder für die Erstellung von Reisepässen zum Einsatz – und bieten deshalb einen vergleichbaren Standard an Sicherheit.

Angesichts der zunehmenden Bedrohung durch Deepfakes und manipulierte Videodaten bieten unsere Kameras zudem die Möglichkeit, Videostreams kryptografisch zu signieren. So können Sie als Kunde verifizieren, dass der Videostream echt ist. Seit 2020/2021 haben wir uns verpflichtet, keine Axis-IoT-Geräte mehr ohne diese Sicherheitsfunktionen auszuliefern.

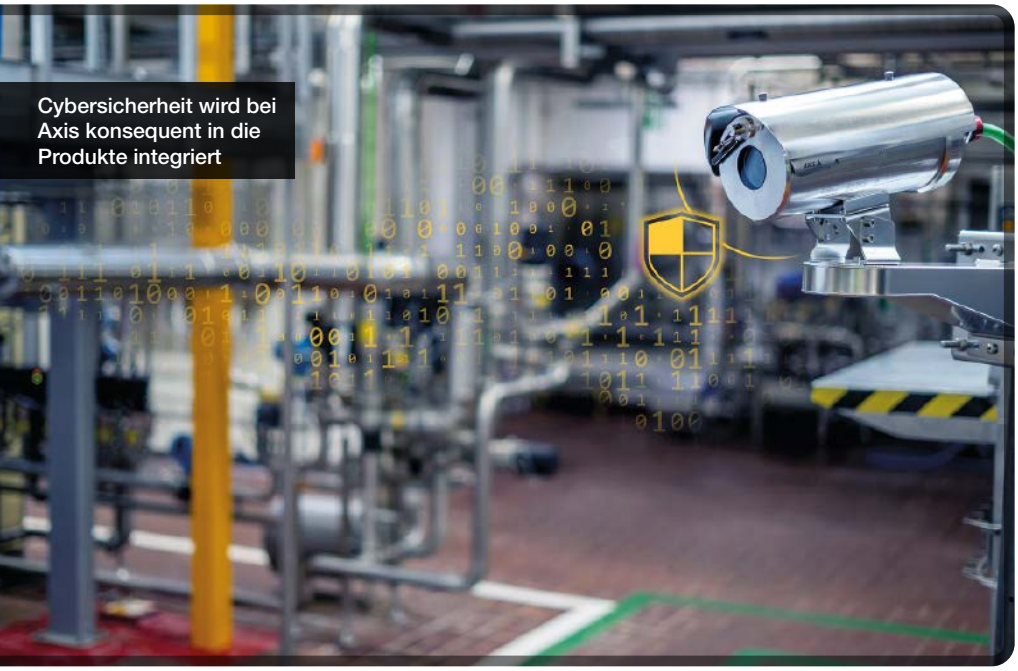
Wenn Sie kritische Software-Schwachstellen in Axis-Anwendungen entdecken, veröffentlichen Sie danach entsprechende Updates. Wie kommt es zur Aufdeckung der Schwachstellen?

Andre Bastert: Wir fördern aktiv die Zusammenarbeit mit unabhängigen Sicherheitsforschern, ethischen Hackern sowie professionellen Security-Unternehmen, zu denen auch viele unserer Kunden zählen. Vertrauen basiert bei uns auf Gegenseitigkeit und Transparenz und Offenheit sind der Schlüssel für erfolgreichen Schutz. Wir begrüßen es daher ausdrücklich, dass viele unserer Kunden von sich aus professionelle Security-Unternehmen damit beauftragen, regelmäßig Penetrationstests durchzuführen, um den Sicherheitsstandard von Axis-Produkten zu überprüfen.

Schwachstellenmeldungen erreichen uns über verschiedene Kanäle: Entweder direkt über ein Online-Formular im Rahmen von Penetrationstests oder über unser Bug-Bounty-Programm in Zusammenarbeit mit dem Team von Bugcrowd. Für die Meldung einer kritischen Sicherheitslücke zahlen wir derzeit bis zu 50.000 US-Dollar – ein klares Zeichen für unser Engagement und unsere Wertschätzung gegenüber der Community.

Wie lange dauert es durchschnittlich vom ersten Report bis zum Patch Day?

Andre Bastert: Generell sind wir je nach Komplexität der Schwachstelle und der Anzahl der betroffenen Produkte in der Lage, innerhalb von sechs bis zwölf Wochen entsprechende Patches bereitzustellen – immer vorausgesetzt, dass wir die Schwachstellenveröffentlichung in enger Abstimmung mit dem Meldenden koordinieren können, sodass unsere Kunden genügend Zeit haben zu patchen. Bei sogenannten „Zero-Day-Schwachstellen", von denen wir glücklicherweise noch keine hat-



Cybersicherheit wird bei Axis konsequent in die Produkte integriert

ten, müssten wir aber selbstverständlich deutlich schneller agieren, da wir es in diesen Fällen mit Schwachstellen zu tun hätten, die schon aktiv ausgenutzt werden könnten.

Bei Axis ist es üblich, dass ein einzelner Patch in der Regel auf bis zu 200 bis 300 Netzwerkprodukte und mehrere Software-Tracks ausgerollt werden muss. Damit dies zeitlich machbar ist, braucht es eine präzise Koordination.

Wie läuft die Kommunikation mit den Kunden ab?

Andre Bastert: Wir empfehlen unseren Kunden, ihre Axis-Netzwerkprodukte regelmäßig und proaktiv auf dem aktuellen Stand zu halten. Das ist der effektivste Schutz vor Sicherheitslücken. Über unseren Release Schedule informieren wir rechtzeitig darüber, in welcher Version eine Schwachstelle behoben wird. Dabei veröffentlichen wir jedoch niemals Details, die den „Responsible Disclosure"-Prozess gefährden könnten. Zudem bieten wir einen Security Notification Service an. Nach der Registrierung erhalten Kunden automatisch eine E-Mail, sobald neue Schwachstellen-Patches verfügbar sind. So bleibt genügend Zeit, um Updates einzuplanen und Risiken zu minimieren. Für weiterführende Fragen stehen unseren Kunden und Partnern selbstverständlich auch unser Vertrieb und technischer Support rund um die Uhr und kostenfrei zur Verfügung.

Wie beraten und unterstützen Sie generell die Endanwender? Sie stellen ja ein umfassendes Paket von Ressourcen zur Verfügung?

Kameras stehen im Fokus von Cyberattacken und müssen daher besonders geschützt werden

Andre Bastert: Unsere Kunden können sich bereits vor dem Kauf transparent und umfassend über die Cybersicherheit der Axis-Produkte informieren, sei es über die Axis-Website, über unsere Partner oder im direkten Dialog per E-Mail oder Telefon mit unserem Vertrieb. Im Axis Trust Center stellen wir laufend Informationen zu internationalen Standards, Zertifizierungen und Penetrationstests bereit.

Für die sichere Konfiguration und den Betrieb unserer Produkte bieten wir einen Hardening Guide mit konkreten Empfehlungen an. Sollte ein Gerät forensisch untersucht werden müssen, etwa nach einem Cyberangriff, hilft der Forensic Guide weiter. Darüber hinaus stellen wir Integrationsanleitungen bereit, etwa für die Zusammenarbeit mit bekannten Netzwerkherstellern wie HPE Aruba Networking. Unser Ziel ist es stets, Kunden proaktiv zu unterstützen, um Axis-Produkte sicher und reibungslos in bestehende IT-Infrastrukturen einzubinden. GIT

Dieses Video zeigt, wie Axis sein Schwachstellenmanagement zum Schutz seiner Firmware Axis OS betreibt:

Axis Communications
www.axis.com

IT-SECURITY

In Zeiten des Systemkonflikts

Cybersicherheit: Warum IT-Entscheidungen heute geopolitisch sind

Technologie galt lange als Brücke zwischen Nationen. Heute wird sie zur Grenze. Die Digitalisierung, die einst als Motor globaler Vernetzung gefeiert wurde, ist inmitten eines geopolitischen Spannungsfeldes angekommen. Halbleiter, Cloud-Infrastrukturen, Netzwerktechnik – was früher als technologische Frage galt, ist heute ein Symbol nationaler Interessen, wirtschaftlicher Autonomie und strategischer Macht. Wer Cybersicherheit heute ausschließlich technisch denkt, ignoriert eine gefährliche Realität, sagt IT-Sicherheitsexperte Thomas Kress, Geschäftsführer der Firma Deutsche Cyberkom, in seinem Beitrag für GIT SICHERHEIT.

IT-Entscheidungen sind keine rein operativen Fragen mehr. Sie sind politische Statements. Und sie erfordern Haltung. Spätestens seit den Eskalationen zwischen den USA und China, den Exportverboten für Hochtechnologie, den Überwachungsenthüllungen aus Russland, Iran oder Nordkorea ist klar: Es geht nicht mehr nur um Schutz vor Cyberkriminellen. Es geht um wirtschaftliche Souveränität und strategische Handlungsfreiheit. Unternehmen geraten unverschuldet in ein Spannungsfeld zwischen staatlich geförderter Spionage, Wirtschaftskrieg und digitaler Einflussnahme.

Zudem nehmen hybride Bedrohungen zu: Infrastrukturen werden nicht mehr nur physisch, sondern auch digital sabotiert. Systeme werden destabilisiert, Wahlen beeinflusst, Wirtschaftsprozesse gestört. Die gezielte Destabilisierung ganzer Branchen durch Desinformation, Datenleaks oder gezielte Angriffe auf Lieferketten ist kein Ausnahmefall mehr, sondern Teil einer neuen Normalität.

Die Realität ist: Europäische Mittelständler und Konzerne müssen sich heute entscheiden, mit welchen Partnern, Plattformen und Infrastrukturen sie arbeiten. Jede Wahl kann Konsequenzen haben. Wer auf eine amerikanische Cloud setzt, öffnet sich US-Behörden. Wer chinesische Technologie integriert, riskiert Lieferstopps oder politischen Druck. Wer auf europäische Lösungen setzt, muss mit Verzögerung und Kostennachteilen leben. Es gibt keine neutrale Lösung mehr. Aber es gibt verantwortbare Entscheidungen.

IT-Strategie braucht geopolitische Intelligenz

Ich halte es für fahrlässig, wenn Unternehmen ihre IT-Architektur allein nach Preis, Performance oder Verfügbarkeit planen. Wir brauchen eine neue Form der strategischen Weitsicht: geopolitische Intelligenz. Das bedeutet, bei jeder Entscheidung auch die Herkunft der Technologie, die Regulierungen des Ursprungslandes und die mögliche politische Einflussnahme zu bedenken.

Geopolitische Intelligenz bedeutet auch, sich nicht nur auf Lieferantenverträge oder Zertifizierungen zu verlassen, sondern auch Worst-Case-Szenarien durchzuspielen. Was passiert, wenn eine kritische Plattform über Nacht aus geopolitischen Gründen gesperrt wird? Was, wenn Supportverträge plötzlich aufgrund von Sanktionen gekündigt werden? Was, wenn Software-Updates zur Sicherheitslücke werden, weil sie aus unsicheren Herkunftsländern stammen?

Die geopolitische Bewertung von IT-Infrastruktur muss daher integraler Bestandteil jeder Business-Impact-Analyse werden. Es reicht nicht, zu wissen, ob ein System ausfällt. Man muss wissen, warum, woher und was es im Kontext globaler Entwicklungen bedeutet.

Zwischen Resilienz und Realismus

Natürlich bedeutet geopolitische Resilienz nicht Autarkie. Niemand kann sich vollständig von globalen Technologien entkoppeln. Aber wir können Abhängigkeiten bewusst steuern. Wir können technologische Diversität schaffen. Wir können sensible Geschäftsbereiche entflechten und Infrastrukturen absichern. Wir können Cloudstrategien mit Exit-Szenarien entwickeln und Plattformabhängigkeiten reduzieren.

Resilienz bedeutet in diesem Zusammenhang nicht Rückzug, sondern Gestaltungsspielraum. Unternehmen, die sich heute breit aufstellen, können in Krisen flexibler reagieren. Dazu gehören nicht nur technische Redundanzen, sondern auch rechtliche und politische Szenarien. Wer etwa ausschließlich auf US-amerikanische oder chinesische Softwarelösungen setzt, ohne Alternativen vorzuhalten, macht sich erpressbar – direkt oder indirekt.

Auch das Thema Datenlokalisierung wird im Zuge geopolitischer Verwerfungen wieder wichtiger. Welche sensiblen Daten dürfen wo gespeichert werden? Welche Gesetze gelten für sie? Und wie schnell lassen sich Systeme migrieren, wenn es erforderlich ist? Wer hier keine Antwort hat, verliert im Ernstfall wertvolle Zeit und Kontrolle.

Cybersicherheit ist auch Standortstrategie

IT-Entscheidungen betreffen längst nicht mehr nur die IT-Abteilung. Sie gehören auf die Ebene der Unternehmensstrategie. Denn mit der Wahl der Infrastruktur, der Anbieter und der Speicherorte treffen Unternehmen auch eine Entscheidung über ihre Zukunftsfähigkeit.

Ein Beispiel: Wer Rechenzentren nur im Ausland betreibt, riskiert Zugriffsrisiken, sei es durch Sanktionen, staatlichen Zugriff oder Netzblockaden. Wer kein Konzept für digitale Souveränität hat, verliert im Krisenfall Kontrolle über seine Daten und Prozesse. Und wer keine Sicherheitsarchitektur für KI-Systeme, hybride Angriffe oder Data Poisoning implementiert, wird langfristig angreifbar bleiben.

Das bedeutet auch: IT-Sicherheit muss gemeinsam mit der Geschäftsführung, mit Einkauf, Recht, Kommunikation und Politikberatung gedacht werden. In einer Welt, in der selbst der Speicherort eines Datenpakets politische Konsequenzen haben kann, darf Cybersicherheit nicht länger eine rein technische Disziplin sein.

Was jetzt zu tun ist

Ich bin der festen Überzeugung, dass Unternehmen drei Dinge dringend brauchen: Erstens ein realistisches Bedrohungsbild, das geopolitische Risiken einschließt. Zweitens eine Sicherheitsstrategie, die auch systemische Risiken adressiert, also nicht nur Hackerangriffe, sondern auch technologische Abhängigkeiten und politische Schocks. Und drittens ein neues Rollenverständnis ihrer IT-Verantwortlichen. Wer heute IT entscheidet, trifft sicherheitspolitische Entscheidungen. Wer Sicherheit plant, plant unternehmerische Resilienz.

Dazu gehört auch der Mut zur Lücke. Kein System kann hundertprozentige Sicherheit garantieren, aber es kann vorbereitet sein. Wer seine Angriffsfläche kennt, sie bewusst managt und im Fall der Fälle schnell reagieren kann, hat einen echten strategischen Vorteil.

Für mich ist klar: Wir brauchen keine Digitalstrategie auf dem Reißbrett, sondern eine Sicherheitsstrategie in der Realität. Eine, die Unsicherheit einkalkuliert, Resilienz aufbaut und gleichzeitig Raum für Innovation lässt. Technologie wird sich weiterhin verändern. Aber wir können entscheiden, wie bewusst wir mit ihr umgehen. GIT

Deutsche Cyberkom GmbH
Cyberkom.ai

Komplettlösung für Zugangskontrolle

Die Mobotix S74 in Kombination mit der kameraintegrierten Vaxtor LPR Multi Lens App und der Mobotix Sync Zusatzsoftware ist eine leistungsstarke Komplettlösung für Zugangskontrollen, Verkehrsmanagement und automatisierte Prozesse. Mit nur einer Kamera, einer App-Lizenz und zwei Sensoren können parallel mehrere Fahrtrichtungen oder Spuren erfasst werden – intelligent, präzise und kostengünstig. Die Ein- und Ausfahrtkontrolle wird mit nur einer Kamera realisiert. Mehrere Spuren oder Fahrtrichtungen können mit einer einzigen S74-Kamera überwacht werden – ideal für Ein- und Ausfahrten in Parkhäusern, Tankstellen oder auf Betriebsgeländen. Die intelligente Kennzeichenerkennung ist weltweit einsetzbar. Die Vaxtor LPR Multi Lens App unterstützt lateinische, hebräische, arabische und thailändische Zeichen – und ist damit bereit für den globalen Einsatz. **www.mobotix.com**

Diesen Monat auf GIT-SICHERHEIT.de

IMPRESSUM

Herausgeber
Wiley-VCH GmbH

Geschäftsführer
Dr. Guido F. Herrmann

Senior Director, Publishing and Content Services
Dr. Katja Habermüller

Publishing Director
Dipl.-Betriebswirt Steffen Ebert

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

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

Anzeigenleitung
Miryam Reubold
+49 6201 606 127

Sales Director
Jörg Wüllner
+49 6201 606 748

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

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

Cinzia Adorno
+49 6201 606 114

Tina Renner
+49 6201 606 021

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

Herstellung
Jörg Stenger
+49 6201 606 742

Claudia Vogel (Anzeigen)
+49 6201 606 758

Satz + Layout
Andreas Kettenbach

Lithografie
Elke Palzer

Sonderdrucke
Miryam Reubold
+49 6201 606 172

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

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

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

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

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

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

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

Originalarbeiten
Die namentlich gekennzeichneten Beiträge stehen in der Verantwortung des Autors. Nachdruck, auch auszugsweise, nur mit Genehmigung der Redaktion und mit Quellenangabe gestattet. Für unaufgefordert eingesandte Manuskripte und Abbildungen übernimmt der Verlag keine Haftung.
Dem Verlag ist das ausschließliche, räumlich, zeitlich und inhaltlich eingeschränkte Recht eingeräumt, das Werk/den redaktionellen Beitrag in unveränderter oder bearbeiteter Form für alle Zwecke beliebig oft selbst zu nutzen oder Unternehmen, zu denen gesellschaftsrechtliche Beteiligungen bestehen, sowie Dritten zur Nutzung zu übertragen. Dieses Nutzungsrecht bezieht sich sowohl auf Print- wie elektronische Medien unter Einschluss des Internet wie auch auf Datenbanken/Datenträger aller Art.
Alle etwaig in dieser Ausgabe genannten und/oder gezeigten Namen, Bezeichnungen oder Zeichen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

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

Druck
westermann DRUCK | pva

Printed in Germany, ISSN 2751-4536

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

WILEY

GIT SICHERHEIT

INNENTITEL – BRANDSCHUTZ

Mehr Informationen auf
www.wagnergroup.com

WAGNER®
DIE BESSERE LÖSUNG IM BRANDSCHUTZ

Das Sauerstoffreduzierungssystem zur aktiven Brandvermeidung Oxyreduct F-Line vereint eine CO_2-neutrale Brandvermeidung, Kosteneffizienz und maximale Sicherheit, beispielsweise in einem Hochregal- oder einem Behälterkompaktlager.

INNENTITEL

Resilienz durch präventiven Brandschutz

Sauerstoffreduzierung als Schlüsseltechnologie

In sicherheitskritischen Infrastrukturen wie Rechenzentren, Archiven oder automatisierten Lagernimmobilien hat die Sicherstellung der Betriebsfähigkeit höchste Priorität. Ein Brand gefährdet nicht nur Sachwerte, sondern auch die Kontinuität von Geschäftsprozessen. Klassische Brandschutzsysteme wie Sprinkler- oder Gaslöschanlagen greifen erst im Ereignisfall – oft mit beträchtlichen Folgeschäden durch Feuer, Rauch oder Löschmittelrückstände. Im Gegensatz zu reaktiven Löschsystemen verhindert die aktive Brandvermeidung durch Sauerstoffreduzierung unter definierten Bedingungen die Brandentstehung und trägt damit wesentlich zur Erhöhung der Resilienz bei. Als integraler Bestandteil einer umfassenden Risikostrategie gewinnt diese Technologie daher auch für Versicherer zunehmend an Bedeutung.

Ob bei Neubauten, Umbauten oder Nutzungsänderungen: eine frühzeitige Analyse der Brandrisiken ermöglicht die Entwicklung maßgeschneiderter Schutzkonzepte, die gesetzlichen Anforderungen genügen und wirtschaftliche Schäden – etwa durch Betriebsunterbrechungen – minimieren. Denn statistisch gesehen entstehen in Deutschland alle zwei Minuten Brände – häufig mit gravierenden Folgen. Besonders gefährdet sind Bereiche mit hoher Packungsdichte, umfangreicher Elektrik und leicht entzündlichen Materialien. Die Folgekosten durch Rauch, Löschmittel und Ausfallzeiten übersteigen den eigentlichen Brandschaden oft um ein Vielfaches.

Prävention statt Reaktion

Die aktive Brandvermeidung beruht auf einem physikalischen Grundprinzip: Kein Feuer ohne ausreichenden Sauerstoff. Eine sauerstoffreduzierte Schutzatmosphäre ist daher unter definierten Bedingungen ein wirksames Mittel gegen Brandentstehung und -ausbreitung. Durch das kontrollierte Einleiten von Stickstoff in einen Schutzbereich wird die Sauerstoffkonzentration dort gezielt unter die materialspezifische Entzündungsgrenze abgesenkt.

Das Brandvermeidungssystem OxyReduct generiert den Stickstoff dafür direkt aus der Umgebungsluft und ist zertifiziert (z. B. VdS, FM Approvals) und eignen sich besonders für automatisierte Lager, Tiefkühllager, IT-Räume und Archive – überall dort, wo hohe Brandlasten bestehen und sich Menschen nur temporär aufhalten. Trotz reduziertem Sauerstoffniveau bleibt der Bereich für gelegentliche Aufenthalte begehbar.

Wasserstoffbasierte Stickstofferzeugung

Über die reine Brandvermeidung hinaus leistet das Wagner-System Oxyreduct F-Line zusätzlich einen besonderen Beitrag zur Resilienz. Diese Variante nutzt eine wasserstoffbasierte Brennstoffzelle zur CO_2-neutralen Stickstofferzeugung. Im Betrieb der Zelle entstehen neben der stickstoffreichen Abluft für die Sauerstoffreduzierung auch gleichzeitig Strom und Wärme. Diese können für andere Verwendungen nutzbar gemacht werden, beispielsweise für den Betrieb weiterer Anlagen. Das erhöht die Unabhängigkeit von externer Energieversorgung und schützt auch kritische Infrastrukturen zusätzlich vor Stromausfällen – ein Aspekt von besonderer Relevanz für Rechenzentren und automatisierte Lager.

Eine Oxyreduct-Sauerstoffreduzierungsanlage trägt dazu bei, Brände präventiv zu vermeiden – wie hier in einem Hochregallager

Die F-Line ist damit ein hybrides Brandschutzsystem, das sowohl präventiv wirkt als auch energetisch nachhaltig ist. In Kombination mit konventionellen Stickstofferzeugern lassen sich auch sehr große Schutzbereiche absichern.

Für Betreiber und Versicherer bietet das System zahlreiche Vorteile:

- Präventiver Schutz: Schutz vor Brand-, Rauch- oder Löschmittelschäden, keine Betriebsunterbrechung.
- Wirtschaftlichkeit: Minimierung von Wiederherstellungskosten und Reputationsverlusten.
- Resilienzsteigerung: Schutz kritischer Prozesse und Werte, auch bei Ausfall anderer Systeme.
- Energieautarkie: Mit F-Line auch bei Stromausfall betriebsfähig.

Die Systeme lassen sich flexibel an bauliche oder betriebliche Veränderungen anpassen. Je nach spezifischen Anforderungen kann die Sauerstoffreduktion kontinuierlich und gleichmäßig oder zeitlich gesteuert erfolgen, etwa mit höherem Sauerstoffanteil während der Betriebszeiten und abgesenktem Niveau in unbeaufsichtigten Phasen. Auch eine Kombination mit Stickstoffflutung zur schnellen Brandunterdrückung ist möglich. Dies greift besonders, sobald etwa ein Kabelschwelbrand detektiert wird.

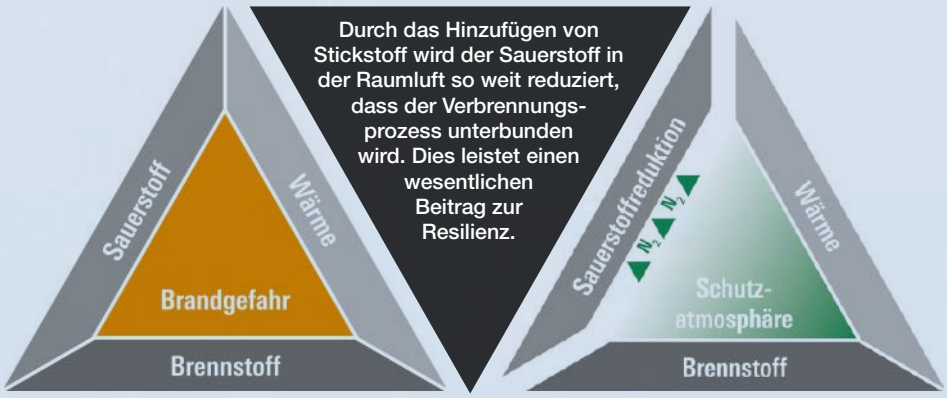
Typische Einsatzbereiche

In verdichteten Lagerstrukturen, IT-Umgebungen oder kompakten Archiven mit sensiblen Beständen ist die Brandbekämpfung oft erschwert. Die Sauerstoffreduktion ist eine wirksame Alternative zu reaktiven Löschsystemen, insbesondere bei hohen Brandrisiken durch dichte Lagerung, elektronische Komponenten und brennbare Materialien. Relevant ist die Technologie beispielsweise in Hochregal- und Kompaktlagern, bei denen enge Lagerverhältnisse und Kunststoffbehälter das Risiko schneller Brandausbreitung erhöhen. In Tiefkühllagern begünstigen trockene Luft und Verpackungsmaterialien die Brandentwicklung, die es zu vermeiden gilt.

Auch das erhöhte Brandrisiko in Rechenzentren, bedingt durch die große Anzahl von Elektronikkomponenten und hohe Wärmeentwicklung, lässt sich mit Oxyreduct wirksam minimieren. In Archiven und Museumsdepots bergen die dort gelagerten Materialien selbst oftmals eine hohe Brandlast. Das Risiko eines unentdeckten Brandes, der sich ungehindert ausbreiten kann, ist zudem durch seltene Begehung erhöht. Hier schützt die Brandvermeidung wertvolle Kulturgüter: kein Brand, keine Folgeschäden durch Rauch oder Löschmittel. Ein Beispiel ist das Newspaper Storage Building der British Library in London, dessen wertvolle Bestände durch eine OxyReduct Sauerstoffreduzierung geschützt sind.

Fazit

Die aktive Brandvermeidung durch Sauerstoffreduzierung ist ein wirksames Mittel zur Sicherung der Betriebsfähigkeit und zur Stärkung der Resilienz. Sie schützt Sachwerte und verhindert Folgeschäden, die lange Ausfallzeiten oder sogar Insolvenzen nach sich ziehen können. Für Betreiber und Versicherer bietet die Technologie eine wirtschaftlich und sicherheitstechnisch überzeugende Lösung – insbesondere in Bereichen mit hohem Risiko und sensibler Infrastruktur. GIT



ADVERTORIAL

Sicherheit benötigt Schutz

Sicherheitstechnische Anlagen wie Brandmelde-, Einbruchmelde-, Videoüberwachungssysteme etc. sind essenziell für den Schutz von Menschen, Sachwerten und kritischen Infrastrukturen. Ihre permanente Verfügbarkeit ist unverzichtbar. Doch gerade diese wichtigen Systeme sind auch anfällig für die Auswirkungen von Blitzströmen und transienten Überspannungen. Schäden können hier schwerwiegende Folgen haben: von Fehlalarmen über Systemausfälle bis hin zur Gefährdung von Menschenleben.

Durch die zunehmende Digitalisierung und Vernetzung von Systemen in Gebäuden steigt die Anzahl empfindlicher elektronischer Komponenten. Die Anforderungen an den Schutz von Gebäuden sowie Anlagen wachsen – ob aus einem gesetzlichen, technischen oder wirtschaftlichen Betrachtungswinkel.

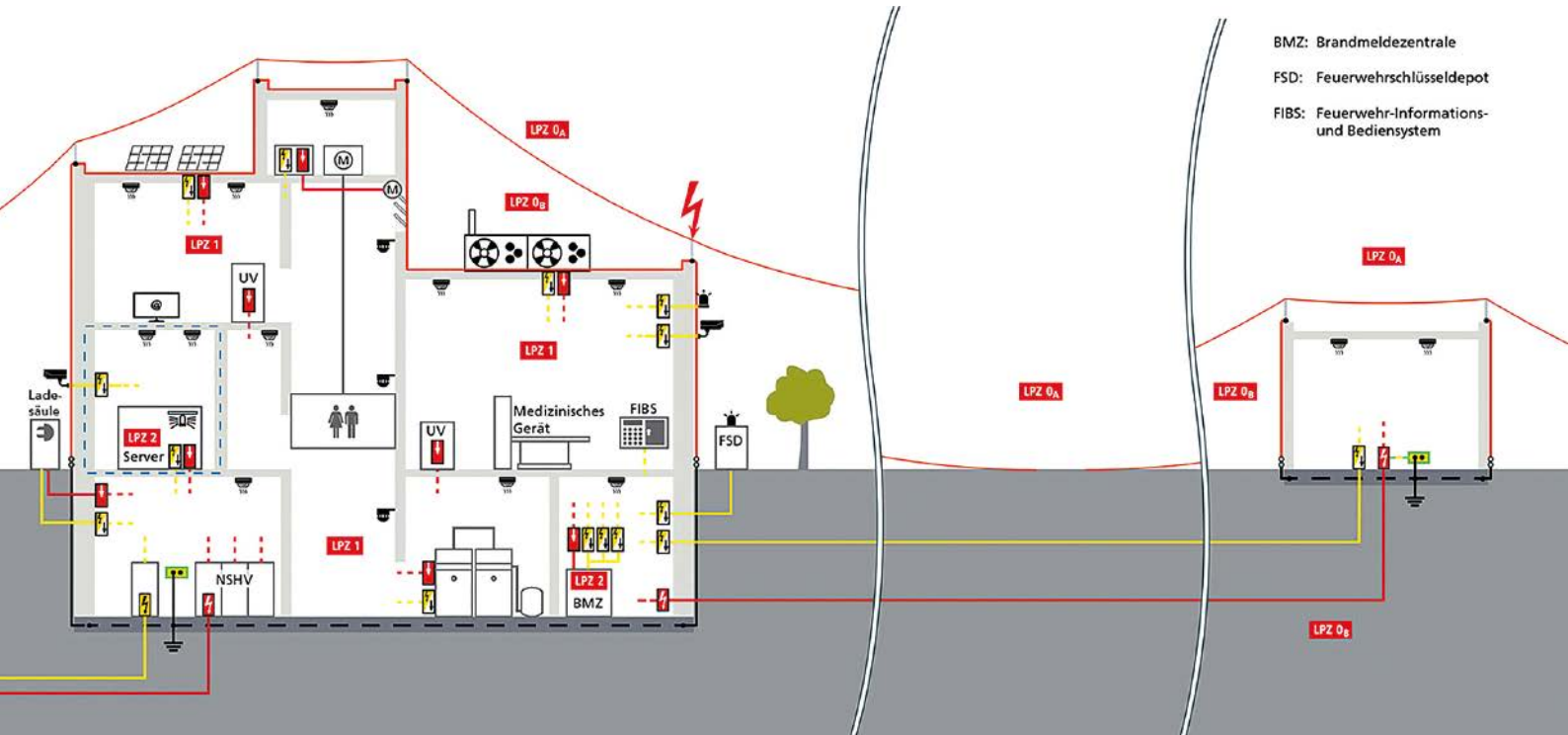
Normen und gesetzliche Vorgaben

Normen wie die DIN EN 62305, DIN VDE 0100-443/-534 oder DIN VDE 0833-1/-2 definieren Schutzmaßnahmen – ob im Neubau oder bei Bestandsgebäuden. Für Sonderbauten greifen zusätzlich die Landesbau- und Sonderbauverordnungen. Darüber hinaus sind zusätzliche gesetzliche Forderungen aus der Betriebssicherheitsverordnung (BetrSichV) oder den technischen Regeln für Betriebssicherheit (TRBS) zu berücksichtigen.

Sicherheitslücken vermeiden mit ganzheitlichen Schutzkonzepten

Wirksamer Schutz beginnt bereits bei der Planung. Ein durchgängiges Blitzschutzkonzept reduziert Risiken entlang der gesamten Elektroinstallation. Grundlage dafür ist das Blitzschutzzonen-Konzept, das Schutzvorkehrungen gezielt an der Gefährdungslage ausrichtet und sowohl äußere als auch innere Maßnahmen berücksichtigt. Das Blitzschutzzonen-Konzept unterteilt Gebäude in unterschiedliche Zonen, die abgestufte Schutzmaßnahmen erfordern:

- Äußerer Blitzschutz
- Erdung und Potentialausgleich
- Überspannungsschutz (innerer Blitzschutz)



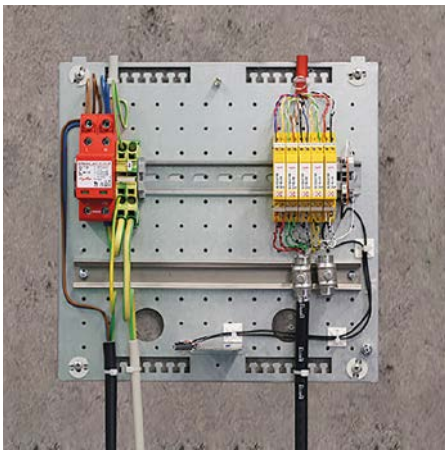
Technisch abgestimmte Schutzlösungen – Praxisbeispiele von DEHN

DEHN ermöglicht ein durchgängiges Schutzkonzept für alle Stufen: Der Kombi-Ableiter DEHNshield (Typ 1) schützt in der Hauptverteilung vor Blitzströmen, DEHNguard (Typ 2) ergänzt in der Unterverteilung. Mit DEHNrail und DEHNflex (Typ 3) entsteht ein komplettes System für die Energietechnik. Für MSR-, Ethernet- und Kommunikationsschnittstellen sorgen BLITZDUCTORconnect, DEHNpatch und DEHNrecord IRCM.

Gerade bei sicherheitstechnischen Anwendungen mit exponierten Außenkomponenten wie IP-Kameras, Feuerwehranlaufstellen oder Schlüsseldepots bietet DEHN zuverlässige Lösungen, um Blitzteilströme sicher abzuleiten.

Verfügbarkeit sichern – Risiken minimieren

Die fachgerechte Installation und Auswahl der Schutzkomponenten sind ebenso entscheidend wie deren Platzierung. Oft werden bei der Umsetzung Details wie Einbaurichtung oder Einbauort nicht ausreichend beachtet - mit negativen Folgen für die Schutzwirkung. Auch nach Blitzereignissen sind klare Handlungsanweisungen wichtig: Austausch beschädigter



Applikation Überspannungsschutzverteiler für FSD-Absicherung

Komponenten, vollständige Funktionsprüfung und ggf. Ergänzung des Schutzsystems nach den Empfehlungen von BHE, VdS und ZVEI.

Herausforderungen und Lösungsansätze in der Praxis

Planer und Errichter stehen immer wieder vor der Herausforderung, dass Schutzmaßnahmen zu spät in der Projektplanung berücksichtigt wurden. Die Folge sind teure und aufwendige Nachrüstungen. Auch eine regelmäßige Wartung und Prüfung der Systeme wird in der Praxis oftmals vernachlässigt. Nur durch kontinuierliche Kontrollen kann sichergestellt werden, dass Schutzmaßnahmen im Ernstfall zuverlässig funktionieren. Eine enge Zusammenarbeit mit spezialisierten Fachfirmen sichert hier Qualität und Wissenstransfer: von der Planung über die Installation bis zur Schulung des technischen Personals.

Fazit: Schutz auf allen Ebenen planen

Blitz- und Überspannungsschutz ist kein optionales Add-on, sondern integraler Bestandteil jedes Sicherheitskonzepts. Wer heute in Sicherheitstechnik investiert, muss auch deren dauerhafte Verfügbarkeit gewährleisten – technisch, normativ und wirtschaftlich. Ein ganzheitliches Schutzkonzept schafft hier die notwendige Basis. Planer und Installateure, die diesen Aspekt frühzeitig berücksichtigen, leisten einen entscheidenden Beitrag für den Schutz von Menschenleben, Infrastruktur und Investitionen.

Kontakt
Dehn SE
www.dehn.de

FLUCHTWEGSTEUERUNG

Führt in die richtige Richtung

Fluchtweglenkung: Dynamisch, adaptiv – und kompensatorisch

Sie ist normative Grundlage für die Planung, Umsetzung und Prüfung richtungsvariabler Systeme zur Fluchtwegkennzeichnung: Die DIN 14036 unterstützt Betreiber, Fachplaner und Behörden dabei, sichere und wirtschaftliche Evakuierungskonzepte zu realisieren – auch in komplexen Gebäudesituationen. Dynamische Systeme reagieren auf Gefahrenlagen und leiten Personen aktiv aus dem Gefahrenbereich. Adaptive Systeme passen die Fluchtrichtung sogar während der Evakuierung flexibel an. Die Norm ermöglicht zudem die Kompensation baurechtlicher Anforderungen und fördert barrierefreie Selbstrettung. Ein Beitrag von Ulrich Höfer von Inotec Sicherheitstechnik.

Ulrich Höfer, Inotec Sicherheitstechnik

Die unkontrollierte Ausbreitung gehört zur Definition des Brandes, also jenes Verbrennungsprozesses unter Flammen-, Glut- und Funkenentwicklung, der vor allem wegen der Rauchentwicklung so gefährlich ist für Menschen und Sachwerte. Greift er in Gebäuden um sich, muss für jeden der sich darin aufhält sofort klar sein, wo es am schnellsten und sichersten nach draußen geht: Dazu dient die Fluchtweglenkung. Sie besteht aus hinterleuchteten Kennzeichen, die den Flüchtenden von jedem Punkt des Gebäudes aus Orientierung und den Weg aus der Gefahrenzone weisen.

Normalerweise ist der kürzeste Weg der schnellste und beste – so sehen es auch die Bauordnungen der Länder. Feuer und Rauch halten sich freilich nicht an feste Regeln – und wenn Teile eines statisch gekennzeichneten Fluchtwegs unpassierbar sind, würde er mitten hinein in die Gefahr führen, statt aus ihr heraus.

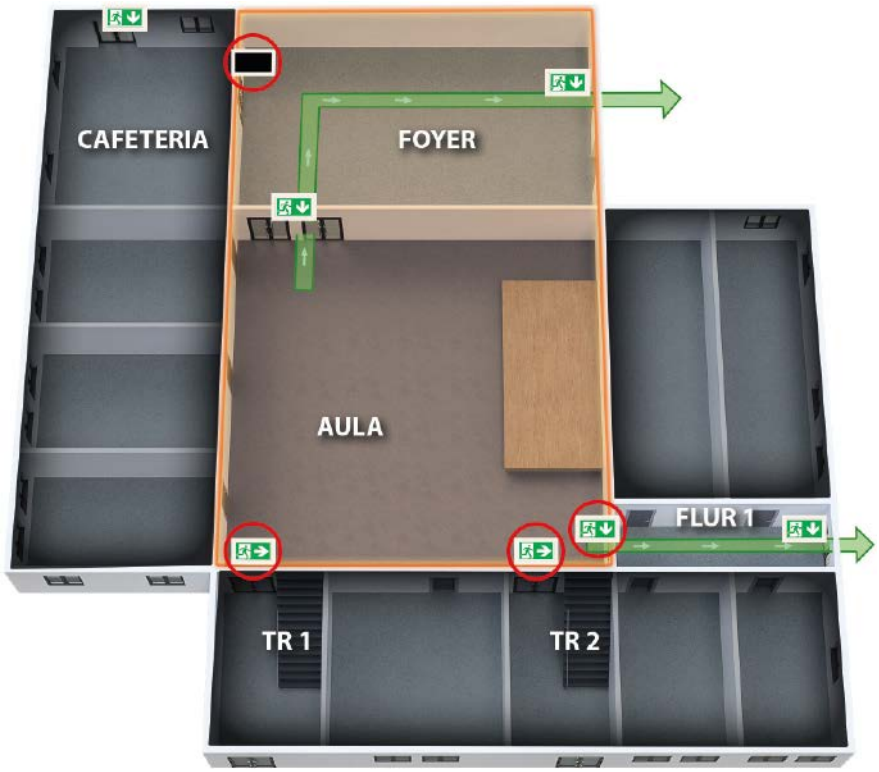
Effektiv ist eine Fluchtweglenkung deshalb dann, wenn sie zwar eindeutig ist – dabei aber so flexibel, wie die Brandentwicklung unvorhersehbar ist. Dies führte zum Gedanken der „dynamischen Fluchtweglenkung“: Sie ist richtungsvariabel und leitet um die gefährdeten Gefahrenbereiche herum bzw. von ihnen weg, wählt also den im konkreten Einzelfall richtigen und sicheren Fluchtweg aus und zeigt ihn an. Die Gefahrenbereiche selbst werden gleichzeitig durch ein Sperrzeichen optisch gesperrt.

Die dynamische Fluchtweglenkung ist eine einfache und in den allermeisten Fällen vollkommen ausreichende Lösung. „Adaptiv“ wird das Ganze zusätzlich dann, wenn sie die Fluchtrichtung an die Entwicklung des Brandes im Zeitverlauf anpasst. Damit das funktioniert, werden Sensoren, also vor allem Brandmelder, Videokameras und Gassensoren eingesetzt. Sie erkennen beispielsweise die Ausbreitung eines Brandes oder Stauungen an Fluchtwegen und weist darauf hin entsprechende alternative und sichere Fluchtwege aus.

Variable Fluchtweglenkung als Kompensationsmaßnahme

Für solche dynamischen (DFWL) und adaptiven (AFWL) Fluchtwegleitsysteme fehlte lange Zeit eine normative Grundlage – seit Dezember 2023 gibt es aber die DIN 14036. Im normativen Teil wird die schutzzielorientierte Realisierung einer

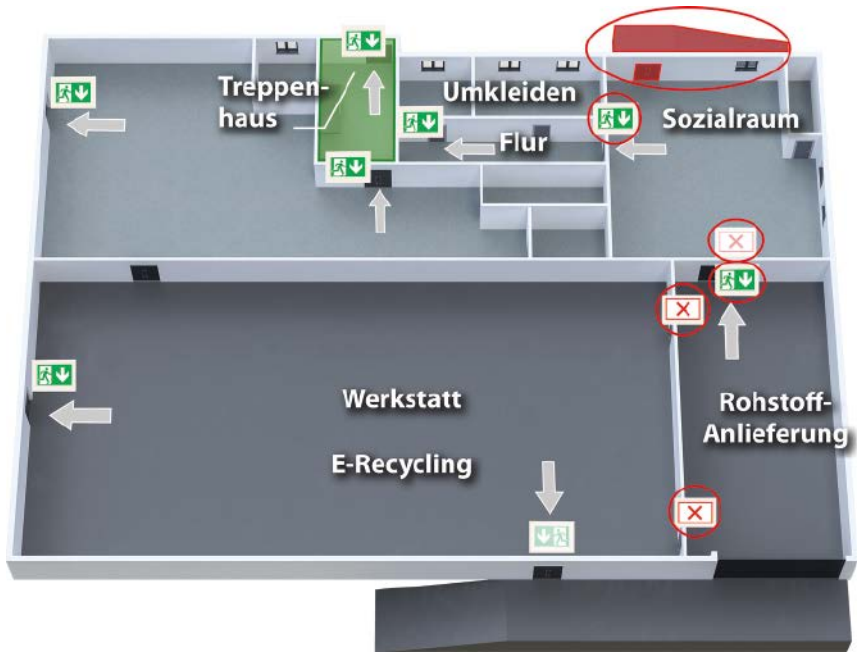
Temporäre Nutzungsänderung in einer Schule:
Während einer Veranstaltung in der Aula kann der Fluchtweg angepasst werden.



Dynamische Rettungszeichenleuchte: Sperrt betroffene Bereiche und zeigt alternative Fluchtwege an

DFWL beschrieben und im informativen Anhang B werden ergänzende Hinweise zum Aufbau einer AFWL gegeben. Weitere Ziele der Norm sind der Einsatz einer variablen Fluchtweglenkung als schutzzielorientierte Kompensationsmaßnahme und als Möglichkeit, beim vorbeugenden Brandschutz in Gebäuden einen größeren Gestaltungsspielraum sowie eine höhere Wirtschaftlichkeit zu erzielen.

So eine variable Fluchtweglenkung kann laut dieser Norm ausdrücklich auch als schutzzielorientierte Kompensationsmaßnahme eingesetzt werden. Nicht nur bei Neubauten, sondern auch bei Umbauten und Sanierungen im Bestand, in denkmalgeschützten Gebäuden sowie bei Nutzungsänderungen sind nachträgliche bauliche Lösungen nach aktuellen Standards oft nicht realisierbar. Die DIN 14036 beschreibt mögliche Szenarien, in denen DFWL/AFWL zur Kompensation baurechtlicher Anforderungen beitragen können.



Einsatz von fünf dynamischen Rettungszeichenleuchten: Der sichere Fluchtweg wird gekennzeichnet, der nicht mehr nutzbare wird optisch gesperrt. Hier: Rampe für Rollstuhlfahrer entfällt.

Nutzungsänderung eines Bestandsbaus

Ein Beispiel dafür ist eine von Inotec Sicherheitstechnik realisierte Lösung für eine Behindertenwerkstatt, die aus einer Nutzungsänderung einer vormaligen Fahrradwerkstatt entstanden ist: Dabei waren eine Sicherheitsbeleuchtung sowie wegen erhöhter Brandlasten eine flächendeckende Brandmeldeanlage gefordert. Die Fluchtwegführung aus dem Sozialraum gestaltete sich schwierig, da die anschließenden Flure wegen erhöhter Brandlasten nicht als notwendiger Flur ertüchtigt werden konnten. Deshalb sollte zur Entfluchtung des Sozialraumes zunächst ein Ausgang aus diesem direkt ins Freie mit einer Notausgangstür in der Außenfassade und einer Rampe für Rollstuhlfahrer errichtet werden.

Zur Kompensation dieser aufwendigen baulichen Maßnahmen wurden stattdessen im Sozialraum zwei und in der Rohstoffanlieferung drei richtungsvariable, dynamische Rettungszeichenleuchten eingesetzt. Sollte es nun in der Werkstatt bzw. im Flur zur Umkleide zu einem Brandfall kommen, wird dies durch die Brandmeldeanlage gemeldet. Der jeweils betroffene Bereich wird dann durch die dynamischen Rettungszeichenleuchten optisch mit einem roten Kreuz gesperrt und nur noch der nutzbare Fluchtweg ausgewiesen. In Verbindung mit der Blinkfunktion zur Erhöhung der Aufmerksamkeit wird sichergestellt, dass die Nutzer des Sozialraumes sicher aus dem

Bitte umblättern ▶

Gebäude geführt werden. Insgesamt wurde durch den Verzicht auf die Notausgangstür und die Rampe eine erhebliche Einsparung bei den Gesamtumbaukosten erzielt.

Temporäre Nutzungsänderung

Ähnliche Anforderungen ergeben sich bei temporären Nutzungsänderungen – so bei einem Projekt, das Inotec Sicherheitstechnik für eine Schule konzipiert hat. Deren Aula im zentralen Bereich dient im Schulbetrieb sowohl als Aufenthaltsbereich als auch für die Zuwegung von Klassen- und Treppenräumen. Bestimmte Treppenräume sind im Schulbetrieb als Fluchtwege gekennzeichnet und führen ins Freie. Weitere Fluchtwege führen durch die Cafeteria und das Foyer ins Freie.

Für Veranstaltungen außerhalb des Schulbetriebes soll die Aula mit ihrer Bühne auch für schulfremde Besucher genutzt werden. Gleichzeitig soll verhindert werden, dass Unbefugte Zugang zur Cafeteria und über die Treppenräume zu den Schulräumen in den oberen Etagen erlangen. Zu diesem Zweck werden die entsprechenden Bereiche abgeschlossen, sodass ein Teil der bislang ausgeschilderten Fluchtwege nicht mehr begehbar ist.

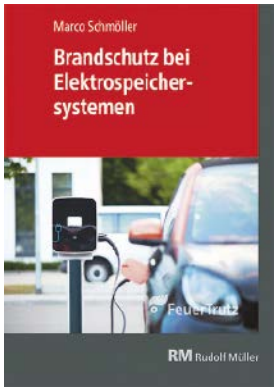
Die erforderliche Anpassung der Fluchtwegkennzeichnung kann problemlos durch richtungsvariable Rettungszeichenleuchten erfolgen. So werden bei einer Abendveranstaltung die betroffenen Treppenräume sowie der Zugang zur Cafeteria von zentraler Stelle aus optisch gesperrt oder durch Ausschalten der Leuchten unkenntlich gemacht. Der im Normalbetrieb nicht vorgesehene Weg durch einen Flur wird als zusätzlicher Fluchtweg angezeigt. Alternativ könnten die Leuchten über den Zugängen zu den Treppenräumen anstelle eines roten Kreuzes auch die alternative Fluchtrichtung zum Flur anzeigen. Dies ist frei programmierbar und erfordert bei Planung, Bestellung und Errichtung keinen zusätzlichen Aufwand.

Zur Realisierung der Fluchtwegausschilderung bei den temporären Nutzungsänderungen in diesem Beispiel mussten lediglich vier statische Rettungszeichenleuchten durch dynamische ersetzt werden. Die Voraussetzung dazu war lediglich das Vorhandensein eines modernen Sicherheitsbeleuchtungssystems zur Ansteuerung von dynamischen Leuchten. Die Ansteuerung der richtungsvariablen Rettungszeichenleuchten erfolgt ohne zusätzliche Buskabel über die dreiadrige Stromversorgung der Rettungszeichenleuchten. GIT

Inotec Sicherheitssysteme
www.inotec-licht.de

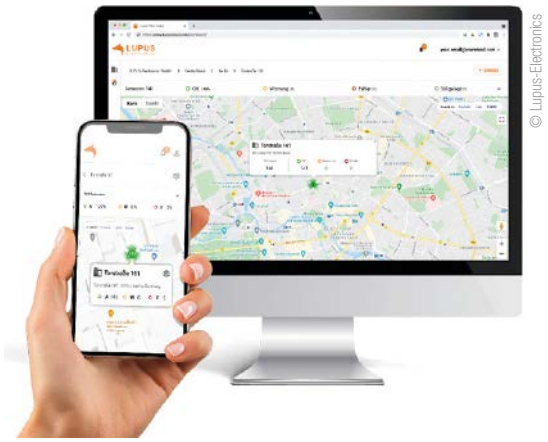
© Bilder: Inotec Sicherheitstechnik GmbH

Brandschutz bei Elektrospeichersystemen



Mit dem Ausbau erneuerbarer Energien gewinnt der Brandschutz bei Batterien und Elektrospeichersystemen zunehmend an Bedeutung. Planung, Ausführung und Betrieb erfordern differenzierte Maßnahmen, um Sicherheit und Funktionsfähigkeit zu gewährleisten. Das Fachbuch „Brandschutz bei Elektrospeichersystemen“ bündelt das aktuelle Wissen zu rechtlichen Grundlagen, technischen Anforderungen und praktischen Lösungen und zeigt, wie sich die spezifischen Risiken dieser Systeme wirksam beherrschen lassen. Das Werk betrachtet Herstellung, Lagerung, Transport, Betrieb, Speichersysteme, Fahrzeuge und Consumertechnik aus den Perspektiven des vorbeugenden, abwehrenden und organisatorischen Brandschutzes. Es beschreibt, welche Anforderungen in den jeweiligen Nutzungsbereichen gelten und wie sie in der Praxis umgesetzt werden können. Der Autor greift dabei sowohl bestehende Regelungen und Richtlinien als auch neue technische Entwicklungen und offene Fragestellungen im Zusammenhang mit der Energiewende auf.

Brandschutz bei Elektrospeichersystemen. Technische und rechtliche Grundlagen für Planung und Betrieb,
ISBN: 978-3-481-04772-6.



Energieeffiziente Sicherheit – alle Vorgänge jederzeit steuerbar und einsehbar, auch per Fernwartung.

Brandschutz von Lupus-Electronics auf der Heikom

Unter dem Motto „Zukunftsfähige Gebäude – intelligent vernetzt“ präsentierte Lupus-Electronics auf der Heikom – Fachmesse für digitales Energie- und Gebäudemanagement – innovative Lösungen für die digitale Transformation von Gebäuden. Mit einem klaren Fokus auf die Digitalisierung von Gebäudetechnik und Energieeffizienz zeigt der Hersteller, wie moderne IoT-basierte Systeme dazu beitragen können, Energieverbrauch zu optimieren, Betriebskosten zu senken und die Sicherheit in Gebäuden zu erhöhen. Besonderes Augenmerk liegt auf Lösungen, die sowohl für Neubauten als auch für Bestandsgebäude geeignet sind. Der OMS-Rauchwarnmelder des Unternehmens ermöglicht eine vollständig digitale Abwicklung der Inspektionspflicht. Die Datenübertragung wird über OMS/Wireless M-Bus realisiert, wodurch lediglich bei der Erstinstallation eine Vor-Ort-Kontrolle notwendig ist. **www.lupus-electronics.de**

Im Notfall die richtige Entscheidung treffen

Sicherheitsanlagen und Gebäudetechnik laufen bei Securiton Deutschland zentral in einem Sicherheitsmanagementsystem zusammen. Ständige Weiterentwicklungen und Verbesserungen der IT machen es Anwendern immer leichter und bequemer, das System zu bedienen und sich bei Entscheidungen auf valide Informationen stützen zu können.

Wie eine Nervenzentrale registriert, verarbeitet und steuert das universelle Managementsystem SecuriLink UMS von Securiton Deutschland Daten und übersetzt sie für Menschen in konkrete Hinweise und Warnungen. Sicherheitsanlagen und Gebäudetechnik unterschiedlicher Hersteller und Systeme speisen ihre Informationen von einem oder vielen weitverzweigten Standorten in die Applikation ein.

Die Softwareversion 15 bietet smarte Funktionalität, zeitgemäßes Design, eine praxisnahe App und startet in eine neue Generation des Sicherheitsmanagements. Bei allen Weiterentwicklungen steht immer der Mensch im Mittelpunkt: Er soll jederzeit den Überblick über alle Anlagen haben und im Ernstfall schnell und effektiv handeln können.

Unternehmen, die Sicherheit ganzheitlich denken und professionell steuern wollen, finden auf der Plattform gut strukturierte und priorisierte Meldungen aller Teilsysteme, wie Videosicherheit, Einbruchschutz, Brandschutz, Sprachalarmierung, Zutrittskontrolle, Zaundetektion, Drohnenabwehr und Roboter zur Bestreifung.

Alle relevanten Ereignisse oder Statusmeldungen der jeweiligen Anlagen erzeugen Meldungen. Eine Liste stellt sie automatisch mit allen notwendigen Informationen und weiterführenden Bearbeitungsmöglichkeiten zusammen. Die vom Anwender auszuführenden Schritte sind standardisiert und so gestaltet, dass er notwendige Maßnahmen effektiv und fehlerfrei einleiten kann. Auch mehrere Meldungen gleichzeitig lassen sich in der neuen Version auswählen und mit nur einem Reaktionsbefehl bearbeiten. Das spart Nutzern viel Zeit, wenn es mal hoch hergeht.

Globale Meldungen können zudem in verschiedene Listen unterteilt werden, etwa in Alarme, Störungen, Abschaltungen oder Wartungsmeldungen. Das ist auch optimal für dezentrale oder weitläufige Areale wie Industrieanlagen, Messen, Einkaufszentren, Justizvollzugsanstalten oder die Einsatzleitstellen von Organisationen wie Gesundheitseinrichtungen, Banken oder Rechenzentren.

Das Oberflächendesign hat ein umfangreiches FreshUp erhalten. Flaches Design und eine intuitive Icon-Sprache kommen den Anwendern entgegen. Je nach persönlicher Vorliebe oder Lichtverhältnissen können sie ganz einfach zwischen dem Light Mode und Dark Mode wechseln.

Datenströme von Sicherheitssystemen nehmen zu. Applikationen für das Sicherheitsmanagement müssen den Menschen sinnvoll unterstützen. Mit der Softwareversion 15 von SecuriLink UMS hat Securiton Deutschland die Bedienbarkeit deutlich verbessert

Sonderbrandmelder können schon sehr früh warnen, bevor ein Feuer ausbricht. Besonders unter schwierigen Umgebungsbedingungen spielen sie ihre Stärken aus, zum Beispiel in der Gas- und Ölindustrie, chemischen Produktionsanlagen oder Motorenprüfständen. Ganz ohne zwischengeschaltete Brandmeldezentrale lässt sich das Wärmesensorkabel SecuriHeat d-List nun über das Modbus-Protokoll direkt in das Managementsystem integrieren.

Neue Trendkurvenanzeigen für analoge und digitale Werte des Ansaugrauchmelders SecuriRAS ASD schaffen in Echtzeit mehr Transparenz und unterstützen das Sicherheitspersonal bei der Auswertung und Bearbeitung der Vorfälle. Relative und absolute Werte der Rauchtrübung und des Luftstroms können mit einem Blick erfasst werden. Eine optimierte BACNet-Anbindung erlaubt die herstellerunabhängige Kommunikation mit weiteren Systemen. Neu ist die Multistate-Objektfunktion, die mehrere Zustände eines Melders – etwa Alarm, Störung oder Abschaltung – in nur einem Objekt abbildet. Das vereinfacht die Bedienung erheblich und macht sie nutzerfreundlicher.

Aus vielen Einzelsystemen entsteht so eine ganzheitliche Sicherheitsarchitektur, die flexibel, modular skalierbar und zukunftssicher ist. Durch die Herstellerunabhängigkeit von SecuriLink UMS zahlen sich Investitionen langfristig aus. Die lückenlose Verschlüsselung schützt vor Datenverlust und Ausfällen und wird aktuellen gesetzlichen Anforderungen voll und ganz gerecht. **www.securiton.de**

Windrad von innen, Blick nach oben: Ein Brand im Rechenzentrum könnte sich auf die gesamte Anlage ausbreiten – die N_2 ORS Brandvermeidungsanlage eliminiert dieses Risiko

BRANDVERMEIDUNG

Am Ursprungsort der Energie

Brandschutz für Rechenzentrum im Windrad mit Sauerstoffreduktionstechnologie

Die Westfalen Wind-Gruppe aus Paderborn integriert erstmals stromintensive Rechenzentren direkt in moderne Windkraftanlagen, wo Energie und Infrastruktur unmittelbar vor Ort verfügbar sind. Wichmann Anlagentechnischer Brandschutz sorgt mit der Brandvermeidungsanlage N2ORS für den sicheren Betrieb des Rechenzentrums und der Windkraftanlage.

Der erste Prototyp der Wind Cores, des nach den Projektbeteiligten weltweit einzigen Rechenzentrums in einer Windenergieanlage, wurde 2018 in Betrieb genommen. Die nächste Ausbaustufe, die sich im Turm der Anlage über mehrere Ebenen erstreckt, wurde im September 2024 im Windpark Huser Klee eröffnet. Durch die Nutzung bestehender Gebäudestrukturen, der vorhandenen Glasfaseranbindung im Windpark und des Stroms, der direkt in der Windenergieanlage erzeugt wird, zählen die Wind Cores II wohl zu den nachhaltigsten Rechenzentren überhaupt.

Für dieses Projekt sorgt Wichmann Anlagentechnischer Brandschutz mit einer N2ORS Brandvermeidungsanlage für den sicheren Betrieb des Rechenzentrums und der Windkraftanlage. Durch die kontinuierliche Senkung des Sauerstoffgehalts und die Erhaltung einer brandsicheren Atmosphäre wird ein potenzielles Brandrisiko effektiv vermieden, sodass Störungen und Ausfälle durch Brände erst gar nicht entstehen können.

Das technologische Herzstück der Anlage ist der VPSA „Adox“ Generator der neuesten Generation. Mit seiner platzsparenden Bauweise eignet er sich besonders für die Integration in einen Windradturm. Darüber hinaus erfüllt der Generator mit einer Anschlussleistung von lediglich 5 kW die strengen Anforderungen an Energieeffizienz – ein entscheidender Vorteil für die nachhaltige Nutzung in einer solchen Umgebung.

Mehr als Brandschutz

Das Wind Cores II-Rechenzentrum ist für sich ein hochsensibles technisches Konstrukt, das aus einer komplexen Anordnung von Servern und peripheren Geräten besteht. Um dieses zuverlässig zu schützen, wurden gleich mehrere zentrale Schutzziele kombiniert: Brandschutz, Ausfallsicherheit, Investitionsschutz und Nachhaltigkeit in einem integrativen Sicherheitskonzept.

Ein Brand in einem Rechenzentrum kann verheerende materielle Schäden verursachen – im Fall des Wind Cores II-Projekts besteht zusätzlich die Gefahr, dass sich das Feuer auf die Windenergieanlage ausbreitet. Die N2 ORS Anlage verhindert dieses Risiko vollständig, indem sie den Sauerstoffgehalt in den Schutzbereichen unter die Entzündungsgrenze senkt. Dadurch wird die physikalische Voraussetzung für ein Brandereignis ausgeschlossen.

Gleichzeitig erfüllt das System behördliche Anforderungen zur Brandlastreduzierung: „In eine Windkraftanlage dürfen maximal 80.000 Kilowattstunden an Brandlast eingebracht werden. Diese ist bereits durch die zur Energieerzeugung notwendigen Komponenten zu einem Großteil erreicht. Die zusätzliche Brandlast der

IT-Infrastruktur dürfte daher eigentlich gar nicht eingebracht werden. Durch die Sauerstoffreduktion kann die Brandlast der IT-Infrastruktur jedoch auf nahezu null reduziert werden – ein wesentlicher Beitrag zur strukturellen Sicherheit des Windrades." erklärt Dr. Fiete Dubberke, Mitgründer von Westfalen Wind IT.

Neben dem physischen Schutz ist die permanente Verfügbarkeit des Rechenzentrums von zentraler Bedeutung. Die Infrastruktur steht Unternehmen verschiedenster Branchen zur Verfügung und muss daher höchste Anforderungen erfüllen, etwa gemäß Tier III und Verfügbarkeitsklasse 3 (VK3-TÜV). Die Brandvermeidungsanlage unterstützt dieses Ziel mittels ihrer durchgehend redundanten Auslegung – entsprechend der Sicherheitsanforderungsstufe SIL3 – und trägt zur Betriebskontinuität bei.

Auch immaterielle Werte wie Daten und digitale Geschäftsprozesse werden geschützt. Durch die Einhaltung relevanter Normen wie der ISO 27001 und der DSGVO ist die Datensicherheit integraler Bestandteil des Brandschutzkonzepts. Die N2 ORS-Anlage stellt sicher, dass auch dieser Schutz kontinuierlich gewährleistet ist.

Technologische Effizienz und Systemarchitektur

Bei der Auslegung des Systems wurde besonderer Wert auf Energieeffizienz, Kompaktheit und Umweltverträglichkeit gelegt. Der VPSA-Generator erzeugt mit lediglich 5 kW elektrischer Leistung bis zu 25 Nm^3 Stickstoff pro Stunde bei 95 % Reinheit – ein im Marktvergleich sehr guter Wert. Durch die kompakte Bauweise nimmt das gesamte System nur rund 2 m^2 Stellfläche ein und passt damit optimal in den begrenzten Raum im Turmfuß einer Windenergieanlage.

Das Brandvermeidungssystem versorgt fünf Schutzbereiche über ein zentrales Ventilverteilsystem. Jeder Bereich wird dabei von drei optischen Sauerstoffsensoren überwacht, die auf dem Prinzip der Lumineszenz-Löschung basieren. Diese Technologie bietet eine präzise, stabile und wartungsarme Messung – sie verbraucht sich nicht selbst und erfordert keinen regelmäßigen Austausch.

Ein weiterer Vorteil ergibt sich im Hinblick auf den Umweltschutz: Ein potenzieller Brand in einer Windkraftanlage hätte neben technischen und wirtschaftlichen Folgen auch ökologische Konsequenzen. Die Brandvermeidungsanlage trägt entscheidend dazu bei, diese Risiken vollständig zu vermeiden.

Fiete Dubberke führt weiter aus: "Nicht nur die installierten Sachwerte, sondern auch die Daten unserer Kunden müssen jederzeit verfügbar und sicher sein. Unsere Kunden stellen Ihre wertvolle IT bei uns unter und wir sind verpflichtet, ihr Investment und ihre Daten zu schützen. Dafür ist die sauerstoffreduzierte Atmosphäre das beste Instrument, das man zum Brandschutz wählen kann. Mit Wind Cores II bringen wir IT-Infrastruktur und erneuerbare Energien auf einzigartige Weise zusammen. Rechenzentren direkt im Windrad zu betreiben, erfordert nicht nur Mut zur Innovation, sondern auch kompromisslose Sicherheitsstandards." GIT

Wichmann Brandschutzsysteme GmbH & Co. KG
www.wichmann.biz

Die Wind Cores II: Wichmann Brandschutzsysteme sorgt mit einer N2ORS Brandvermeidungsanlage für den sicheren, nachhaltigen Betrieb

Außenansicht eines der fünf sauerstoffreduzierten Schutzbereiche des Rechenzentrums

Das Herzstück der N_2 ORS Brandvermeidungsanlage: Der energieeffiziente VPSA „Adox" Generator

Bernhard Goßen, Vertriebsleiter von Multicomsystem

GERÄTEINTEGRIERTER BRANDSCHUTZ

Echter Brandschutz kommt von innen

Gezielte Prävention kann existenzsichernd sein

Vorbeugender Brandschutz in elektrischen Anlagen wird häufig unterschätzt – dabei entstehen viele Brände genau dort: in Geräten, Schaltschränken und Steuerungen. Bernhard Goßen, Vertriebsleiter von Multicomsystem, erläutert, warum herkömmliche Konzepte nicht ausreichen, welche innovativen Lösungen bereits verfügbar sind und wie Unternehmen durch gezielte Prävention nicht nur Schäden vermeiden, sondern auch ihre Existenz sichern können.

Herr Goßen, der vorbeugende Brandschutz ist einer der wichtigsten Geschäftsbereiche der Multicomsystem. Welchen Ansatz fahren Sie hier?

Bernhard Goßen: Beim vorbeugenden Brandschutz geht es uns um eines der wichtigsten und oft dennoch am meisten unterschätzten Bereiche, nämlich den geräteintegrierten Brandschutz.

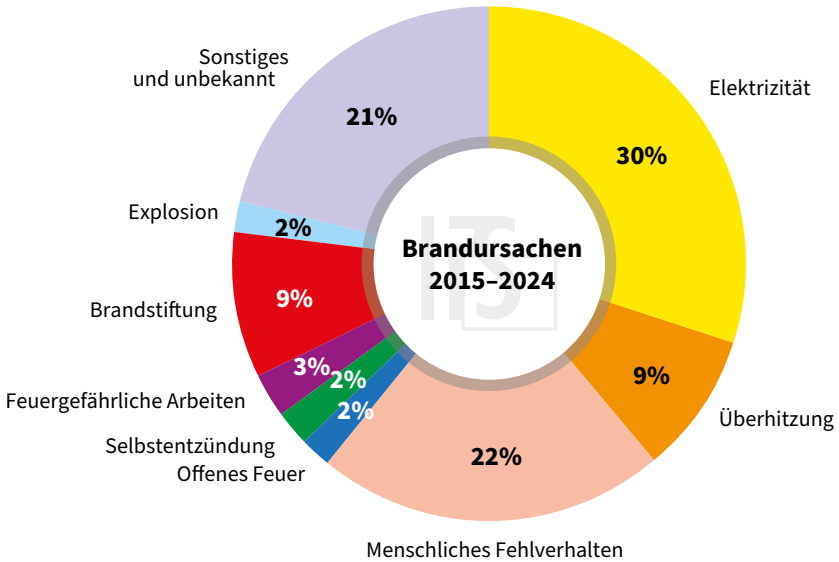
Also ein Schutz von innen sozusagen...

Bernhard Goßen: Richtig. Viele Brände entstehen nämlich innerhalb von Schaltschränken, oder ganz generell innerhalb von Geräten und Maschinen. Deshalb ist es effektiver, Brände gleich dort, also am Entstehungsort, zu bekämpfen, anstatt erst außerhalb der Geräte anzusetzen. So entsteht ein erheblich geringerer Schaden.

Die Gefahr wird häufig unterschätzt wie Sie mir schon in unserem Vorgespräch aus Ihrer Erfahrung berichteten: So mancher sagt sich offenbar, „in den letzten Jahrzehnten hat es bei mir nie gebrannt – und im Ernstfall springt doch die Versicherung ein“...

Bernhard Goßen: Dann haben diese Unternehmen schlichtweg Glück gehabt. Aber Glück ist keine Strategie. Ein Brand kann jederzeit entstehen – und wenn er es tut, sind die Folgen oft verheerend. Die Versicherung mag den Sachschaden regulieren, aber Produktionsausfälle, verlorene Kunden und der langwierige Wiederaufbau sind meist nicht abgedeckt. Statistisch gesehen geht ein Drittel der betroffenen Unternehmen direkt nach einem größeren Brandereignis insolvent, ein weiteres Drittel innerhalb von zwei bis drei Jahren. Nur ein Drittel überlebt langfristig.

Elektrizität gehört mit 32% zu den häufigsten Schadensursachen



Quelle: Institut für Schadenverhütung und Schadenforschung der öffentlichen Versicherer e.V. (IFS)

Was sind Ihrer Meinung nach die Schwachstellen im aktuellen Brandschutzkonzept?

Bernhard Goßen: Die bestehenden Normen und Konzepte konzentrieren sich auf den Raumschutz mit Löschanlagen, Melderpflichten und Materialvorgaben. Was fehlt, ist der integrierte Brandschutz direkt im Gerät – also dort, wo die meisten Brände entstehen. Die Versicherungsstatistiken zeigen klar: Der Ursprung liegt häufig in elektrischen Geräten. Doch genau hier gibt es keine verbindlichen Vorschriften.

Welche Lösungen schlagen Sie vor, um diese Lücke zu schließen?

Bernhard Goßen: Es gibt bereits praktikable und kostengünstige Lösungen. Dazu gehören etwa: Permanente Temperaturmessung an stromführenden Kabeln, drahtlose Sensoren an Stromschienen, Gehäusen und Bauteilen sowie automatisch auslösende Kleinfeuerlöscher direkt im Gerät. Diese Systeme erkennen kritische Temperaturen frühzeitig und können im Ernstfall selbstständig löschen – ohne Folgeschäden, da das Löschmittel nichtleitend und rückstandsfrei ist.

Vorgeschrieben sind solche Systeme ja nicht?

Bernhard Goßen: Nein, eine Pflicht gibt es bislang nicht. Aber ich empfehle dringend das VdS-Merkblatt 4026. Es bietet eine solide Grundlage für den vorbeugenden Brandschutz in elektrischen Anlagen. Wer als Brandschutzbeauftragter die beschriebenen Lösungen kennt und sie nicht weitergibt, handelt fahrlässig. Die Geschäftsleitung erwartet, dass Erkenntnisse aus Fachvorträgen und Weiterbildungen in konkrete Verbesserungsvorschläge münden. Das ist nicht nur verantwortungsbewusst – es kann auch die eigene Position im Unternehmen stärken.

Können Sie konkrete Produkte nennen, die sich bewährt haben?

Bernhard Goßen: Der drahtlose Temperatursensor von Sensolus etwa überträgt per BLE-Protokoll die Daten an einen Tracker. Der mit dem Fraunhofer Institut entwickelte drahtlose TempTag BLE löst bei Überschreitung einer Schwellwerttemperatur eine Störmeldung aus und kann sogar den Kleinfeuerlöscher aktivieren. Diese Löschsysteme funktionieren wie eine Sprinkleranlage – nur ohne Wasserschäden. Sie überbrücken die kritische Zeit zwischen Brandentstehung und Eintreffen der Feuerwehr.

Wie sieht der Ablauf nach einem solchen Brandereignis aus?

Bernhard Goßen: Der automatische Feuerlöscher löscht den Brand sofort, die Brandmeldeanlage informiert die Feuerwehr. Nach der Sichtkontrolle heißt es: „Feuer aus“. Der Schaltschrank wird freigegeben, die defekten Komponenten repariert – und die Produktion läuft weiter. Kein Reinigungsaufwand, keine Rückstände. So sollte moderner Brandschutz aussehen.

Wo können sich Interessierte weiter informieren?

Bernhard Goßen: Bei mir persönlich oder auf der Webseite www.multicomsystem.de finden Sie viele Anregungen zu kabellosen Temperatursensoren und integrierten Löschsystemen. Auch das Fraunhofer-Institut bietet spannende Einblicke unter www.ims.fraunhofer.de. GIT

Multicomsystem
www.multicomsystem.de

Temperatursensor

Der Temperatusensor von Sensolus überträgt per BLE-Protokoll die Temperaturdaten an einem Tracker und alles drahtlos. Dieser vieleinsetzbare wartungsfreier Tracker kann in vielen Bereichen die Arbeit im Alltag erleichtern. Für die Zustandsüberwachung von Tore, Schranken usw. oder der Messungen von Innen- und Außentemperaturen sowie Feuchtigkeit stehen mobile externe Sensoren zur Verfügung. Mit dieser Lösung können Sie schnell, bequem, zeitnah und kostensparend handeln und über alles den Überblick behalten.

Tracker von Sensolus empfangen per Datenübertragung von den Sensoren Informationen über Temperaturen, Feuchtigkeit, Zustände von Tür und Tor und weitere Navigationsdaten.

Die Connected Services von Chubb agieren als digitaler Sicherheitsdienst und fungieren als „Remote-Sicherheitskraft“ für Unternehmen

LEITSTELLEN

Connected Services

Ganzheitliche Sicherheitsstrategien für vernetzte Systeme und Anlagen

Betriebliche Abläufe, der Schutz von Mitarbeitern sowie von Gebäuden und Umgebungen – all das wird nur dann gewährleistet, wenn moderne Sicherheitskonzepte präventiv und zuverlässig ineinandergreifen. Im digitalen Zeitalter eröffnen vernetzte Dienstleistungen – sogenannte Connected Services – optimale Möglichkeiten, um Anlagen, Systeme und Vermögenswerte rund um die Uhr zu überwachen und zu schützen. Mit den „Connected Services“, eine Leistung der Marke Chubb Vision, verknüpft Chubb die eigene zertifizierte Notruf- und Serviceleitstelle mit Remote-Services und ermöglicht die direkte Bedienung an sicherheitsrelevanten Schnittstellen.

Die Anforderungen an Sicherheitskonzepte gehen weit über den klassischen Einbruchschutz hinaus und umfassen beispielsweise auch Videoüberwachung und Analyse, Zutrittskontrolle, Perimetersicherheit sowie Brand- und Gefahrenmeldetechnik. Dank der Möglichkeit der Vernetzung und Fernüberwachung kann ein Monitoring von beliebigen Standorten erfolgen. Connected Services überzeugen durch ihre Skalierbarkeit und Kosteneffizienz, da Vor-Ort-Einsätze dank der Remote-Services deutlich reduziert werden können und zu einer ganzheitlichen Sicherheitsstrategie beitragen. Damit revolutionieren diese Art der Dienstleistungen die traditionelle Sicherheitsbranche, da sie proaktive und präventive Lösungen sowie einen „Remote-Sicherheitsdienst“ bieten, der dennoch die menschliche Komponente bewahrt.

Digitale Detektion und menschliches Urteilsvermögen

Mit den Connected Services, eine Leistung der Marke Chubb Vision, verknüpft Chubb die eigene zertifizierte, professionell besetzte Notruf- und Serviceleitstelle mit Remote-Services und ermöglicht die direkte Bedienung an sicherheitsrelevanten Schnittstellen. Das führt im Sinne des Kunden zu einer schnelleren Alarmverifikation, reduzierten Fehlalarmen, transparenter Beweisdokumentation und geringeren Betriebskosten im Vergleich zu rein personellen Schutzkonzepten während gleichzeitig Ausfallsicherheit und Servicequalität steigen.

Ein Baustein ist beispielsweise das Videoguarding, bei dem digitale Kontrollgänge erfolgen und Objekte in Echtzeit überwacht werden. Ergänzend erfolgt die Remote-Bedienung von Einbruchmeldeanlagen, sodass die Leitstelle sämtliche Anlagen nach Kundenwunsch scharf oder unscharf schalten kann. All das erfolgt von der Chubb Notruf- und Serviceleitstelle ausgehend, die nach VdS-Richtlinien sowie DIN EN ISO 9001 zertifiziert ist und rund um die Uhr professionelle Überwachungs- und

Servicedienstleistungen bietet. Eingehende Notruf- und Störmeldungen werden unmittelbar erkannt, bewertet und bearbeitet. Insbesondere in der Logistikbranche oder dem Finanzwesen bieten die Connected Services ein hohes Maß an Sicherheit.

Ein unsichtbarer Beschützer

Die Connected Services agieren als digitaler Sicherheitsdienst und fungieren als „Remote-Sicherheitskraft" für Unternehmen. Anders als traditionelle Sicherheitsdienste, die physisch vor Ort präsent sein müssen, bietet dieser digitale Ansatz eine lückenlose Überwachung ohne räumliche Beschränkungen. Die vernetzten Dienstleistungen können dabei nahezu alle Systeme und Anlagen beim Kunden beinhalten. Chubb schafft vor Ort die Voraussetzungen für die Aufschaltung, sodass diese lückenlos von geschulten Disponenten per Fernzugriff überwacht werden können. Im Falle eines Ereignisses greift ein vom Kunden definierter Interventionsplan mit konkreten Handlungsabläufen. Sobald die Meldung in der Leitstelle eingeht, öffnet der Disponent dieses Protokoll und arbeitet es Punkt für Punkt ab. Dabei werden sämtliche Prozesse sekundengenau dokumentiert. Dies bietet wichtigen Input für eine spätere Aufarbeitung und stellt sicher, dass jeder Schritt nachvollzogen werden kann.

Ein entscheidender Vorteil ist, dass der ‚digitale Sicherheitsdienst' nicht nur rund um die Uhr einsatzbereit ist, in Sekunden auf Alarme und kritische Ereignisse reagiert sowie gleichzeitig mehrere Standorte überwachen kann. Er arbeitet zudem wirtschaftlicher und sicherer als ein physischer Sicherheitsdienst. Dabei wird die menschliche Kompetenz nicht ersetzt, sondern intelligent mit modernen Technologien kombiniert. Die aufgeschalteten Connected Services bieten den Anwendern schließlich zahlreiche Vorteile im täglichen Betrieb: Die Leitstellen-Integration gewährleistet nicht nur eine Video-Verifikation, sondern auch die Alarmbearbeitung mit dokumentiertem Beweis-Management. Aufgrund der hybriden Services wird die Remote-Überwachung mit einem bedarfsgerechten Eingreifen vor Ort kombiniert. Eine solche 2-Faktor-Strategie ermöglicht das Beste aus beiden Welten, da Technologie sinnvoll durch menschliche Einschätzungen ergänzt wird. Das heißt: Selbst, wenn die Technik eine Unregelmäßigkeit erkennt, prüft und verifiziert ein Mensch. Dadurch ist eine erhöhte Ausfallsicherheit gewährleistet, da im Zweifelsfall präventiv und nicht reaktiv reagiert werden. Ergänzend dazu ist eine schnelle Wiederherstellung des ursprünglichen Zustandes gegeben.

Zudem profitieren die Kunden von reduzierten Verlusten und Schadenshöhen sowie potenziell geringeren Versicherungsprämien durch zertifizierte Leitstellen-Prozesse und deren Nachweisbarkeit gegenüber Versicherern.

Der Weg zur vernetzten Sicherheit

Für eine erfolgreiche Einführung empfiehlt sich ein strukturiertes Vorgehen, das von der professionellen Analyse der aktuellen Sicherheitslage über die Definition von Zielen bis hin zur Auswahl passender Connected Services reicht. Bereits bestehende Sicherheitstechnik stellt kein Hindernis dar, da die Integration seitens Chubb völlig herstellerunabhängig erfolgt und sich das modulare System flexibel auf neue Objekte oder Anwendungen erweitern lässt. Mit einer durchdachten Strategie und der Auswahl eines verlässlichen Partners wie Chubb können Unternehmen ihre Sicherheitsprozesse somit nachhaltig modernisieren und Werte nachhaltig schützen. Dank der Möglichkeiten moderner Technologien wird ein höheres Sicherheitslevel, mehr Effizienz und Transparenz für Unternehmen geschaffen. GIT

Chubb Fire & Security
www.chubbfs.com/de-de

© Bilder:

Hifire 4100 XS: kompakter Aufbau, einfache Parametrierung

© Telenot

Speziell für die Anforderungen in Kindergärten und Kindertagesstätten, Hotels oder kleinen Pensionen sowie Seniorenheimen hat Telenot die Brandwarnanlage Hifire 4100 XS entwickelt. Die Hifire 4100 XS hat einen kompakten Aufbau, die Möglichkeit einer bequemen Parametrierung mit oder ohne Computer, eine intuitive Bedienung sowie Anschlussmöglichkeiten von Komponenten per Funk oder Draht. Kontinuierlich baut der Hersteller sein Portfolio im Bereich Brandmeldetechnik weiter aus. „Dieser Bereich der Sonderbauten war über viele Jahre weitgehend ungeregelt. Mit der DIN VDE V 0826-2 wird nun klar definiert, welche Anforderungen Brandwarnanlagen für diesen Bereich erfüllen müssen. So wird beispielsweise festgelegt, dass alle Komponenten der EN-54-Reihe entsprechen müssen", erklärt Simon Schurr, Produktmanager Brandmeldetechnik bei Telenot. **www.telenot.com**

GIT SICHERHEIT

Die GIT SICHERHEIT ist für mich wichtig, weil sie ein facettenreiches Fachforum ist und die kontinuierliche Auseinandersetzung (im Sinne von Lesen, Lernen, Diskutieren, Machen) mit dem spannenden Themengebiet „Sicherheit" anregt. Bitte weiter so!

Jens Greiner,
Director, Forensic Services
bei PwC Deutschland

PFAS-VERBOT

EU verbietet PFAS in Schaumlöschmitteln

Warum Betriebe jetzt auf fluorfreie Feuerlöscher umstellen sollten

Mit dem Inkrafttreten des lange erwarteten PFAS-Verbots in Schaumlöschmitteln (EU-Verordnung 2025/1988) am 23. Oktober 2025 steht fest: Alte PFAS-haltige Feuerlöscher müssen ausgetauscht werden – idealerweise frühzeitig. So vermeiden Betreiber unnötige Risiken.

Autor: Markus Dumrath, Geschäftsführer Minimax Mobile Services

Die Umstellung von PFAS-haltigen auf fluorfreie Feuerlöschgeräte ist mit dem Beschluss der EU-Kommission nicht mehr wie bisher eine umweltfreundliche Option, sondern ein verpflichtender Schritt. Während dahingehend für Betreiber nun Klarheit herrscht, lauern gleichzeitig nicht nur wegen der Komplexität der Verordnung Risiken im Rahmen der gegebenen Übergangsfristen.

PFAS – das unsichtbare Risiko im Brandschutz

PFAS, per- und polyfluorierte Alkylverbindungen, wurden jahrzehntelang wegen ihrer wasser-, fett- und schmutzabweisenden Eigenschaften und ihrer extremen Hitzebeständigkeit in zahlreichen Produkten eingesetzt – wie Pfannen, Lebensmittelverpackungen, Kleidung und auch Feuerlöschschaum. PFAS verliehen Löschschaum eine sehr hohe Wirksamkeit bei Flüssigkeitsbränden bei wesentlich geringerer Gefahr eines Löschschadens. Ende der 1990er Jahre löste der Feuerlöscher mit AFFF-Schaum daher in unseren Breiten den Pulverlöscher als Standard zur Abdeckung der Brandklassen A (Feststoffbrände) und B (Flüssigkeitsbrände) weitgehend ab. Doch heute ist klar: PFAS sind kaum abbaubar, reichern sich in Umwelt und Körper an und können ernsthafte Krankheiten wie Krebs, Leber- und Hormonstörungen verursachen. Die „Ewigkeitschemikalien" wurden weltweit im Grundwasser, in Lebensmitteln und im Blut nachgewiesen.

Seit 2009 reguliert die Europäische Union schrittweise verschiedene PFAS-Untergruppen in Feuerlöschmitteln, wie PFOS, PFOA oder PFHxA. Die neue Regelung geht deutlich weiter, sie betrifft alle PFAS-Zusätze und sieht gestaffelte Übergangsfristen vor.

Was bedeutet das für Betreiber von Feuerlöschern?

Das Inverkehrbringen von PFAS-haltigem Löschschaum in Feuerlöschern ist bereits ab Oktober 2026 verboten. Inzwischen bieten alle deutschen Feuerlöscherhersteller fluorfreie Produkte an. Moderne fluorfreie Schaumfeuerlöscher stehen in ihrer Löschleistung den bisherigen PFAS-haltigen Produkten in nichts nach. Sie sind für die Brandklassen A und B geeignet und erfüllen alle Anforderungen an einen sicheren, umweltfreundlichen und zukunftsfähigen Brandschutz.

Für Betriebe heißt das: Wer noch PFAS-haltige Feuerlöscher besitzt, sollte dringend auf fluorfreie Alternativen umsteigen. Auch wenn die Übergangsfristen bis Ende 2030 reichen, steigen die Risiken zwischenzeitlich enorm an. Zum einen steigt jetzt die Nachfrage nach PFAS-freien Feuerlöschern. Wer früh seine Geräte austauscht, kann Kosten sparen und eventuelle Liefer-

So gelingt die Umstellung auf fluorfreie Feuerlöscher

1. Gerätebestand prüfen: Prüfen Sie, welche Feuerlöscher in Ihrem Betrieb verwendet werden. Vom PFAS-Verbot betroffen sind nur Schaumfeuerlöscher (Brandklassen A + B). Geräte mit der Kennzeichnung „PFAS-frei“ oder „fluorfrei“ gelten als unbedenklich. Bei Unsicherheit hilft der Hersteller oder Ihr Wartungsdienst.

2. Umrüst-Beratung nutzen: Viele Feuerlöscherhersteller bieten die Umrüstung ausgewählter PFAS-haltiger Feuerlöscher ihrer Eigenmarken zu PFAS-freien Geräten an. Lassen Sie sich von Ihrem Feuerlöscher-Lieferanten oder Ihrem Wartungsunternehmen beraten.

3. Fachgerechte Entsorgung sicherstellen: PFAS-haltige Feuerlöscher und die darin enthaltenen Löschschäume müssen als Sondermüll entsorgt werden. Lassen Sie dies nur von zertifizierten Entsorgungsbetrieben durchführen oder von Ihrem Wartungsunternehmen, sofern dieses über die entsprechende Genehmigung verfügt.

4. Fluorfreie Alternativen wählen: Setzen Sie auf fluorfreie Schaumfeuerlöschgeräte mit geprüfter Löschleistung für die Brandklassen A + B. Diese sind umweltschonend und erfüllen alle gesetzlichen Vorgaben des PFAS-Verbots.

5. Dokumentation aktualisieren: Erfassen Sie die Umstellung in Ihrer Brandschutzdokumentation und informieren Sie gegebenenfalls Ihre Mitarbeiter über die neuen Geräte und deren Handhabung.

Minimax-Schaumfeuerlöscher WX 6 nG fluorfrei zur Abdeckung der Brandklassen A + B

© Bilder: Minimax Mobile Services GmbH

engpässe umgehen. Zum anderen ist die Entsorgung fluorhaltiger Löschmittel als Sondermüll aufwendig und die Kapazitäten sind begrenzt. Erfolgt die Entsorgung nicht fachgerecht und wird sie nicht entsprechend dokumentiert, drohen dem Betreiber als Abfallverursacher empfindliche Strafen.

Ob bei einer Übung oder im Ernstfall: Beim Einsatz PFAS-haltiger Löschmittel besteht die Gefahr des Schadstoffeintrags in Kanalisation, Böden und Gewässer. Eventuell folgende Schadenersatzforderungen können für Unternehmen in die Millionen gehen. Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) empfiehlt Versicherern daher bereits, Schäden durch PFAS in den Allgemeinen Versicherungsbedingungen zunächst grundsätzlich auszuschließen, um Risiken anschließend im Einzelfall zu bewerten.

Fazit: Wer wartet, zahlt drauf

Für Unternehmen ist jetzt die Zeit zu handeln. Denn wer wartet, zahlt drauf. Und wer jetzt auf fluorfreie Löscher umstellt, schützt nicht nur Umwelt und Gesundheit, sondern auch den eigenen Betrieb vor unnötigen Kosten und rechtlichen Risiken. Denn eines ist gewiss: PFAS gehören nicht in unsere Betriebe – und schon gar nicht in unsere Umwelt. GIT

Hier finden Sie Ausführliche Informationen zum Verbot PFAS-haltiger Schaumlöschmittel inkl. Podcast zum Thema

Minimax Mobile Services GmbH
www.minimax-mobile.com

Die beiden Vertragspakete Comfort und Rent decken unterschiedliche Bedürfnisse ab

FEUERLÖSCHERWARTUNG

Service im Paket

Wartungspakete für Feuerlöscher vorgestellt

Minimax Mobile Services stellt seine neuen Wartungspakete für Feuerlöscher vor. Damit will das Unternehmen ein deutliches Plus an Sicherheit und Service bieten – ohne versteckte Kosten.

Comfort umfasst automatisierte und transparente Wartung, Rent heißt das Mietmodell

Mit Comfort und Rent stellt Minimax Mobile Services zwei Vertragspakete vor, die unterschiedliche Bedürfnisse abbilden und jeweils klar definierte Leistungen bieten:

Comfort umfasst automatisierte, transparente und zuverlässige Wartung. Dieses Paket bietet eine Lösung für die regelmäßige Wartung der Feuerlöscher. Ergänzend zu den regulären Standard-Wartungsleistungen umfasst die Comfort-Variante umfangreiche Inklusivleistungen, wie Fahrtkosten, sonstige wartungsbedingte Services und Ersatzteile, Füllungen sowie Löschmittelentsorgung, und stellt damit ein komplettes Wartungspaket mit voller Kostenkontrolle dar. Dank der automatischen Terminierung behält der Kunde seine Prüfzyklen jederzeit im Blick. Zusätzlich kann er von Rabatten auf Neukauf und von weiteren Services profitieren. Flexible Zahlungsmodelle, wie die jährliche Vorauszahlung mit Rabatt oder die monatliche Zahlungsweise zur gleichmäßigen Verteilung der Raten, runden das Angebot ab. Es richtet sich an Unternehmen, die Wert auf Sicherheit und Effizienz legen.

Bequemes Mieten

Rent heißt das Mietmodell für sorgenfreien Brandschutz. Damit bietet Minimax ein Rundum-sorglos-Paket für Unternehmen, die ihre Feuerlöscher nicht kaufen, sondern bequem mieten möchten. Während der gesamten Mietdauer sind sämtliche Feuerlöscher sowie alle Wartungsleistungen inklusive – ohne versteckte Kosten, wie der Hersteller betont. Die volle Planbarkeit der Ausgaben ermöglicht eine zuverlässige Budgetkontrolle. Bestehende Altgeräte können zu vergünstigten Konditionen entsorgt werden, und auch auf weitere ausgewählte Services gewährt Minimax attraktive Preisnachlässe. Kunden profitieren zudem von einem Preisvorteil bei jährlicher Vorauszahlung oder können alternativ den Betrag bequem auf monatliche Raten verteilen. Die Mindestvertragslaufzeit beträgt 24 Monate.

„Unsere neuen Wartungspakete sind nicht nur transparent und flexibel, sondern auch auf höchste Servicequalität ausgelegt“, sagt Holger Messner, Leiter der Business Unit Feuerlöscher bei der Minimax Mobile Services. „Damit setzen wir neue Standards in der Brandschutzbranche. Unternehmen erhalten nicht nur technische Sicherheit, sondern auch organisatorische Entlastung – und das bei voller Kostenkontrolle.“ GIT

Minimax Mobile Services GmbH
www.minimax.de

GIT SICHERHEIT

INNENTITEL – HEFT IM HEFT | MASCHINENSICHERHEIT

Neue RFID Sicherheitszuhaltung „SLO“

ergänzt bestehendes SMART Safety System

Neues „Gänseblümchen“ hält Türen geschlossen

Die elektronische Zuhaltung SLO ergänzt die „Daisy Chain“ von Bernstein

Die neue Sicherheitszuhaltung SLO („Safety Lock OSSD“) ergänzt das bestehende Smart Safety System des Anbieters für industrielle Sicherheits- und Gehäusetechnik um eine Funktion, die in vielen Maschinen unverzichtbar ist: Das sichere Zuhalten von beweglich trennenden Schutzeinrichtungen wie zum Beispiel Schutztüren und Hauben, solange noch ein Risiko besteht.

Seit Einführung seiner elektronischen RFID-Sensoren (SRF) zur Überwachung von trennenden Schutzeinrichtungen vergleicht Bernstein sein Smart Safety System gerne mit einer Kette aus Gänseblümchen – einer „Daisy Chain“. Jeder Sensor, jeder Not-Halt-Schalter, jede Komponente reiht sich ein, nimmt das Sicherheitssignal auf, ergänzt es um eigene Informationen und reicht es weiter. So entsteht ein durchgängiges System – modular, zuverlässig und platzsparend. Mit dem neuen SLO hält nun eine Zuhaltung Einzug in diese Kette elektronischer Komponenten. Eine „Blüte“, die nicht nur die Tür überwacht, sondern sie auch fest verschlossen hält, solange noch eine Gefahr besteht.

Technische Merkmale

Der SLO ist eine elektromechanische Sicherheitszuhaltung der Bauart 4 nach DIN EN ISO 14119 mit RFID-Codierung und sicherer Zuhaltungsüberwachung. Trotz seiner kompakten Bauform von 30 × 30 × 135 mm bietet er eine Zuhaltekraft von 3000 N und Schutzart IP69. Die Türüberwachung und die Zuhaltungsüberwachung können jeweils, je nach Variante, bis zu Performance Level e (PL e) erreichen, womit sie für anspruchsvolle Anwendungen geeignet sind. Durch variable Codierstufen (gering, hoch, unikat) lässt sich der Manipulationsschutz individuell an die Anforderungen der Anwendung anpassen.

Diagnosefähig und vernetzbar

Wie die anderen Elemente in der Kette ist auch der SLO voll in die Daisy Chain Diagnostic (DCD) eingebunden. Das bedeutet: Jeder SLO überträgt über die bestehende 4- oder 5-polige Leitung seinen Status. Es handelt sich dabei um eine Vielzahl von Informationen wie zum Beispiel, ob die Tür geschlossen, bzw. die Zuhaltung aktiv ist oder ein Fehler vorliegt.

Die Zustandsdaten können per Diagnosegerät über NFC auf ein Smartphone übertragen, mit I/O-Link in die Steuerung eingebunden oder über weitere Module von Bernstein wie SCR P und SCx – per Profinet oder Ethernet an übergeordnete Systeme weitergeleitet werden. Das spart

Die neue Sicherheitszuhaltung SLO ergänzt das bestehende Smart Safety System um eine Funktion, die in vielen Maschinen unverzichtbar ist: Das sichere Zuhalten von beweglich trennenden Schutzeinrichtungen wie zum Beispiel Schutztüren und Hauben, solange noch ein Risiko besteht.

Zeit bei der Inbetriebnahme, vereinfacht die Fehlersuche und ermöglicht die vorausschauende Wartung. Die Predictive Maintenance-Funktion bietet den Nutzern einige Vorteile:

- Ausfallvermeidung: Vermeidung von Kosten durch ungeplante Stillstände
- Wartung nach Bedarf: keine starren Wartungszyklen
- Längere Lebensdauer der Maschinen: Verhinderung von Folgeschäden durch rechtzeitige Wartung
- Höhere Anlagenverfügbarkeit: mehr Produktion, weniger Stillstand

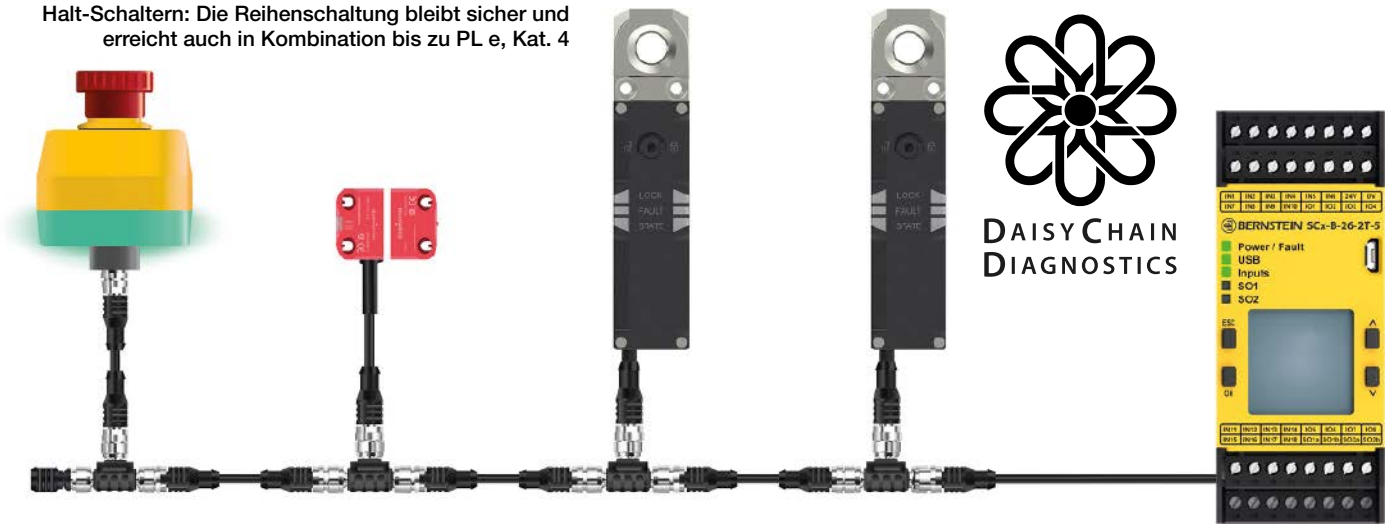
Der SLO lässt sich in Reihe schalten. Ob mit anderen SLOs, SRF-Sensoren oder SEU-Not-Halt-Schaltern: Die Reihenschaltung bleibt sicher und erreicht auch in Kombination bis zu PL e, Kat. 4. So reduziert sich der Verdrahtungsaufwand. Gleichzeitig bleibt die Diagnosefähigkeit jedes einzelnen Elements erhalten.

Vielseitig einsetzbar nach DIN Norm

Der SLO erfüllt eine zentrale Anforderung der DIN EN ISO 14119: Eine Schutztür darf nur dann geöffnet werden, wenn die Gefahr beseitigt ist. Genau dort kommt der SLO zum Einsatz – in Verpackungsmaschinen, Holzbearbeitung, Spritzgussanlagen oder Werkzeugmaschinen. Ob Tür, Klappe oder Haube – wo sichere Zuhaltung erforderlich ist, passt sich der SLO flexibel ein. Mit der Integration des SLO in das bestehende Smart Safety System mit DCD-Diagnose, flexibler Schnittstellenwahl und umfassender Reihenschaltfähigkeit, bietet Bernstein eine sinnvolle Ergänzung für zukunftssichere Sicherheitsarchitekturen an. GIT

Bernstein AG
www.bernstein.eu

Der SLO lässt sich, wie jede Komponente, in Reihe schalten. Ob mit anderen SLOs, SRF-Sensoren oder SEU-Not-Halt-Schaltern: Die Reihenschaltung bleibt sicher und erreicht auch in Kombination bis zu PL e, Kat. 4



TITELTHEMA

Made in Europe, gedacht für Deutschland

Pizzato baut seine Präsenz in Deutschland weiter aus

Im Interview mit GIT SICHERHEIT geben Giuseppe Pizzato, CEO von Pizzato, und Matthias Höhl, Country Sales Manager Deutschland, Einblicke in die aktuelle Entwicklung des italienischen Spezialisten für industrielle Sicherheitstechnik. Sie berichten über das starke Wachstum des Unternehmens, die strategische Bedeutung des deutschen Marktes, neue Innovationen wie die NX-Serie und die Pizzato Academy sowie die Herausforderungen durch europäische Regularien. Das Gespräch beleuchtet, wie Pizzato mit Flexibilität, Kundennähe und „Made in Europe"-Qualität auf die Anforderungen der Branche reagiert.

GIT SICHERHEIT: Herr Pizzato, im großen GIT SICHERHEIT-Interview vor fünf Jahren haben Sie Ihre „Passion for Quality" betont. Was hat sich seither bei Pizzato und an den wirtschaftlichen Rahmenbedingungen verändert – und wie sehen Sie heute die Rolle des deutschen Marktes für Ihr Unternehmen?

Giuseppe Pizzato: Unser Interview fand 2020 kurz vor dem Ausbruch der Pandemie statt. Fünf Jahre sind eine lange Zeit – aber tatsächlich fühlt es sich so an, als wären es zehn gewesen! In unserem Unternehmen hat sich sowohl strukturell als auch wirtschaftlich enorm viel verändert. Im Vergleich zu damals sind wir stark gewachsen. Wir haben vier neue Niederlassungen eröffnet und sind heute mit insgesamt acht Niederlassungen weltweit vertreten. Unser Vertriebsnetz wurde weiter ausgebaut, sodass wir heute eine noch flächendeckendere Präsenz gewährleisten können. Wir haben nicht nur die Covid-Zeit, sondern auch die Chipkrise erfolgreich gemeistert und sind dabei stetig gewachsen.

Aber das ist noch nicht alles: Vor 5 Jahren habe ich Ihnen erzählt, dass wir soeben in unseren neuen 25.000 m² großen Firmensitz in Marostica umgezogen sind. Heute kann ich Ihnen berichten, dass bereits seit einigen Monaten Erweiterungsarbeiten an der Produktion und den Verwaltungsbüros im Gange sind. Parallel zur Erweiterung des Vertriebsnetzes und unseres Hauptsitzes wollten wir außerdem unsere Kunden-

Intelligente und automatisierte Produktion ermöglichen es Pizzato auf höchstem Standard zu fertigen

Giuseppe Pizzato, CEO von Pizzato

Matthias Höhl, Country Sales Manager Deutschland bei Pizzato

betreuung weiterentwickeln – daraus entstand ein völlig neues Projekt: die Pizzato Academy. Die Möglichkeit, fachspezifische Schulungen in unserer Branche anzubieten und die entsprechenden Rechtsvorschriften kompetent zu vermitteln, stellt einen Mehrwert dar, der Teil unserer kontinuierlichen Weiterentwicklung ist. Es ist daher kein Zufall, dass einige unserer erfahrensten Ingenieure seit den letzten Jahren an den wichtigsten technischen Ausschüssen der Branche mitwirken.

Was hingegen unsere Zielmärkte betrifft, so bleibt Deutschland – in einem allgemein von Veränderungen geprägten internationalen Marktumfeld – weiterhin ein sehr wichtiger Markt für Pizzato. Deutschland steht unserem Unternehmen, das sich im Nordosten Italiens befindet, kulturell und geographisch nahe. Der deutsche Markt ist außerdem ein Schlüsselmarkt und gilt in Europa als Maß der Dinge, wenn es um Industrie und Automatisierung geht. Genau deshalb sieht Pizzato es als einen Markt von grundlegender Bedeutung und plant auch künftig weiter in dieses Land zu investieren.

Herr Höhl, als Country Sales Manager, sind Sie seit April diesen Jahres das neue Gesicht von Pizzato in Deutschland. Was hat Sie persönlich dazu bewegt, zu Pizzato zu wechseln? Was fasziniert Sie an diesem Unternehmen, insbesondere im Vergleich zu deutschen Herstellern?

Matthias Höhl: Pizzato ist ein Unternehmen, das mir schon früher positiv aufgefallen ist. Dabei habe ich schnell festgestellt, dass Innovation, Flexibilität und Qualität einen Einklang hat. Zudem haben mich die Produktreihen aus der Arbeitssicherheit und deren Vielfalt imponiert und begeistert. Hier hat Pizzato in den letzten Jahren richtig Gas gegeben und zugelegt und Produkte entwickelt, die an der Spitze der Technologie rund um die Maschinensicherheit stehen. Das Design, die einfache Bedienung und Funktionalitäten spielen hier auch eine sehr große Rolle. Pizzato kann sich unkompliziert auf unterschiedliche Märkte schnell und gezielt einstellen. Das sind alles Voraussetzungen für den internationalen Markt und damit auch für den deutschen Markt. Einige Hersteller versuchen deutsche Produkte international zu vermarkten, erlauben aber nicht die lokalen Bedürfnisse und Anforderungen zuzulassen. Das ist bei Pizzato anders, hier sieht man den deutschen Markt und versucht Produkte für dessen Bedürfnisse anzubieten und entsprechend zu konfigurieren. Pizzato ist aber nicht nur ein Technologie getriebenes, sondern auch ein sehr stark Mitarbeiter orientiertes Unternehmen. Es macht mich stolz ein Teil dieses Teams zu sein.

Welche Vorteile bietet eine deutsche Pizzato-Filiale direkt vor Ort für deutsche Kunden? Wie können Sie und Ihr Team sie unterstützen und etwas bewirken?

Matthias Höhl: Unser oberstes Ziel ist es, stets nah am Kunden zu sein. Mit unserem Team in Deutschland verstehen wir die Bedürfnisse und Anforderungen unserer Kunden viel besser. Meine Berufserfahrung zeigt mir, dass man im jeweiligen Land präsent sein muss, um als wertvolles und engagiertes Unternehmen auf dem lokalen Markt wahrgenommen zu werden. Wir leben in einer sich schnell verändernden Welt, in der sich Technologien und Vorschriften, insbesondere Normen in der Sicherheitstechnik, ständig ändern. Hier möchten wir nah dran sein und unsere Kunden direkt mit den neuesten Trends und Technologien unterstützen. Darüber hinaus bieten wir unsere Pizzato Academy an, in der Kunden im Selbststudium mehr über unsere Produkte und Dienstleistungen erfahren können.

Was unterscheidet Pizzato als europäisches Unternehmen von anderen Anbietern – insbesondere im Hinblick auf Werte, Innovationskraft und das Preis-Leistungsverhältnis?

Giuseppe Pizzato: Beginnen wir mit den Fakten: Während der Chipkrise der vergangenen Jahre ist es Pizzato gelungen, den Anforderungen seiner Kunden gerecht zu werden und dabei Produktions- und Lieferkontinuität aufrechtzuerhalten. Außerdem konnten wir auf die Anfragen jener Kunden reagieren, die bei anderen Lieferanten kein Material beschaffen konnten. Diese Tatsache haben wir den Werten zu verdanken, auf denen unser Unternehmen aufgebaut ist: Flexibilität, vollständige Kontrolle der Produktionsprozesse und Innovationsfähigkeit. Unser Unternehmen konnte zum Beispiel einige unserer wichtigsten Sicherheits-Produkte intern und in sehr kurzer Zeit überarbeiten und so dem Problem fehlender Teile am Markt entgegenwirken.

Bitte umblättern ▶

Bei der NX Serie, handelt sich nach Angaben von Pizzato um den weltweit kleinsten RFID-Sicherheits-Schalter mit Zuhaltung in Bezug auf das Volumen

So konnten und können wir bis heute unseren Kunden Stabilität und Kontinuität bieten – auch im Hinblick auf das Preis-Leistungsverhältnis.

Matthias Höhl: Unternehmenswerte schaffen eine authentische Unternehmenskultur und sind maßgebend der Richtungsweiser für Entscheidungen, Kommunikation und Zusammenarbeit. Werte sind eine solide Grundlage für das Kundenvertrauen und ganz speziell unsere stets angestrebte Kundenzufriedenheit. Wir möchten die Kundenbedürfnisse verstehen und sind bestrebt hier innovative Lösungen im entsprechendem Preis-Leistungsverhältnis in enger Zusammenarbeit zu finden. Hierfür muss man flexible, innovativ und auch offen sein. Und das sind wir.

Die Herkunft von Produkten „Made in Europe“ gewinnt auch mit Blick auf die Entwicklungen in Asien und den USA immer mehr an Bedeutung. Wie begegnen Sie diesem Trend und wie positioniert sich Pizzato in diesem Kontext?

Giuseppe Pizzato: Die Welt verändert sich ständig. Die globale Marktsituation ist komplex und aufgrund der anhaltenden Handelskonflikte besonders instabil. In diesem sich wandelnden und von Unsicherheit geprägten Umfeld sind wir überzeugt, dass Europa weiterhin wesentliche Werte bewahrt – Werte, die dank der Arbeit der Hersteller, die Mehrwert und Innovation schaffen, langfristig für die nötige Stabilität sorgen können. Vor diesem Hintergrund müssen Unternehmen zunehmend flexibler werden und sich an die verschiedenen Rahmenbedingungen und Marktgegebenheiten anpassen können.

Matthias Höhl: Durch die geopolitischen Gegebenheiten wird „Made in Europe“ für europäische Maschinenhersteller ein Teil der Entscheidungen in der Lieferantenauswahl sein. Es gibt ihnen eine Qualitäts- und Transparenzgarantie, die durch strenge europäische Standards und Vorschriften gewährleistet wird. Es fördert zudem den Zugang zu einem großen Binnenmarkt, stärkere Lieferantenbindungen und fördert das Image von Qualität und Ethik. Produkte aus Europa stehen für eine robuste und zunehmend innovative Produktionsbasis und darauf setzen wir. Pizzato produziert ausschließlich in Europa und bezieht seine Materialien und Komponenten überwiegend von dort. Intelligente und automatisierte Produktion ermöglichen es uns, auf höchstem Standard zu fertigen. Zudem sind wir krisensicher in Bezug auf Materialverfügbarkeit aufgestellt. Wir, Pizzato, möchten unseren Teil in Bezug auf „Made in Europe“ dazu beisteuern.

Neue europäische Regularien wie die Maschinenverordnung (MVO) und der Cyber Resilience Act (CRA) stellen die Branche vor Herausforderungen. Wie ist Pizzato produktseitig darauf vorbereitet?

Giuseppe Pizzato: Es handelt sich um wichtige Verordnungen und Richtlinien, die angesichts der aktuellen Ereignisse notwendig und nützlich sind. Als Unternehmen gehen wir solche Themen ernsthaft und konkret an. Wir statten das Unternehmen mit dem Personal und den Werkzeugen aus, die für die Erlangung zukünftiger Cybersicherheitszertifizierungen für unsere Produkte erforderlich sind, und zwar auf die gleiche Weise, wie wir die elektrische und funktionale Sicherheit angehen.

Gibt es aktuelle Produktneuheiten oder Innovationen, die Sie besonders hervorheben möchten – etwa im Bereich Manipulationsschutz oder bei der Entwicklung der „kleinsten Zuhaltung im Markt“?

Giuseppe Pizzato: Ein hervorragendes Beispiel für Innovation ist unsere Serie NX. Es handelt sich hierbei um den weltweit kleinsten RFID-Sicherheits-Schalter mit Zuhaltung in Bezug auf das Volumen. Dies war eine bedeutende technologische Herausforderung, die wir gemeistert haben, indem wir ein Produkt mit den höchsten Sicherheits-Niveaus PL e und SIL 3 bei äußerst reduziertem Volumen umgesetzt haben. Etwa ein Jahr nach Produktionsbeginn können wir nun sagen, dass unsere Kunden sehr zufrieden sind und wir dieses Produkt stetig weiterentwickeln. Auf der diesjährigen SPS-Messe werden wir die Ausführung mit sämtlichen äußeren Metallteilen aus Edelstahl AISI 316L präsentieren.

Ein weiteres innovatives Produkt, das es bisher am Markt nicht gab und das aus unserer jahrzehntelangen Erfahrung im Bereich der industriellen Sicherheit hervorgegangen ist, ist die Serie der Sicherheits-Module CS AM für die Überwachung von Stillständen, Drehzahl und Drehrichtung des Motors: Kunden können mit einer speziellen Software die Abläufe in Echtzeit verfolgen und so die nötigen Parameter optimal einstellen.

Pizzato auf der SPS 2025:
Halle 7, Stand 290

Pizzato Elettrica S.r.l.
www.pizzato.com

Gesamte B&R-Produktentwicklung nach IEC 62443-4-1 zertifiziert

B&R, die Machine Automation Division von ABB, hat für seine gesamte Produktentwicklung die Zertifizierung nach IEC 62443-4-1 erhalten. Dieses Audit, durchgeführt vom TÜV Rheinland, bestätigt: B&Rs Entwicklungsprozesse erfüllen den international anerkannten Standard für sichere Produktentwicklung in der industriellen Automatisierung. Die Zertifizierung gilt für alle Produktgruppen und Entwicklungsteams bei B&R und ist ein Beleg dafür, dass Cybersicherheit über den gesamten Entwicklungszyklus hinweg integriert ist – von Spezifikation und Design bis hin zu Implementierung, Prüfung und Wartung. Der besonders sicherheitskritische Bereich Softwareentwicklung wurde mit dem Reifegrad „Maturity Level 3“ ausgezeichnet – einem der höchsten innerhalb des internationalen Standards IEC 62443-4-1. „Software ist heute von strategischer Bedeutung in der Automatisierung,“ sagt Florian Schneeberger, Chief Technology Officer bei B&R.

www.br-automation.com

Erweiterungsmodul für Funktionale Sicherheit

Herzstück des nur 17,5 mm schmalen Erweiterungsmoduls RK 6929 der Safemaster-Serie ist das Sicherheitsrelais OA 5642 von Dold, das aufgrund seiner zwangsgeführten Kontakte nach IEC 61810-3 auch Anwendungsfelder im Bereich der Funktionalen Sicherheit eröffnet, beispielsweise im Maschinen- und Anlagenbau als auch in Anwendungen für Feuerungsanlagen nach EN 50156-1. Für den Einsatz im Anwendungsbereich von EN 61010-1 sind die Luft- und Kriechstrecken des Erweiterungsmoduls RK 6929 zwischen Netzstromkreisen und berührbaren Spannungen sowie Netzstromkreisen untereinander entsprechend doppelter Isolierung bemessen. Übersteigt die Stromaufnahme nachgeschalteter Aktoren die Leistung des Ausgangs einer Sicherheitssteuerung oder eines Lichtgitters, schaltet das Erweiterungsmodul diese Aktoren über seine Relaiskontakte zuverlässig und potentialfrei.

www.dold.com

Sicherheitslaserscanner RSL 200 von Leuze auf der SPS

Ultra-kompakt, vielseitig, zukunftsweisend: Die Sensor People von Leuze präsentieren auf der SPS 2025 den kleinsten Sicherheitslaserscanner am Markt sowie weitere Highlights für die industrielle Automatisierung. Der RSL 200 sichert Maschinen, fahrerlose Transportsysteme und Roboter. Dank minimaler Abmessungen lässt er sich auch bei wenig Platz sehr einfach integrieren. Am neu konzipierten Messestand präsentieren die Sensor People von Leuze außerdem mehr als 20 weitere innovative Lösungen aus der Welt präziser Sensorik und zuverlässiger Sicherheitstechnik. Neu in diesem Jahr: täglich vier Expertentalks am Leuze Stand. Im Fokus stehen aktuelle Branchenthemen wie der neue RSL 200, die Maschinenrichtlinie, Auto-ID-Lösungen (RFID, 1D- und 2D-Codes), Security in der Automatisierung und innovative Gesamtlösungen.

SPS: Halle 7A, Stand 230 **www.leuze.com**

© © Schütte

Mit den Schleifmaschinen von Schütte lassen sich komplexe Werkzeuge, beispielsweise Bohrer oder Fräser, aber auch Medizinalprodukte wie zum Beispiel Knie- oder Hüftimplatate herstellen

ASi macht Schleifmaschinen smarter

Mehr Sicherheit und Flexibilität dank dezentraler Peripherie und IO-Link-Integration mit Bihl+Wiedemann

AS-Interface hat bei der Schütte Schleiftechnik GmbH eine lange Tradition. Gestartet mit der Verdrahtung von Ventilen und Standardsensorik, realisiert Schütte mittlerweile neben der Anbindung der gesamten dezentralen Peripherie in seinen Schleifmaschinenserien 105linear, 330linear und 335linear auch die komplette Sicherheitstechnik mit ASi und ASi Safety Lösungen von Bihl+Wiedemann. Auch die Zukunft hat man bei Schütte mit der Integration von IO-Link Sensoren über ASi-5 im Blick.

Die Firma Alfred H. Schütte ist ein deutscher Werkzeugmaschinenhersteller mit Sitz in Köln. Zum Produktspektrum gehören Mehrspindel-Drehautomaten und 5-Achsen-CNC-Schleifmaschinen. Das 2007 gegründete Tochterunternehmen Schütte Schleiftechnik GmbH entwickelt und produziert hochpräzise Schleifmaschinen und Schleiflösungen für die metallverarbeitende Industrie und zählt zu den führenden Experten in der Schleiftechnologie. Das Produktportfolio umfasst Maschinen für verschiedene Anwendungen wie Werkzeug- und Formenbau, Medizinaltechnik, Automobilindustrie und Luftfahrt.

Schleifmaschinen von Schütte

Die Schütte Schleiftechnik GmbH bietet Schleifmaschinen der Baureihen 105linear, 330linear und 335linear an. Während die 105linear als kompakte Produktionsmaschine mehr auf die Herstellung von komplexen Werkzeugen, beispielsweise Bohrern oder Fräsern, in großen Stückzahlen und hohen Genauigkeitsanforderungen ausgelegt ist, handelt es sich bei der 330er Baureihe, insbesondere der 335linear, um Universalschleifmaschinen mit fünf Achsen, mit denen sich alle Anforderungen für die Produktion und das Nachschleifen von Werkzeugen jeglicher Art realisieren lassen. Darüber hinaus können damit auch Medizinalprodukte wie zum Beispiel Knie- oder Hüftimplantate hergestellt werden. Beide Baureihen sind mit einer Vielzahl von Automatisierungsoptionen für eine kontinuierliche Anpassung und Erweiterung verfügbar.

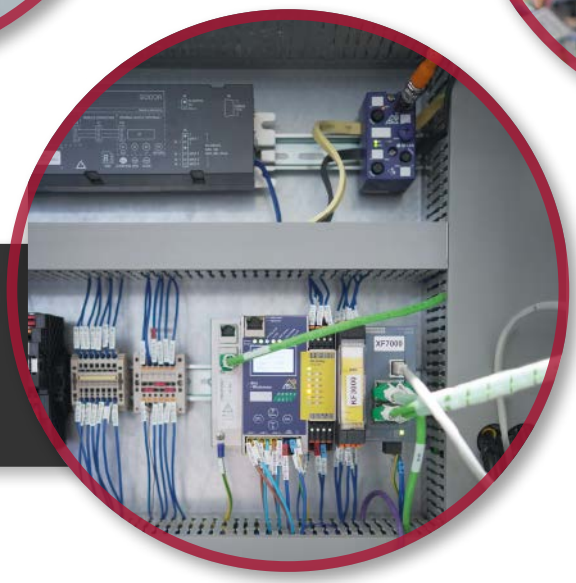
Entscheidung für AS-Interface bei Schütte

Die Historie von AS-Interface bei Schütte reicht zurück bis ins Jahr 1998. Damals wurden im Rahmen der Entwicklung der 300er Baureihe erstmals ASi Komponenten eingesetzt – ASi Ventilinseln und Endschalter von pneumatischen Ventilen.

Im Laufe der 25 Jahre nach Einführung von AS-Interface hat die Komplexität der Schleifmaschinen bei Schütte stetig zugenommen. Deutlich geworden ist das insbesondere im Bereich der Sicherheitstechnik, die in dieser Zeit weiterhin hardwaremäßig in den Schaltschrank verdrahtet wurde. Durch die guten Erfahrungen mit ASi im Standardbereich hat man sich bei Schütte deshalb im Jahr 2013 entschlossen, ab diesem Zeitpunkt auch alle Sicherheitsfunk-

ASi 4E/4A Module von Bihl+Wiedemann

Aktiver Verteiler ASi Safety BWU3373 von Bihl+Wiedemann für die Integration von Sicherheitsschaltern in das ASi Netzwerk



Für die Nutzung von Prozessdaten können IO-Link Sensoren einfach über ASi-5 Module mit integrierten IO-Link Mastern (oben) und ASi-5/ASi-3 Safety Gateways (unten) von Bihl+Wiedemann in bestehende ASi Netzwerke integriert werden

tionen wie Türverriegelungen mit Zuhaltung, berührungslose Sicherheitstechnik oder Not-Halt-Kreise über ASi Safety at Work zusammen mit Bihl+Wiedemann zu realisieren.

Schütte profitiert von vielen ASi Vorteilen

Die Entscheidung für ASi und ASi Safety sowie die Tatsache, dass beim Einsatz von AS-Interface für Sicherheits- und Standardapplikationen eine gemeinsame Infrastruktur, ein gelbes ASi Profilkabel, verwendet werden kann, hat für Schütte viele Vorteile.

Ein Punkt war das einfache Anschlusskonzept von AS-Interface. Module können bei ASi ohne Stecker und vorkonfektionierte Kabel einfach per Durchdringungstechnik dezentral in der Maschine genau dort an das gelbe Profilkabel „aufgeschraubt" werden, wo sie gerade benötigt werden.

Aus der kompletten Anbindung der dezentralen Peripherie über AS-Interface ergibt sich für Schütte ein weiterer Vorteil. Die Schleifmaschinen können unabhängig von der verwendeten Steuerungstechnik effizienter gebaut werden. Die Ausstattung des jeweiligen Maschinenkörpers wird dabei durch die zukünftige Funktionalität bestimmt. Welche Steuerung – Siemens Sinumeric One oder NUM Flexium+ – am Ende eingesetzt wird, ist an dieser Stelle für die Montage unerheblich. Die Anbindung an eine der beiden Varianten erfolgt erst im Schaltschrank über die Auswahl eines entsprechenden ASi Safety Gateways, die Bihl+Wiedemann mit Schnittstellen zu vielen verschiedenen (sicheren) Feldbussen anbietet.

Und schließlich ist eine Lösung mit AS-Interface für Schütte nicht nur technologisch, sondern auch aus Kosten- und Effizienzgründen interessant.

ASi-5 und IO-Link

Schütte entwickelt seine Schleifmaschinen stetig weiter. Um die Maschinen noch effizienter und präziser zu machen und deren Funktionsumfang zu erweitern, setzt das Unternehmen künftig auf die Integration von IO-Link.

Über diese Sensoren werden eine Vielzahl von Prozessdaten an verschiedenen Stellen in der Maschine erfasst und für erweiterte Diagnosen und Predictive Maintenance zur Verfügung gestellt. Für Schütte ist es zum Beispiel wichtig, dass die Maschinen in einem thermischen Gleichgewicht sind. So muss im Bereich der Kühlschmierstoffanlagen, die sehr aufwendig und energieintensiv sind, ein konstantes Temperaturniveau herrschen. Mögliche Defekte oder falsche Einstellungen etwa eines Kühlers, die bisher nicht nachweisbar waren, können mit Hilfe von IO-Link Temperatursensoren erkannt, diagnostiziert und behoben werden. Ein weiterer Vorteil, die komplette dezentrale Peripherie in der Maschine über AS-Interface anzubinden. Denn für die Integration von IO-Link Sensoren über ASi-5 muss am bestehenden Maschinenkonzept kaum etwas geändert werden. GIT

Autor:
Thomas Rönitzsch
Bihl+Wiedemann GmbH, Mannheim

Bihl+ Wiedemann auf der SPS: Halle 7, Stand 200+201

Bihl+Wiedemann GmbH
www.bihl-wiedemann.de

„Die SPS als ermutigendes Signal“

Im Gespräch: Sylke Schulz-Metzner, Vice President SPS bei der Mesago Messe Frankfurt

Warum die SPS zum Ende eines wirtschaftlich wenig erfreulichen Jahres ein Lichtblick ist, welche neuen Märkte sich auftun könnten und wie die Messe zeigen will, welche Chancen sich durch den Einsatz von KI in der Industrie ergeben. Im Gespräch mit Sylke Schulz-Metzner.

GIT SICHERHEIT: Frau Schulz-Metzner, das sind doch gute Nachrichten: Auf der SPS werden dieses Jahr 1.150 Aussteller erwartet, also rund 40 mehr als im vergangenen Jahr. Wie kommt das und welche weiteren Entwicklungen der Messe stimmen außerdem positiv?

Sylke Schulz-Metzner: Dass die SPS auch in wirtschaftlich herausfordernden Zeiten ihre zentrale Bedeutung für die Automatisierungsbranche bewahrt, ist für die gesamte Branche ein wichtiges und ermutigendes Signal. Der Besuch der Messe bietet wie gewohnt einen umfassenden Überblick über alle aktuellen Produkte und Entwicklungen in der industriellen Automatisierung. Zudem gibt er einen Ausblick darauf, welche Technologien und Trends morgen den Stand der Technik prägen werden.

Wo sehen Sie ganz klar den USP der SPS?

Sylke Schulz-Metzner: Der USP der SPS – Smart Production Solutions liegt in ihrem sehr klaren Fokus. Sie bildet den Markt der smarten und digitalen Automatisierung vollumfänglich ab, das heißt mit allen relevanten Herstellern und ihren Produkten und Lösungen. Besucher erhalten so einen umfassenden Überblick und finden Raum für intensiven fachlichen Austausch, um die besten Lösungen für ihre anstehenden Automatisierungsaufgaben zu entdecken.

Welche Pläne gibt es, die SPS – Smart Production Solutions weiterzuentwickeln?

Sylke Schulz-Metzner: Die Weiterentwicklung der Messe ist bei uns ein kontinuierlicher Prozess. Wir sind mit unseren Kunden im Gespräch und hören zu, wenn beispielsweise neue Themen oder Anforderungen für die SPS formuliert werden. So prüfen wir jedes Jahr, inwieweit eventuelle Anpassungen sinnvoll sind, um die Messe weiterhin so relevant und attraktiv für die Branche zu halten.

Die Industrie befindet sich in einer Phase der Konsolidierung. Wie wirkt sich das auf die Automatisierungsbranche und die Messe aus?

Sylke Schulz-Metzner: Die Industrie und mit ihr die Automatisierungsbranche durchlebt derzeit ein wirtschaftlich schwieriges Jahr mit sich verändernden Märkten. Wann eine Trendwende zurück auf einen Wachstumskurs führt, lässt sich aktuell nicht verlässlich vorhersagen. Gerade vor diesem gesamtwirtschaftlichen Hintergrund setzt die SPS ein starkes Zeichen: Sie bietet wie gewohnt ein umfassendes Angebot mit allen führenden Anbietern. Dies unterstreicht sehr nachdrücklich, dass zum einen die SPS eine sehr hohe Bedeutung für die Automatisierungsanbieter hat, zum anderen, dass die Automatisierung eine Enabling-Technologie für die industrielle Produktion bleibt.

China verliert an Dynamik als Exportmarkt – wie verändert sich dadurch die internationale Ausrichtung der SPS? Inwieweit sind chinesische Aussteller in Nürnberg vertreten?

Sylke Schulz-Metzner: Ob China seine Dynamik als Exportmarkt verliert, ist eine komplexe Frage, die wirtschaftliche, geopolitische und strukturelle Faktoren enthält. Zu sehen sind aktuell Anzeichen für eine Abschwächung durch zum Beispiel eine geringere Nachfrage in westlichen Märkten, geopolitische Einflüsse, Überkapazitäten oder auch Herausforderungen in der chinesischen Binnenwirtschaft. China bleibt aber weiterhin ein wichtiger Akteur auf dem Weltmarkt. Dies zeigt sich auch am wachsenden Interesse chinesischer Aussteller auf der SPS, die mit ihren Produkten neue Märkte erschließen und sich dem internationalen Wettbewerb stellen möchten.

Welche Rolle spielen neue Märkte wie Indien für die Automatisierungsbranche und die Messe?

Sylke Schulz-Metzner: Indien ist ein BRIC-Staat und ein zunehmend wachsender Markt. Es entwickelt sich strategisch in mehreren Schlüsselbereichen, die für die Automatisierung relevant sind. Mit dem Ziel, die Produktivität zu steigern oder die Fertigungsqualität zu verbessern, beginnt die indische Industrie zum Beispiel im Automotiv- oder Pharmabereich mit der Einführung von Automatisierungslösungen. Zusätzlich

verlagern viele Unternehmen Teile ihrer Produktion von China nach Indien und bringen dabei Automatisierungstechnologien mit. Auch als Software- und KI-Standort für Automatisierung wird Indien immer relevanter. Diese Entwicklung wird sicher den Anteil von Besuchern aus Indien, die sich bei der SPS informieren wollen, deutlich erhöhen.

Wie gelingt es der SPS, sowohl etablierte Unternehmen als auch Start-ups und junge Talente zu integrieren?

Sylke Schulz-Metzner: Die SPS ist die ideale Messe für alle Anbieter von Automatisierungsprodukten und -lösungen. Das belegen auch die rund 1.150 Aussteller in diesem Jahr. Um insbesondere Start-ups den Einstieg und die Teilnahme zu vereinfachen, bieten wir zwei Gemeinschaftsstände an. Damit ermöglichen wir jungen Unternehmen eine unkomplizierte und kostengünstige Präsenz auf der Messe. Gleichzeitig möchten wir gezielt junge Talente wie Auszubildende, Studierende, Absolventen und Berufseinsteiger für die SPS begeistern. Dafür gibt es verschiedene Aktionen, etwa den täglich stattfindenden Makeathon oder den Young Talents Day am dritten Messetag mit geführten Touren zu verschiedenen Unternehmen und eine Karriereberatung. So schaffen wir attraktive Angebote für die nächste Generation der Automatisierungsbranche.

Die Technology Stage in Halle 3 widmet sich unter anderem Industrial AI und einer nachhaltigen Produktion. Welche Impulse erwarten Sie von diesem Format?

Sylke Schulz-Metzner: Unser Fokusthema Industrial AI spielt auf den insgesamt vier Stages eine wichtige Rolle. Dort wird ein umfangreiches Vortragsprogramm geboten, das dem Wissenstransfer und der Informationsgewinnung dient. Ganz besonders intensiv wird das Thema Industrial AI auf der Technology Stage am zweiten Messetag behandelt. Gemeinsam mit dem VDMA und dem ZVEI wurde dafür ein hochkarätiges Programm zusammengestellt, das gezielt auf die Bedürfnisse der Fachbesucher eingeht, mit Vorträgen, Podiumsdiskussionen und Präsentationen. Hier können sich Interessenten umfassend informieren, je nach individuellem Bedarf.

Inwieweit ist Industrial AI bereits in der industriellen Praxis angekommen?

Sylke Schulz-Metzner: Industrial AI ist per se nichts Neues – in der Industrie werden KI-Algorithmen, wenn auch eher im Verborgenen, seit Jahren eingesetzt. Mit Chat GPT hat das Thema in der öffentlichen Wahrnehmung allerdings einen ganz neuen Stellenwert bekommen, der auch stark auf die Industrie ausstrahlt. Heute setzen sich die Unternehmen intensiv mit der künstlichen Intelligenz für alle möglichen Einsatzfälle auseinander. KI wird zunehmend zum zentralen Baustein und Treiber der digitalen Transformation in der Fertigung. Ihr Einsatz in der Industrie bietet Kostenersparnis, Wettbewerbsvorteil, eine höhere Produktivität. Ergo: Um den Besuchern der Messe ein breites Informationsangebot zu Einsatzmöglichkeiten von AI in der Industrie zu bieten, stellen wir das Thema auf der diesjährigen Messe auch ganz besonders in den Fokus.

Wie unterstützt die SPS den Transfer von Schlüsseltechnologien wie KI, digitalen Zwillingen und IT-Security in die industrielle Praxis?

Sylke Schulz-Metzner: Lassen Sie mich beim Beispiel von Industrial AI bleiben: Das Thema gewinnt zunehmend an Bedeutung. Uns geht es uns nicht nur darum, KI auf der SPS sichtbar zu machen, sondern auch darum, sie verständlich zu vermitteln. Wir möchten Hemmschwellen abbauen und zeigen, welche Chancen sich durch den Einsatz von KI in der Industrie ergeben.

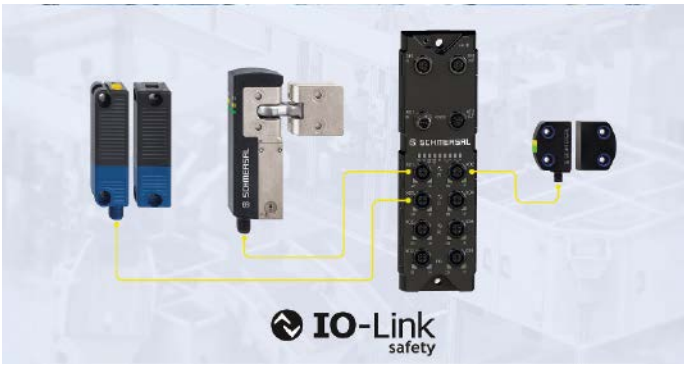
Die Aussteller haben auf der Messe die Möglichkeit, ganz konkret zu zeigen, welche Anwendungen in der Industrie bereits heute mit KI realisierbar sind. Dabei wird deutlich, wie stark sich Prozesse durch den Einsatz von KI optimieren lassen. Die Effizienzsteigerungen, die damit möglich sind, können die Aussteller den Besuchern sehr anschaulich vermitteln. GIT

Mesago Messe Frankfurt GmbH
https://sps.mesago.com

Intelligent vernetzte Sicherheit

Schmersal auf der SPS 2025: Neues IO-Link Safety-System für die nahtlose Kommunikation

Vernetzte Anlagen, flexible Fertigungsprozesse und digitale Technologien setzen neue Maßstäbe und stellen die Maschinensicherheit vor völlig neue Herausforderungen. Auf der SPS 2025 in Nürnberg zeigt die Schmersal Gruppe, wie sich Sicherheitstechnik intelligent vernetzen lässt, um Effizienz und Produktivität zu steigern ohne dabei das Thema Sicherheit außer Acht zu lassen.



Mit der Markteinführung des Sicherheitssensors RSS362 (rechts) und die Sicherheitszuhaltung AZM42 (links daneben) setzt Schmersal neue Maßstäbe in der IO-Link-Safety-Integration

Schmersal bietet im TwinStore 4-D-Modelle an, die über ein Real-time-Target an eine reale Steuerung angeschlossen werden können. Die virtuelle Inbetriebnahme von Maschinen wird so simuliert

Mit dem neuen IO-Link Safety-System präsentiert das Unternehmen eine intelligente Verbindung von funktionaler Sicherheit und Datentransparenz. Die nahtlose Kommunikation zwischen Maschine und Steuerung reduziert Stillstandszeiten und steigert somit die Effizienz. Mit der geplanten Markteinführung der Sicherheitszuhaltung AZM42 und des Sicherheitssensors RSS362 gegen Ende des ersten Halbjahres 2026 wird ein weiterer Meilenstein für IO-Link-Safety-Anwendungen gesetzt. Damit zählt die Firma zu den Pionieren der IO-Link-Safety-Integration. Beide Geräte erweitern das IO-Link-Safety-Installationssystem für industrielle Sicherheitsanwendungen und bieten eine bidirektionale, sichere Kommunikation über eine 3-adrige Leitung. Damit lassen sich sichere Anwendungen bis Performance Level e, Kategorie 4 bzw. SIL 3 realisieren und flexibel in bestehende Anlagen integrieren.

Das tec.nicum zeigt auf der SPS 25 praxisnahe Lösungen für Maschinen- und Anlagensicherheit, Digitalisierung und Outsourcing

Digitaler Zwilling mit neuen Möglichkeiten

Schmersal erweitert sein digitales Portfolio um realitätsnahe 4D-Modelle sicherheitstechnischer Komponenten und schafft somit mehr Möglichkeiten für die virtuelle Maschinenplanung. Mit digitalen Zwillingen der Sicherheitszuhaltung AZM40, des Türgriffsystems DHS und des Bedienfelds BDF40 lassen sich sicherheitsrelevante Funktionen detailgetreu simulieren und in digitale Entwicklungsprozesse integrieren. Nennenswert ist hier ebenso die Veröffentlichung des AZM40-Modells im „TwinStore“, einem Online-Marktplatz für sofort einsetzbare 4D-Simulationsmodelle. Diese Innovation ermöglicht eine effizientere Planung, virtuelle Inbetriebnahme und praxisnahe Schulung und schafft somit den Schritt in Richtung Industrie 4.0.

Neue Services

Die Dienstleistungssparte tec.nicum präsentiert KI-gestützte Sicherheitsüberwachung, digitale Lockout-Tagout-Prozesse sowie innovative Tools zur Energieoptimierung. In Kombination mit Augmented Reality-Anwendungen zeigen die Experten, wie sich Prozesse sicherer, effizienter und zukunftsfähig gestalten lassen. GIT

Schmersal auf der SPS 2025:
Halle 9, Stand 460

K.A. Schmersal GmbH & Co. KG
www.schmersal.com · www.tecnicum.com

BHE-Fachsymposium

Die Sicherheits-Profis!

BHE Bundesverband
Sicherheitstechnik e.V.

Einbruchschutz

9./10. Februar 2026

Kongresszentrum Hotel Esperanto, Fulda

Ausstellung ◆ Vortragsprogramm ◆ Networking

Neuheiten und Trends in Sachen Einbruchschutz für:

- Errichter, Planer- und Ingenieurbüros sowie Hersteller
- Sicherheitsbeauftragte von Anwendern, z.B. Banken, Logistik, Flughäfen, Krankenhäuser
- Versicherer
- Notruf- und Serviceleitstellen
- Behördenvertreter

Anmeldung und Programm beim BHE (Telefon 0 63 86 / 92 14-28)

… oder unter **www.bhe.de/fachsymposium-einbruchschutz**

Wasserstoff marsch!

Explosionsschutz trifft Energiewende

Als Pionier im Explosionsschutz begleitet Pepperl+Fuchs seit Jahrzehnten industrielle Wasserstoffanwendungen. Mit dem Aufschwung der Wasserstoffwirtschaft verändern sich die Anforderungen: Dezentrale, mobile und modulare Anlagen verlangen nach flexiblen, zertifizierten Lösungen. Im Interview mit GIT SICHERHEIT erläutert Alexander Aust, wie das Unternehmen sein Portfolio weiterentwickelt hat – von überdruckgekapselten Steuerungen bis hin zu eigensicheren Mobilgeräten – und welche Rolle Technologien wie die Überdruckkapselung in der Praxis spielen. Ein Gespräch über Sicherheit, Automatisierung und die Zukunft der Wasserstoffwirtschaft.

Alexander Aust, Product Marketing Manager bei Pepperl+Fuchs

GIT SICHERHEIT: Herr Aust, das Thema Explosionsschutz gehört praktisch zur DNA von Pepperl+Fuchs. Auch das Bereitstellen von Produkten und Lösungen für Wasserstoff-Anwedungen spielt dabei schon lange eine Rolle. Durch die Energiewende und den beginnenden Aufbau einer Wasserstoffwirtschaft haben sich jedoch die Applikationen verändert. Um welche Änderungen handelt es sich dabei und welche konkreten Anpassungen waren dennoch notwendig, um diesen gerecht zu werden?

Alexander Aust: Pepperl+Fuchs begleitet den Umgang mit Wasserstoff schon seit Jahrzehnten – etwa in der Chemie und Petrochemie, wo das Gas als Prozessmedium oder Nebenprodukt vorkommt. Mit dem Hochlauf der Wasserstoffwirtschaft hat sich der Fokus jedoch deutlich verschoben: Heute entstehen zunehmend dezentrale, modulare und mobile Anwendungen – von der Erzeugung über die Verdichtung und Speicherung bis hin zur Nutzung in Brennstoffzellen oder Tankstellen. Diese Strukturen stellen andere Anforderungen an Sicherheit, Flexibilität und Wartung.

Daraus ergeben sich auch neue Aufgaben für den Explosionsschutz. Pepperl+Fuchs hat sein Portfolio daher gezielt erweitert: Neben bewährten Komponenten bietet das Unternehmen heute auch vorkonfigurierte Systemlösungen, überdruckgekapselte Steuerungen und kompakte Gehäuselösungen für den Ex-Bereich. Ergänzt wird dies durch eigensichere Mobilgeräte, mit denen sich Anlagen sicher bedienen und Zustände im Feld direkt erfassen lassen. Ziel ist es, den Explosionsschutz nahtlos mit moderner Automatisierungs- und Kommunikationstechnik zu verbinden – für mehr Sicherheit und Effizienz entlang der gesamten Wasserstoff-wertschöpfungskette.

Eine beispielhafte GDRM (Gasdruck-regel- und Mess-) Anlage für den Betrieb mit Wasserstoff mt Pepperl+Fuchs Produkten und Lösungen. Diese regelt und misst den Druck des Gases um eine sichere und konstante Versorgung zu gewährleisten

Welche Rolle spielen Technologien wie die Überdruckkapselung in aktuellen Wasserstoffanwendungen, und wo sehen Sie deren größten Nutzen?

Alexander Aust: Die Zündschutzart Überdruckkapselung, also Purge and Pressurization, hat in vielen Wasserstoffanwendungen aufgrund ihrer Flexibilität eine wichtige Rolle eingenommen. Sie ermöglicht den sicheren Einsatz von Standard-Industriekomponenten in explosionsgefährdeten Bereichen, indem ein kontrollierter Überdruck verhindert, dass zündfähige Gasgemische in das Gehäuse eindringen. Anwender können dadurch Steuerungen, HMIs oder ganze Schaltschränke einsetzen, ohne ausschließlich auf speziell Ex-zertifizierte Einzelkomponenten angewiesen zu sein. Das erhöht die Flexibilität und senkt Installations- wie Wartungskosten. Da viele Wasserstoffanlagen modular und international ausgerichtet sind, bietet die Überdruckkapselung zudem den Vorteil, dass eine einmal entwickelte Lösung häufig viele für Märkte zertifziert werden und daruch weltweit eingesetzt werden kann. Sie schafft also die technische Freiheit, um sichere, wirtschaftliche und global einsetzbare Lösungen umzusetzen.

Welche Produkte und Lösungen von Pepperl+Fuchs kommen derzeit besonders häufig in wasserstoffbasierten Anwendungen zum Einsatz – etwa in Pipelines, Brennern oder bei der Betankung von AGVs?

Alexander Aust: Pepperl+Fuchs sieht sich als Technologiepartner, der Unternehmen dabei unterstützt, ihre Prozesse sicher und zuverlässig zu gestalten – unabhängig davon, ob es sich um Elektrolyse, Verdichtung, Transport oder Anwendung handelt.

Entlang der Wasserstoffwertschöpfungskette kommen zahlreiche Lösungen zum Einsatz: In Pipelines und Speicheranlagen sichern eigensichere Trennbarrieren und Interface-Module die Signalübertragung zwischen Feld- und Steuerungsebene. In Brennern und Verdichtereinheiten sorgen Sensoren zur Erfassung von Druck, Temperatur oder Position für zuverlässige Prozessüberwachung.

Ein besonders anschauliches Beispiel ist die Zusammenarbeit einem Hersteller von Wasserstofftankstellen aus Deutschland. Hier kommen explosionsgeschützte Ex e-Gehäuselösungen von Pepperl+Fuchs zum Einsatz, die eine flexible, zertifizierte Signalverarbeitung ermöglichen. Dank ihres modularen Aufbaus können Anlagenhersteller Komponenten individuell konfigurieren, ohne jedes Mal eine Neuzertifizierung durchführen zu müssen. Das spart Zeit und Kosten und ermöglicht zugleich maßgeschneiderte Lösungen für unterschiedliche Märkte und Klimazonen.

Darüber hinaus gewinnen eigensichere Tablets und Smartphones zunehmend an

Bitte umblättern ▶

Überdruckgekapselte Gehäuselösung mit Analysegeräten zur Messung des Wasserstoffreinheitsgrades. Eingesetzt wird diese an Wasserstofftankstellen

Ein Mobile Worker überwacht den Betankungsprozess an einer Wasserstofftankstelle mit einem eigensicheren Tab-Ex 03 Tablet

Bedeutung – etwa bei der mobilen Datenerfassung und Wartung in Ex-Bereichen. Diese Geräte ermöglichen den sicheren Zugriff auf Messwerte, Dokumentationen oder Wartungsprotokolle direkt vor Ort und tragen so entscheidend zu einer vernetzten, effizienten Instandhaltung bei.

Wie bewerten Sie die Entwicklung der globalen Wasserstoffwirtschaft aus Sicht von Pepperl+Fuchs – insbesondere im Hinblick auf Nachfrage, Märkte und regulatorische Anforderungen?

Alexander Aust: Die Wasserstoffwirtschaft entwickelt sich weltweit dynamisch – wenn auch mit regional unterschiedlichen Schwerpunkten. Während in Europa und Asien massive Investitionen in Infrastruktur und Erzeugung fließen, entstehen auch in Nordamerika, Australien und Teilen Afrikas bedeutende Projekte. Mit zunehmender Skalierung steigen zugleich die Anforderungen an Sicherheit, Standardisierung und internationale Zertifizierungen.

Pepperl+Fuchs ist auf diese Entwicklung gut vorbereitet. Als global aufgestellter Anbieter mit Engineering- und Produktionsstandorten auf allen Kontinenten kann das Unternehmen internationale Projekte umfassend begleiten – von der Planung über die Dokumentation bis hin zur Zertifizierung nach ATEX, IECEx oder NEC. Die Kombination aus jahrzehntelanger Erfahrung im Explosionsschutz und moderner Automatisierungstechnologie macht Pepperl+Fuchs zu einem verlässlichen Partner für die Branche. Langfristig wird Wasserstoff eine tragende Rolle in der Dekarbonisierung von Industrie, Verkehr und Energieversorgung spielen. Ziel von Pepperl+Fuchs ist es, diesen Wandel technologisch zu unterstützen – mit Lösungen, die Sicherheit, Verfügbarkeit und Effizienz in einem komplexen Umfeld gewährleisten.

Inwiefern unterstützt Pepperl+Fuchs die Automatisierung der PEM-Elektrolyse zur Herstellung von grünem Wasserstoff, und welche Sensorlösungen kommen dabei konkret zum Einsatz?

Alexander Aust: Wir verstehen uns weniger als Spezialist für einzelne Anwendungen, sondern als Partner, der den gesamten Wasserstoffsektor technologisch unterstützt. Die PEM-Elektrolyse ist nur ein Beispiel dafür, wie vielfältig unsere Lösungen eingesetzt werden. Unser Ziel ist es, die technologische Basis bereitzustellen, auf der Unternehmen ihre Prozesse sicher und effizient gestalten können – vom einzelnen Sensor bis zur sicheren Signalübertragung und elektrischen Ausrüstung. Kurz gesagt: Wir schaffen keine Prozesse, sondern liefern die Technologie, die sie sicher, automatisiert und zukunftsfähig macht.

Welche Perspektiven sehen Sie für Pepperl+Fuchs in der Wasserstoffwirtschaft der kommenden Jahre – sowohl technologisch als auch strategisch?

Alexander Aust: Wasserstoff ist ein wichtiger Energieträger der Zukunft. Überall dort, wo Wasserstoff erzeugt, gespeichert, transportiert oder genutzt wird, spielt Sicherheit eine zentrale Rolle. Und da kommt Pepperl+Fuchs ins Spiel. Mit unserem jahrzehntelangen Know-how im Explosionsschutz, einem weltweit aufgestellten Engineering-Netzwerk und dem bereits beschriebenen, breiten Produktportfolio sind wir bestens positioniert, Teil dieser Reise zu sein.

Wir verstehen uns als Partner für sichere, automatisierte und vernetzte Prozesse. So leisten wir unseren Beitrag, die Wasserstoffwirtschaft sicher, effizient und nachhaltig voranzubringen GIT

Pepperl+Fuchs auf der SPS 2025: Halle 7A, Stand 330

Pepperl+Fuchs
www.pepperl-fuchs.com

© Bilder: Pepperl+Fuchs

SPS 2025: Ethernet-APL- und Ethercat-Neuheiten von Moxa

Moxa Europe GmbH stellt auf der SPS 2025 seine Ethercat- und Ethernet-APL-Neuheiten vor. Die Ethercat-Junctions und -Gateways des Unternehmens unterstützen industrielle Anwendungen mit schneller, kostengünstiger und deterministischer Ethercat-Technologie. Dank robuster Zuverlässigkeit im Dauerbetrieb, intuitiver Benutzeroberfläche für die einfache Konfiguration sowie kompakter Größe ermöglichen sie den Aufbau flexibler Topologien und die Umstellung serieller Netzwerke auf industrielles Ethernet. Die Ethercat-Junctions der EJS-Serie wurde entwickelt, um industriellen Ethercat-Netzwerken mehr Flexibilität und Effizienz zu ermöglichen. Durch die einfache Konfiguration von Stern-, Linien-, Ring- und Baumtopologien lassen sich Ethercat-Geräte modular und effizient verbinden. Dank zweier Stromeingänge kann ein redundantes Netzteil angeschlossen werden, das beim Ausfall der Hauptstromversorgung einen durchgehenden Betrieb gewährleistet.

SPS: Halle 5, Stand 419 **www.moxa.com**

© Moxa

Cellulink Outdoor-Mobilfunk-Router für EX-Bereiche

Die Produktreihe Cellulink Outdoor-Mobilfunk-Router von Phoenix Contact wird erweitert: Es sind neue Varianten erhältlich, die speziell für den Einsatz in explosionsgefährdeten Bereichen der Zone 2 entwickelt wurden. Die Geräte haben eine IECEx- und ATEX-Zulassung und ermöglichen damit den sicheren Betrieb in anspruchsvollen Industrieumgebungen. Besonders hervorzuheben ist die ganzheitliche Zulassung des Mobilfunksystems Cellulink mit integrierter Antenne. Die Zertifizierung umfasst nicht nur die einzelne Komponente, sondern das gesamte System aus Router, Antennenpfad und Antenne, die in einem vandalismussicheren Outdoor-Gehäuse untergebracht sind. Die Endanwendenden können so das Produkt ohne weitere Risikoanalysen, Nachzertifizierungen oder Dämpfungsmaßnahmen in explosionsgefährdeten Bereichen in Betrieb nehmen. **www.phoenixcontact.com/de**

Produktvarianten für Schutztürsystem PSENmgate

Für das sichere Schutztürsystem PSENmgate von Pilz stehen weitere Produktvarianten zur Verfügung: Eine Variante für mehr Bedienfunktionen und eine weitere mit optimierter Kabelführung zur schnelleren Installation. Zudem ergänzt ein Türgriff-Modul speziell für Schwenktüren das System. PSENmgate bietet damit mehr Bedienkomfort und einen flexibleren Einbau. Die neuen Varianten des Schutztürsystems schließen so weitere Anwendungsfelder – z. B. für die Verpackungstechnik, im Maschinenbau oder bei Roboterapplikationen – ein. Damit weitet PSENmgate die Möglichkeit aus, individuelle Sicherheitskonzepte zur Zugangsabsicherung passgenau umzusetzen. Eine neue Variante PSENmgate mit längerem Gehäuse hat Platz für mehr Bedienelemente wie beispielsweise Drucktaster und beleuchtete Taster oder Schlüsselschalter. **www.pilz.com**

Sicher und regelkonform

Cybersecurity im Maschinenbau wird zur Pflicht

Die digitale Transformation des Maschinen- und Anlagenbaus bringt enorme Möglichkeiten. Doch je stärker Maschinen und Automatisierungssysteme miteinander interagieren, desto größer wird auch die Angriffsfläche für Cyberattacken. Sicherheit ist daher eine Grundvoraussetzung, sie entscheidet über den Schutz von Anlagen hinaus auch über Wettbewerbs- und Zukunftsfähigkeit von Unternehmen. Hinzu kommt regulatorischer Druck: Ab 2027 werden verbindliche Vorgaben Realität. Die zentrale Frage lautet also, welche Maßnahmen sind notwendig, um auch in Zukunft rechtssicher zu agieren?

Der Maschinen- und Anlagenbau steht vor einer besonderen Ausgangslage. Jahrzehntealte SPS laufen Seite an Seite, unterschiedlichen Protokolle und proprietäre Systeme müssen koordiniert werden. Diese technologische Vielfalt ist für den Betrieb zwar unvermeidlich, erschwert aber die Einführung einheitlicher Sicherheitsstandards. Hinzu kommt die Konvergenz von OT und IT. Es sind zwei Welten mit unterschiedlichen Sicherheitsphilosophien und Prioritäten.

Ab 2027 greift mit der neuen Maschinenverordnung (MVO) und dem Cyber Resilience Act (CRA) ein doppelter regulatorischer Rahmen, der Cybersecurity nicht mehr als freiwillige Maßnahme, sondern als rechtlich bindende Voraussetzung für Marktzugang und Produkthaftung definiert.

Maschinensicherheit wird digital erweitert

Ab Januar 2027 ersetzt die neue Maschinenverordnung (MVO) die bisherige Maschinenrichtlinie. Sie trägt den tiefgreifenden Veränderungen durch Digitalisierung, KI und Vernetzung Rechnung. Cybersecurity wird hierbei explizit als Bestandteil der Maschinensicherheit verankert. Hersteller müssen künftig nachweisen, dass ihre Maschinen nicht nur technisch einwandfrei laufen, sondern dass sie auch digitalen Risiken standhalten, Damit wächst die Verantwortung der Entwickler: Sicherheitsbetrachtungen müssen bereits im Konstruktions- und Entwicklungsprozess berücksichtigt werden.

Der Cyber Resilience Act (CRA): Neue Pflichten für Hersteller

Der EU Cyber Resilience Act ist keine Zukunftsvision mehr: Er trat am 10. Dezember 2024 in Kraft und wird ab dem 11. Dezember 2027 verbindliche Sicherheitsanforderungen für „Produkte mit digitalen Elementen" in allen Lebenszyklen vorgeben. Bereits ab dem 11. September 2026 gelten Meldepflichten für erkannte Schwachstellen und schwerwiegende Sicherheitsvorfälle. Der CRA führt das CE-Zeichen auf ein neues Niveau, denn Produkte müssen zukünftig auch Cyber-Resilienz nachweisen. Für besonders kritische Systeme ist sogar eine Drittparteienprüfung vorgesehen. Zudem gelten Vorgaben zu technischer Dokumentation (z. B. SBOM, Risikomodelle, sichere Designs), Update-Mechanismen und transparente Anwenderanweisungen.

Wer nach 2027 Maschinen oder Steuerungskomponenten neu auf den Markt bringt, muss diese Regelwerke erfüllt haben, andernfalls drohen Sanktionen – bis zu 15 Mio. € oder 2,5 % des weltweiten Jahresumsatzes.

Orientierung durch Normen: IEC 62443 als Praxisrahmen

Während der Cyber Resilience Act und die Maschinenverordnung rechtlich verbindliche Anforderungen setzen, liefert die Normenreihe IEC 62443 ein praxisnahes, international anerkanntes Rahmenwerk für

die Umsetzung industrieller Cybersecurity. Sie richtet sich an alle Beteiligten entlang des Lebenszyklus einer Anlage.

Die Normenreihe ist modular aufgebaut und deckt sowohl organisatorische als auch technische Aspekte ab. Ein zentrales Konzept der IEC 62443 sind die sogenannten Security Levels. Sie definieren abgestufte Schutzklassen, die von einem grundlegenden Schutz gegen unbeabsichtigte Fehlhandlungen bis hin zu Maßnahmen gegen hochprofessionelle und gezielte Angriffe reichen. Damit können Unternehmen ihre Sicherheitsarchitektur gezielt anhand der individuellen Bedrohungsszenarien und Risikoprofilen gestalten.

Für den Maschinen- und Anlagenbau bedeutet die IEC 62443 zweierlei: Einerseits bietet sie eine klare Orientierung und praxistaugliche Vorgaben, die sich auf bestehende Architekturen übertragen lassen. Andererseits schlägt sie die Brücke zur Regulierung, da sie es Herstellern und Betreibern ermöglicht, die Vorgaben von CRA und MVO methodisch umzusetzen. Wer sich frühzeitig mit der Normenreihe auseinandersetzt, schafft nicht nur eine belastbare Grundlage für die Erfüllung künftiger rechtlicher Vorgaben, sondern auch eine nachvollziehbare Dokumentation gegenüber Kunden und Aufsichtsbehörden und damit einen wichtigen Wettbewerbsvorteil in einer zunehmend regulierten Industrie.

Wichtige technische Maßnahmen für Unternehmen

Netzwerksegmentierung und Zero-Trust-Ansätze trennen Automatisierungsbereiche klar von unternehmensweiten IT-Netzen. Steuerungen und Embedded-PCs sollten gehärtet werden; sichere, dokumentierte Konfigurationen müssen Standard sein. Patch-Strategien sind unerlässlich: Updates sollten separiert von Funktionsupdates automatisiert einspielbar und nachvollziehbar sein. Monitoring und IDS/Anomalie-Erkennung im OT-Bereich erlauben frühe Warnung – insbesondere relevant bei Ransomware-Attacken. Für Remote-Wartung braucht es sichere Authentifizierung, Verbindungsnachweis und Logging.

In den Webinaren von Wieland Electric werden die Begrifflichkeiten eingeordnet und verständlich erklärt. Anschließend wird praxisnah aufgezeigt, welche Anforderungen Hersteller selbst umsetzen müssen und welche nur im Zusammenspiel mit Betreibern erfüllt werden können. Damit erhalten Teilnehmende nicht nur eine technische Einführung, sondern auch konkrete Handlungsanleitungen für die Umsetzung.

Cybersecurity als Teil der Unternehmensstrategie

Wer Maschinen und Anlagen entwickelt, sollte Sicherheitsrisiken von Anfang an in den Entwicklungsprozess integrieren. Eine fundierte Risikoanalyse erkennt Schwachstellen und legt die Basis für wirksame Schutzmaßnahmen. Ebenso wichtig ist die klare Verteilung von Verantwortlichkeiten: Jedes Unternehmen muss benennen, wer für Cybersicherheit zuständig ist und wie Schnittstellen zwischen Entwicklung, Betrieb und Service organisiert werden. Wenn Entwickler, Techniker und Servicemitarbeiter geschult und für das Thema sensibilisiert sind, lässt sich ein nachhaltiges Sicherheitsniveau erreichen. Schließlich braucht es vorbereitete Notfallpläne und Incident-Response-Prozesse, die sicherstellen, dass im Falle eines Sicherheitsvorfalls schnell und strukturiert gehandelt werden kann. Das ist eine Anforderung, die durch die Meldepflichten des Cyber Resilience Act ab 2026 zusätzliche Relevanz erhält.

Wissenstransfer: Webinare & Expertenforum von Wieland Electric

Wieland Electric bietet seit Anfang Oktober 2025 eine praxisorientierte Webinarreihe zu industrieller Cybersecurity an, in der konkrete Praxisfälle und Handlungsempfehlungen im Mittelpunkt stehen. Ergänzend dazu lädt das Expertenforum von Wieland Electric „Funktionale Sicherheit & Cybersecurity“ am 2. Dezember 2025 online zu einem intensiven Austausch ein. Hier haben Teilnehmende die Möglichkeit, mit Fachleuten aktuelle Entwicklungen zu diskutieren und vertiefende Einblicke in innovative Sicherheitsstrategien zu gewinnen. GIT

Wieland Electric auf der SPS 2025: Halle 9, Stand 440

Hier gelangen Sie zur Anmeldung zu den Webinaren:

Wieland Electric GmbH
www.wieland-electric.com

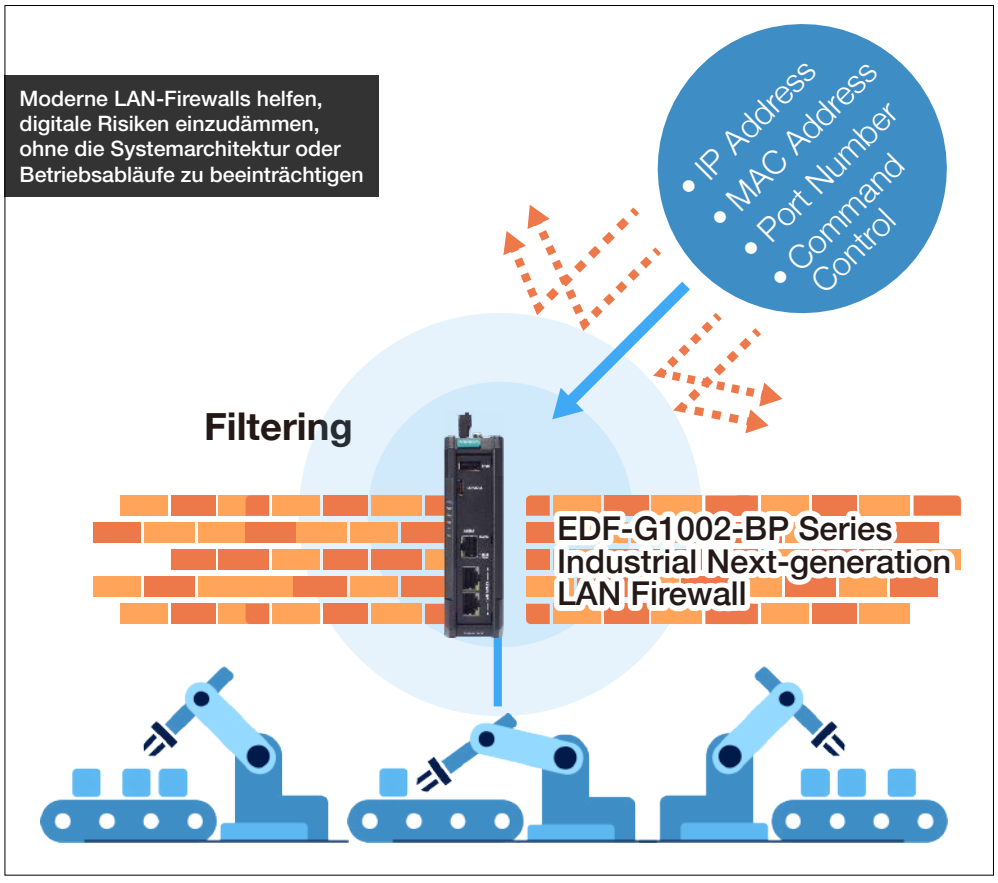
Sichere Maschinen, stabile Netze

Warum Next-Gen LAN-Firewalls ein Schlüssel zur modernen Maschinensicherheit sind

Cyberangriffe auf industrielle Systeme nehmen zu – und betreffen längst nicht mehr nur kritische Infrastrukturen. Auch Produktionsanlagen und vernetzte Maschinen geraten immer häufiger ins Visier, da sie zunehmend mit Unternehmensnetzwerken und Cloud-Systemen verbunden sind. Umso wichtiger ist es, Maschinen- und Anlagensicherheit ganzheitlich zu denken – von der physischen Sicherheit bis zur Absicherung der digitalen Schnittstellen. Ein Beitrag von Laurent Liou, Product Marketing Manager, Moxa Europe.

Laurent Liou, Product Marketing Manager, Moxa Europe

Um die Widerstandsfähigkeit industrieller Systeme zu erhöhen, reagieren Regierungen und Normungsgremien weltweit mit strengeren Vorgaben – in Europa etwa mit der NIS2-Richtlinie, die höhere Anforderungen an die Cyberresilienz von Organisationen in kritischen und wichtigen Sektoren stellt. Auch wenn die nationale Umsetzung in einigen EU-Mitgliedsstaaten noch im Gange ist, gelten die Anforderungen der NIS2-Richtlinie inhaltlich bereits als Maßstab für ein angemessenes Sicherheitsniveau. Betreiber industrieller Netzwerke sollten daher proaktiv handeln und ihre Sicherheitsarchitektur frühzeitig an die neuen Standards anpassen – insbesondere mit Blick auf Netzwerkschutz und kontinuierliche Betriebsfähigkeit.



Verteidigung in der Tiefe bleibt entscheidend

Aktuelle Standards und Regularien wie IEC 62443 empfehlen ein mehrschichtiges Sicherheitskonzept (Defense-in-Depth), um Risiken zu minimieren. Neben dem Schutz der Netzgrenzen spielt dabei die Segmentierung innerhalb des Netzwerks eine entscheidende Rolle. Denn auch interne Bedrohungen – etwa durch infizierte mobile Datenträger oder kompromittierte Endgeräte – können den gesamten Betrieb gefährden.

Gerade im Umfeld der Maschinensicherheit ist diese Segmentierung essenziell. Moderne Maschinen sind häufig über industrielle Ethernet-Strukturen miteinander verbunden. Ohne eine sichere Trennung von Produktions- und IT-Netzwerken steigt das Risiko, dass Schadsoftware oder Fehlkonfigurationen ganze Linien lahmlegen.

Industrielle Firewalls sind hierbei ein zentrales Element, da sie Datenverkehr filtern und unbefugte Zugriffe verhindern. Dennoch begegnen viele Betreiber bei der Im-

plementierung klassischen Hürden – von Netzwerkanpassungen bis hin zu Performancefragen.

Es gibt vier typische Herausforderungen bei der Firewall-Integration:

- 1. Bestehende Netzwerke müssen unangetastet bleiben

In vielen Anlagen ist die Netzwerktopologie fest definiert. Jede Änderung an IP-Subnetzen oder Routing-Strukturen kann zu Stillstandszeiten führen – ein Risiko, das sich kritische Anwendungen kaum leisten können.

- 2. Performance darf nicht leiden

Neue Sicherheitskomponenten dürfen weder die Latenz erhöhen noch die Kommunikationsstabilität gefährden. Auch ein Geräteausfall darf nicht zum Single Point of Failure werden.

- 3. Legacy-Geräte benötigen besonderen Schutz

Viele Steuerungen und HMI-Systeme basieren auf älteren Betriebssystemen, die nicht regelmäßig aktualisiert werden können. Dennoch müssen sie gegen aktuelle Angriffsformen wie DoS oder Exploits abgesichert werden.

- 4. Netzwerküberwachung bleibt komplex

Sicherheitsereignisse und Anomalien erfordern ständige Aufmerksamkeit. Ohne zentrale Überwachungslösungen riskieren Betreiber, Angriffe oder Störungen erst spät zu erkennen.

Neuer Ansatz für LAN-Sicherheit

Neue LAN-Firewalls für industrielle Anwendungen setzen genau hier an. Im „Transparent Mode“ lassen sie sich direkt vor kritischen Assets einfügen – ohne Änderungen an bestehenden IP-Strukturen. Funktionen wie LAN-Bypass verhindern Ausfälle, selbst wenn ein Gerät gewartet oder neu gestartet wird.

Darüber hinaus kombinieren moderne Firewalls Intrusion Prevention (IPS) und Deep Packet Inspection (DPI), um auch ältere Anlagen zuverlässig zu schützen. Damit lassen sich Kommunikationsregeln bis auf Protokollebene – etwa Modbus oder DNP3 – definieren und Manipulationsversuche frühzeitig erkennen.

Für Betreiber, die viele verteilte Standorte absichern müssen, ist zudem die zentrale Verwaltung entscheidend. Über Managementplattformen wie Moxas MXsecurity oder MXview One lassen sich Firewalls, Ereignisse und Richtlinien effizient überwachen und steuern. Das reduziert manuelle Konfigurationen und ermöglicht schnelle Reaktionen im Ernstfall.

Fazit

In einer Zeit, in der Maschinen, Steuerungen und Netzwerke immer stärker miteinander verschmelzen, ist Netzwerksicherheit ein integraler Bestandteil der Maschinensicherheit. Moderne LAN-Firewalls helfen, digitale Risiken einzudämmen, ohne die Systemarchitektur oder Betriebsabläufe zu beeinträchtigen.

So wächst zusammen, was zusammengehört: Maschinensicherheit und Netzwerkschutz – für sichere, verfügbare und resiliente Produktionsumgebungen. GIT

Moxa auf der SPS 2025:
Halle 5, Stand 419

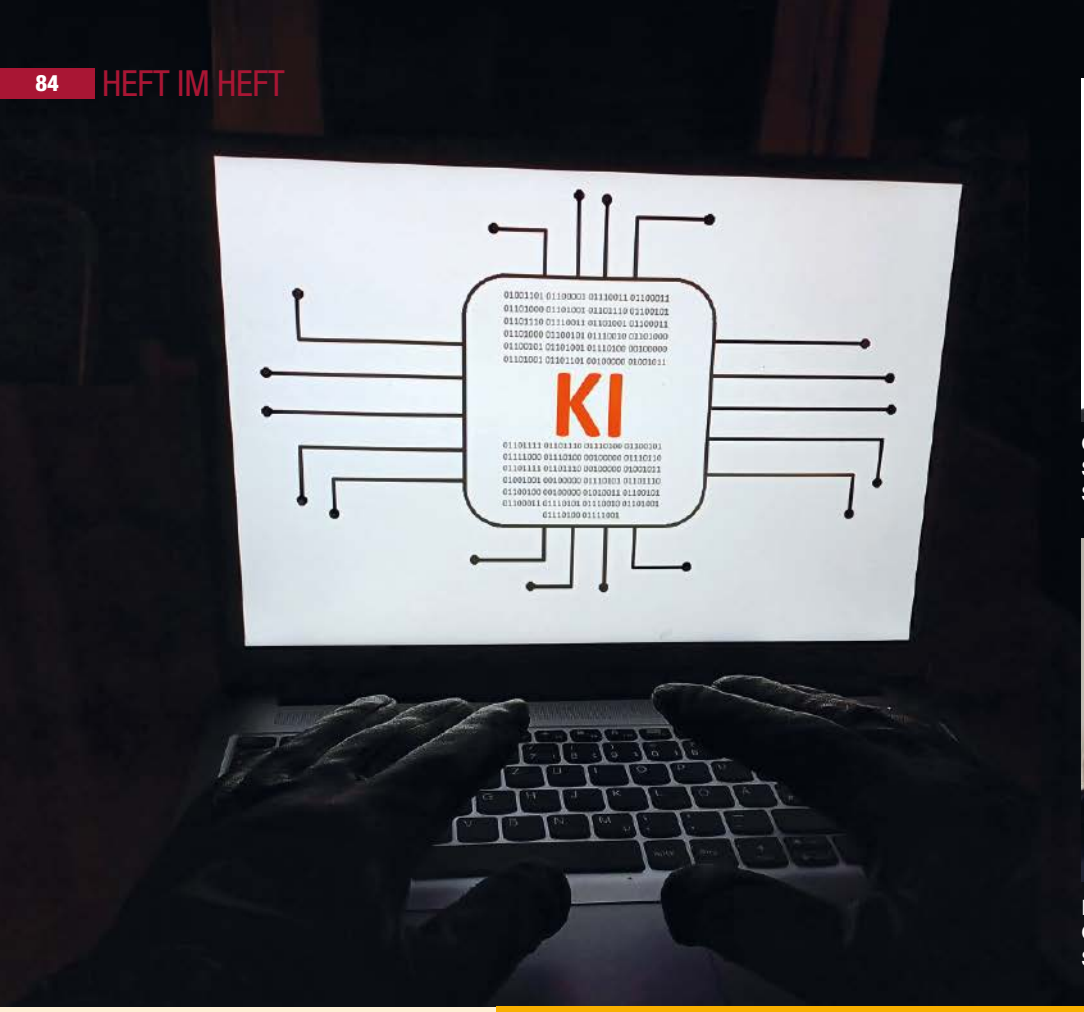
Moxa Europe
www.moxa-europe.com

© Bilder Moxa

KI-gestützte Sensorlösung zur Umfeld- und Personenerkennung

Sick stellt mit dem Visionary AI-Assist eine KI-basierte Sensorlösung vor, die Outdoor-Kollisionsschutz und Umfeldüberwachung ermöglicht und um eine Personenerkennung ergänzt. Die Sensorlösung kombiniert die 2D- und 3D-Bildverarbeitung. Sie erkennt zuverlässig Personen und Objekte und bestimmt deren Entfernung zum Sensor. Die integrierte KI sorgt, auch bei schwierigen Bedingungen, für verlässliche Personenerkennung und verhindert Fehlalarme. Die Sensorlösung Visionary AI-Assist besteht aus zwei Komponenten: der 3D-Stereokamera Visionary-B Two und der Software AI-Assist. Die Kamera dient zur Distanzmessung, Objektdetektion und Umfelderkennung im Innen- und Außenbereich. Die Software AI-Assist verwendet künstliche Intelligenz zur Klassifizierung von Personen. Dadurch können aktuelle Gefahren im Arbeitsbereich einer mobilen Maschine beurteilt und selektive Warnungen ausgegeben werden.

www.sick.com



© Phoenix Contact

Carsten Gregorius, Manager Strategic Product Marketing Safety bei Phoenix Contact

© Leuze Electronic

Frank Bauder, Head of Competence Center Services bei Leuze

Maschinensicherheit im Kontext von KI und Security

Cyber Resilience Act und Maschinenverordnung: Herausforderungen und Chancen neuer Regularien

Künstliche Intelligenz (KI) stellt den Maschinenbau im Allgemeinen und die Funktionale Sicherheit von Maschinen und Anlagen im Besonderen vor neue Herausforderungen. In diesem Interview beleuchten Frank Bauder, Head of Competence Center Services bei Leuze, und Carsten Gregorius, Manager Strategic Product Marketing Safety bei Phoenix Contact, wie KI das Verhalten von Maschinen beeinflusst und welche Rolle die Risikobeurteilung spielt. Zudem wird den Themen Security, den normativen Rahmenbedingungen und dem Zusammenspiel von neuer Maschinenverordnung (MVO) und Cyber Resilience Act (CRA) im Kontext der Maschinensicherheit auf den Grund gegangen. Welche Herausforderungen und Chancen ergeben sich für Hersteller und den Produktionsstandort Deutschland/Europa?

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

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

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

VDMA Elektrische Automation

GIT SICHERHEIT

zvei electrifying ideas

GIT SICHERHEIT: Herr Bauder, Herr Gregorius, bevor wir auf den Einfluss von KI auf die Funktionale Sicherheit eingehen, stellt sich zunächst die Frage, was KI genau ist und welche Arten es gibt.

Frank Bauder: Geprägt wurde der Begriff der „künstlichen Intelligenz" bereits in den 50er-Jahren des letzten Jahrhunderts, insbesondere durch den Mathematiker und Informatiker Alan Turing. Danach war es eine ganze Zeit still um das Thema und erst Ende der 80er-Jahre wurden erste kommerzielle Anwendungen sichtbar. Seither hat die KI nach und nach Einzug in viele Bereiche unseres Lebens gehalten, zuletzt insbesondere durch den Chatbot ChatGPT. Definiert wird „KI" als Fähigkeit von Maschinen, Aufgaben autonom auszuführen, wobei diese angepasst an neue Situationen reagieren und aus Erfolg und Misserfolg lernen. Dieses Verhalten ähnelt dem menschlichen Lernen. Heute sind vier Teilbereiche am häufigsten anzutreffen: „Machine Learning", „Künstliche neuronale Netze", „Deep Learning" und „Natural Language Processing".

Wie beeinflusst KI den Maschinenbau gegenwärtig und welche Entwicklungen sind hier in den kommenden Jahren zu erwarten?

Carsten Gregorius: Der Einfluss von KI auf den Maschinenbau ist schon heute deutlich wahrzunehmen. Maschinelles Lernen wird beispielsweise genutzt um Produktionsprozesse zu optimieren indem Fertigungsabläufe permanent analysiert und verbessert werden. Weiterhin ermöglicht KI auch „Predictive Maintenance", indem Daten analysiert werden und Prognosen für die Ausfallwahrscheinlichkeit bereitgestellt werden. Hierzu können beispielsweise digitale Zwillinge genutzt werden, um bei verschleißbehafteten Komponenten wie Relais einen rechtzeitigen Austausch einzuplanen und damit Produktionsstillstände zu minimieren.

Aber auch bei der sicherheitsgerichteten Konstruktion von Maschinen sowie der dynamischen Integration von Anlagenkomponenten verspricht die Anwendung von KI viele Möglichkeiten. In diesem Zusammenhang sei auf das Forschungsprojekt „AutoS²" unter Federführung des Fraunhofer IOSB-INA hingewiesen.

Ein weiterer wichtiger Aspekt, auf den die Nutzung von KI maßgeblichen Einfluss hat, ist das Thema Security. Wie sieht der normative Rahmen hierzu aus?

Carsten Gregorius: Das Thema „Security" hat mittlerweile breiten Einzug in das europäische Rahmenregelwerk gehalten. Insbesondere durch den Cyber Resilience Act (CRA) wird eine große Mehrheit von industriellen Produkten erfasst, die für die Automation von morgen von entscheidender Bedeutung sind. Unter den Anwendungsbereich fallen Produkte, die „digitale Elemente" verwenden oder als Softwareprodukt in Verkehr gebracht werden. Ab dem Stichtag 11. Dezember 2027 (entspricht 36 Monate nach Inkrafttreten) sind alle Anforderungen aus dem CRA vor dem erstmaligen Inverkehrbringen eines Produktes zu berücksichtigen. Weiterhin ist der Behandlung von Schwachstellen über den gesamten Lebenszyklus Rechnung zu tragen.

Gestützt wird die Anwendung des CRA durch die Verwendung von Normen, die gerade in der Entwicklung sind und bis zum Stichtag harmonisiert sein sollen. Hierbei entstehen jeweils drei sogenannte „horizontale Normen" und „vertikale Normen". Vorteil ist die sogenannte Konformitätsvermutung bei Anwendung dieser Normen. Aber auch andere europäische Regelwerke greifen das Thema „Security" auf: So hat beispielsweise die neue Maschinenverordnung (MVO) unter dem Kapitel „Schutz gegen Korrumpierung" entsprechende Schutzziele bei Maschinen und Sicherheitsbauteilen definiert. Einen ähnlichen Ansatz findet man auch in der Funkanlagen-Richtlinie (RED).

Wie wirkt sich das Zusammenspiel von Maschinenverordnung (MVO), Cyber Resilience Act (CRA) sowie weiterer Regularien wie KI-Verordnung auf den Maschinenbau aus?

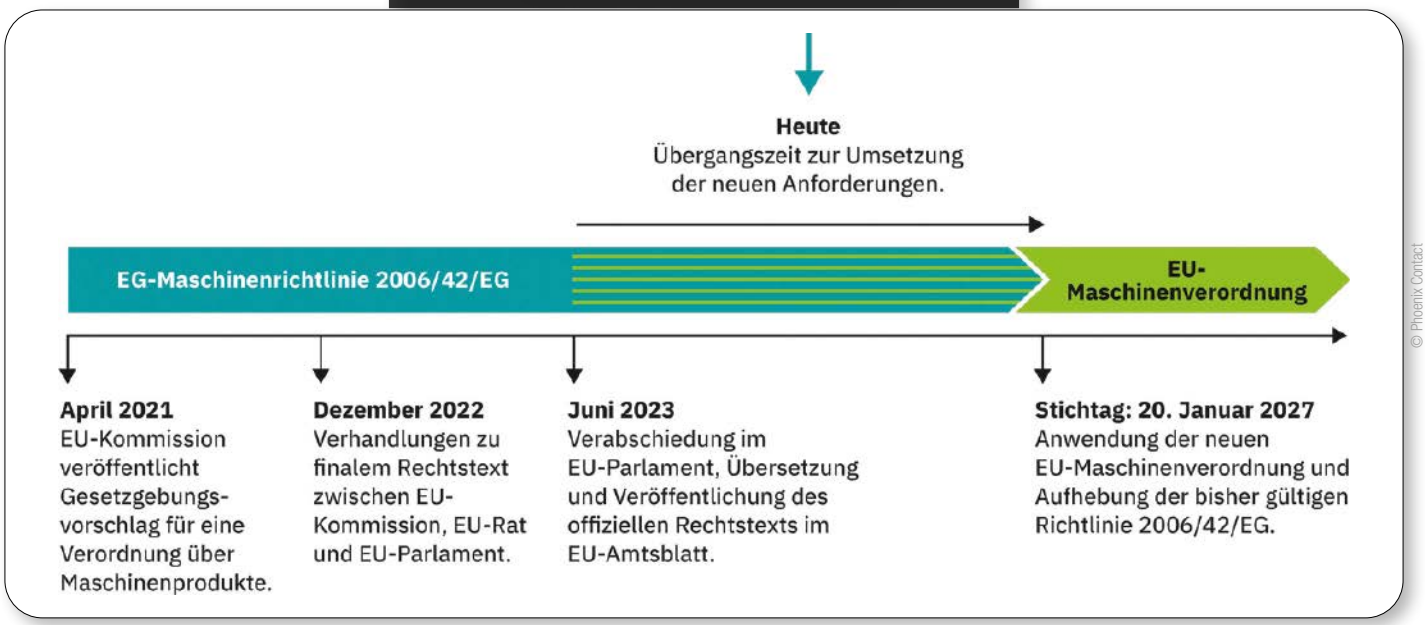
Frank Bauder: Für Hersteller von Maschinen ergeben sich durch die Maschinenverordnung (MVO) einige neue Aspekte. Die Themen Security und KI werden in der MVO konkret thematisiert. Danach hat der Maschinenhersteller Maßnahmen zu treffen, damit sich z. B. aus einem Angriff auf Datenschnittstellen an seiner Maschine keine negativen Einflussmöglichkeiten auf die Maschinensicherheit (= Funktionale Sicherheit) ergeben. Weiterhin beschreibt die MVO nun Anforderungen an autonome Maschinen, die z. B. Verfahren zum „self evolving behaviour" nutzen – also sich selbst weiterentwickeln können. Wichtig für den Maschinenbau ist die Tatsache, dass die Umsetzung dieser Anforderungen durch neue Konzepte z. B. bei der Durchführung der Risikobeurteilung Zeit brauchen. Es ist also erforderlich, zeitnah zu starten.

Bitte umblättern ▶

Kernanforderungen an die Cyber-Sicherheit digitaler Produkte entlang ihres gesamten Lebenszyklus – von der Planung bis zur Wartung

- Cyber-Sicherheit muss in der **Planungs-, Design-, Entwicklungs-, Produktions-, Liefer- und Wartungsphase** berücksichtigt werden
- **Security-Schwachstellen** müssen für die erwartete **Produktlebensdauer** effektiv gehandhabt werden (min. 5 Jahre)
- Alle **Cyber-Sicherheitsrisiken** sind dokumentiert
- **Klare und verständliche Anweisungen für die Verwendung** von Produkten mit digitalen Elementen
- Hersteller müssen **aktiv ausgenutzte Schwachstellen melden**
- **Sicherheits-Updates** müssen **mindestens zehn Jahre** lang verfügbar sein

Zeitstrahl zum Übergang von der EG-Maschinenrichtlinie zur neuen EU-Maschinenverordnung



Welche Herausforderungen sehen Sie bei der Umsetzung von KI und Security in der Funktionalen Sicherheit?

Frank Bauder: Security und Funktionale Sicherheit gehören aus meiner Sicht eng zusammen. Die Herausforderung liegt in der Tatsache, dass im Maschinenbau bisher während der Konstruktion eine Risikobeurteilung durchgeführt wurde. Bei bestimmungsgemäßer Verwendung der Maschine, der Beachtung der Warn- und Sicherheitshinweise und der Restrisiken war somit ein sicherer Betrieb über die gesamte Lebenszeit möglich. Speziell Cybersecurity benötigt Konzepte, die Bedrohungs-Szenarien „von innen" und „von außen" berücksichtigen. Wichtig zu verstehen ist, dass nicht nur die Komponentenlieferanten und die Maschinenhersteller, sondern auch die Betreiber eine aktive Rolle spielen. Die Zusammenarbeit zwischen Hersteller und Betreiber wird also über den reinen Kauf hinausgehen.

KI stellt eine Herausforderung in Richtung funktionaler Sicherheit und Datenschutz dar. Bei Anwendungen mit KI ist das Einsatz-Szenario sehr detailliert zu beschreiben. Die Risikobeurteilung muss auf Basis dieser Szenarien erweitert werden. Die geeignete Auswahl der Trainingsdaten für die KI anhand der Umgebungsbedingungen stellt die nächste Herausforderung dar. Es muss sichergestellt sein, dass die KI in Anwendungen mit Funktionaler Sicherheit nicht „improvisiert". Zurzeit entstehen Systeme, in der die KI in Anwendungen mit Funktionaler Sicherheit lernt, bevor sie in der realen Anwendung eingesetzt wird. Hierdurch ist das Einsatz-Szenario eindeutig beschreibbar, die Reaktionen der KI sind vorhersehbar.

Welche Maßnahmen sollten Unternehmen ergreifen, um die Funktionale Sicherheit und Security ihrer Maschinen zu gewährleisten?

Carsten Gregorius: Spätestens mit der neuen MVO, die ab dem 20. Januar 2027 greift, müssen Maschinenhersteller den Security-Aspekt im Kontext der Funktionalen Sicherheit bereits berücksichtigen. Hierbei steht insbesondere eine sorgfältige Bedrohungsanalyse im Vordergrund aus der dann der „Security-Kontext" definiert und weitere Maßnahmen abgeleitet werden. Als eine wichtige Norm in diesem Zusammenhang sei auf die in der Entwicklung befindliche Norm prEN 50742 hingewiesen, die wertvolle Hinweise zur Anwendung der spezifischen Anforderungen aus der MVO geben wird. In Hinblick auf den CRA sollte dieser Themenkomplex jedoch ganzheitlich betrachtet werden.

Da der gesamte Prozess sehr aufwändig sein kann und zum Teil zunächst ein Know-how-Aufbau stattfinden muss, verbleibt bis zum Stichtag nicht mehr viel Zeit. Maschinenhersteller müssen daher jetzt reagieren und das Thema auf die Tagesordnung setzen. Der VDMA hat sich dieser Herausforderung ebenfalls angenommen und unter dem Projekt „Supply Chain Security" eine praxistaugliche Dokumentenreihe veröffentlicht, die den Austausch von Security-Anforderungen zwischen den Marktteilnehmern standardisieren und damit erleichtern soll.

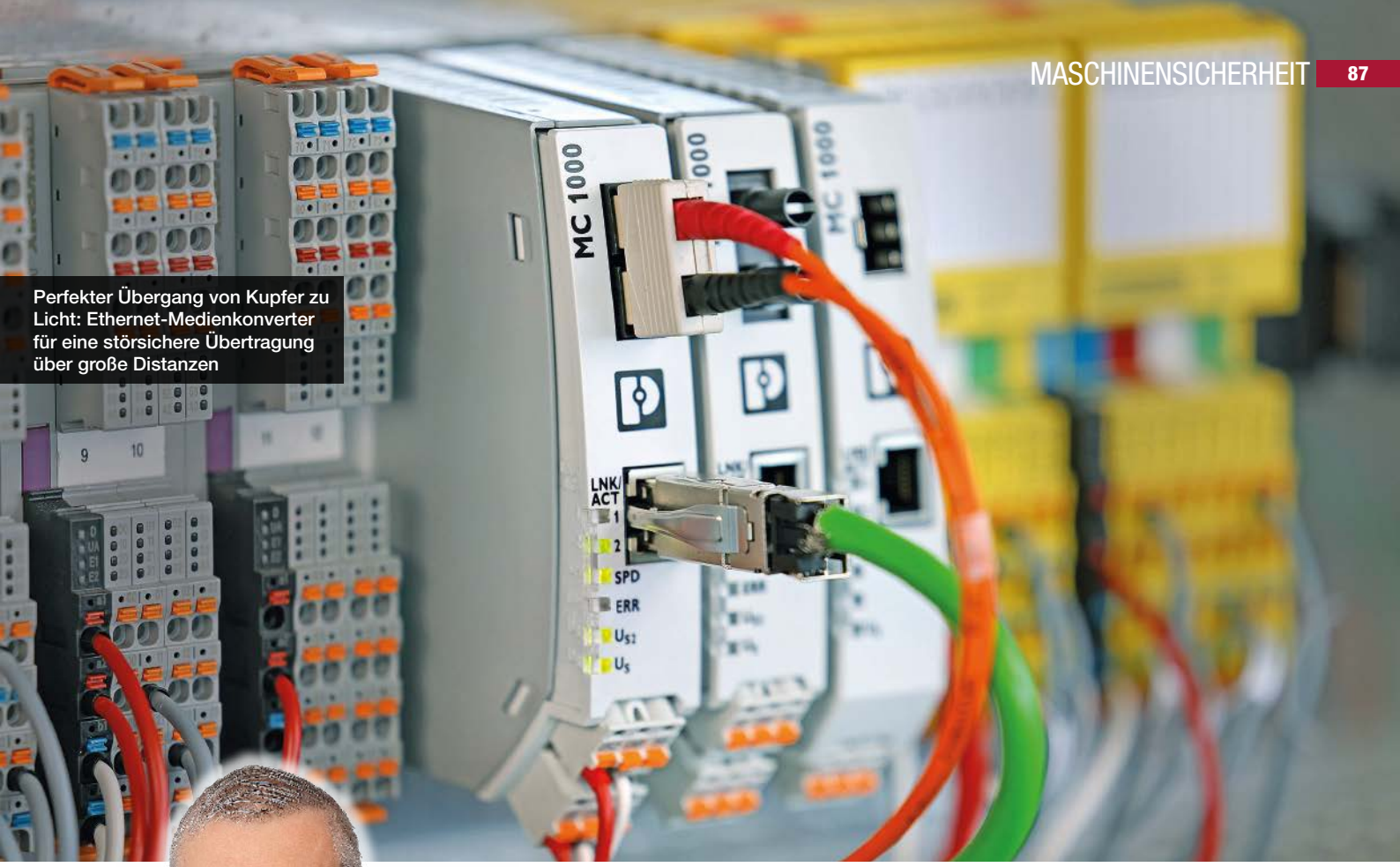
Welchen Einfluss haben die genannten Richtlinien und Verordnungen der EU ihres Erachtens auf den Produktionsstandort Deutschland/Europa?

Frank Bauder: Es bestehen Risiken für den Wirtschaftsstandort, wenn Verordnungen den technischen Fortschritt stoppen und in der globalen Sicht andere Wirtschaftsräume z. B. in Amerika oder Asien hier einfacher forschen und entwickeln können. Weiterhin erzeugen Verordnungen oft zusätzliche Bürokratie beispielsweise durch erweiterte Dokumentation oder zusätzlich erforderliche Zulassungen und Genehmigungen.

Grundsätzlich schaffen aber Verordnungen zunächst den rechtlichen Rahmen für die sichere Anwendung und den sicheren Betrieb. Auf dieser Grundlage werden Harmonisierung und Standardisierung möglich. Das bietet für Europa und Deutschland die Chance auf einen fairen Wettbewerb. GIT

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

Phoenix Contact GmbH & Co. KG
www.phoenixcontact.com



Perfekter Übergang von Kupfer zu Licht: Ethernet-Medienkonverter für eine störsichere Übertragung über große Distanzen

Mehr Reichweite, mehr Sicherheit

Ethernet-Medienkonverter für anspruchsvolle Industrieumgebungen

In der Welt der industriellen Automatisierung bilden stabile und leistungsfähige Netzwerke das Rückgrat effizienter Prozesse. Ethernet-Medienkonverter übernehmen dabei eine Schlüsselrolle: Sie verbinden unterschiedliche Übertragungsmedien wie Kupfer und Glasfaser. Damit ermöglichen sie flexible,- störsichere und zukunftsfähige Netzwerkinfrastrukturen. Ein Beitrag von Bernd Rosenbaum, Produktmanager im Bereich Automation Infrastructure bei Phoenix Contact.

Besonders in rauen Industrieumgebungen oder bei großen Distanzen stellen Ethernet-Medienkonverter entscheidende Vorteile zur Verfügung. Dazu gehören eine erhöhte Reichweite, EMV-Schutz sowie die einfache Integration in bestehende Systeme. Für Anwender ergeben sich daraus mehr Planungssicherheit, geringerer Installationsaufwand und eine zuverlässige Kommunikation auch unter anspruchsvollen Bedingungen.

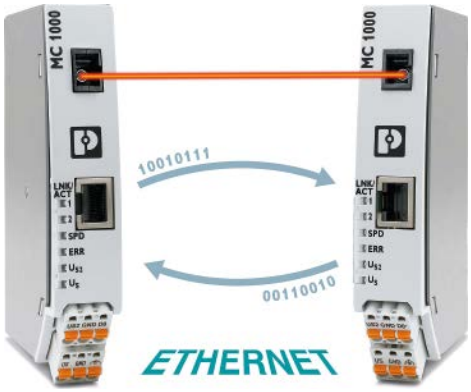
Die Anforderungen an industrielle Netzwerke sind so vielfältig wie die Anwendungen selbst. Um den verschiedenen Bedingungen gerecht zu werden, hat Phoenix Contact die neue Medienkonverter-Familie MC 1000 in drei Serien unterteilt. Jede Serie ist auf spezifische Einsatzszenarien zugeschnitten: von der einfachen Konvertierung im Schaltschrank bis zur Nutzung in explosionsgefährdeten Bereichen oder unter extremen Umweltbedingungen.

Die Basisserie MC 1000 eignet sich bestens für Standardanwendungen in der Gebäudeautomation oder im Maschinenbau. Sie bietet Gigabit-Datenraten sowie eine automatische Betriebsartenwahl und kompakte Bauform für die Hutschienenmontage. Die Baureihe MC 1000 T wurde für anspruchsvollere Umgebungen entwickelt. Mit einem robusten Metallgehäuse, erweitertem Temperaturbereich und einer redundanten Spannungsversorgung erweisen sich die Geräte als besonders widerstandsfähig – etwa in der Verkehrstechnik, Offshore-Anlagen oder der industriellen Fertigung.

Die Serie MC 1000 E richtet sich an Anwendungen mit speziellen Zulassungsanforderungen. Sie erfüllt internationale

Bitte umblättern ▶

Mit den neuen Medienkonvertern MC 1000 von Phoenix Contact findet sich für jede Applikation und Anforderung das passende Gerät



WDM-Medienkonverter zur Vollduplex-Übertragung über eine LWL-Faser eignen sich insbesondere für rotierende Anwendungen

Normen wie ATEX, IECEx, IEC 61850 und die DNV-Schiffbauzulassung. Ethernet-Medienkonverter dieser Baureihe sind somit prädestiniert für explosionsgefährdete Bereiche, die Energieverteilung und kritische Infrastrukturen.

Alle Serien zeichnen sich durch eine zuverlässige Medienkonvertierung - wahlweise bis zu 1 Gbit/s - und unterschiedliche Anschlüsse für Multimode- und Singlemode-Glasfaser aus. Eine hohe EMV-Festigkeit und flexible Verwendungsmöglichkeiten bilden die zukunftssichere Grundlage für industrielle Netzwerke.

Schnelle Fehlererkennung und -behebung

Eine nützliche Funktion moderner Medienkonverter stellt das sogenannte Link Fault Pass Through (LFPT) dar. LFPT sorgt dafür, dass ein Verbindungsfehler auf einer Seite der Konvertierung – zum Beispiel am Glasfaser-Port – ebenfalls auf dem gegenüber liegenden Kupfer-Port signalisiert wird. Auf diese Weise lässt sich ein Fehler aktiv weitergeben. Angeschlossene Geräte oder übergeordnete Systeme können den Ausfall erkennen und entsprechend reagieren. Der Vorteil für den Anwender liegt in der schnellen Fehlererkennung. Ein defekter Link wird nicht als „aktiv" angezeigt, obwohl keine Kommunikation möglich ist. Durch das Abschalten des anderen Ports bei einem Link-Verlust detektieren Netzwerk-Management-Systeme oder Steuerungen den Ausfall sofort und können eine definierte Reaktion auslösen, beispielsweise das Umschalten auf Redundanzverbindungen. Gerade in redundanten Ringen wie Profinet MRP ist diese Funktion unerlässlich. Hier zeigt sich der Vorteil von Medienkonvertern gegenüber vergleichbaren Unmanaged Switches mit LWL-Port. Diese würden bei Ausfall des LWL-Links den Kupfer-Port-Link aufrechterhalten, obgleich keine Daten mehr übertragen werden. Die Folge: schwer nachvollziehbare Fehlerbilder, unnötige Stillstandzeiten und eine aufwendige Fehlersuche. Mit LFPT wird der Fehler hingegen transparent und umgehend sichtbar. Das erweist sich als klarer Vorteil für die Wartung, Diagnose und Anlagenverfügbarkeit.

Kurze Latenzzeiten im Nanosekunden-Bereich

Ein weiteres Merkmal moderner Medienkonverter ist ihre Fähigkeit zur Echtzeitkommunikation. Das unterscheidet die Geräte der neuen Serie MC 1000 von herkömmlichen Medienkonvertern und Switches. Ermöglicht wird die Echtzeitfähigkeit durch den sogenannten Cut-Through- oder Pass-Through-Modus. Beim klassischen Store-and-Forward-Verfahren wird ein Datenpaket vollständig empfangen, geprüft und erst dann weitergeleitet. Im Gegensatz dazu beginnt der Konverter im Cut-Through-Modus bereits mit der Übertragung, sobald die Zieladresse erkannt wurde. Dadurch reduziert sich die Latenz auf ein Minimum – ein entscheidender Vorteil in zeitkritischen Anwendungen.

Die Cut-Through-Funktion erlaubt einen nahezu verzögerungsfreien Datenaustausch und bietet sich damit für industrielle Echtzeitprotokolle wie Profinet IRT, Ethercat, Powerlink oder Sercos III an. Die Latenzzeiten sind Frame-unabhängig immer gleich groß im Nanosekunden-Bereich. Der Medienkonverter MC 1000 erkennt die Notwendigkeit zur Cut-Through- oder Store-and-Forward-Kommunikation selbstständig und schaltet je nach Anwendung automatisch um. Für den Anwender bedeutet das eine höhere Performance, zuverlässige Datenübertragung in synchronisierten Prozessen sowie flexible Integration in moderne Automatisierungsnetzwerke.

Flexible und platzsparende Installation

Das Zubehör der Medienkonverter MC 1000 umfasst den FL DIN-Rail Adapter. Das Gerät unterstützt unterschiedliche Anbauarten

Flexible und platzsparende Montage mit dem DIN-Rail Adapter für unterschiedliche Einbaulagen

auf der Hutschiene für eine flexible und platzsparende Installation. Durch die kompakte Bauform des Adapters und die einfache Schnappmontage auf der Tragschiene ohne Schrauben oder zusätzliches Montagematerial lassen sich die Medienkonverter und Switches bei beengten Platzverhältnissen sicher und effizient einbauen.

Insbesondere in Anwendungen mit hoher Packungsdichte oder bei nachträglichen Erweiterungen im Schaltschrank eröffnet der Adapter entscheidende Vorteile: Die Geräte lassen sich vertikal oder horizontal ausrichten, was die Luftzirkulation verbessert und die thermische Belastung verringert. Zudem sorgt die mechanische Stabilität des Adapters für eine vibrationsfeste Befestigung. Die werkzeuglose Montage spart Zeit bei der Installation und erleichtert den Austausch im Servicefall. Somit trägt der FL DIN-Rail Adapter 22.5 zu einer durchdachten, modularen Schaltschrankgestaltung bei.

Kostengünstige Kommunikation über nur eine Glasfaser

Mit den WDM-Varianten der Medienkonverter MC 1000 stellt Phoenix Contact eine effiziente Lösung für die optische Datenübertragung über nur eine Glasfaser zur Verfügung. Durch das Wavelength Division Multiplexing (WDM) werden Sende- und Empfangssignale auf verschiedenen Wellenlängen ohne Einschränkungen in Vollduplex weitergeleitet. Das senkt den Installationsaufwand und die Kosten erheblich. In den verlegten Glasfaser-Bündeln bleiben also mehr Fasern für weitere Installationen frei.

Rückgrat der modernen Videoüberwachung

In modernen Videoüberwachungssystemen spielt die zuverlässige Anbindung entfernter Kamerastandorte eine zentrale Rolle. Gerade in weitläufigen Industrieanlagen oder Verkehrsinfrastrukturen stoßen klassische Kupferleitungen schnell an ihre Grenzen – sei es durch Reichweitenbeschränkungen, elektromagnetische Störungen oder Sicherheitsanforderungen. Hier kommen die neuen Medienkonverter wie die Geräte der Serie MC 1000 von Phoenix Contact ins Spiel. Sie ermöglichen die einfache und verlustfreie Umsetzung von Kupfer- auf Glasfaserverbindungen und umgekehrt. So lassen sich IP-Kameras auch über mehrere Kilometer hinweg stabil und störungsfrei in das Netzwerk einbinden. Gleichzeitig profitieren Anwender von einer erhöhten Ausfallsicherheit und besseren Trennung von Netzsegmenten. Medienkonverter stellen damit ein unverzichtbares Bindeglied zwischen klassischer Netzwerktechnik und moderner Glasfaserinfrastruktur dar.

Die WDM-Technologie spielt ihre Stärken insbesondere in drehenden Anwendungen aus, zum Beispiel Windenergieanlagen mit optischem Schleifring. Hier erlaubt sie eine zuverlässige, störungsfreie Kommunikation zwischen Gondel und Turm. Der Datenaustausch über eine Glasfaser ersetzt die Übertragung über elektromechanische Schleifringe, die wartungsaufwendig und störanfällig ist. Die Medienkonverter MC 1000 WDM kombinieren mit ihrer Einfaser-Lösung hohe Performance mit einfacher Integration und bieten sich damit für zukunftssichere, platzsparende Netzwerkinfrastrukturen an (Bild 4).

Umfangreiche Zulassungen

Bei den neuen Medienkonvertern der Serie MC 1000 handelt es sich um Allrounder für industrielle Netzwerke: robust, leistungsfähig und vielseitig einsetzbar. Besonders die Varianten der Serien MC 1000 T und MC 1000 E überzeugen durch umfangreiche Zulassungen. Ob ATEX und IECEx für explosionsgefährdete Bereiche, DNV für maritime Anwendungen oder IEC 61850 im Rahmen der Energieverteilung: Die Geräte lassen sich weltweit normkonform nutzen. Auf diese Weise sorgen sie für hohe Planungssicherheit bei den Betreibern kritischer Infrastrukturen, Maschinenbauern und Systemintegratoren. Die Kombination aus Gigabit-Performance, hoher EMV-Festigkeit und automatischer Betriebsartenwahl macht die Medienkonverter zur idealen Lösung für anspruchsvolle Applikationen in rauen Umgebungen. GIT

Phoenix Contact auf der SPS 2025:
Halle 9, Stand 310, 410, 420, 520

Phoenix Contact
www.phoenixcontact.com

Florian Schneider, Product Manager CodeMeter License Reporting bei Wibu-Systems

Effiziente Lizenz-überwachung

Ein Tool, das Softwareherstellern detaillierte Einblicke und datengestützte Entscheidungen ermöglicht

Auf der diesjährigen Hannover Messe stellte Wibu-Systems mit CodeMeter License Reporting ein innovatives Tool vor, das die Art und Weise, wie Softwarehersteller ihre Lizenznutzung überwachen und analysieren, verbessern könnte. Diese neue Technologie bietet umfassende Einblicke in die Nutzung von Softwarelizenzen, ermöglicht detaillierte Nutzungsberichte und hilft Unternehmen, fundierte Entscheidungen zu treffen. GIT SICHERHEIT führte hierzu ein ausführliches Gespräch mit Florian Schneider, dem Product Manager für CodeMeter License Reporting bei Wibu-Systems.

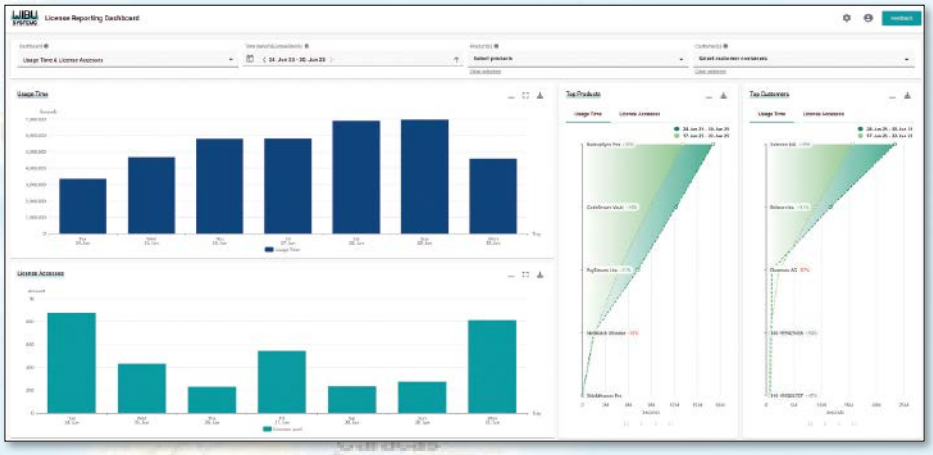
GIT SICHERHEIT: Herr Schneider, auf der Hannover Messe 2025 hat Wibu-Systems mit CodeMeter License Reporting sein neuestes Produkt der Öffentlichkeit vorgestellt. Ihr Unternehmen kommt damit nach eigener Aussage dem Wunsch Ihrer Kunden nach „klare Einblicke in die Nutzung ihrer Softwareprodukte zu erhalten". Welche Einblicke erlaubt Code Meter License Reporting genau?

Florian Schneider: CodeMeter License Reporting (CmLR) erlaubt Softwareherstellern präzise Einblicke in die tatsächliche Nutzung der Softwarelizenzen, indem automatisiert erfasst wird, wann und wie lange Anwendungen im Einsatz sind und in welchen Regionen sie genutzt werden. Auf übersichtlichen und interaktiven Dashboards können Verantwortliche zum Beispiel sehen, wie hoch die Auslastung bestimmter Module ist und ob es Nutzungspeaks oder auffällige Muster gibt. Gleichzeitig macht das System transparent, wenn Nutzer an vereinbarte Lizenzobergrenzen stoßen. Dadurch lassen sich potenzielle Risiken frühzeitig erkennen, etwa wenn bestimmte Regionen oder Zeiträume ein unerwartet hohes Nutzungsverhalten aufweisen. All das ermöglicht eine datengestützte Entscheidungsgrundlage, um Lizenzplanung, Produktstrategien und Weiterentwicklungen zu gestalten.

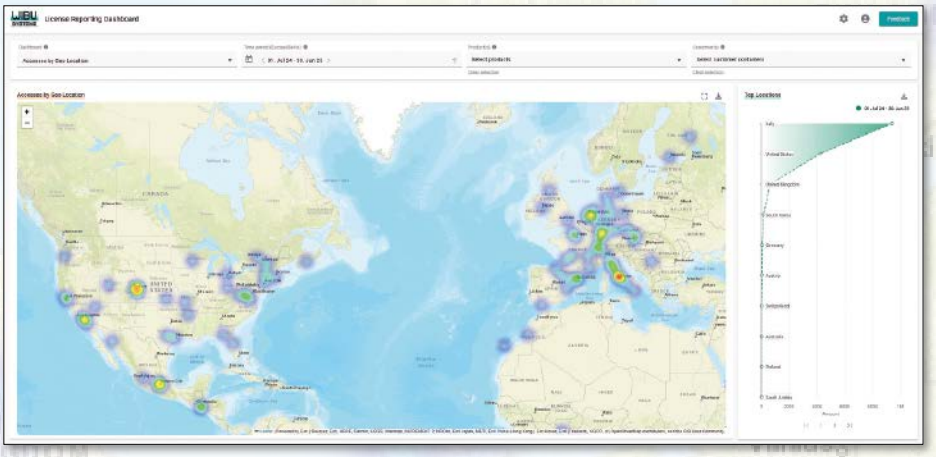
Welchen wesentlichen Zusatznutzen bietet CodeMeter License Reporting Ihren Kunden?

Florian Schneider: Neben den reinen Nutzungsstatistiken eröffnet CodeMeter License Reporting weitere Mehrwerte, die im Wettbewerb entscheidende Vorteile darstellen können.

- Proaktive Maßnahmenplanung: Durch die Erkennung von Nutzungstrends oder sich anbahnenden Engpässen können etwa IT-Sicherheitsbeauftragte oder Lizenzmanager frühzeitig reagieren, z.B. wenn einzelne Lizenzpools knapp werden oder ungewöhnlich viele Fehlzugriffe stattfinden.
- Zielgerichtete Produktoptimierung: Anhand konkreter Feature-Nutzungsdaten lässt sich ermitteln, welche Funktionen in Anwendungen besonders häufig genutzt werden und wo Potenzial für Verbesserungen oder Erweiterungen liegt.



Das Hauptdashboard liefert eine Übersicht über die wichtigsten Kennzahlen, darunter die Nutzungszeit, die Anzahl der Zugriffe, die meistgenutzten Produkte und die Topkunden des betrachteten Zeitraums



Visualisierung globaler Lizenzaktivitäten mittels Heatmaps zur regionalen Strategieoptimierung

- Gezielte Betreuung von Trial-Versionen: Das System zeigt, wie intensiv Evaluierungslizenzen beim Kunden tatsächlich genutzt werden. Wurde die Testversion überhaupt gestartet? Vertrieb oder Customer-Success-Teams können so zielgerichtet eingreifen und beispielsweise Hilfe bei der Einrichtung anbieten. Ein direkter Hebel zur Steigerung der Conversion-Rate.
- Weiterentwicklung von Geschäfts- und Lizenzmodellen: CodeMeter License Reporting schafft die Basis für Pay-per-Use- oder nutzungsabhängige Abrechnungsmodelle. Gerade in hoch spezialisierten Bereichen, in denen sich Software-Einsatz, Wartungsintervalle oder Kapazitätsanforderungen oft kurzfristig ändern können, erlaubt dieses Modell eine exaktere Kalkulation.
- Transparenz und Compliance: Durch präzise Auswertungen lassen sich sowohl interne Compliance-Regeln als auch externe Sicherheits- und Datenschutzvorgaben besser prüfen und dokumentieren.

Durch das Systen wird Lizenznutzung aktiv gesteuert, optimiert und für verschiedene Sicherheits-, Compliance- und Business-Zwecke genutzt. Dies gibt Unternehmen die Möglichkeit, Risiken gezielt zu minimieren und neue Umsatzchancen zu erschließen.

Gibt es bestimmte Unternehmen bzw. Branchen, die besonders von dem Einsatz einer solchen Technologie profitieren können?

Florian Schneider: Am stärksten profitieren Softwarehersteller, deren Produkte schützenswertes geistiges Eigentum (Intellectual Property, IP) enthalten. Gerade für Anbieter, die komplexe Algorithmen, proprietäre Verfahren oder branchenspezifische Funktionalitäten entwickelt haben, ist es entscheidend, nicht nur den Zugriff zu kontrollieren, sondern auch die tatsächliche Nutzung im Feld nachvollziehen zu können.

Besonders interessant ist das für Anbieter modular aufgebauter Softwarelösungen oder hochspezialisierter Engineering-Tools, bei denen einzelne Komponenten separat lizenziert werden. Wenn ein Anbieter erkennt, dass ein bestimmtes Modul regelmäßig an seine Nutzungsgrenze stößt, kann dies als Indikator für eine Upselling-Chance sein, oder darauf hinweisen, dass das bestehende Lizenzmodell zu restriktiv ist.

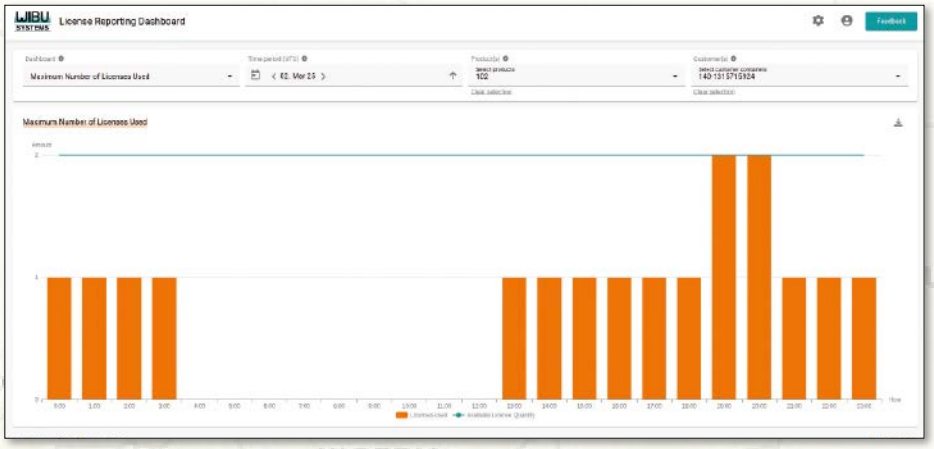
Natürlich spielt bei Wibu-Systems das Thema Sicherheit immer eine zentrale Rolle: Ist es im Rahmen des Monitorings auch möglich, den missbräuchlichen Einsatz von Lizenzen aufzudecken?

Florian Schneider: Das System visualisiert die Lizenznutzung, wodurch auch Unregelmäßigkeiten aufgedeckt werden können. Häufen sich etwa fehlerhafte Lizenzzugriffe, treten Nutzungspeaks zu ungewöhnlichen Zeiten auf oder erfolgen Lizenzzugriffe in Regionen, in denen die Software offiziell gar nicht vertrieben wird, kann dies ein Hinweis auf Lizenzdiebstahl oder unzulässige Kopien sein. Dank übersichtlicher Dashboards erkennen Verantwortliche schnell, wann Nutzerdaten oder Zugriffsmuster stark vom erwarteten Verhalten abweichen. So lässt sich zeitnah reagieren, zum Beispiel durch individuelle Analysen oder das Sperren und Anpassen betroffener Lizenzen über Remote-Update-Funktionen.

Beim Thema Sicherheit gibt es immer zwei Seiten zu beachten: Sicherheit für das Unternehmen auf der einen und der Schutz persönlicher Daten auf der anderen Seite. Wie wird eine DSGVO-Konformität bei CodeMeter License Reporting gewährleistet?

Florian Schneider: Datenschutz ist für uns ein zentrales Thema. CodeMeter License Reporting verarbeitet ausschließlich technische Nutzungsdaten im Zusammen-

Bitte umblättern ▶



Analyse der maximal gleichzeitig genutzten Lizenzen zur Ermittlung von Upselling-Potenzialen. Unternehmen können Engpässe in der Lizenzvergabe erkennen und proaktiv Lösungen anbieten ▶

hang mit Lizenzen. Zusätzlich erfolgt die Speicherung und Übermittlung der Daten verschlüsselt.

Wichtig ist: Die Übertragung dieser kann nur per explizitem Opt-in auf Nutzerseite aktiviert werden. Für unsere Kunden bedeutet das: vollständige DSGVO-Konformität und maximale Datensouveränität.

Auch die konkrete Auswahl der Technologie und die verwendeten Infrastrukturen spielen eine wesentliche Rolle, wenn es um die Sicherheit von Daten geht. Wie sichert sich Ihr Unternehmen diesbezüglich ab?

Florian Schneider: Wir setzen auf ISO-zertifizierte Rechenzentren innerhalb der EU, deren redundante Infrastruktur stets aktuelle Industriestandards erfüllt, insbesondere hinsichtlich Verfügbarkeit, Zugriffsschutz und Verschlüsselung. Zum konsequenten Schutz der Daten nutzen wir die bewährten CodeMeter-Sicherheitsmechanismen und gewährleisten durchgängige Verschlüsselung bei Speicherung und Übertragung. Ergänzend stellen kontinuierliche Sicherheitsprüfungen und Weiterentwicklungen sicher, dass die Datenintegrität gewahrt bleibt und wir neuen Bedrohungen stets wirksam begegnen können.

Nur ein kompromisslos sicheres System erfüllt die Erwartungen unserer Kunden und wird am Markt langfristig akzeptiert.

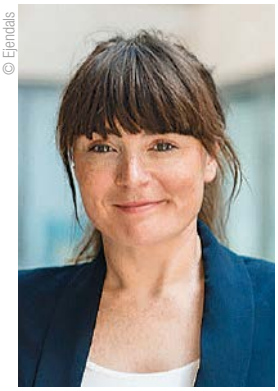
Bislang ist Code Meter License Reporting noch nicht auf dem Markt erhältlich. Wann wird das Produkt voraussichtlich verfügbar sein?

Florian Schneider: Wir planen die offizielle Markteinführung von CodeMeter License Reporting im zweiten Halbjahr 2025. Derzeit läuft ein Early-Access-Programm mit ausgewählten Kunden aus verschiedenen Branchen, um die Technologie unter realen Bedingungen zu erproben und finales Feedback einzuholen.

Damit stellen wir sicher, dass nicht nur Funktionalität und Sicherheitsstandards höchsten Ansprüchen genügen, sondern auch die Benutzerfreundlichkeit (Usability) überzeugt und wertvolles Nutzerfeedback berücksichtigt wird. Sobald die Erkenntnisse und das Feedback aus der laufenden Testung in die finale Version eingeflossen sind, erfolgt die offizielle Freigabe. Unternehmen, die sich frühzeitig ein Bild machen möchten, laden wir ein, sich über Möglichkeiten zur Teilnahme am Early-Access-Programm zu informieren oder CodeMeter License Reporting in einer Live-Demo kennenzulernen. GIT

Wibu Systems auf der SPS 2025:
Halle 6, Stand 428

Wibu-Systems AG
www.wibu.com



Patrick Nock, Technical Training and Support Manager DACH, und Distribution Relationship Managerin DACH bei Ejendals

Ejendals stärkt Marktpräsenz in der DACH-Region

Mit der Schaffung zweier neuer Schlüsselpositionen setzt Ejendals ein klares Zeichen für die individuelle Betreuung und den Wissenstransfer in der DACH-Region. Veronika Seliger, Master of Engineering seit 2020 bei Ejendals, übernimmt die neu geschaffene Funktion der Distribution Relationship Managerin für Deutschland, Österreich und die Schweiz. In dieser Rolle wird sie die Zusammenarbeit mit Distributoren und Einkaufsverbänden weiter ausbauen. Patrick Nock, seit 2019 Teil des Unternehmens und zertifizierter Fachberater für PSA, übernimmt die Position des Technical Training and Support Managers. Sein Fokus liegt auf der Durchführung technischer Produktschulungen für Handelspartner und Endkunden – sowohl eigenständig als auch in Kooperation mit den Vertriebsteams und innerhalb der Ejendals DACH-Akademie. Darüber hinaus vertritt er die DACH-Region in internationalen Referenzgruppen und sorgt für einen kontinuierlichen Austausch zu Markt-, Produkt- und Servicefragen. **www.ejendals.de**

Kübler ergänzt Weather-Workwear

Pünktlich zum Herbstanfang hat Kübler sein variantenreiches Wettersortiment wieder erweitert. Die wegen ihres urbanen Looks im Außendienst und bei Dienstleistern beliebte Hybridjacke wurde um eine Hybridweste ergänzt. Charakteristisch für beide ist die Kombination von melierter Strick- und symmetrischer Steppoptik. Das hier eingesetzte Strickfleece mit gestrickter Außen- und flauschiger Innenseite sorgt zusammen mit dem wattierten Innenfutter im Rumpfbereich für eine gute Wärmeisolierung bei gleichzeitiger Atmungsaktivität. Zum angenehmen Tragegefühl bei kühleren Temperaturen tragen außerdem der hochschließende Innenkragen aus anschmiegsamem Strickfleece sowie Armloch und Jackensaum bei, die mit elastischem Band eingefasst sind. Für mitgeführte Utensilien stehen links eine Napoleontasche mit Reißverschluss und rechts eine große Innentasche für Tablets bis zu 10 Zoll zur Verfügung. **www.kuebler.eu**

Konfigurierbare, intelligente Safety Relais

© Zander Aachen

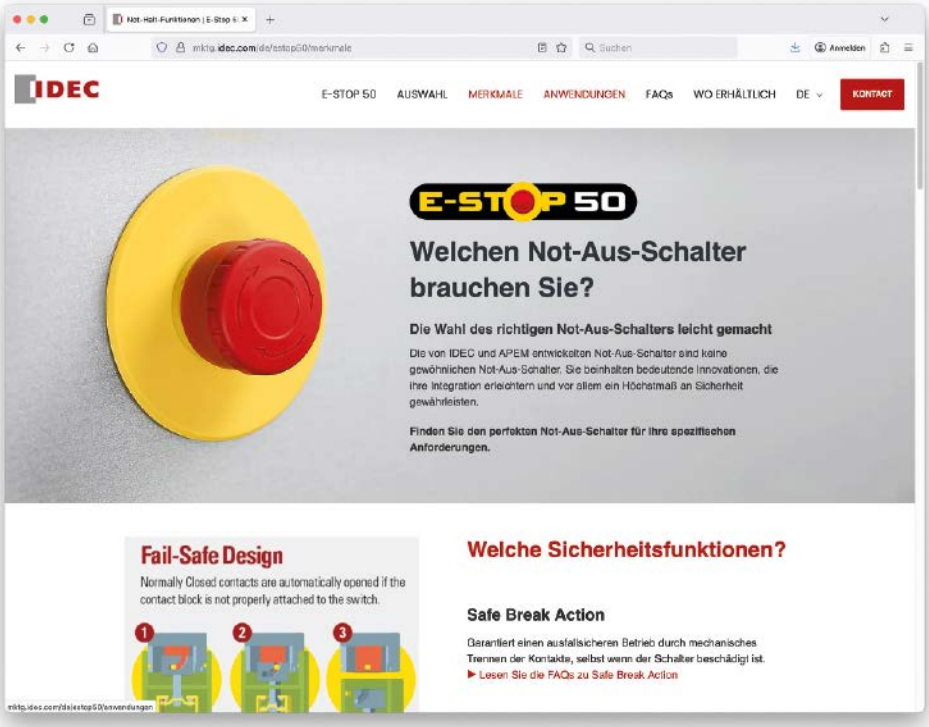
Zander Aachen zeigt auf der SPS in Nürnberg sein Safety-Portfolio, beispielsweise das Safety Relais Talos. Durch ein neues, einfaches Konfigurationstool wird aus der Safety Steuerung Talos ein sehr vielseitig einsetzbares Multifunktionssicherheitsrelais, das bis zu sieben klassische Safety Relais ersetzt. Das heißt, man erhält mit wenigen Klicks ein individuelles Sicherheitsrelais ohne großen Programmieraufwand.

Hier lassen sich mit einem einfachen Softwaretool die Art der Eingänge für alle handelsüblichen Sensoren und die logische Zuordnung zu den Ausgängen parametrieren. Folgende Parameter können eingestellt werden: Querschlussüberwachung: ja/nein; Sensor Art: OSSD, Antivalent, klassisch; Timer: Ein- und Ausschaltverzögerung für jeden sicheren Ausgang, Zeiteinstellung auch im Nachgang über Druck/Drehtaster am Gerät möglich; Retrigger-Funktion; Wischer-Funktion; Ausgangs-Schaltbedingungen. Das Besondere ist die einfache grafische Parametrieroberfläche. Hier sind auf einen Blick die gesamten Möglichkeiten der 14 sicheren Eingänge zu sehen. Diese werden durch eine kombinierte UND/ODER Architektur beliebig mit den drei sicheren Ausgängen verknüpft. Zudem stehen drei Start-/Reset-Eingänge zur Verfügung, die den sicheren Ausgängen zugeordnet werden können.

Das alles bis zum Performance Level e nach EN 13849-1. Zusätzlich ist Talos nach der neuen EN 13577-4 (ehemals 746-2) für Thermoprozessanlagen zertifiziert und für den Einsatz von Feuerungsanlagen im Dauerbetrieb nach EN 50156-1 konzipiert. Zudem erfüllt Talos die Anforderungen der allgemeinen Prozess-Industrie Norm nach EN 61511-1.

Somit hat man mit Talos eine platzsparende und kinderleicht parametrierbare Safety-Logik-Lösung zur Verfügung, ein perfekter Hybrid zwischen den klassischen Safety Relais und den wesentlich aufwendiger zu programmierenden sicheren Kleinsteuerungen. Talos ist bestens geeignet für Anwendungen in mittleren Anlagen im Maschinenbau und auch für die Prozessindustrie.

Zander auf der SPS 2025: Halle 7, Stand 191 **www.zander-aachen.de**



Die Online-Plattform eStop50 von APEM/IDEC bietet einen kompakten Überblick über gängige Not-Halt-Schalter und ihre sicherheitsrelevanten Merkmale

Mit wenigen Klicks zum passenden Not-Aus-Schalter

Umfangreiche Übersicht auf neuer Online-Plattform

Die Wahl des passenden Not-Aus-Schalters hängt von vielen Faktoren ab – von der Einbautiefe über Rückstellmechanismus, Schutzart, Beleuchtung und EMO-Funktion bis hin zur Versorgungsspannung. Mit der Aktionsplattform eStop50 bietet APEM/IDEC eine zielgerichtete Vorauswahl von 50 Varianten, die für die häufigsten Anwendungen im Maschinen- und Anlagenbau geeignet sind.

Die mit der Aktion eStop50 vorgestellten Not-Aus-Schalter richten sich an Entwickler, Konstrukteure und Sicherheitsverantwortliche, die kompakte und zuverlässige Lösungen für industrielle Anwendungen suchen. Typische Einsatzbereiche finden sich im Maschinen- und Anlagenbau, in der Automatisierungstechnik, in mobilen Systemen wie fahrerlosen Transportsystemen (AGVs), in der Robotik sowie in Handbediengeräten und batteriebetriebenen Steuerungen. Dank hoher Schutzarten, kompakter Bauform und Varianten mit geringer Betriebsspannung eignen sich die Serien XA und XW auch für anspruchsvolle Umgebungen – etwa in der Bildverarbeitung, im Außeneinsatz oder in sicherheitskritischen Bereichen mit beengtem Bauraum.

Serie XA für beengte Einbausituationen

Die Serie XA ist für Anwendungen mit begrenztem Platzangebot ausgelegt. Sie basiert auf einem robusten Unibody-Gehäuse und eignet sich für 16 mm-Einbauöffnungen. Trotz der kompakten Bauweise bietet sie eine Pilzgröße von 30 mm bzw. 40 mm, bis zu vier Schaltkontakte und Schutzarten bis IP69K. Je nach Ausführung liegt die Einbautiefe unter dem Panel bei nur 12,6 mm oder 17,0 mm – ideal für sehr schlanke Bedieneinheiten oder Gehäuse mit geringer Bautiefe. Die Entriegelung erfolgt durch Drehen oder Ziehen, wodurch Verwechslungen beim Zurücksetzen vermieden werden. Der Schalter wird an der Rückseite des

Auf der Aktionswebsite kann auch eine Auswahlübersicht heruntergeladen werden. In übersichtlicher Form werden die Not-Aus-Schalter nach Funktion, Bauform und technischen Merkmalen verglichen

Bedienfeldes verschraubt und kann nicht über die Vorderseite ausgebaut werden – ein sicherheitsrelevantes Merkmal, das Manipulationen erschwert und zusätzlich zur Robustheit beiträgt.

Serie XW entspricht IEC-Zertifizierung

Die Serie XW ist für 22 mm-Einbauöffnungen konzipiert und unterstützt zusätzlich die EMO-Funktion gemäß IEC 60204-1. Sie basiert auf der gleichen robusten Unibody-Bauweise wie die Serie XA und ist ebenfalls in einer besonders flachen Ausführung erhältlich. Auch hier liegt die Einbautiefe unter dem Panel – je nach Ausführung – bei 12,6 mm oder 17,0 mm. Varianten mit Dreh- oder Zugentriegelung, optionaler LED-Beleuchtung sowie Ausführungen mit 3–6 V LED-Spannung bieten hohe Flexibilität bei der Integration in bestehende oder mobile Systeme. Auch hier erfolgt die Befestigung über die Rückseite des Bedienfeldes.

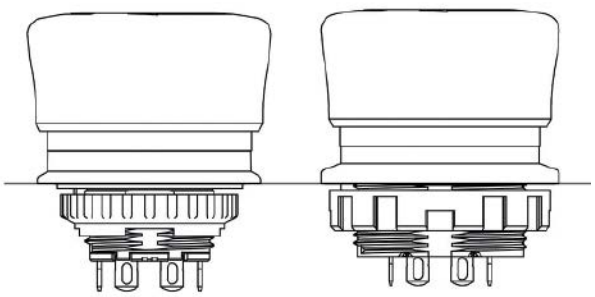
Umfangreiche Informationen zu verschiedenen Aspekten

Neben grundlegenden Informationen zur Produktauswahl bietet die Aktionsplattform praxisorientierte Inhalte zu Konformität und Standards, Funktionalität und Merkmalen, Einbau und Wartung sowie Anwendung und Nutzung. Thematisiert werden unter anderem normgerechte Entriegelungsmechanismen, EMO-Funktion sowie die Auswahl geeigneter Varianten für mobile Geräte mit begrenzter Stromversorgung. Für alle Produktserien stehen Datenblätter und 3D-Modelle zum Download bereit.

Ergänzend zu den technischen Informationen bietet die Aktionsplattform auch ein kompaktes White Paper zum Download an. Es behandelt zentrale Aspekte der sicherheitstechnischen Auslegung von Not-Aus-Schaltern und geht dabei auf typische Fehlerquellen sowie Anforderungen an moderne Lösungen ein. GIT

Apem auf der SPS 2025: Halle 7, Stand 493

Hier gelangen Sie zur Aktionsplattform



Die Serie XA ist auch in beleuchteter Ausführung erhältlich – im Bild wird der Unterschied zwischen aktiviertem und nicht aktiviertem Zustand deutlich

APEM GmbH
www.apem.de | eu.idec.com

Der MFT Pro 294 bietet, wie alle Handschuhe aus der MFT Pro-Reihe, durch die Verwendung von Mikrofaserfäden eine verbesserte Atmungsaktivität und Komfort

SCHUTZHANDSCHUHE

Showa auf der A+A 2025

Neue Handschuhlösungen, nachhaltige Initiativen und digitale Services für mehr Arbeitssicherheit von Showa

Eines der Hifhlights auf dem Stand von Showa war der CC700 der Chemikalien- und Schnittschutz vereint

Showa stellte auf der A+A in Düsseldorf zahlreiche Produktneuheiten vor, die auf die aktuellen Anforderungen im Bereich Arbeitsschutz eingehen. Im Mittelpunkt standen insgesamt 16 neue Handschuhmodelle, die laut Unternehmen fortschrittliches Design und verbesserte Schutzeigenschaften vereinen.

Zu den Highlights zählte der Showa CC700, der Chemikalien- und Schnittschutz mit erhöhter Fingerfertigkeit kombiniert und damit insbesondere für Branchen wie Maschinenbau, Chemie und Bauwesen entwickelt wurde. Ebenfalls vorgestellt wurde der Temres 282-02, ein atmungsaktiver, wasserabweisender und wärmeisolierter Handschuh für den Einsatz in kalten und nassen Umgebungen. Mit dem S-Tex Alpha präsentierte Showa ferner eine Weiterentwicklung im Bereich der schnittfesten Handschuhe auf Wolframbasis, die eine hohe Widerstandsfähigkeit bei gleichzeitig guter Beweglichkeit bietet. Die Anfang des Jahres eingeführte MFT Pro-Reihe, ausgestattet mit Mikrofaserfaden für verbesserte Atmungsaktivität und Komfort, wurde ebenfalls gezeigt.

Live-Demonstrationen und Produkttests

Im Product Demo Hub konnten Messebesucher die neuen Handschuhe unter realitätsnahen Bedingungen testen. Demonstrationen umfassten unter anderem Schnitt- und Chemikalienbeständigkeitstests für den CC700, Messer-basierte Schnittprüfungen mit dem S-Tex Alpha sowie Vergleiche der Feuchtigkeitsaufnahme und Atmungsaktivität mit der MFT Pro Serie. Zudem wurde die SafeDoff-Technologie vorgestellt, die ein sicheres Ausziehen der Handschuhe ohne Kontaminationsrisiko ermöglicht.

Nachhaltigkeit und digitale Services im Fokus

Neben den Produktneuheiten legte Showa auf der Messe einen Schwerpunkt auf Nachhaltigkeit. Das Unternehmen präsentierte seinen aktuellen Nachhaltigkeitsbericht „Showa In Balance“, der die Fortschritte bei der Reduzierung der Umweltauswirkungen in der Handschuhproduktion sowie den Einsatz nachhaltiger Materialien dokumentiert.

Showa stellte außerdem zwei spezialisierte Serviceplattformen vor, die Unternehmen bei der Einhaltung von Sicherheitsstandards unterstützen sollen. Die Plattform Sentinel by Showa kombiniert Vor-Ort-Bewertungen mit strukturierten Handschuhtests, um Risiken zu identifizieren und den Arbeitsschutz zu verbessern. Ergänzend dazu bietet die frei zugängliche Datenbank ChemRest detaillierte Informationen zur Chemikalienbeständigkeit von Handschuhen und unterstützt Anwender bei der Auswahl geeigneter Schutzausrüstung. Um das Wissen rund um ChemRest zu vertiefen, veranstaltet Showa am 21. November ein Webinar für die DACH-Region. GIT

Showa Group
www.showagroup.com

Praxisgerechte Lösungen für die sichere Lagerung von Gefahrstoffen

Ob Lacke, Öle, Chemikalien oder Gasflaschen – überall, wo Gefahrstoffe lagern, ist Sicherheit Pflicht. Schon ein kleiner Zwischenfall kann gravierende Folgen haben: Gefährdung von Mitarbeitern, Umweltschäden oder hohe Bußgelder. Deshalb schreiben Vorschriften wie WHG, TRGS und die bundesweit gültige AwSV klare Regeln vor. Sie fordern unter anderem dichte Lagerflächen, Rückhalteeinrichtungen und ein Konzept, das Risiken minimiert.

In der Praxis zeigt sich: Viele Betriebe tun sich schwer, alle Vorgaben im Blick zu behalten. Hier setzt die Firma Säbu Morsbach an. Seit 1987 entwickelt das Unternehmen praxisgerechte Lösungen für die sichere Lagerung von Gefahrstoffen. Mit der Produktlinie „Safe“ unterstützt Säbu Betreiber, ihre gesetzlichen Pflichten zuverlässig zu erfüllen. Die Gefahrstofflager verfügen über integrierte Auffangwannen, gefertigt nach StawaR (Stahlwannenrichtlinie) mit überwachten Schweißprozessen und Dichtheitsprüfung. Sie sind zugelassen durch die allgemeine bauaufsichtliche Zulassung des Deutschen Instituts für Bautechnik (DIBt, Berlin).

Das Ergebnis: flexible Lagersysteme, die sowohl Standardlösungen als auch individuelle Anforderungen abdecken. Bei kurzfristigem Bedarf bietet der Onlineshop fladafi.de passende Produkte – eine praktische Ergänzung für die Umsetzung betrieblicher Sicherheitskonzepte.

Betreiber profitieren von praxisnahen, geprüften Lagersystemen und von der Erfahrung eines Herstellers, der seit Jahrzehnten Sicherheit, Umwelt- und Arbeitsschutz in Einklang bringt. **www.saebu.de**

Sicherheit auf kleinem Raum: Das Gefahrstoffdepot „Safe Master“ mit aufklappbarem Dach ermöglicht schnellen Zugriff

SCHUTZFASER

Woher kommt meine Schutzbekleidung?

Transparente Lieferketten mit Lenzings Fasererkennungssystem für Schutzbekleidung

Durch Beimischung anderer Hochleistungsfasern zu Lenzing FR Fasern entstehen schwer entflammbare und flammhemmende Mischgewebe mit hohem Tragekomfort

Seit dem 1. Januar 2023 ist in Deutschland das sogenannte Lieferkettensorgfaltspflichtengesetz, kurz LkSG, in Kraft. Dadurch sollen Umwelt und Menschenrechte im globalen Handel besser geschützt werden. Ein hehres Ziel, dass jedoch nach wie vor massiv kritisiert wird. So bemängeln Umweltverbände- und Menschenrechtsorganisationen, dass die dortigen Regelungen nicht weit genug gehen, da sich die Sorgfaltspflicht der Unternehmen nur auf die unmittelbaren Zulieferer bezieht und nicht auf die gesamte Lieferkette. Umgekehrt sehen Wirtschaftsvertreter im LkSG eine weitere unzumutbare bürokratische Hürde, die in der veranschlagten Form von den betroffenen Unternehmen nicht erbracht werden könne, die Risiken allein auf die Unternehmen abwälze und einen weiteren Wettbewerbsnachteil für die deutsche Wirtschaft darstellt.

Um diesem Problem zu begegnen, hat die Lenzing AG, Hersteller von Spezialfasern, auf der diesjährigen A+A in Düsseldorf eine Lösung präsentiert, die die Transparenz in der Lieferkette und die Rückverfolgbarkeit der in Schutzbekleidung verwendeten Materialien erlaubt. Mit welchen Herausforderungen sich die Branche gegenwärtig und zukünftig konfrontiert sieht und wie die Lösung von Lenzing dazu beitragen kann, diesen zu begegnen, hat Oliver Spöcker, Leiter des Segments Schutz- und Arbeitsbekleidung bei Lenzing im Interview mit GIT SICHERHEIT erläutert.

GIT SICHERHEIT: Herr Spöcker, wie beurteilen Sie das LkSG? Welche Bedeutung hat das Gesetz und andere rechtliche Vorgaben, wie der Entwurf der EU-Kommission für eine Richtlinie über die Sorgfaltspflicht gegenüber Unternehmen im Bereich der Nachhaltigkeit (Corporate Sustainability Due Diligence Directive) für die Textilindustrie im Allgemeinen bzw. den Bereich Schutz- und Arbeitskleidung im Speziellen?

Oliver Spöcker: Lenzing begrüßt die Verabschiedung des LkSG. Es schafft Klarheit im gemeinsamen Kampf für einen besseren Schutz von Umwelt und Menschenrechten im globalen Handel. Nachhaltigkeit ist ein zentraler Wert für Lenzing und wir sind für unsere Bemühungen in den Bereichen verantwortungsvolle Beschaffung, energieeffiziente Produktion, nachhaltige Innovation und Verantwortung gegenüber den Menschen weithin anerkannt.

Dennoch muss Lenzing weiterhin auf Risiken achten und sicherstellen, dass unsere Lieferanten, Kunden, Geschäftspartner, Stakeholder und Mitarbeiter Verantwortung übernehmen und ihren Beitrag zum Schutz der Umwelt und der Menschenrechte leisten. Es ist wichtig, entlang der gesamten Wertschöpfungskette so zu denken und zu handeln, dass Lenzing Umweltbelastungen reduzieren und Menschenrechte schützen kann. Wir verpflichten unsere Lieferanten alle geltenden Gesetze und

Vorschriften einzuhalten und ermutigen sie, die Mindestanforderungen nach Möglichkeit zu übertreffen.

Transparenz ist die Grundlage für glaubwürdige Nachhaltigkeitsleistungen und schafft Vertrauen bei Kunden und Konsumenten. Deswegen setzt sich Lenzing für die Förderung digitaler Lösungen in der gesamten Lieferkette und für die Verbesserung der Transparenz und Rückverfolgbarkeit in der Schutzbekleidungsbranche ein.

Worin sehen sie die größten Herausforderungen für Unternehmen aus der Schutzbekleidungsbranche, wenn es darum geht, mehr Transparenz in den Lieferketten sicher zu stellen?

Oliver Spöcker: Komplexe globale Herausforderungen in der Lieferkette erfordern einen kooperativen Ansatz zur Entwicklung von Systemlösungen, an denen viele Akteure beteiligt sind. Lieferketten, die sich über mehrere Regionen und Länder erstrecken, bilden ein globales Netzwerk, das eine Vielzahl an lokalen Regeln, Vorschriften, Kulturen, Prozessen und Systemen einhalten muss. In der Schutzbekleidungsindustrie gibt es in jeder Region unterschiedliche Normen und Standards. Es ist daher besonders wichtig, dass all diese Normen eingehalten werden – Billigimporte oder Fälschungen bekannter Markenprodukte müssen unbedingt vermieden werden – sie sind in unserer Branche nicht akzeptabel, denn wir tragen Verantwortung. Die Kunden, die die Schutzkleidung letztlich tragen, müssen auf das Produkt vertrauen können.

Lenzing begegnet diesen Herausforderungen mit einem Vier-Säulen-Ansatz, der „Teilen", „Beweisen", „Kooperieren" und „Nachverfolgen" umfasst. Durch die enge Zusammenarbeit mit weltweit anerkannten Partnern, die Gewährleistung der Echtheit von Lenzing FR Fasern, die Unterstützung unserer Partner bei ihrer Entscheidungsfindung und die Sicherstellung der Rückverfolgbarkeit mittels Blockchain oder physikalischer Fasermarkierung entlang der gesamten Lieferkette setzen wir auf Transparenz, um die Herkunft seiner FR Fasern zu verifizieren.

Wie genau sieht die Lösung von Lenzing im Bereich Schutzbekleidung aus?

Oliver Spöcker: Als Antwort auf die steigende Nachfrage nach nachhaltigen Innovationen hat Lenzing hochwertige und zuverlässige Lenzing FR Produkte entwickelt. Dabei handelt es sich um eine nachhaltig produzierte Cellulosefaser, die auf dem bekannten Lenzing Produktionsprozess für Modalfasern basiert. Diese wird üblicherweise mit anderen Hochleistungsfasern gemischt, um einzigartige Schutzlösungen für eine Vielzahl von industriellen Anwendungen zu schaffen. Lenzing FR Fasern tragen in diesen Mischungen typischerweise sowohl zu den Schutzeigenschaften als auch zu einem verbesserten Tragekomfort bei.

Die Cellulosefasern werden aus Holz gefertigt und eignen sich für Schutzbekleidung, die unter extremen Bedingungen eingesetzt wird. Sie werden in Schutzbekleidung für Feuerwehr, Militär, Polizei, in der Öl- und Gasindustrie sowie in der metallverarbeitenden Industrie in über 100 Ländern eingesetzt. Zudem entsprechen die FR Fasern der Definition von inhärent schwer entflammbaren und flammhemmenden Fasern, wie sie vom Europäischen Chemiefaserverband CIRFS festgelegt wurden und sind mit dem EU Ecolabel zertifiziert.

Oliver Spöcker,
Leiter des Segments Schutz- und Arbeitsbekleidung bei Lenzing

Wie kann Ihre Lösung dabei helfen, dass die Schutzbekleidungsbranche die hohen gesetzlichen Rahmenbedingungen in Zukunft erfüllen kann? Welchen Vorteil bietet es den betroffenen Unternehmen?

Oliver Spöcker: Mit dem Lenzing Fasererkennungssystem gewährleisten wir die Rückverfolgbarkeit und Qualitätskontrolle in jeder Phase der Produktion und setzen einen neuen Standard für die Authentizität von Schutzbekleidung. Das System gibt unseren Partnern in der Wertschöpfungskette die Gewissheit, dass echte, hochwertige Lenzing FR Fasern verwendet werden und stärkt so auch ihr Vertrauen in die Lieferkette. Unsere kontinuierliche Zusammenarbeit mit Akteuren entlang der Lieferkette ermöglicht eine durchgängige Planung, Flexibilität und Reaktionsfähigkeit.

Wenn es um die Frage geht, woher meine Schutzbekleidung kommt, ist es natürlich auch wichtig die Quelle der Rohstoffe zu kennen. Woher bezieht Lenzing seine Rohstoffe?

Oliver Spöcker: Lenzing FR Fasern werden aus Holz hergestellt, das gemäß der Lenzing Wood and Pulp Policy aus nachhaltig bewirtschafteten Wäldern stammt. Diese Wälder wachsen ohne chemische Düngemittel und nehmen große Mengen an Kohlendioxid auf. Die FR Fasern werden dann in einem voll integrierten Produktionsprozess hergestellt. Die dabei verwendete Energie stammt zu mehr als 83 Prozent aus erneuerbaren Energiequellen und führt damit zu 80 Prozent weniger Treibhausgasemissionen als bei der Produktion herkömmlicher Modalfasern. Für Partner in der Wertschöpfungskette, die ihren CO_2-Fußabdruck reduzieren möchten, ohne Kompromisse bei Schutz und Komfort einzugehen, bieten wir auch die Option klimaneutraler Lenzing FR Fasern, zertifiziert durch ClimatePartner. GIT

Lenzing AG
www.lenzing.com

© Bilder: Lenzing

Liebe Leserinnen und Leser,

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

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

SICHERHEITS MANAGEMENT

Sicherheitsmanagement

barox
Switche für Video

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

Sicherheitsmanagement

FREIHOFF 24 GRUPPE

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

Sicherheitsmanagement

BOSCH

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

Sicherheitsmanagement

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

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

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

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

Security Robotics®

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

Sicherheitsmanagement

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

VIDEO ÜBERWACHUNG

GEBÄUDE SICHERHEIT

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

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

Gebäudesicherheit

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

Videoüberwachung

Ihr Value Added Distributor für Videosicherheitstechnik „Made in Germany“

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

Gebäudesicherheit

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

Gebäudesicherheit

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

Videoüberwachung

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

Gebäudesicherheit

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

PERIMETER SCHUTZ

Videoüberwachung

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

Gebäudesicherheit

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)

Perimeterschutz

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

Videoüberwachung

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

Videoüberwachung

HIKVISION

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

Zeit + Zutritt

DoorBird
Technology meets Design.

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

www.doorbird.com

Zeit + Zutritt

FEIG

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

Videoüberwachung

i-PRO

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

cryptin
CICHON STOLBERG

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

Zeit + Zutritt

gantner
INSPIRED ACCESS

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

Videoüberwachung

Zeit + Zutritt

deister electronic

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

Zeit + Zutritt

GUNNEBO

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

Zeit + Zutritt

DNAKE

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

Zeit + Zutritt

pcs

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

Zeit + Zutritt

AceProx
Identifikationssysteme GmbH

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

Zeit + Zutritt

dormakaba

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

Zeit + Zutritt

phg
Die richtige Verbindung

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

Zeit + Zutritt

AZS
SYSTEM AG

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

Zeit + Zutritt

ELATEC
RFID Systems

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

Zeit + Zutritt

primion
AZKOYEN Time & Security Division

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

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

BRAND SCHUTZ

ARBEITS SICHERHEIT

Zeit + Zutritt

salto
INSPIRED ACCESS

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

Brandschutz

DENIOS
UMWELTSCHUTZ & SICHERHEIT

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

Arbeitssicherheit

ELTEN

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

Zeit + Zutritt

TKH SECURITY

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

Brandschutz

Hertek
Brandschutzsysteme

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

Arbeitssicherheit

Hailo

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

NOTRUF SERVICE LEITSTELLE

GEFAHRSTOFF MANAGEMENT

Notruf- und Service-Leitstelle

HWS

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

Brandschutz

seTec

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

Gefahrstoffmanagement

asecos

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 Umluft-schränke, Druckgasflaschenschränke, Gefahrstoffar-beitsplätze, Absauganlagen, Raumluftreiniger uvm.

Notruf- und Service-Leitstelle

Fernwirk-Sicherheitssysteme Oldenburg
FSO
Ihr Security-Provider

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

Brandschutz

WAGNER
DIE BESSERE LÖSUNG IM BRANDSCHUTZ

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

Gefahrstoffmanagement

BAUER
SÜDLOHN

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

MASCHINEN ANLAGEN SICHERHEIT

Maschinen + Anlagen

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

Gefahrstoffmanagement

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

Maschinen + Anlagen

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

Maschinen + Anlagen

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

GASMESS TECHNIK

Maschinen + Anlagen

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

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

Gasmesstechnik

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

Maschinen + Anlagen

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

Maschinen + Anlagen

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

Sicherheit komplett

aus dem Wiley Verlag

NEWSLETTER
GIT-SICHERHEIT.de
Jetzt kostenfrei registrieren

www.git-sicherheit.de/newsletter

WILEY
Industry Talks

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

Ausgabe ONLINE lesen

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

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

WILEY

DIE VIP LOUNGE

Thorsten Neumann

President & CEO, Transported Asset Protection Association; Vorstandsvorsitzender der ASW Nord

- verheiratet, drei Kinder
- Dipl.-Ing (FH) Elektrotechnik (Fachrichtung Automatisierungstechnik)
- 10 Jahre bei Motorola, zum Schluss als Head of Supply Chain Security
- 8 Jahre Nokia, am Ende CSOO
- 7 Jahre Microsoft, Senior Director Global Supply Chain Resilience
- Seit 2020 Vorstandsvorsitzender des ASW Nord
- Seit 2012 NATO Industrie-Experte im Bereich Resilience, Kommunikation & Cyber Threats
- Seit 25 Jahren bei der TAPA EMEA, 20 Jahre im Board, 13 Jahre Chair of the Board und nun seit 2019 hauptberuflich bei der TAPA EMEA als President & CEO
- zweimaliger Deutscher Meister im BMX Freestyle

Ihr Berufswunsch mit 20 war: Ganz klar BMX-Profi, habe aber relativ schnell gemerkt, dass die Knochen und der Kopf in Bezug auf das körperliche Risiko irgendwann im Weg standen – daher der Umschwung in Richtung Ingenieur und später Sicherheit.

Was hat Sie dazu bewogen, eine Aufgabe im Bereich Sicherheit zu übernehmen? Als Elektroingenieur habe ich am Anfang meines Berufslebens fast immer das Gleiche gemacht. Dies ist in der Sicherheitswelt komplett anders und das hat mich bewogen, komplett in den Bereich Sicherheit zu wechseln. Es macht einfach Riesenspaß und man hat täglich neue Herausforderungen, um den Kriminellen hoffentlich einen Schritt voraus zu sein.

Welche sicherheitspolitische Entscheidung oder welches Projekt sollte Ihrer Meinung nach schon längst umgesetzt sein? Erstmal muss die Politik überhaupt verstehen, wie riesengroß und facettenreich der Bereich Sicherheit ist. Leider sind Politiker mediengetrieben und aus diesem Grunde fallen vielen Sicherheitsthemen bei der Politik durch das Raster. Ein nationales Lagezentrum Sicherheit ist definitiv ein sehr wichtiges Ziel. Und das Mindset: Wir sollten Sicherheit nicht mehr als lästig, sondern als notwendig und wichtig ansehen.

Die beste Erfindung im Bereich Sicherheit ist Ihrer Meinung nach: Das fängt bei einem guten Schloss an, geht über GPS-Systeme und endet derzeit klar in der Richtung von guten KI-Lösungen. Sicherheitssysteme machen das Leben zwar oft einfacher aber nicht immer sicherer – das Wichtigste das Zusammenspiel zwischen Mensch und Technologie.

Ein Erfolg, den Sie kürzlich errungen haben, war: Den deutschen OSPA für das Lebenswerk und, dass ich die schwarze Downhill-Strecke in Leogang ohne Probleme runtergekommen bin.

Wer hat Ihrer Meinung nach eine Auszeichnung verdient? Polizisten und Polizistinnen sowie jeder Sicherheitsmitarbeiter auf der Straße oder bei Events. Leider wird deren Arbeit zu oft unterbewertet und viele verstehen nicht wie wichtig Sicherheit für unsere Freiheit und Demokratie ist.

Wobei entspannen Sie? Beim MTB-Fahren und bei Lego. Ich liebe Lego und mein letztes Projekt hatte über 13000 Teile. Meine drei Jungs sind immer dabei und derzeit bauen wir einen republikanischen Sternenzerstörer der Venator-Klasse mit etwas über 6000 Teilen - wie man hört, liebe ich Star Wars.

Welchen Urlaubsort können Sie empfehlen? Ganz klar die USA, morgens Downhill MTB und abends einen Sprung in den Ozean. Wir lieben Kalifornien und natürlich Seattle, wo wir als Familie gewohnt haben. Ja auch unter Trump mögen wir das Land und die Leute. In Europa steht Italien an erster Stelle, da ich das italienische Essen liebe und mit einer Frau mit italienischen Wurzeln verheiratet bin.

Welche Zeitschriften lesen Sie regelmäßig? Bei mir ist alles online und dazu gehören die Welt, BBS, CNN und die Bild. Sonst das Freedom BMX Magazin und das Red Bull Action Sports Magazin.

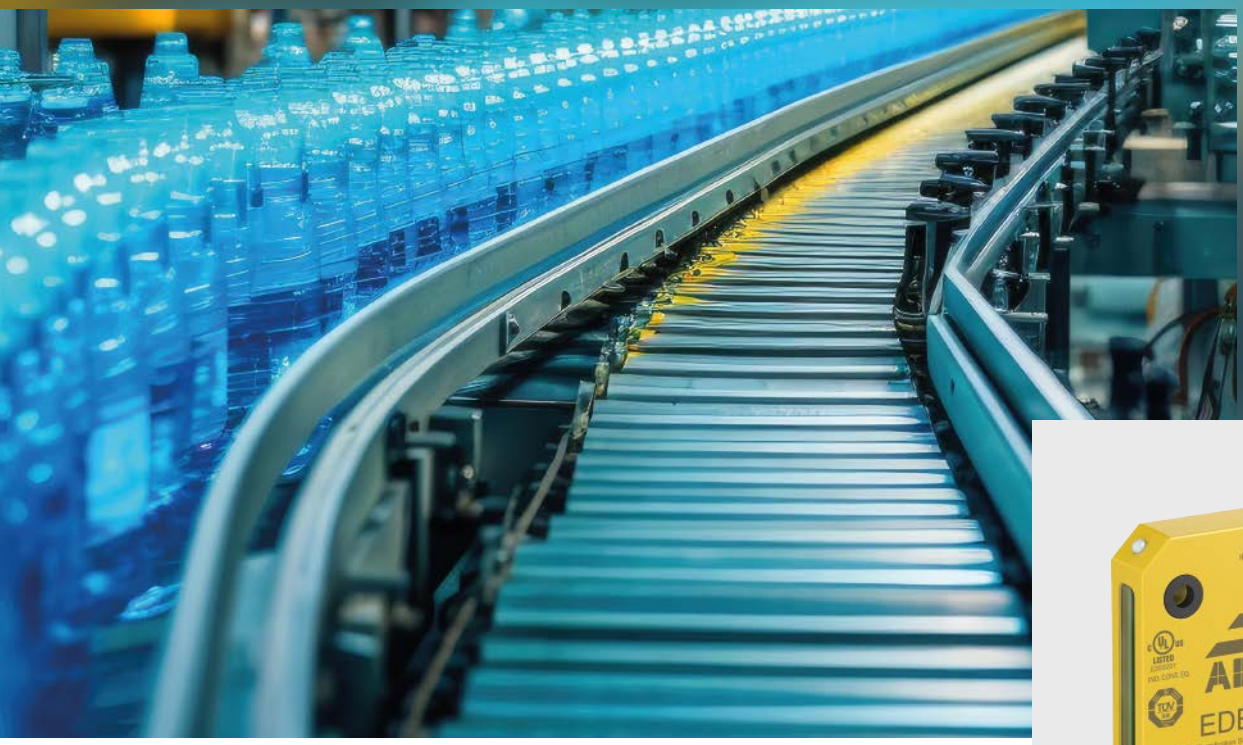
Die GIT SICHERHEIT ist für mich wichtig, weil … es spannend ist zu sehen, welche Themen Kolleginnen und Kollegen aus unserer Branche so bewegen und voranbringen und weil man einen schnellen Überblick über die Herausforderungen und Lösungen in der Sicherheitswelt bekommen kann. Des Weiteren kann man voneinander lernen und bekommt neue Ideen.

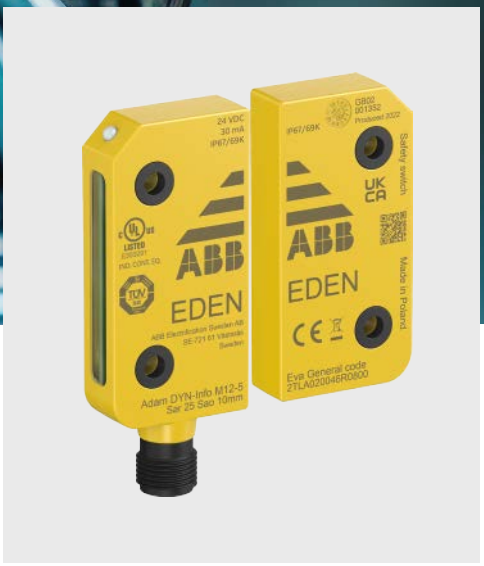
Welche Musik hören Sie am liebsten? Alles – aber ich liebe noch immer den klassischen Hip Hop wie Dr. Dre, NWA, Easy E, Cool & the Gang usw. Höre aber auch gerne etwas Ruhigeres wir Hans Zimmer

Was motiviert Sie? Meine Familie, Old School-Sachen, Gestaltungsspielraum, Kreativität, neue Technologien und mein Lebensmotto: „Keep it simple“ ist mein Megamotivator.

Worüber machen Sie sich Sorgen – und was stimmt Sie zuversichtlich? Ehrlich gesagt, mache ich mir wenig Sorgen, da ich extrem positiv bin. Ich fokussiere mich auf das, was ich kontrollieren kann, und arbeite daran, mögliche Risiken im Blick zu behalten und vorbereitet zu sein. Sorgen macht mir die gegenwärtige geopolitische Lage und das Gefühl, dass an der Realität vorbei diskutiert wird.

Welches Buch haben Sie zuletzt gelesen? „Das lustige Taschenbuch.“





MIT SICHERHEIT VERPACKT.

Eden C für anspruchsvolle Umgebungen

Dank beschichteter Elektronik gewährleisten die berührungslosen Sicherheitssensoren Eden C trotz schneller Temperaturschwankungen und hoher Luftfeuchtigkeit wie in der Lebensmittelindustrie höchste Sicherheit bei der Türverriegelung und Positionserfassung. Eden C ist sowohl mit dem ABB-eigenen Sicherheitssignal DYNlink als auch in der OSSD-Variante erhältlich. **solutions.abb/de-eden**

Jetzt QR-Code scannen
für mehr Informationen

Besuchen Sie uns auf der **SPS 2025!**
25.-27. November in Nürnberg
Halle 4, Stand 420

ENGINEERED TO OUTRUN

BIHL-WIEDEMANN.DE ■ JAHRGANG 19 ■ AUSGABE 02.2025

AS-INTERFACE MASTER NEWS

DAS MAGAZIN VON BIHL+WIEDEMANN

TECHNOLOGIE / INTERVIEW

Zukunftssicher automatisieren mit ASi-5 und ASi-5 Safety

APPLIKATION

Verpacken 2.0: Übersichtlich und flexibel – mit Sicherheit

Was Endanwender von ASi erwarten – und erhalten

ASi ... läuft!

Bihl + Wiedemann

Was Endanwender von ASi erwarten – und erhalten

ASi ... läuft!

AS-Interface – kurz ASi – hat sich im industriellen Einsatz den Ruf einer einfachen, kostengünstigen und gleichzeitig zukunftssicheren Verdrahtungs- und Steuerungstechnologie erworben und ist deshalb seit Langem in vielen Branchen wie der Verpackungstechnik, der Lager- und Fördertechnik oder der Prozesstechnik etablierter Standard. Ein wichtiger Grund für die Beliebtheit ist, dass nicht nur Maschinenbauer, sondern auch deren Kunden – die Endanwender – die vielen Vorteile der ASi Technologie schätzen.

ASi steht ganz allgemein für einfache, verpolsichere und topologieoffene Verdrahtung in Durchdringungstechnik – also ohne Stecker – an einem einzigen Profilkabel, die Übertragung von sicheren Signalen und Standardsignalen über die gleiche Leitung, bis zu 62 ASi-5 und ASi-3 Teilnehmer im gleichen ASi Kreis, umfangreiche Diagnosemöglichkeiten sowie nahtlose Konnektivität zwischen unterlagerten Systemen wie IO-Link und der Steuerungs- und IT-Welt. Dazu kommen ein umfangreiches Portfolio an Gateways und Modulen sowie Softwaretools zur effizienten Auslegung von ASi Netzwerken und Safety-Anwendungen. Eine Menge Gründe, warum Maschinenbauer gerne die Vorteile nutzen, die ihnen die ASi Lösungen von Bihl+Wiedemann bieten. Und die Tatsache, dass deren Kunden – also die Betreiber der Maschinen – ebenfalls signifikant von AS-Interface profitieren können, macht die etablierte Feldbuslösung für die untere Automatisierungsebene damit zu einer echten Win-Win-Technologie.

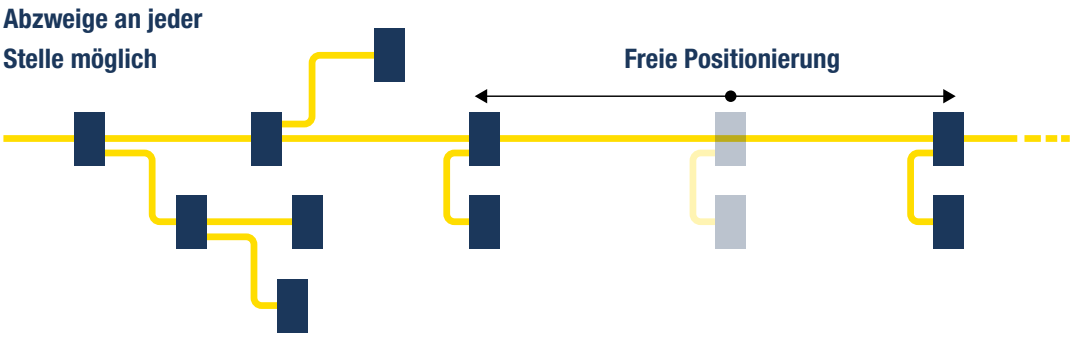
Schnelle und effiziente Integration und Inbetriebnahme

Doch bedingt die große Funktionalität nicht zwangsläufig eine hohe Komplexität? Weit gefehlt, denn Maschinenbauer – und damit auch Endkunden – können mit den Software-Suites von Bihl+Wiedemann eine einfache und intuitive Hardwarekonfiguration, Adressierung und Projektierung von ASi Netzwerken durchführen, was nicht nur Zeit spart, sondern auch Fehler vermeidet. Per Drag and Drop werden aus dem digitalen Hardwarekatalog, der in der Software hinterlegt ist, die passenden Module ausgewählt und zur Konfiguration hinzugefügt. Dabei bietet die Software stets passende Grundeinstellungen, die an individuelle Bedürfnisse angepasst werden können. Ist das Projekt vollständig konfiguriert, kann es am Bildschirm optimiert und in der finalen Auslegung vorab in Betrieb genommen werden. Im Rahmen der Hardwarekonfiguration können sehr leicht Teilkonfigurationen und Modulparameter von anderen Modulen oder Projekten übernommen werden. Die physische Inbetriebnahme vor Ort lässt sich dadurch wesentlich beschleunigen und die Suche nach möglichen Fehlern auf ein Minimum reduzieren.

Gleichzeitig bieten die unkomplizierte Verdrahtung mit Durchdringungstechnik und die gerade bei ASi-5 effiziente – weil auto-

Bild: Bihl+Wiedemann GmbH

Freie Wahl der Topologie



matische oder softwaregestützte – Adressierung von ASi Teilnehmern die Möglichkeit, während der Inbetriebnahme beispielsweise zusätzliche Sensoren und Aktuatoren zu integrieren oder vorhandene Geräte zu versetzen. Ein weiterer Vorteil der Lösungen von Bihl+Wiedemann gegenüber anderen Automatisierungslösungen zeigt sich bei der Verwaltung von IT-Schnittstellen: Während z. B. bei einer PROFINET-Anlage mit 50 Modulen die IT-Abteilung 50 IP-Adressen verwalten und absichern und für 50 netzwerkfähige Geräte und deren Industrie-4.0-Schnittstellen (z. B. OPC UA) regelmäßige Security-Updates durchführen muss, kann das bei ASi alles mit nur einem Gateway und einer einzigen IP-Adresse umgesetzt werden.

In Summe profitiert der Endanwender durch ASi somit von einer zeiteffizienteren Konfiguration und Inbetriebnahme – ohne funktionale Überraschungen, dafür aber mit der Option der flexiblen Erweiterung und Optimierung der ASi Installation.

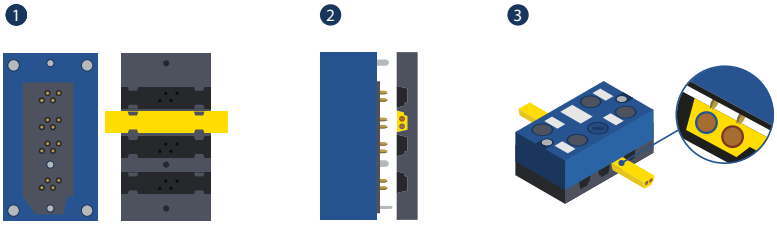
Einfache Wartung und Fehlerbehebung – auch in Eigenregie

Die weite Verbreitung von ASi in Branchen wie der Verpackungstechnik, der Lager- und Fördertechnik oder der Prozesstechnik hängt in erheblichem Maße mit dem hochgradig ausfallsicheren Betrieb der Technologie zusammen. Sollte es dennoch zu einer Störung durch eine Sensor-, Steuerungs- oder Antriebskomponente kommen, können sich Betreiber in vielen Fällen in Eigenregie helfen und eine mögliche Stillstandszeit der Maschine minimieren. Hierfür bietet Bihl+Wiedemann softwaregestützte Hilfestellungen wie die Online Businformation oder eine Diagnosesoftware, aber auch einen umfangreichen technischen Support, der mit Anleitungen zur Fehlerbehebung unterstützt und eine eventuell erforderliche Ersatzkomponente schnellstens auf den Weg bringt. Der Modultausch vor Ort wird per Autoadressierung zum Kinderspiel: Nach dem Austausch eines ASi Moduls wird dieses automatisch vom Gateway adressiert und parametriert und als Ersatz für das defekte Gerät in Betrieb genommen. Und für den Fall, dass ein Gateway getauscht werden müsste, kann die integrierte Chipkarte mit der gespeicherten Konfiguration einfach vom Alt- in das Austauschgerät umgesteckt werden. Dieses ist dann ohne weiteren Konfigurations- oder Programmieraufwand sofort betriebsbereit. Das erleichtert dem Maschinenbauer den Support und dem Betreiber die Reparatur – der Aufwand geht gegen null.

Diagnosefunktionen für hohe Verfügbarkeit bei minimierten Ausfallzeiten

Gezielte Diagnosen zur Überwachung von laufenden Prozessen ermöglichen es Maschinenbetreibern, schnell und gezielt auf mögliche Störungen zu reagieren. Bihl+Wiedemann bietet für jeden Einsatzfall zahlreiche Diagnose-Tools und eine breite Auswahl an Visualisierungsmöglichkeiten. Von Haus aus liefern die ASi Geräte verschiedene Diagnoseinformationen – über sich selbst, über die Performance von Bus und Leitungen, über den Zustand und die Funktion von Ports und Sensoren oder über Prozess- und Energiedaten.

Einfacher Modulanschluss dank Durchdringungstechnik



Diagnosesoftware von Bihl+Wiedemann

Darüber hinaus hat Bihl+Wiedemann mit der Diagnosesoftware ein leistungsstarkes Tool für alle ASi Netzwerke mit Komponenten des Unternehmens und von Drittanbietern – unabhängig davon, ob ASi-3, ASi-5, ASi-3 Safety at Work oder ASi-5 Safety eingesetzt wird. Der Betreiber kann Diagnosemessungen direkt an einem PC über das ASi-5/ASi-3 Feldbus Gateway durchführen – weitere Hardware ist hierfür nicht erforderlich. Kommunikationsstrukturen in Maschinen und Anlagen können so – kontinuierlich oder auch bei Bedarf – vom Maschinenbetreiber sehr einfach und zuverlässig auf Fehler untersucht werden. Probleme bei der Verdrahtung im Netzwerk, Kontaktierungsfehler, Erdschlüsse, Telegrammwiederholungen, fehlende ASi Teilnehmer oder Peripheriefehler – beispielsweise durch defekte Sensoren oder Aktuatoren – werden von der Diagnosesoftware zuverlässig erkannt, als solche klar verständlich angezeigt und um eine Handlungsempfehlung zur Störungsbeseitigung ergänzt. All dies ermöglicht ein effizientes Condition Monitoring, reduziert Zeit und Kosten für die Instandsetzung und minimiert die Stillstandszeiten und den Produktionsausfall der Maschine. Zudem können schon vorab getestete Maschinen an Endkunden ausgeliefert werden, weil auch der Maschinenbauer die Diagnosesoftware für Abnahme- und Freigabemessungen nutzen kann.

Technischer Support, schnelle und langjährige Ersatzteilverfügbarkeit

ASi Netzwerke kennen kein Haltbarkeitsdatum – sie sind oftmals jahrzehntelang im Einsatz. Entsprechend wichtig ist, dass Maschinenbetreiber – wie bei Bihl+Wiedemann – mindestens ebenso lange auf gute Betreuung, auf technischen Support und auf eine lange Verfügbarkeit von Ersatzteilen vertrauen können. Darüber hinaus stellt das Unternehmen auch für Endanwender gedachte Schnellstartanleitungen, Troubleshooting Guides und Schulungsmaterialien per Download zur Verfügung. In der Bihl+Wiedemann Academy werden zudem Online-Workshops und Kurse mit interaktiven Inhalten und kostenlosen Lehrmaterialien angeboten – alles mit dem Ziel, dass auch Betreiber ASi noch besser verstehen und optimal nutzen können. Vertrauen können die Endkunden auch auf regelmäßige Updates bei Soft- und Firmware, die ihre ASi Installation auf dem aktuellen Stand der Technik halten, sowie auf eine langfristige Verfügbarkeit von Ersatzteilen. Selbst sehr alte Gerätetypen, die schon vor mehr als 20 Jahren ausgeliefert wurden, sind heute noch verfügbar. Auch das macht die ASi Lösungen von Bihl+Wiedemann zu einer zukunftssicheren Technologie.

Schutz durch funktionale Sicherheit und Cyber-Security

Funktionale Sicherheit nimmt bei Bihl+Wiedemann ebenfalls einen breiten Raum ein. Während ASi Safety at Work vor allem bei der Integration von einzelnen NOT-HALT Tastern oder Lichtgittern punktet, bietet sich ASi-5 Safety für mehrere sichere Signale an einem Ort oder zukünftig auch für sichere Analogwerte und die Integration von IO-Link Safety an. Da es ASi erlaubt, sichere Signale und Standardsignale über dasselbe Kabel zu übertragen, profitieren Maschinenbetreiber – über die funktionale Sicherheit hinaus – somit von einer übersichtlichen und effizienten Hardware- und Verkabelungstopologie in ihrer Maschine.

Mit der Digitalisierung im Maschinen- und Anlagenbau ist Safety jedoch ohne Security – also den Schutz vor Cyberangriffen – kaum mehr denkbar. Dies zeigt sich auch in der neuen europäischen Verordnung (EU) 2023/1230 über Maschinen – kurz MVO, die ohne Übergangsfrist am 20. Januar 2027 in Kraft treten und die bis dahin gültige Maschinenrichtlinie 2006/42/EG (MRL) ablösen wird. In der MVO gewinnen Security-Aspekte und Cyber-Gefahren im Kontext von Maschinen, die beispielsweise für Software-Updates oder zur Fernüberwachung mit dem Internet verbunden sind, eine völlig neue Bedeutung. Die gleiche Stoßrichtung hat der Cyber Resilience Act (CRA) der Europäischen Union, der die Regeln zur Cybersicherheit von Produkten mit digitalen Elementen EU-weit vereinheitlichen wird und ebenfalls ab 2027 gilt.

Mehr Security in der Automatisierungstechnik wird kommen – und Maschinenbetreiber können mit ASi Lösungen von Bihl+Wiedemann auf höchste Daten- und Kommunikationssicherheit vertrauen. Denn die ASi Gateways des Unternehmens entkoppeln das ASi Netzwerk einer Maschine physisch von den IT- und Feldbusebenen – den typischen Einfallstoren für Cyberattacken. Dieser kommunikative Bruch zwischen ASi und TCP/IP isoliert die ASi Netzwerkteilnehmer nach außen und lässt so mögliche Sicherheitslücken erst gar nicht entstehen. Somit ist das ASi Gateway das einzige Security-relevante Gerät im Netzwerk. Um es zu schützen, werden bereits in der Entwicklung und auch bei der Inbetriebnahme von Bihl+Wiedemann umfangreiche Tests mit einer breiten Palette an Werkzeugen aus dem Bereich der Cybersicherheit durchgeführt, um die Unempfindlichkeit

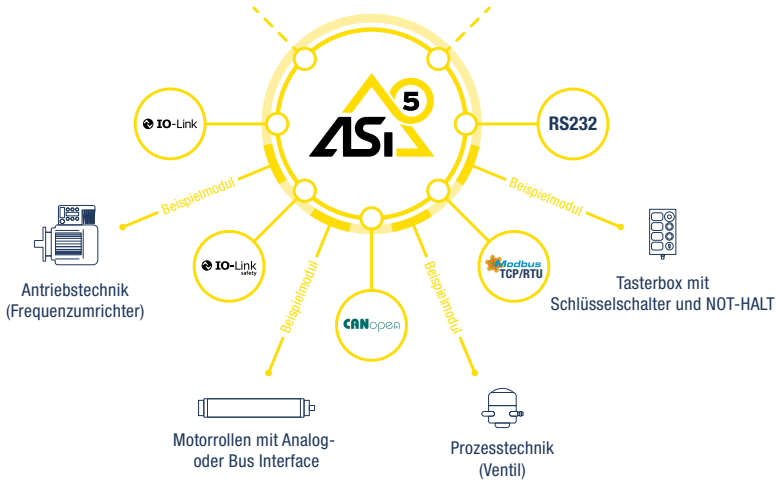
gegen Angriffe aus dem Internet sicherzustellen. Anlagenbetreiber – und insbesondere deren IT-Abteilungen – profitieren also sowohl davon, dass ASi über die Reduktion von Ethernetschnittstellen zu einem erheblich geringeren Securityrisiko innerhalb einer Anlage beiträgt, als auch davon, dass die verbleibende Verbindung zwischen ASi und Ethernet – das Gateway – ein Höchstmaß an Cybersicherheit gewährleistet.

ASi-5 hat Industrie 4.0 und das IIoT an Bord

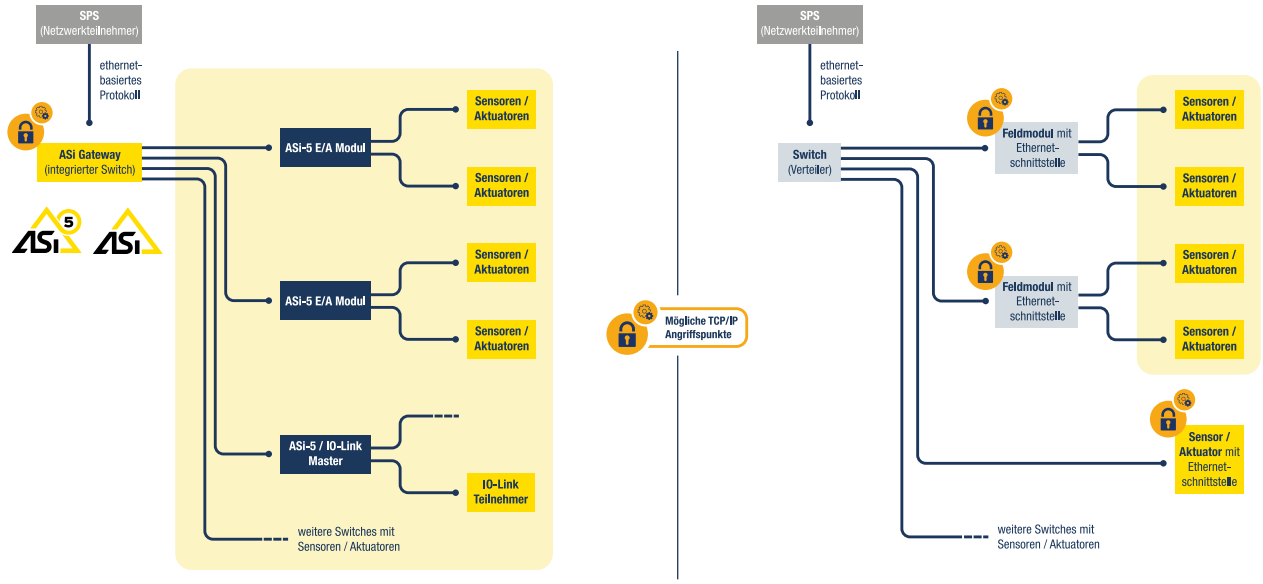
Industrie 4.0, die Smart Factory und das IIoT sind heute in der Industrie Synonyme für technologische Zukunftssicherheit. Daten sind für diese Technologien der entscheidende Rohstoff, den es auf intelligente und effiziente Weise zu sammeln, auszuwerten und in OT- und IT-Umgebungen zu übertragen gilt. Die ASi Gateways von Bihl+Wiedemann spielen hierbei eine wichtige Rolle, denn in ihrer Doppelfunktion als Schnittstelle und Netzwerkknoten auf der unteren Feldebene greifen sie als erste und direkt auf die Daten von Sensoren und Aktuatoren zu. Dank ihrer integrierten IT-Schnittstellen OPC UA und REST-API bieten sie direkte und zukunftssichere Kommunikationskanäle für Daten von der Edge bis in die Cloud. Dies ermöglicht es Endanwendern, über ASi heute oder später in jedem gewünschten Umfang in die Digitalisierung und Vernetzung seiner Maschine einzusteigen.

Wer seine Maschinen mit ASi Infrastruktur – insbesondere auch mit ASi-5 und ASi-5 Safety – betreibt, setzt damit auf eine leistungsstarke, zukunftssichere Verdrahtungs- und Steuerungstechnologie, bei der er von vielen Vorteilen profitieren kann.

Beispiele für die Konnektivität von ASi-5 (Safety)

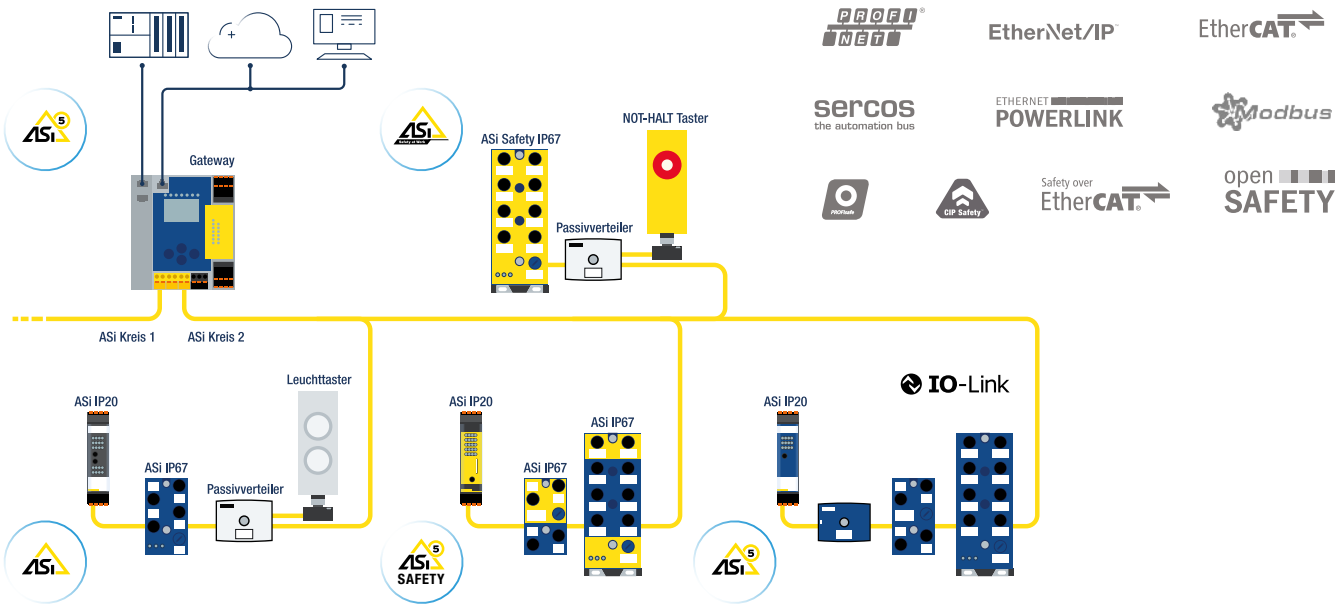


Im Gegensatz zu ethernetbasierten Feldbuslösungen ist bei ASi das Gateway das einzige Security-relevante Gerät im Netzwerk



Technologie

ZUKUNFTSSICHER AUTOMATISIEREN MIT ASi-5 UND ASi-5 SAFETY

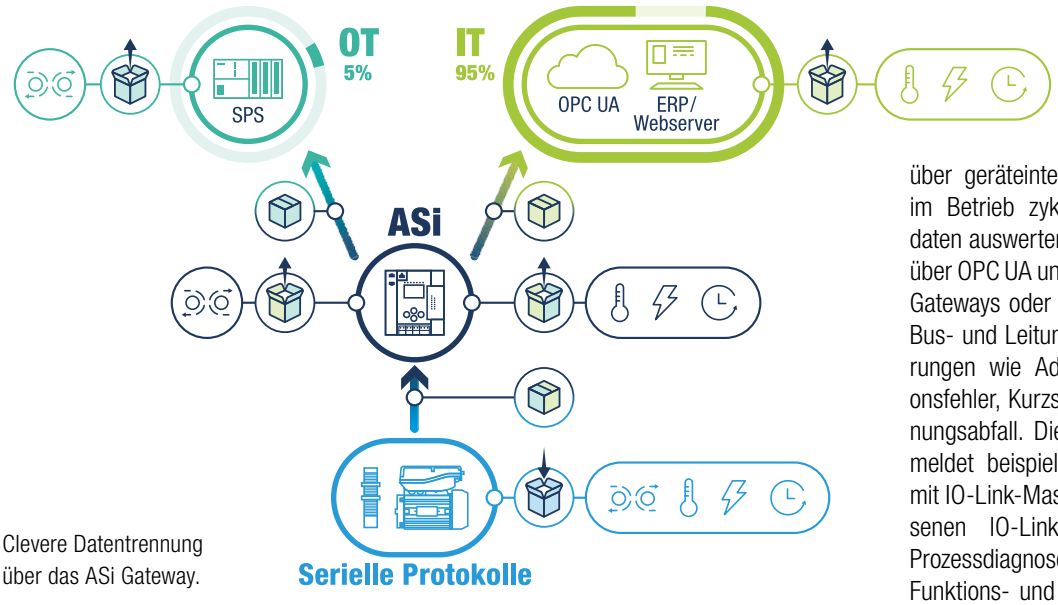


Unzählige Maschinenbauer etwa in der Lager- und Fördertechnik, in der Verpackungsautomatisierung oder der Prozesstechnik setzen seit Jahrzehnten bei der Verdrahtung und Automatisierung ihrer Maschinen und Anlagen auf AS-Interface und auf Bihl+Wiedemann. ASi-3 und ASi Safety at Work folgte vor wenigen Jahren mit ASi-5 und ASi-5 Safety ein technologisches Update. Es wurde zum großen Markterfolg, weil es alle Voraussetzungen zur zukunftssicheren Lösung auch anspruchsvollerer Applikationen mit sich bringt.

Wie heißt es in einem Sprichwort: „Erfolg kommt nicht von ungefähr." Das gilt auch für ASi-5 und ASi-5 Safety. Maßgeblich für die breite Akzeptanz der jüngsten AS-Interface-Generation sind weiterentwickelte oder neue Technologie-Merkmale wie

- die hohe Übertragungsgeschwindigkeit,
- die große Datenbandbreite,
- die clevere Integration von Smart Devices wie IO-Link Geräten, Ventilköpfen oder Frequenzumrichtern,
- die Möglichkeit, viele sichere Signale und Standardsignale unter nur einer Adresse zu nutzen oder
- die portgenauen Diagnosen und Zusatzinformationen, die die perfekte Datengrundlage für Industrie 4.0 liefern.

Während ASi-3 und ASi Safety at Work immer dann punkten, wenn es darum geht, einfache Standardanwendungen kostengünstig zu lösen, lassen sich mit ASi-5 und ASi-5 Safety jetzt auch deutlich komplexere Applikationen wie die Integration von IO-Link (Safety) Devices, moderne Antriebslösungen oder zukunftssichere Prozesstechnik-Applikationen effizient realisieren. In der Praxis



Clevere Datentrennung über das ASi Gateway.

sind ASi-3 und ASi-5 häufig als gemischtes System anzutreffen, weil sie als „Dream Team“ die Stärken beider Generationen verbinden. Hinzu kommen die für beide Standards typischen Vorteile der Verdrahtungs- und Bustechnologie auf der unteren Automatisierungsebene – also

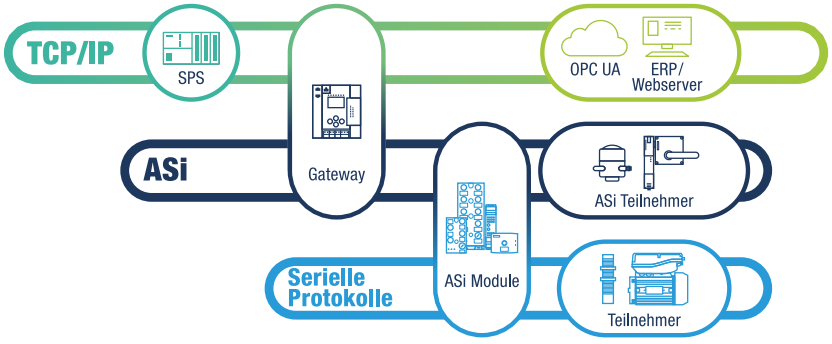
- der reduzierte Verdrahtungsaufwand mit Hilfe des ASi Profilkabels,
- der Anschluss von Teilnehmern per fehlersicherer Durchdringungstechnik genau dort, wo sie benötigt werden,
- die freie Wahl zwischen Stern-, Ring- oder Linienstrukturen beim Anlagenlayout,
- die Übertragung von Standard- und Safety-Signalen auf derselben Leitung,
- die umfangreichen Diagnosemöglichkeiten sowie
- die komfortable Integration mit der PC-Software von Bihl+Wiedemann mit Drag and Drop Systemkonfiguration, Parameter-Cloning zur schnelleren Inbetriebnahme identischer Teilnehmer und Inbetriebnahme-Assistent.

Weil die AS-Interface-Technologie auf Durchdringungstechnik und Profilkabel setzt und damit in der Regel auf vorgefertigte Kabel, Steckverbinder oder sonstige Hardware verzichten kann, bietet sie höchste Flexibilität beim Anschluss oder beim Versetzen von Netzwerkteilnehmern. Und ihre Performance sorgt dafür, dass ASi-5 auch als kostengünstige, einfache – und bereits in der Praxis bewährte – Alternative zu ethernetbasierten Lösungen überzeugt.

Umfangreiche Diagnosemöglichkeiten mit ASi-5

Mit ASi-5 werden die Prozesstransparenz und die Möglichkeiten der Predictive Maintenance moderner Maschinen und Anlagen wesentlich verbessert. Grundlage hierfür sind die umfangreichen Diagnosemöglichkeiten, die die Technologie bietet. Die Lösungen von Bihl+Wiedemann verfügen über geräteintegrierte Basisdiagnosen, die im Betrieb zyklisch anfallende Diagnosedaten auswerten – direkt über den ASi Bus, über OPC UA und REST-API, das Display des Gateways oder den integrierten Webserver. Bus- und Leitungsdiagnosen erkennen Störungen wie Adressier- und Kommunikationsfehler, Kurzschluss, Überlast oder Spannungsabfall. Die Geräte- und Portdiagnose meldet beispielsweise bei ASi-5 Modulen mit IO-Link-Mastern Fehler von angeschlossenen IO-Link-Geräten. Zustands- und Prozessdiagnosen liefern Daten zu Energie-, Funktions- und Umweltüberwachung direkt im Feld. Praktisch für die Remote-Wartung und das Ersatzteilmanagement sind die Parametrierungs- und Identifikationsdaten, die von jedem ASi-5 Device bereitgestellt werden. All diese Diagnosedaten lassen sich direkt an der Maschine anzeigen und nutzen – sie können aber auch über die ASi-5 Gateways von Bihl+Wiedemann mit OPC UA in MES/ERP-Systeme oder Cloud-Anwendungen eingebunden werden.

Ergänzend zu den genannten Möglichkeiten bietet Bihl+Wiedemann mit seiner Diagnosesoftware noch ein einfach zu bedienendes Tool, das Fehler und auch Fehlerpotenziale im gesamten ASi Netzwerk schon vor Eintritt einer eigentlichen Funktionsstörung sucht, schnell findet und beschreibt sowie konkrete Fehlerinformationen und direkte Lösungsvorschläge liefert.



Der kommunikative Bruch zwischen den einzelnen Kommunikationsebenen - vor allem zwischen ASi und TCP/IP - erhöht die Sicherheit.

ASi-5 Lösungen: Stand Alone oder Upgrade für Anlagen mit ASi-3

Weitere Gründe für die breite Marktdurchdringung von AS-Interface sind zum einen die Tatsache, dass es sich dabei um einen internationalen Standard handelt, der unabhängig von Anlage und Hersteller ist, weshalb in der Praxis auch herstellergemischte ASi Netzwerke ohne Probleme funktionieren. Zum anderen können ASi-5 und ASi-5 Safety Module zusammen mit früheren ASi Generationen im selben Netzwerk eingesetzt werden. Weil dafür lediglich das Gateway getauscht werden muss, können z. B. bestehende ASi-3 Applikationen so ganz einfach um ASi-5 erweitert und damit zukunftssicher gemacht werden. Und so verwundert es auch nicht, dass sich ASi-5 in kürzester Zeit zur perfekten Ergänzung zu ASi-3 entwickelt hat, was nicht zuletzt die weit über eine viertel Million bereits installierten Geräte der jüngsten ASi Generation im Feld belegen.

ASi Gateways von Bihl+Wiedemann bieten ein hohes Maß an Cybersicherheit

Wie wichtig es für Maschinenbauer und Anlagenbetreiber ist, auf dem Stand der Technik zu bleiben und nicht von Fortschritten der Technologie selbst oder von der Umsetzung wichtiger Zukunftsanforderungen ausgeschlossen zu werden, zeigt auch das immer aktueller werdende Thema Cybersicherheit, das gemäß der neuen, ab 20. Januar 2027 in Kraft tretenden europäischen Verordnung (EU) 2023/1230 über Maschinen – kurz MVO – explizit zu berücksichtigen ist. Bei smarten Devices mit integrierter Feldbusschnittstelle wie beispielsweise IO-Link Mastern, Frequenzumrichtern oder I/O-Devices besteht die Gefahr, dass dort Cyberattacken über die Ethernetbuchse im Feld erfolgen können und damit der Angriffspunkt und das Gefahrenpotenzial sogar bis weit ins Feld verschoben werden. Bei ASi-5 sind diese Cybergefahren dagegen nicht gegeben. Zum einen wurden bei der Entwicklung dieser Technologie Anforderungen aus der Normenreihe IEC 62443 über „Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme“ berücksichtigt. Zum anderen ergibt sich ein vielleicht noch wichtigerer Security-Aspekt aus der Funktionalität der ASi Gateways von Bihl+Wiedemann selbst. Ein ASi-5 Gateway mit OPC UA ist zwar mit seiner Verbindung zu TCP/IP das Bindeglied zwischen der äußeren Feldbus- und IT-Welt und der datentechnischen Netzwerkstruktur einer Maschine – es kann aber trotzdem nicht zum Einfallstor oder zur Angriffsplattform für Cyberattacken werden, denn das Gateway entkoppelt physisch die ethernetbasierten Schnittstellen von der Feldebene mit ASi. Dieser kommunikative Bruch zwischen ASi und TCP/IP isoliert die ASi Netzwerkteilnehmer nach außen und lässt so mögliche Sicherheitslücken gar nicht erst entstehen - ein Vorteil, von dem die Technologie auch als idealer Zubringerbus für Sensoren und Aktuatoren mit IO-Link oder IO-Link Safety profitiert.

Weil lediglich das ASi-5 Gateway selbst mit seiner IP-Adresse als Einfallstor möglicher Angriffe relevant ist, werden, um es cybersicher zu machen, bereits in der Entwicklung und auch bei der Inbetriebnahme von Bihl+Wiedemann umfangreiche Cyber-Security-Tests durchgeführt. Und auch nach der Installation, wenn die Maschine beim Anwender im Einsatz ist, können Firmware-Updates im Feld durchgeführt werden. Diese sind nicht nur absolut cybersicher, sondern auch explizit für Safety-Funktionen zugelassen. Entsprechendes gilt auch für Module und Geräte – wodurch es möglich ist, die ASi-5 Devices des Unternehmens immer mit den neuesten Security-Updates auszustatten.

Wer also seine Maschinen technologie-, cyber- und damit zukunftssicher und zugleich kosteneffizient automatisieren will, kommt an AS-Interface mit ASi-5 und ASi-5 Safety nicht vorbei.

Interview mit Josef Alaaddin, stellvertretender Teamleiter Technischer Support bei Bihl+Wiedemann

„ASi-5 und ASi-5 Safety haben sich im Markt etabliert“

ASi MASTER NEWS: Wie hat sich ASi-5 aus Sicht von Bihl+Wiedemann entwickelt?

Josef Alaaddin: ASi-5 und ASi-5 Safety haben sich im Markt flächendeckend etabliert. Dies beweisen u. a. die weit mehr als 250.000 ASi-5 Geräte von uns und anderen Herstellern, die bereits in Maschinen und Anlagen installiert sind. Die Technologie überzeugt dabei sowohl in reinen ASi-5 Applikationen wie als perfekte Ergänzung zu ASi-3. Und die Nachfrage insbesondere aus der Lager- und Fördertechnik, der Verpackungsautomatisierung und der Prozesstechnik bewegt sich weiterhin auf hohem Niveau. Dies liegt auch daran, dass mit ASi-5 in vielen Aufgabenstellungen aufwendige ethernetbasierte Lösungen vermieden oder ersetzt werden können. Und weil ASi-5 für uns ganz klar eine Erfolgsstory ist, entwickeln wir gerade auch einen ASi-5 Repeater, mit dem sich die mögliche Leitungslänge von ursprünglich 200 m zukünftig vervielfachen lässt.

ASi MASTER NEWS: Leitungslänge ist ein Thema – welche Vorteile bietet ASi-5 denn bei der Energieverteilung im Feld?

Josef Alaaddin: ASi-5 als Feldbus der unteren Automatisierungsebene macht die Energieverteilung, eine elementare Komponente der Technologie, sehr effizient und flexibel. Energie und Daten laufen über das bekannte gelbe 1,5 mm² Profilkabel, das für eine auf acht Ampère begrenzte Übertragungsleistung völlig ausreicht. Wenn aber, etwa für Antriebe oder Ventile, Bedarf für mehr Leistung besteht, kann dieser über ein zweites, schwarzes Profilkabel realisiert werden – mit einem Leitungsquerschnitt von 2,5 mm² sogar bis 20 A. Ebenfalls umgesetzt werden kann über das schwarze Profilkabel auch passive Sicherheit bis SIL3/PLe. Die Installation in Durchdringungstechnik ohne Stecker und weitere Module spart darüber hinaus nicht nur Verdrahtungsaufwand, Materialkosten und Montagezeit, sondern macht die Installation im Vergleich zu klassischen Feldbussen oder Punkt-zu-Punkt-Verbindungen auch viel schlanker und übersichtlicher. Da ein ASi-5 Strang bis zu 62 Teilnehmer versorgen kann, kann die Energieverteilung ohne zusätzliche Verkabelungen stufenweise angepasst werden.

ASi MASTER NEWS: Was bedeuten die zusätzlichen Möglichkeiten von ASi-5 für die Konfiguration von ASi Netzwerken?

Josef Alaaddin: Grundsätzlich können, wie schon bei ASi-3, alle Netzwerke mit ASi-5 Komponenten über ein Handadressiergerät und den Master konfiguriert werden. Wie komplex die Konfiguration wird, hängt dabei ganz wesentlich von der Komplexität der angestrebten Automatisierungslösung ab. Da wir unsere Kunden dabei so gut wie möglich unterstützen möchten, bieten wir ihnen mit unseren Software-Suites eine Lösung, mit der sie ihre Konfiguration deutlich vereinfachen und beschleunigen können. Damit lassen sich z. B. IO-Link Devices komfortabel konfigurieren oder Frequenzumrichter parametrieren, und die Parameterdaten können danach auch einfach von Modul zu Modul und sogar von Projekt zu Projekt kopiert werden. Außerdem können Anwender per

Drag and Drop ihre Projekte direkt aus dem integrierten Hardwarekatalog umsetzen und auch am Bildschirm testen.

Aber wir haben nicht nur die Maschinenbauer im Blick, sondern auch deren Kunden, die Anlagenbetreiber, denn sie sind es ja, die die Maschinen am Ende optimal nutzen sollen. Dafür macht es aber Sinn, dass sie unsere Produkte und Lösungen besser kennen und verstehen. Und deshalb unterstützen wir von Bihl+Wiedemann die Anwender nicht erst mit technischem Support, wenn sie ihn aktuell benötigen sollten, sondern schon von Anfang an mit Informations- und Schulungsmaterialien. Dazu zählen nicht nur unsere Installationsempfehlungen, Best Practises und der Troubleshooting Guide sowie eine Vielzahl von Schulungsvideos zu allen möglichen Themen auf unserer Webseite, sondern seit kurzem auch unsere Bihl+Wiedemann Academy.

ASi MASTER NEWS: Stichwort Installation: Warum bietet eine Installation mit ASi-5 Gateways Vorteile hinsichtlich der Cybersicherheit gegenüber anderen ethernetbasierten Lösungen?

Josef Alaaddin: Bei ASi-5 ist das Gateway mit OPC UA das Bindeglied zwischen TCP/IP und der ASi Installation, es entkoppelt aber auch physisch die ethernetbasierten Schnittstellen und die Feldebene mit ASi. Durch diesen kommunikativen Bruch kann das ASi Netzwerk nicht zur Angriffsplattform für Cyberattacken werden. Wird also statt eines IO-Link Masters mit integrierter Ethernetschnittstelle ein ASi-5 Modul mit integriertem IO-Link Master eingesetzt, können mögliche Sicherheitslücken gar nicht erst entstehen. Wenn also eine Kombination cybersicher ist, dann die von ASi-5 mit IO-Link. ASi-5 spannt hier quasi den Schutzschirm auf, unter dem IO-Link dann ohne Gefahren von außen betrieben werden kann.

ASi MASTER NEWS: Herr Alaaddin, vielen Dank für das Gespräch.

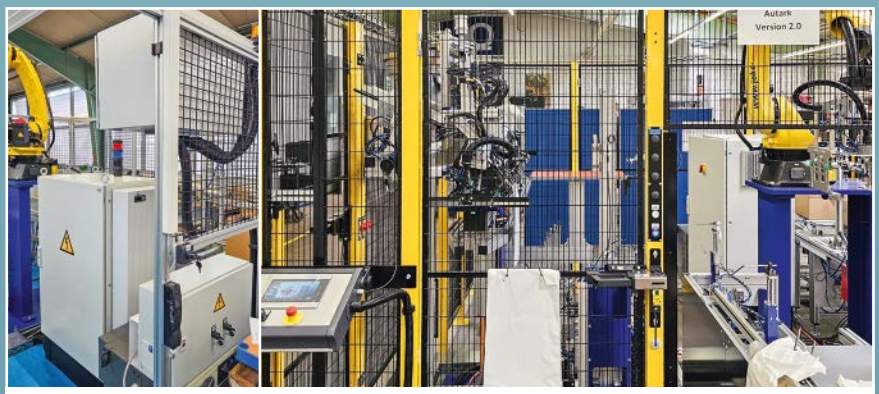
ASi-5 und ASi Safety statt Einzelverdrahtung bei joke mechanix

VERPACKEN 2.0: ÜBERSICHTLICH UND FLEXIBEL – MIT SICHERHEIT

Johannes Mück und Marcel Hammes von joke mechanix.

Statt sechs Schaltschränke nur noch einer und statt unzählige Kabelbündel nur noch zwei ASi Profilkabel und damit deutlich weniger Kabel(-wirrwar) und Verdrahtungsaufwand – dafür aber vereinfachte Fehlersuche und Diagnose, flexible Anpassung und Erweiterbarkeit auf Kundenwunsch und Safety inklusive. Argumente genug für joke mechanix, um bei seiner Roboterzelle „Robo Pack System" zur vollautomatisierten Verpackung von Seiten-Trennnaht-Klappenbeuteln zukünftig auf die ASi-5 und ASi Safety Lösungen von Bihl+Wiedemann zu setzen.

Die joke mechanix GmbH in Bergisch Gladbach wurde 1940 von Josef Joisten und Robert Kettenbaum als joke Folienschweißtechnik GmbH gegründet. Seitdem ist das Verschweißen von Folien und anderen Kunststoffen ein fester Kernbereich des Unternehmens. Über die Jahre hat sich joke nicht nur als Hersteller von Folienschweißgeräten, Impulssteuerungseinheiten, Schienen, Folienverarbeitungssystemen und kundenspezifischen Sonderlösungen einen Namen gemacht, sondern zunehmend auch als Dienstleister und Systemhaus für Robotic und Automatisierung. Während der Fokus zunächst eher auf kleineren Tischgeräten lag, erweiterte joke sein Angebotsspektrum nicht zuletzt durch die 2014 erfolgte Integration der Firma RENO-TEC um große und komplexe Anlagen zur Folienverarbeitung. Heute arbeitet das 2022 in joke mechanix GmbH umfirmierte Unternehmen eng mit seinem Schwesterunternehmen – der joke Technology GmbH – zusammen und nutzt die sich daraus ergebenden Synergien. Zu den aktuellen Produkten der joke mechanix GmbH zählen unter anderem der „joke Wicketer" zur Herstellung von Seiten-Trennnaht-Klappenbeuteln und das „Robo Pack System" für deren vollautomatisierte Verpackung.



Die Umsetzung der zweiten Version des Robo Pack Systems hat joke mechanix mit ASi Lösungen von Bihl+Wiedemann realisiert. Während für die erste Version (links) sechs Schaltschränke und dicke Kabelbündel benötigt wurden, kommt das Update mit einem Schaltschrank und zwei ASi Kreisen aus.

Wicketer und Robo Pack System

Der joke Wicketer ist eine Hochleistungs-Produktionsanlage für die präzise Herstellung von Seiten-Trennnaht-Klappenbeuteln aus Folien. Die Beutel werden beispielsweise für Brot, Obst, Gemüse, Gewürze oder Hygieneartikel verwendet. Um sie zu produzieren, zieht die Maschine die für die späteren Beutel verwendete Folie zunächst von einer Folienrolle über ein Faltdreieck. Danach werden die Beutelklappen eingefaltet und die Löcher zum Aufhängen mit einer pneumatischen Zweilochstanze in die Folie gestanzt. Anschließend werden die Ränder geschweißt, die Beutel an der Trennnaht getrennt und schließlich einzeln über ein Flügelrad zu einer Stapelkette mit einem Stiftstapler transportiert, wo sie – je nach Bedarf – in entsprechenden Stückzahlen übereinandergelegt werden. Danach wandert der Stapel eine Position weiter in Richtung Verpackungsort. Die Verpackung der Beutel in Kartons kann dann entweder manuell erfolgen, oder aber – was deutlich effizienter und schneller geht – vollautomatisiert.

Eine solche vollautomatisierte Verpackungslösung bietet joke mechanix mit dem Robo Pack System ebenfalls an. Das System kann dabei sowohl als Ergänzung zum Wicketer, aber auch als autarke Lösung für andere Maschinen eingesetzt werden. „Die Robo Pack Applikation ist so konzipiert“, erklärt Marcel Hammes, zuständig für Konstruktion und Engineering bei joke mechanix, „dass wir sie mit geringem Aufwand auch kompatibel zu Produktionsmaschinen anderer Hersteller machen können.“ Die Verpackung der produzierten Beutel erfolgt in einer sicherheitstechnisch überwachten Roboterzelle. Dort wird zunächst eine Pappe als Unterlage auf einem Drahtbügel platziert. Anschließend nimmt der Roboter einen Beutelstapel von einer Zuführung und steckt ihn auf den Bügel. Wenn sich die vorgegebene Menge an Beuteln auf dem Bügel befindet, werden eine zweite Papplage als Deckblatt und ein Stopfen als Halterung über den Beuteln auf dem Bügel platziert, bevor der Roboter das ganze Paket wieder aufnimmt und an die nächste Position – dem sogenannten Verschupper – transportiert. Dort wird der Bügel umgeklappt, damit er beim Stapeln im Karton später die darüberliegende Lage nicht aufspießt. Im Anschluss daran nimmt der Roboter die Beutellage erneut auf und legt das Bündel schließlich in den bereitstehenden aufgeklappten Karton auf einer Rollenbahn. Sobald der Karton voll ist, wird er über die Rollenbahn aus der Roboterzelle ausgeschleust.

Die Anbindung der NOT-HALT Taster, Türzuhaltungen und Lichtgitter wurde über aktive Verteiler ASi und aktive Verteiler ASi Safety umgesetzt, die platzsparend am oberen Rand der Roboterzelle über ein einziges ASi Profilkabel an das ASi Gateway im Schaltschrank angeschlossen wurden.

Einzelverdrahtung auf Klemmleisten: aufwendig und fehleranfällig

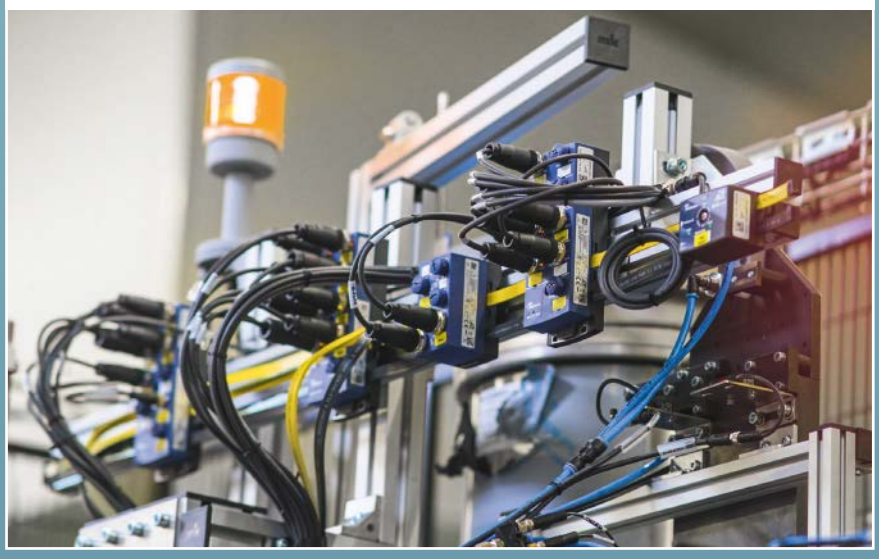
In einer ersten Version des Robo Pack Systems hat joke mechanix alle Signale und Funktionalitäten einzeln über Klemmleisten verdrahtet. Das hatte zur Folge, dass für die Umsetzung der Abläufe in der Roboterzelle enorme Mengen an Kabeln in Form von dicken Kabelbündeln über zum Teil weite Wege verlegt werden mussten. Dafür wurden sechs Schaltschränke benötigt, die vereinzelt noch mit dezentralen Steuerungen als Ergänzung zur Hauptsteuerung bestückt waren.

Da das Robo Pack System zukünftig auch autark funktionieren und damit auch mit anderen Beutel-Produktionsanlagen als dem Wicketer kombinierbar sein sollte – Stichwort Flexibilität – hat man sich, so Johannes Mück, Leiter Elektrotechnik bei joke mechanix, schon bald gefragt: „Wie können wir das System besser machen? Wie können wir den Aufwand minimieren, den wir aktuell haben mit der ganzen Verdrahtung oder auch bei der Fehlersuche? Und wie können wir das System (zukunfts-) sicher machen – da haben wir dann auch über Themen wie Safety und Security, IO-Link oder Industrie 4.0 gesprochen.“

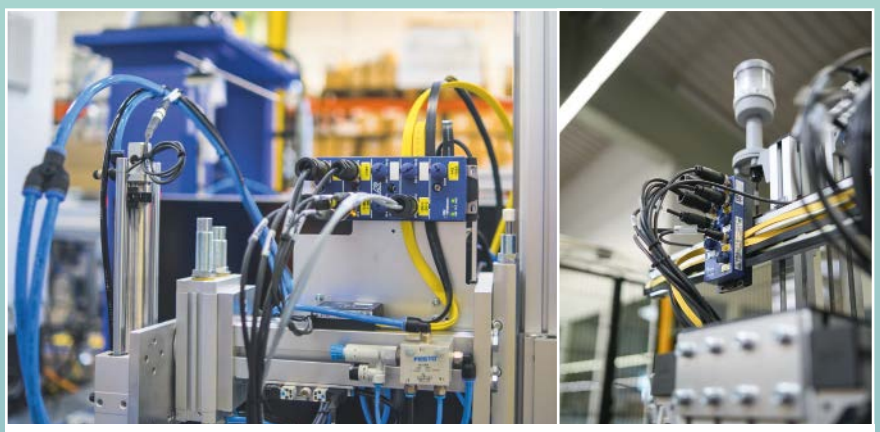
Weniger Aufwand und mehr Flexibilität mit AS-Interface

Obwohl man bis zu diesem Zeitpunkt selbst noch keine Applikationen damit realisiert hatte, war das Thema AS-Interface bei joke mechanix nicht gänzlich unbekannt. Durch erste Gespräche auf Messen und die Teilnahme an der „explore“-Workshopreihe von Bihl+Wiedemann hatte man bereits einen ersten Einblick davon bekommen, was mit den ASi und ASi Safety Lösungen des Mannheimer Unternehmens alles möglich war. In weiteren Gesprächen mit dem Außendienst von Bihl+Wiedemann wurde relativ schnell klar, dass sich – mit Ausnahme des Roboters – sowohl die Sicherheitstechnik für die Zelle als auch die Steuerung sämtlicher pneumatischer Bewegungen mit ASi-3, ASi-5 und ASi Safety realisieren lassen würde – und zwar mit deutlich weniger Verdrahtungsauf-

Für die Anbindung der IO-Link Ventilinseln für die pneumatischen Bewegungen und den Wendelförderer wurden ASi-5 Module mit integrierten IO-Link Master Ports und selbstkonfigurierende E/A Module von Bihl+Wiedemann verwendet.



wand, deutlich vereinfachter Fehlersuche und verbesserter Diagnose und deutlich höherer Flexibilität in Bezug auf zukünftige Veränderungen und Anpassungen etwa bei Kundenwünschen, als es die bisherige Lösung ermöglichte. „Und dass es mit AS-Interface möglich war, alle Funktionen inkusive Safety und IO-Link dezentral über einen einzigen Bus abzubilden“, erzählt Johannes Mück, „war für uns eine super Sache“. So hat man sich bei joke mechanix dann relativ schnell entschieden, die zweite Version des Robo Pack Systems mit der ASi Technologie zusammen mit Bihl+Wiedemann umzusetzen. „Was uns bei der Umsetzung natürlich immens geholfen hat“, so Mück, „war die tolle Unterstützung durch den Außendienst und den technischen Support von Bihl+Wiedemann bei der Auswahl der passenden Hardware und auch bei der Inbetriebnahme in Verbindung mit der Software ASIMON360“.



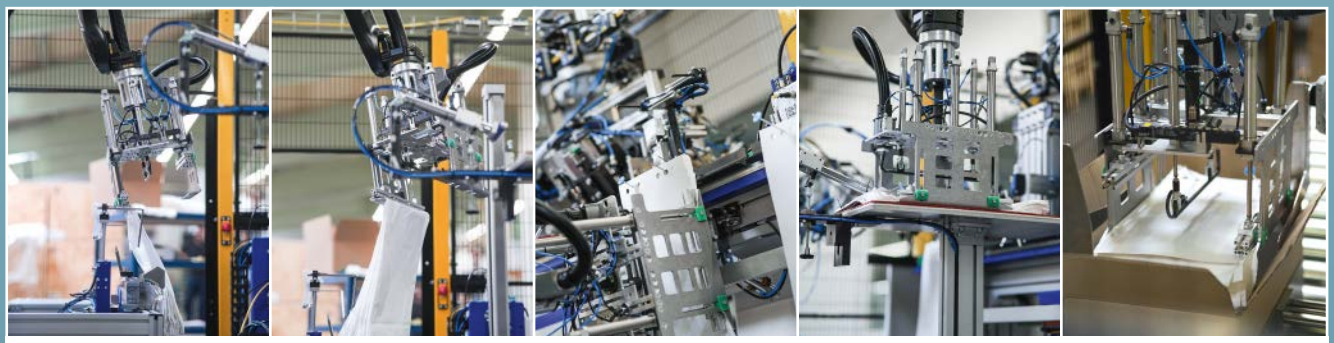
ASi-5 Modul BWU4230 von Bihl+Wiedemann.

Safety über eine einzige Leitung

Am deutlichsten sieht man die Unterschiede bei der neuen Version des Robo Pack Systems an der Menge der eingesetzten Kabel und Schaltschränke. Im Vergleich zur alten Lösung befindet sich in der Roboterzelle jetzt nur noch ein Schaltschrank, in dem neben der Robotersteuerung und dem ASi-5/ASi-3 openSAFETY über POWERLINK Gateway BWU3865 von Bihl+Wiedemann mit integriertem Sicherheitsmonitor für zwei ASi Kreise auch schon vordefinierte Schnittstellen für andere Beutelherstellungsanlagen untergebracht sind. Da die komplette Peripherie nur über zwei ASi Kreise – also lediglich über je zwei gelbe ASi Profilkabel für Daten und zwei parallel dazu geführte schwarze Profilkabel für zusätzliche Energie – angebunden ist, konnte auf die ganzen Kabelbündel und Klemmleisten und damit auf fünf von sechs Schaltschränke verzichtet werden. „Wir sparen uns mit der neuen AS-Interface-Lösung damit nahezu den kompletten Schaltschrankbau und natürlich einen ganz großen Teil vom Verdrahtungsaufwand“, so Johannes Mück. „Und zukünftig können wir diesen noch weiter reduzieren, wenn wir dort, wo wir Kabel benötigen – etwa bei der Anbindung der Pneumatik an die Ventile oder der IO-Link Komponenten an die ASi Module – diese nicht mehr selbst konfektionieren müssen, sondern passgenau bestellen können.“

In der Roboterzelle gibt es verschiedene Safety-Applikationen, die über einen der beiden ASi Kreise – gesteuert und überwacht vom ASi Safety Gateway – realisiert werden. Über Türzuhaltungen an mehreren Stellen wird dafür gesorgt, dass niemand während des Betriebs eine der Schutztüren des Zauns um die Roboterapplikation öffnen und den Innenraum betreten kann. Stellen, an denen sich Löcher im Schutzzaun befinden, damit bei Bedarf entweder Pappe nachgefüllt oder eine Stichprobe zur Qualitätskontrolle entnommen werden kann, sind über Lichtgitter abgesichert. Und selbstverständlich ist der Schutzzaun auch mit mehreren NOT-HALT Tastern an unterschiedlichen Stellen bestückt, um den Roboter bei Bedarf auch auf diese Weise stillzusetzen. Alle Safety-Komponenten hängen dabei an einem einzigen, mit dem Gateway im Schaltschrank verbundenen ASi Profilkabel, das einmal rundherum am oberen Rand des Schutzzauns verlegt wurde.

Zur Umsetzung der oben genannten Sicherheitsfunktionen ist an dieser Stelle noch eine Besonderheit zu erwähnen: Sowohl bei den Lichtgittern wie auch den Türzuhaltungen und NOT-HALT Tastern handelt es sich um Safety-Geräte ohne eigene ASi Safety Funktionalität.



Transport eines Beutelstapels vom Ablageort über das Anbringen von Pappe und Stopfen sowie das Verschuppen des Bügels bis zur Ablage in den Karton.

Solche Sicherheitskomponenten können aber über aktive Verteiler von Bihl+Wiedemann wie BWU3599 und BWU3719 ohne großen Aufwand „ASi Safety fähig“ gemacht und dann wie vergleichbare ASi Safety Komponenten genutzt werden. Für Hersteller von Maschinen hat diese einfache Möglichkeit den Charme, dass sie noch flexibler auf Kundenwünsche eingehen können, etwa was die Präferenz für bestimmte Geräte oder Hersteller betrifft, und nicht auf mit einer bestimmten Technologie ausgestattete Komponenten beschränkt sind.

Ebenfalls über ASi Safety umgesetzt wird das Thema Muting. Damit das System nicht immer angehalten werden muss, wenn ein leerer Beutelkarton nachgeschoben beziehungsweise ein voller Karton ausgeschleust werden soll, kann über Muting ein sicherer automatisierter Materialtransport in die Roboterzelle hinein oder aus ihr heraus ermöglicht werden. Mit Hilfe von zwei aktiven Verteilern ASi zur Erfassung der Mutingsensoren und einem aktiven Verteiler ASi Safety für das Lichtgitter werden dabei die Bewegung(srichtung) des Kartons überwacht und, wenn die Voraussetzungen erfüllt sind – also sichergestellt ist, dass es sich um einen Karton und nicht um einen Menschen handelt – die Schutzfunktion des Lichtgitters an der entsprechenden Stelle für den benötigten Zeitraum unterdrückt, so dass der Karton im laufenden Betrieb des Roboters in die Zelle oder aus ihr heraus bewegt werden kann. Wenn dagegen eine Person durch die Muting-Applikation identifiziert wird, wird die Maschine umgehend stillgesetzt.

Bewegungen umgesetzt mit Hilfe von IO-Link und ASi-5

Neben der funktionalen Sicherheit spielt der Bereich Pneumatik im Robo Pack System ebenfalls eine zentrale Rolle. Alle Dreh- und Schwenkbewegungen, die für die Schritte zwischen der Übernahme des Beutelstapels von der Produktionsmaschine bis zur Ablage im Karton nötig sind und die nicht vom Roboter selbst ausgeführt werden – also für die Bereitstellung des Drahtbügels, die Anlieferung und Positionierung der Pappen und der Stopfen sowie das Verschuppen des Bügels – werden über Pneumatikzylinder in

ASi-5 Modul BWU4088 mit einem IO-Link Master Port (links) und BWU4067 mit vier IO-Link Master Ports (rechts).

Verbindung mit IO-Link Ventilinseln umgesetzt. Für IO-Link Ventilinseln hat man sich unter anderem deshalb entschieden, weil man so auch viel mehr Prozessdaten erfassen kann – Stichwort Industrie 4.0. Eingebunden werden diese Ventilinseln über den zweiten ASi Kreis über ASi-5 Module mit integrierten IO-Link Master Ports von Bihl+Wiedemann. Auch hier hat sich der Einsatz von AS-Interface für joke mechanix sowohl technisch wie auch aus Kostensicht als Vorteil erwiesen. Im Vergleich zu anderen Lösungen, bei denen man standardmäßig auf 4-Port- oder gar 8-Port-Module zurückgreifen und damit nicht genutzte Ports teuer bezahlen muss, kann man bei der Integration von IO-Link über ASi-5 bei Bihl+Wiedemann aus einem Portfolio von Modulen mit ein, zwei, vier oder acht IO-Link Master Ports immer genau die passende Option wählen, die man gerade braucht – je nachdem, wie viele IO-Link Master Ports Class A oder Class B an der jeweiligen Stelle gerade benötigt werden.

Flexibel dank AS-Interface

Zusätzlich zu den Ventilinseln hängen am zweiten ASi Kreis – integriert zum Beispiel über die ASi-5 Module BWU4230 mit 16 selbstkonfigurierenden E/As – auch die Ansteuerung für den Wendelförderer, der die blauen Stopfen für die Drahtbügel bereitstellt, und mehrere Sensoren, unter anderem Lichtsensoren, sowie ein Referenzsensor für den Motor, der die Bügelkette zur Aufnahme der Beutelpakete antreibt.

Gerade in diesem Teil der Anlage zeigen sich für Johannes Mück noch weitere Vorteile der ASi Lösungen von Bihl+Wiedemann. „ASi-5 und ASi-3 über die gleiche Leitung laufen lassen zu können, ist schon klasse. Man spart Adressen, ist deutlich flexibler bei den Anwendungen und dadurch, dass viele der Feldmodule von Bihl+Wiedemann, die wir hier verwenden, über vier Anschlüsse für Profilkabel – zwei für das ASi Kabel und zwei für das AUX Kabel – verfügen, können wir bei Bedarf auch Abzweige ganz leicht umsetzen, ohne dafür ein zusätzliches Modul einsetzen zu müssen“.

Das Robo Pack System von joke mechanix ist – allein durch eine Vorher-/Nachher-Betrachtung – ein gutes Beispiel dafür, das zeigt, wie viele (Einspar-)Potenziale die ASi und ASi Safety Lösungen von Bihl+Wiedemann Maschinenbauern für eine einfache, flexible und (zukunfts-)sichere Automatisierung ihrer Maschinen bieten.

ASi-5/ASi-3 openSAFETY über POWERLINK Gateway BWU3865 von Bihl+Wiedemann mit integriertem Sicherheitsmonitor für zwei ASi Kreise.

CONNECTION

Connection Zone auf der SPS 2025 – Kleiner Rundgang, großes Potenzial

Noch nie war es so leicht, zusätzliche Potenziale für Ihre Automatisierung live zu entdecken. In unserer neuen Connection Zone erfahren Sie in kurzer Zeit, wie Sie Ihre Anlagen produktiver, nachhaltiger und zukunftssicherer automatisieren – und dabei nahtlos mit allen gängigen Feldbussen verbinden.

Lassen Sie sich Schritt für Schritt von unseren Produktspezialisten auf der SPS 2025 durch die Zone führen und erleben Sie hautnah, wie Sie

- bis zu 68 % Verdrahtungskosten sparen dank ASi Profilkabel
- funktionale Sicherheit ohne zusätzliche Infrastruktur integrieren
- IO-Link-Anwendungen mit bis zu 50 % geringeren Kosten realisieren
- IIoT-Projekte einfach über moderne IT-Schnittstellen umsetzen
- Antriebe effizient ansteuern und Montageaufwand stark reduzieren

Ein kleiner Rundgang durch die Connection Zone und Sie wissen genau, welches Potenzial die ASi Lösungen von Bihl+Wiedemann bieten – und wie Sie sie gezielt für neue Anlagen oder Retrofit-Projekte einsetzen.

Starten Sie Ihre Entdeckungsreise zu effizienter Verdrahtung und smarter Automatisierung. Wir freuen uns auf Sie in Nürnberg.

ZONE AUF DER SPS 2025

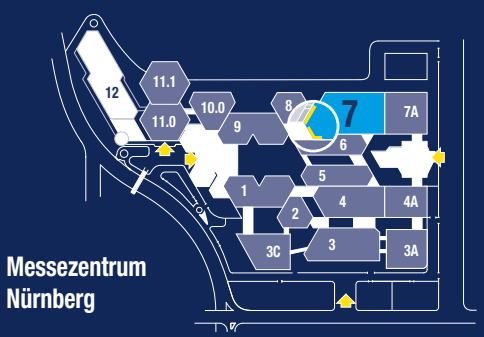
Zeit sparen
Keine Stecker, keine vorkonfektionierten Kabel

Flexibel bleiben
Kompatibel mit gängigen Feldbussen und Schnittstellen

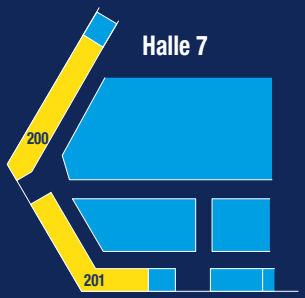
Investition sichern
Zukunftssichere Integration von IO-Link und analogen Signalen

Schaltschrankplatz optimieren
Konsequente Dezentralisierung in der Anlage

Ressourcen schonen
Weniger Material, Energie und Abfall



Messezentrum Nürnberg



sps
smart production solutions

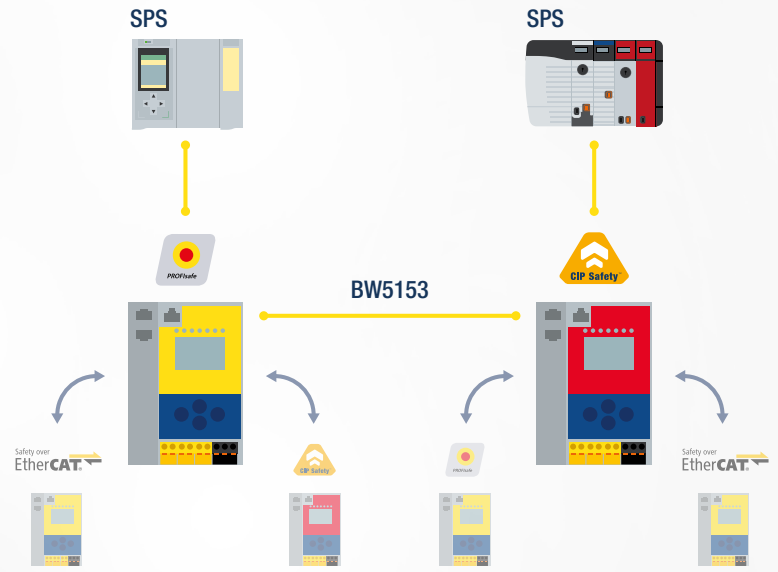
25.11. - 27.11.2025
Nürnberg | Halle 7
Stand 200 + 201

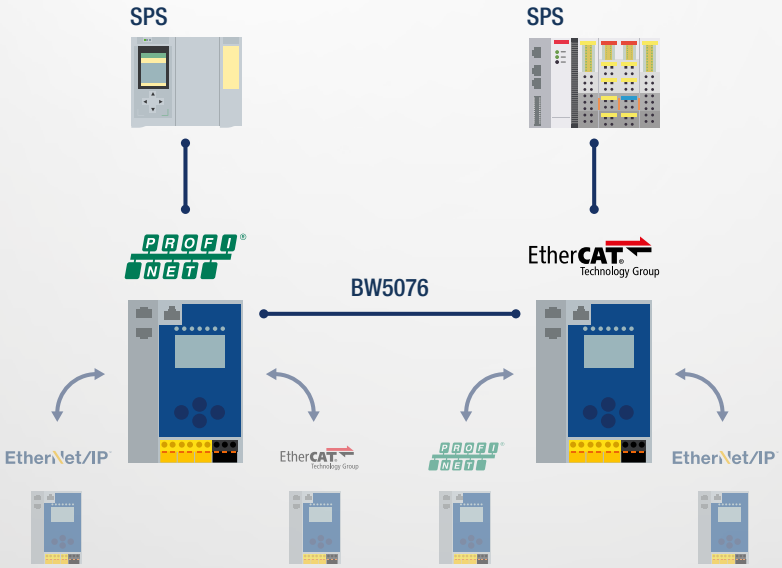
Besuchen Sie uns auf der SPS 2025

Sichern Sie sich Ihr Gratis-Ticket

ASi-5 UND ASi HIGHLIGHTS

Einfache Kopplung von Safety- und Feldbusprotokollen mit ASi-5 Gateways





Zwei unterschiedliche (sichere) Steuerungen miteinander zu verbinden und damit alle Signale des einen Netzwerks jeweils auch im anderen zu nutzen, war noch nie so leicht wie mit modernen ASi-5 Feldbus Gateways und den Software-Suites von Bihl+Wiedemann.

Mit der Funktionalität „Sichere Kopplung“ (BW5153) können Daten zwischen ASi Safety Gateways mit unterschiedlichen sicheren Feldbusprotokollen wie PROFIsafe, CIP Safety oder FSoE via Safe Link über die Ethernet-Diagnoseschnittstellen der Gateways ausgetauscht werden. Nachdem die zu koppelnden Geräte in ASIMON360 ausgewählt und die Lizenz für die „sichere Kopplung“ auf den entsprechenden Gateways freigeschaltet worden ist, erfolgt die Zuweisung der zu übertragenden Daten automatisch. Im Rahmen der „Sicheren Kopplung“ lassen sich bis zu 16 Byte komfortabel zwischen sicheren Feldbusprotokollen austauschen.

Die Funktionalität „Feldbus-Kopplung“ (BW5076) ermöglicht dagegen den Austausch von bis zu 256 Byte Standardsignalen über eine Ethernetverbindung zwischen zwei Gateways – und zwar sowohl zwischen solchen zu unterschiedlichen Feldbussen als auch zwischen solchen mit gleichen Feldbusschnittstellen. Nach Freischaltung der Lizenz auf den Geräten lassen sich die Konfiguration und das Datenmapping der Verbindung über ASIMON360 bzw. ASi Control Tools360 realisieren.

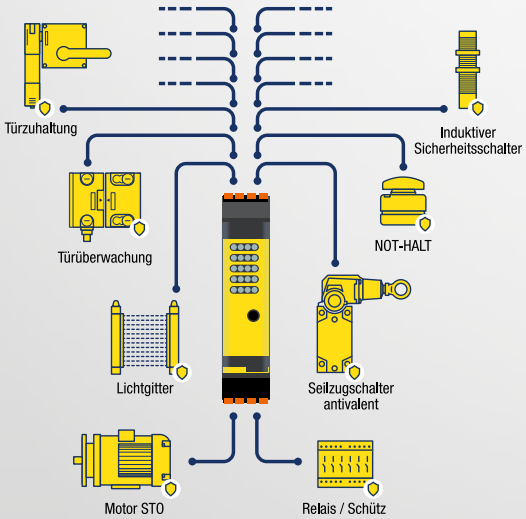
Im Gegensatz zu herkömmlichen Buskopplern lässt sich mit den Funktionalitäten „Sichere Kopplung“ und „Feldbus-Kopplung“ von Bihl+Wiedemann fast jede Steuerung mit einer anderen verbinden. Und die Tatsache, dass beide Koppelvarianten auch noch problemlos miteinander kombiniert werden können, sorgt für noch mehr Flexibilität.

VON BIHL+WIEDEMANN

ASi-5 Safety E/A Module

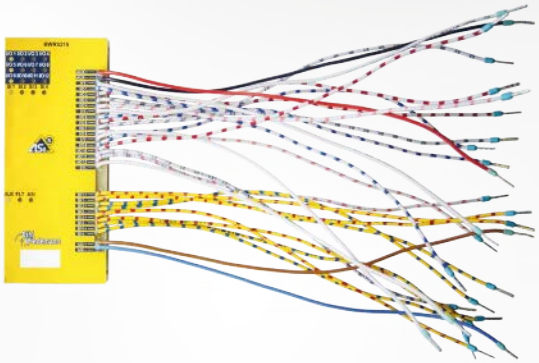
Neben dem Sortiment an ASi-5 Safety Gateways wächst auch das Portfolio an ASi-5 Safety Modulen von Bihl+Wiedemann kontinuierlich. Zu den ASi-5 Safety Modulen im großen IP67-Gehäuse und in IP20 mit je 12 Standardsignalen und bis zu vier ein- bzw. zwei zweikanaligen sicheren Eingängen für potentialfreie Kontakte, für OSSDs und für die Kombination potentialfreier Kontakt/OSSD gibt es mit dem BWU4393 nun auch eine Variante für potentialfreie Kontakte mit vier Standardsignalen im kleinen IP67-Gehäuse. Es ist immer dort eine Alternative, wo nur wenige Standardsignale an einer Stelle in der Anlage eingesammelt werden müssen. Außerdem gehören zum Portfolio das ASi-5 Safety Muting Modul BWU4411, mit dem unterschiedliche Mutinglösungen bis SIL3/PLe einfach, effizient und deutlich kostengünstiger realisiert werden können als mit vergleichbaren ethernetbasierten Lösungen, und das ASi-5 Safety E/A Modul BWU4277 mit bis zu 14 einkanalig sicheren Eingängen und zwei elektronischen sicheren Ausgängen. Ganz neu ist jetzt das ASi-5 Safety Leiterplattenmodul BWR5215 mit bis zu vier einkanaligen sicheren Eingängen und bis zu 12 digitalen Ein- oder Ausgängen.

ASi-5 Safety E/A Modul, IP20, 14SE/2SA (BWU4277)



Das ASi-5 Safety E/A Modul BWU4277 in IP20 verfügt über 14 Eingänge, die entweder als bis zu 14 einkanalige sichere Eingänge, als bis zu sieben zweikanalige sichere Eingänge (mit einstellbarer Testpulsbreite) oder als bis zu 14 digitale Eingänge verwendbar sind. Die sicheren Eingänge können so für nahezu jeden Sensor konfiguriert werden – jeweils als Standard- oder antivalente Schalter, für OSSDs oder potentialfreie Kontakte. Auch eine optionale Verwendung der beiden sicheren Eingänge SI13 und SI14 als EDM-Eingänge als Rückführkreis zur Schützkontrolle ist möglich. Neben den (sicheren) Eingängen verfügt das Modul darüber hinaus über zwei elektronische sichere Ausgänge (zwei Freigabekreise) mit erhöhter Verfügbarkeit. Die sicheren Ausgänge (bis PLe) lassen sich bei Bedarf auch als Standardausgänge konfigurieren. Das ASi-5 Safety E/A Modul BWU4277 von Bihl+Wiedemann, das nur eine ASi-5 Adresse belegt, besticht aber nicht nur durch seine umfangreiche Ausstattung, mit der sich die Kosten für sichere Ein- und Ausgänge an ASi optimieren lassen, sondern bietet mit einer Modulbreite von nur 22,5 mm auch ein erhebliches Einsparpotenzial im Schaltschrank.

ASi-5 Safety Leiterplattenmodul BWR5215 für den kompakten Anschluss von vielen sicheren Signalen und Standardsignalen



Bihl+Wiedemann hat sein Portfolio an ASi-5 Safety Modulen um ein sicheres Leiterplattenmodul in einem kompakten Gehäuse erweitert. An das neue, für Tasterboxen optimierte ASi-5 Safety Modul BWR5215 können bis zu vier ein- bzw. zwei zweikanalige sichere Eingänge und bis zu 12 digitale Ein- oder Ausgänge angeschlossen werden, und zwar unter einer einzigen ASi-5 Adresse.

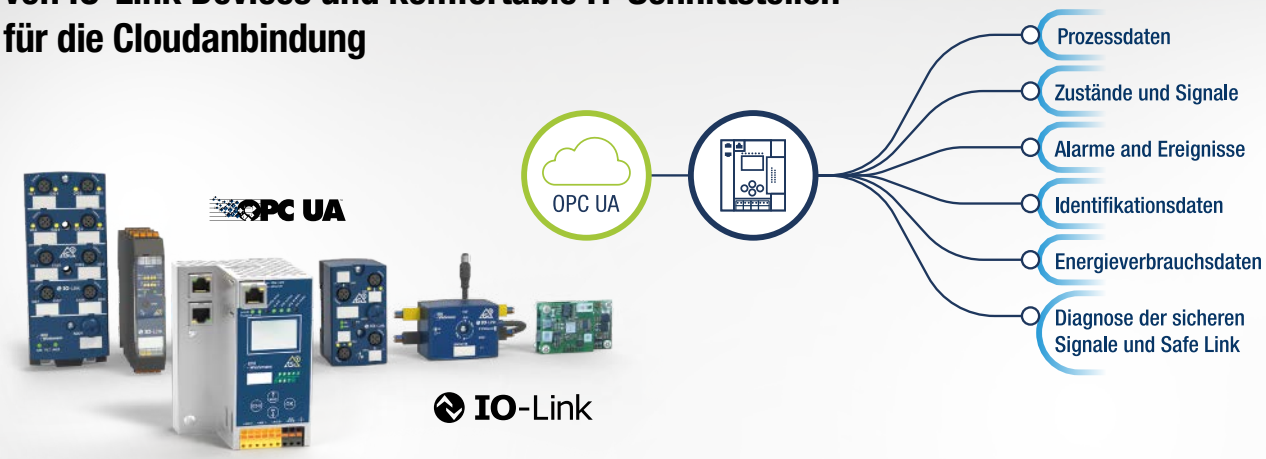
Seine kompakte Bauweise von 110 x 45 x 16 mm macht das ASi-5 Safety Leiterplattenmodul zu einer idealen Lösung für alle Anwendungen, bei denen der verfügbare Platz ein entscheidendes Kriterium ist. Es kann etwa dafür genutzt werden, um einen zweikanaligen NOT-HALT, einen Schlüsselschalter und zusätzlich bis zu sechs Leuchttaster in einer kleinen Tasterbox zu realisieren. Da sich das Modul in einem vergossenen Gehäuse befindet, verfügt es über einen Berührungsschutz, der effektiv auch vor Kurzschlüssen in Metallgehäusen schützt, sowie über einen effizienten Vibrationsschutz. Und im Gegensatz zu konventionellen Lösungen, bei denen viele einzelne Adern ins Feld geführt werden müssen und deshalb große, vielpolige Stecker zum Einsatz kommen, erfolgt die Verdrahtung hier direkt in der Tasterbox. In der Anlage selbst werden nur noch ein gelbes ASi und ein schwarzes AUX Profilkabel benötigt.

Neue ASi-5 Kabelkanal-Motormodule für 24 V und 48 V Motorrollen EC5000 BI

Bihl+Wiedemann verfügt bereits heute über ein umfangreiches Sortiment an Motormodulen für vielfältige Antriebslösungen mit ASi-5 und ASi-3. Das gilt sowohl für die Ansteuerung von Gleichstrommotoren und Frequenzumrichtern wie für Motorrollen. Und das Portfolio wächst weiter. Neu dazugekommen sind die ASi-5 Kabelkanal-Motormodule für die 24 V und die 48 V Motorrollen EC5000 BI von Interroll. Während sich mit dem Motormodul BWU5178 zwei 24 V Motorrollen ansteuern lassen, sind die Module BWU5208 bzw. BWU5209 in der Lage, jeweils vier 24 V bzw. 48 V Motorrollen anzusteuern. Alle drei Module können dabei über das Bus Interface (BI) digital mit den Rollen kommunizieren und auf diese Weise Zusatzinformationen wie z. B. Antriebstemperaturen und Stromaufnahme auslesen.

Die neuen ASi-5 Kabelkanal-Motormodule in Schutzart IP54 werden über M8 Snap-in Kabelbuchsen mit den Rollen verbunden, der Anschluss an ASi und AUX erfolgt per Durchdringungstechnik und Profilkabel. Zusätzlich zum Motoranschluss verfügt BWU5178 noch über vier digitale Eingänge zum Anschluss von Sensoren, während BWU5208 und BWU5209 sogar noch jeweils acht digitale Eingänge bereitstellen.

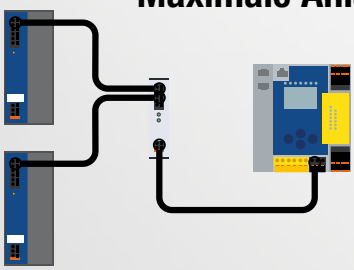
IO-Link und die Cloud: Einfache Konfiguration von IO-Link Devices und komfortable IT-Schnittstellen für die Cloudanbindung



Die Anbindung von IO-Link Devices an überlagerte Systeme oder eine Cloud wird durch die ASi-5 Module mit integriertem IO-Link Master von Bihl+Wiedemann deutlich vereinfacht. Zum einen profitieren Anwender von der Einfachheit und Kosteneffizienz des Verdrahtungssystems AS-Interface. So lassen sich etwa bei der Integration von 40 IO-Link Devices über ASi nicht nur über 40 % an Modulkosten und gut zwei Drittel an Verdrahtungskosten im Vergleich zu anderen Feldsbuslösungen sparen, sondern auch wertvolle Ressourcen bei der Planung, Installation und Inbetriebnahme. Zum anderen lässt sich das Parametrieren auch von sehr vielen IO-Link Devices mit Hilfe der benutzerfreundlichen Software-Suites ASIMON360 und ASi Control Tools360 äußerst komfortabel umsetzen. Und ganz wesentlich: Dank der integrierten IT-Schnittstellen wie OPC UA oder REST-API stehen die immer wichtiger werdenden Zusatzinformationen – egal, ob von einem einzigen oder mehreren hundert IO-Link Devices oder ASi Teilnehmern – unkompliziert, gebündelt und ohne die Steuerung zu belasten, unter nur einem Knoten – dem Gateway – zur Verfügung. Mit dem neuen, individuell über ASIMON360 oder ASi Control Tools360 konfigurierbaren OPC UA Objektbaum kann jetzt auch definiert werden, welche Informationen der OPC UA Client erhalten soll und welche nicht. Dazu werden die gewünschten Knoten einfach per Mausklick ausgewählt und anschließend bei der Inbetriebnahme im Gateway gespeichert, wo der Baum dann über jeden OPC UA Client genutzt werden kann.

Bihl+Wiedemann bietet mit seiner Lösung damit eine kostengünstige, flexible und zukunftssichere Anbindung von IO-Link Geräten. Der nahtlose Informationsaustausch zwischen der IO-Link Device-Ebene und übergeordneten Systemen wird so deutlich vereinfacht – ein wesentlicher Faktor für die moderne Automatisierung und die Vernetzung in Industrie-4.0-Anwendungen.

Maximale Anlagenverfügbarkeit mit dem 30 V Redundanzmodul



Ein unerwarteter Maschinenstillstand kann teuer werden. Nicht selten ist der Auslöser dafür ein defektes Netzteil. Mit dem Redundanzmodul BW5182 von Bihl+Wiedemann wird das ASi Gateway – und damit die gesamte Anlage – wirkungsvoll vor Ausfällen geschützt und so für dauerhaft hohe Verfügbarkeit und mehr Betriebssicherheit bei minimalem Aufwand gesorgt.

Das kompakte Redundanzmodul in IP20, das ohne aufwendige Umbauten im Schaltschrank untergebracht und damit problemlos in bestehende Installationen eingebunden werden kann, erlaubt den Anschluss von zwei 30 V Netzteilen mit jeweils bis zu 8 A. Fällt ein Netzteil aus, übernimmt automatisch das zweite – ohne Unterbrechung und ohne manuelles Eingreifen. Durch die integrierte aktive Entkopplung der Netzteile im Modul ist so eine stabile, redundante Stromversorgung des Gateways gewährleistet. Das erhöht nicht nur die Betriebssicherheit, sondern reduziert auch Stillstandszeiten und Serviceeinsätze.

IMPRESSUM

Herausgeber:
Bihl+Wiedemann GmbH
Floßwörthstraße 41
D-68199 Mannheim
Telefon: +49 (621) 339960
Telefax: +49 (621) 3392239
info@bihl-wiedemann.de
www.bihl-wiedemann.de

Herstellung:
MILANO medien GmbH
Mainberger Straße 24
D-97422 Schweinfurt
Telefon: +49 (69) 48000540
Telefax: +49 (69) 48000549
info@milanomedien.com
www.milanomedien.com

Redaktion:
Dirk Heyden,
Thomas Rönitzsch

Bihl + Wiedemann

WENIGER STECKER
MEHR VERBINDUNG
DURCH AS-INTERFACE

MEHR-VERBINDUNG.DE

sps
smart production solutions

25.11.2025 - 27.11.2025
Messe Nürnberg
Halle 7, Stand 200 + 201