WILEY
27. JAHRGANG
JUNI
2018
6
30 926

GIT SICHERHEIT + MANAGEMENT

MAGAZIN FÜR SAFETY UND

PERIMETERSCHUTZ
Luftraum sichern S.60

CYBER SECURITY
Heft im Heft:
Großes Special ab S. 79

VIDEOSICHERHEIT
Cyber Security für Errichter,
Planer, Betreiber S.84

KRITIS
Wer jetzt was tun muss S.100

SICHERE AUTOMATION
Safety-to-Cloud-Lösung S.116

PSA
Schutzausrüstung
intelligent und vernetzt S.127

IHRE STIMME FÜR DAS BESTE PRODUKT
WWW.SICHERHEIT-AWARD.DE

VIP:
Prof. Dr. Udo Weis S. 146

Titelthema Seite 88:

IT AUF NUMMER SICHER
RITTAL RZ-CONTAINER FÜR ENE'T

WILEY

SMARTHANDLE **AX**

Schafft Raum für Schönes. Mit Sicherheit.

www.simons-voss.de
keyless

Simons Voss technologies

Die Stunde der Leser

Sie sind ein Spiegel der Innovationskraft unserer Branche: Die Zahl der Einsendungen, Vorschläge und Ideen für den GIT SICHERHEIT AWARD 2019 war auch diesmal enorm. Inzwischen hat die neutrale Stimme der Experten-Jury gesprochen und aus sämtlichen Bewerbern die aus ihrer Sicht preiswürdigsten Bewerber als Finalisten ausgewählt. Und jetzt geht es im Prinzip so ähnlich weiter wie beim Eurovision Song Contest: Denn auch bei uns haben die Zuschauer, pardon unsere Leser, ein entscheidendes Mitspracherecht bei der Besetzung des Siegertreppchens – in allen sechs Award-Kategorien von Safety, Cyber Security und Brandschutz bis zu Video, Zutritt und Smarthome. Ab Seite 12 stellen wir sie Ihnen in Wort und Bild ausführlich vor – und Sie, die Leserinnen und Leser der GIT SICHERHEIT, können jetzt Ihr Votum online abgeben. Gehen Sie dazu einfach auf www.sicherheit-award.de und stimmen Sie unter Angabe Ihrer Firmenadresse ab. Bis zum 24. August haben Sie noch Zeit für Ihre persönliche Stimmabgabe, zu gewinnen gibt es eine schöne Spiegelreflexkamera.

Während Sie in aller Ruhe auswählen, möchten wir Ihre Aufmerksamkeit zusätzlich auf ein Thema lenken, das die ganze Branche zunehmend bewegt: Das Schlagwort Cyber Security – einschließlich der Prävention und des Schutzes gegen Cyber-Attacken. Wir beginnen in dieser Juni-Ausgabe der GIT SICHERHEIT mit einem großen Special GIT Cyber Security, das wir im September mit einem separaten Heft (samt Smart Magazine) fortsetzen werden.*

Dabei werfen wir beispielsweise einen genauen Blick auf die aktuelle Cyber-Sicherheitslage: Der ZVEI hat gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) die gesamte Elektroindustrie unter die Cyber-Lupe genommen. Grundlage dafür ist eine umfassende Befragung von 101 Unternehmen aus 21 Industriesektoren – alles dazu ab Seite 80. Auf Seite 83 begeben wir uns mit Steffen Zimmermann vom Verband Deutscher Maschinen- und Anlagenbau (VDMA) in die Produktionshallen. Er zeigt auf, welche Rolle der Maschinen- und Anlagenbau bei der sicheren und zuverlässigen Fertigung spielt. Es folgt ein Beitrag des BHE speziell zur Cyber-Sicherheit in der Videotechnik, denn hier gibt es ja seit längerem schon den starken Trend, analoge Kameras gegen IP-Kameras auszutauschen: Ab Seite 84 gibt der BHE Empfehlungen ab für Errichter, Planer und Betreiber von Videoanlagen. Praxisberichte und Tipps ergänzen dieses Special Teil I in dieser Ausgabe.

Im Übrigen sind auch diesmal alle anderen Rubriken der GIT SICHERHEIT wieder prall mit Lesenswertem gefüllt – wie wäre es etwa mit dem Thema Brandschutz in kleinen Sonderbauten (ab Seite 74)?

Wir wünschen Ihnen eine treffsichere Hand bei Ihrem Votum für den GIT SICHERHEIT AWARD – und eine spannende und anregende Lektüre!

Steffen Ebert
für das Team von Wiley und
GIT SICHERHEIT

* Heft im Heft in dieser Ausgabe – separates Special im September. Für weitere Infos schreiben Sie mich gerne an:
Steffen.Ebert@Wiley.com

TITEL:

IT auf Nummer sicher

ene't ist ein auf die Energiebranche spezialisiertes IT-Systemhaus, das seinen Kunden branchenspezifische Anwendungen als Service und stets aktuelle Daten zum Strom- und Gasmarkt liefert. Hierfür betreibt das Unternehmen ein eigenes Rechenzentrum mit höchsten Sicherheitsstandards. Und das muss ausfallsicher sein. Unser Titelthema zu Cyber-Security, physikalische und organisatorische Sicherungsmaßnahmen – und ein effizientes Rechenzentrum.

Seite 88

INNENTITEL:

Sicherheit und Produktivität gehen Hand in Hand

Safety-to-Cloud-Lösung von Schmersal unterstützt Predictive Maintenance

Seite 115

Nicolas Stobbe

Peter Martin Schroer

Pascal Heinkele

EDITORIAL

03 Die Stunde der Leser
Steffen Ebert

MANAGEMENT

GIT SICHERHEIT AWARD

12 Neue Finalisten
Gewinnen Sie den Leser-Preis!

KONZERNSICHERHEIT

30 Service im Park
Sicherheitsdienstleistungen für den Industriepark Weinheim

ZUTRITTSSTEUERUNG

36 Läuft nicht gibt's nicht!
Zum 40. Jubiläum von Deister Electronic

SOT 2019

40 Startschuss für die Security on Tour 2019
Roadshow der Sicherheitsbranche nimmt Berlin und Ingolstadt in das Tour-Programm auf

PROZESSOPTIMIERUNG

42 Blick über den Tellerrand
Videomanagement-Software schützt und unterstützt Lebensmittelproduktion bei Feinkost-Hersteller Wernsing

SECURITY

VIDEOTECHNIK

52 Koaxiale Vielfalt
Technologisch vielseitige Multisignal-produkte von Eneo

ALARMIERUNG

54 Alarm in Farbe
Firmengebäude sichern, Wochenendhaus schützen: Videoverifikation für Alarmsystem

VIDEOMANAGEMENT

56 Historische Themen, aktuelle Sicherheit
Themenpark verbessert Sicherheit und Service mit Genetec Security Center

INTERNET OF THINGS

58 Smart IoT Industriepark
Dahua bringt Produktivität und Qualität auf ein neues Niveau

VIDEOÜBERWACHUNG

60 Gleich in die Luft gehen?
Zur Grundstückssicherung gehört inzwischen auch die Absicherung des Luftraums

71 Kein Herz für Hacker
IPS veröffentlicht Software-Release 9.0

ZUTRITTSSTEUERUNG

63 Beständig durch Zeit und Raum
Stabilus investiert in Zutrittskontrolle und Zeiterfassung

64 Im Fluss
Workflow-Szenarien in der Zutrittskontrolle und Zeiterfassung

66 Im Dampf der Brühwurstküche
Zutrittssteuerung in der Lebensmittelproduktion

PERIMETERSCHUTZ

68 6 Fragen . . .
. . . die sich stellen sollte, wer einen Gebäudeschutz-Plan entwickeln will

Probe&Kontakt:
sophie.platzer@wiley.com

BRANDSCHUTZ

VERANSTALTUNG

72 Brandschutz für die Chemie
Dechema-Praxisforum „Brandschutz in der chemischen Industrie"

BRAND- UND RAUCHMELDUNG

74 Kinder, Gäste und Senioren
Branderkennung und -warnung für „kleine Sonderbauten" wie Kitas, Pensionen und Seniorenwohnheime

BRANDBEKÄMPFUNG UND PRÄVENTION

76 Die Bio-Milch macht's
Brandschutz in der Milchproduktion

GIT CYBER SECURITY

ZVEI-UMFRAGE

80 Sicherheitslagebild auf Grundlage der ZVEI-Umfrage
ZVEI-Sicherheitslagebild: Wie steht es um die Cybersicherheit in der Elektroindustrie?

INDUSTRIAL SECURITY

83 Sicher in die digitale Zukunft – Industrial Security

104 Safety meets Security
Gemeinsame Strategie erforderlich

VIDEOSICHERHEITSTECHNIK

84 Cyber Security bei Videoanlagen
BHE liefert wichtige Hinweise für Errichter, Planer und Betreiber

TITELTHEMA

88 IT auf Nummer sicher
Rechenzentrum-Container von Rittal für höchste Ausfallsicherheit bei IT-Systemhaus ene't

Aleksandar Mitrovic *Siegfried Rüttger* *Achim Sorg*

INDUSTRIE 4.0

92 Cyberangriffe gegen Industrie-Rechner
Verstärkter Krypto-Malware-Befall bei Industrierechnern nach Bitcoin-Boom

VIDEOTECHNIK

96 Angriff durch die Hintertür
Schutz gegen Cyber-Angriffe: Auch an die Absicherung der Videosysteme denken!

ISOLATIONSTECHNIK

98 Browser in der Box
So wird das Internet zum sichersten Ort der Welt

KRITIS

100 Kritische Infrastrukturen gefordert
Definitionen, Pflichten und Möglichkeiten zur Sicherung von Kritischen Infrastrukturen – Teil 1

INTERNET OF THINGS

108 Winds of Change
Safety und Security in Zeiten des Internets der Dinge

NETZWERKE

112 Draußen und sicher
Wie sich mit industriellen PoE-Switches zuverlässige Outdoor-IP-Überwachungsnetzwerke erstellen lassen.

RUBRIKEN

5 Firmenindex
6 News
44 Jerofskys Sicherheitsforum
46 Security
78 Brandschutz
118 Safety
139 Impressum
140 GIT BusinessPartner
146 VIP Couch

SAFETY

INNENTITEL

116 Sicherheit und Produktivität gehen Hand in Hand
Safety-to-Cloud-Lösung unterstützt Predictive Maintenance

MASCHINEN- UND ANLAGENSICHERHEIT

124 Cobots Claus, Clara & Co: kollaborative Robotik mit Sick Safety
Flexibilität, Kollaboration und Sicherheit der Mitarbeiter – schlanke MRK-Lösung bei Continental

132 Vorschriftsgemäß gesichert
Maschinensicherheitsnormen in der Praxis. Teil 5 – Risikoeinschätzung mit EN 23125

VERNETZTE SICHERHEIT

127 PSA intelligent
Sicherheit 4.0: Auch Persönliche Schutzausrüstung wird intelligenter und stärker vernetzt

SERIE: WAS IST EIGENTLICH...

130 DNV-GL
In jeder Ausgabe erklären Sicherheitsexperten Begriffe aus der Maschinen- und Anlagensicherheit.

GEFAHRSTOFFLAGERUNG

134 Wohin mit den Batterien?
Lagern wie Gefahrstoffe: Lithium-Batterien in Arbeitsräumen

138 Wohin bloß damit?
Wirtschaftliche Gefahrstofflagerung bei maximaler Sicherheit

PSA

136 Weit mehr als ein Hingucker
Exklusive Warnschutzkleidung für Assistance Partner

ORGANISATIONEN INSTITUTIONEN UND UNTERNEHMEN IM HEFT

INDEX
SCHNELLFINDER

3M	121	Hanwha	48, 4. US
ABB	47	Hikvision	10
ABI	49	Hinte	120
Abus	50	Honeywell	33
Advancis	6, 46	Interflex	63
Allnet	49	Interkey	50, 70
Asecos	7, 120, 121	Isgus	10
Assa Abloy	100, 46, 48	K. A. Schmersal	115, 116
Astrum IT	39	Kaspersky	92
Atral-Secal	74	KEB	118
Automatic System	50	Kentix	105
Axis	6, 46, 68	Leuze	119
B&R	118, 130	Life Safety	127
BAuA	120, 121	Meiko	137
Bauer	123	Messe Essen	45
BGW	121	Messe München	107
BHE	44, 84	Mewa	120, 123
Bird Home	51	Mobotix	11, 96
Bosch	65, 108	Monacor	49
BSI	107	Moxa	93
C.Ed.	31	Netcomm	44, 73
Dahua	9, 58	Novar	76
Dallmeier	51	Nürnberg Messe	107
Datalogic	122	Omron	119
Dechema	7, 72	Operational	103
Dehn & Söhne	122	Paul H. Kübler	136
Deister	17, 36	Paxton	6, 27
Denios	121, 123, 138, Beilage	PCS	41, 66
Deutsche Bahn	45	Pepperl + Fuchs	120
Deutsche Post	61	Pfannenberg	122, 130
DGUV	11	Phoenix	104
Die Akademie Fresenius	6	Pilz	118
Digivod	49	Pizzato	118
Dom	69	Primion	7, 64, 81
Drägerwerk	10	Rittal	88, Titelseite
E. Dold	119	Rohde & Schwarz	97, 98
EFB	7, 51	Salto	3, 8, 48
Ei	78	Schraner	78
Eneo	52	Securitas	10, 29
EPS	51, 54	Securiton	8, 45, 60, 71
Erbstößer	134	SeeTec	11, 42
Eucamp	40	SeTec	77
Euchner	118, 125, 132	Sick	120, 122, 124
Evva	11	SimonsVoss	47, Titel Corner, 2. US
Eyevis	6	Siqura	25
Fiessler	121	Süd-Metall	35
Flir	46	Tisoware	47
Freudenberg	30	Uhlmann & Zacher	48, 50, 95
FVSB	7	Uniview	67
Genetec	56	VDMA	83
Geutebrück	46	Videor E. Hartig	35, 57
Geze	8	Vitel	70
GfS	43	Wagner	78
Giesecke & Devrient	10	Wanzl	53
Gira	50	Wieland	119
Gretsch-Unitas	10	ZVEI	80

NEWS

Neuer Gebietsverkaufsleiter Süddeutschland

Stefan Savolyi

Paxton, weltweit tätiger Entwickler und Hersteller elektronischer Zutrittskontrollsysteme und Türsprechanlagen, hat Stefan Savolyi zum Area Sales Manager für Süddeutschland ernannt. Mit Sitz in Karlsbad wird Savolyi die Errichter und Händler in den Ländern Baden-Württemberg und Bayern unterstützen, um neue Möglichkeiten im Markt zu erschließen und um zu gewährleisten, dass sie über die komplette Produktpalette von Paxton auf dem Laufenden gehalten werden. Savolyi kommt mit über 16 Jahren Erfahrung im Einzelhandel und Vertrieb zu Paxton. Nach fünfeinhalb Jahren im Vertrieb in der Sicherheitsbranche (CCTV) war er zudem bei Media Markt, Vivotek/Secomp und zuletzt bei CBC (Europe) tätig.

www.paxton-gmbh.de ■

Eyevis wird Teil der Leyard-Gruppe

Die weltweiten Anbieter von Visualisierungsprodukten, Leyard und Planar, kündigten ihre Absicht an, die eyevis GmbH, deutscher Hersteller von Visualisierungslösungen, zu erwerben. Mit der Übernahme setzen Leyard und Planar ihre geografische Expansion weiter fort. Kunden in den EMEA-Märkten profitieren durch die Übernahme zukünftig von den gebündelten Ressourcen aller Unternehmen in den Bereichen Marketing, Vertrieb, Projektinstallation sowie Service.

Eyevis, deutscher Hersteller von Großbildsystemen, ist einer der führenden Anbieter und Integrator von Visualisierungssystemen für professionelle Anwendungen in den Bereichen Kontrollraum, Broadcast-Studios, Virtual Reality und Simulation. Zu den Lösungen von eyevis gehören Displays, Grafikcontroller, Software und Zubehör. Teracue, ein Hersteller und Anbieter professioneller IPTV-Lösungen und Video Networking-Produkten, 2014 von eyevis übernommen, ist ebenso Teil der Absichtserklärung, eyevis zu kaufen, und wird genauso wie die Tochterfirma eyevis France SAS von Leyard übernommen. Die Akquisition unterliegt den üblichen Abschlussbedingungen und wird voraussichtlich im zweiten Quartal 2018 abgeschlossen sein.

www.eyevis.de ■

Gelebtes Arbeitsschutzmanagement

Am 28. und 29. Juni 2018 findet in Düsseldorf die siebte Fresenius-Praxistagung Arbeitssicherheit statt. Zehn Referenten aus der Industrie berichten, wie man mit neuen Ansätzen Unfälle vermeiden, die Arbeitssicherheit erhöhen und Mitarbeiter für das Thema sensibilisieren kann. Auf der Tagesordnung stehen z. B. Compliance-Fragen im Arbeitsschutz. Rechtsexperten geben einen Überblick über Gesetzesänderungen und diskutieren Fragen aus der Praxis zu Verantwortung und Haftung im Arbeitsschutz. Außerdem erhalten die Teilnehmer Hilfestellungen zur Unterweisung von Mitarbeitern: Wie man sie richtig „abholt" und verständlich kommuniziert. Aus der täglichen Praxis berichtet Mathias Geiger über Arbeitsschutz im Industriepark Hoechst in Frankfurt. Kim Andres beschreibt den Umgang mit Gefahrensituationen im Großmotorenwerk MAN Diesel & Turbo.

www.umweltakademie-fresenius.de/2543 ■

Frühjahrstagung Werkfeuerwehrverband Hessen

Über 80 Teilnehmer sowie 15 Aussteller im Innen- und Außenbereich konnte Advancis in Langen bei der Frühjahrstagung des Werkfeuerwehrverbands Hessen begrüßen. Ralf Klotzbach (Vorstandsmitglied des Fachverbandes der hessischen Werkfeuerwehren) führte mit seiner Moderation durch die spannenden Vorträge u.a. zum Einsatz von Gefahrenmanagementsystemen, zu technischen Neuerungen beim Brandschutz sowie zum Thema Ausbildung und Nachwuchs bei der Werkfeuerwehr. Besonderer Dank gilt Bernd Saßmannshausen (1. Vorsitzender des Werkfeuerwehrverbands Hessen), Harald Uschek (Landesbranddirektor, Ministerium des Innern und für Sport) und den zahlreichen Ausstellern, die mit ihren Beiträgen sowie der begleitenden Fachausstellung maßgeblich zum Erfolg der Veranstaltung beigetragen haben.

www.advancis.de ■

Axis: Verstärkung für Österreich

Als Sales Engineer unterstützt Christoph Petz (34) in Österreich seit Mitte Februar als technischer Experte den Vertriebsbereich von Axis Communications. Sein Fokus liegt darauf, das Team in allen technischen Belangen zu unterstützen und Kunden sowie Partner gleichermaßen im Hinblick auf IP-basierte Lösungen zu beraten. Für den schwedischen Anbieter von Sicherheitslösungen war dabei besonders wichtig, einen erfahrenen Kollegen ins Boot zu holen, der den technischen Hintergrund und die Funktionsweise der Produkte kennt und vermitteln kann. So unterstützte Petz bei Frequentis u.a. die Videoüberwachungs-Leitzentrale von Scotland Yard vor Ort in London. Die technische Expertise bringt der Absolvent der Fachschule Elektrotechnik Wr. Neustadt aus Tätigkeiten als Techniker bei UHL Security, sowie als Solution-Designer im Bereich Service- Alarm- und Zutrittssysteme bei Kapsch BusinessCom, einem langjährigen Partner von Axis, mit.

Christoph Petz blickt auf langjährige Erfahrung im IP-basierten Sicherheitsbereich zurück.

www.axis.com ■

Andreas Kupka ist neuer CEO bei primion

Andreas Kupka

Der 47-jährige Andreas Kupka gilt als exzellenter Kenner der Branche – und ist nun neuer CEO bei primion. In den vergangenen 25 Jahren war er in verschiedenen namhaften Unternehmen der Branche in leitender Position tätig. Andreas Kupka hat sich vor allem durch die Gründung und den Aufbau des Abus Security Center in Augsburg einen Namen gemacht. Seit 2011 war er als Executive Vice President bei der Evva Sicherheitstechnologie in Wien verantwortlich für die Bereiche Vertrieb, Marketing und Produkte. Andreas Kupka tritt die Nachfolge von Horst Eckenberger an, der das Unternehmen Ende Februar verlassen hatte. In der Zwischenzeit hatte CFO Jorge Pons interimsweise das Amt des CEO mit übernommen. Der Aufsichtsrat der primion Technology AG hat die Belegschaft jetzt aktuell über die Personalie informiert und dem neuen CEO seine volle Unterstützung zugesichert. Eduardo Unzu, Group Managing Director der Muttergesellschaft Azkoyen: „Wir sind davon überzeugt, dass wir mit Andreas Kupka einen exzellenten Kenner der Branche an Bord geholt haben, der durch sein Wissen und seine über 25-jährige Erfahrung primion voranbringen und unsere Stellung im europäischen Markt festigen und weiter verbessern wird."

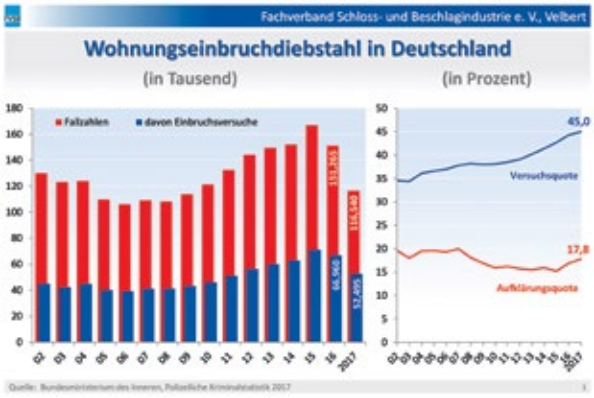
www.primion.de ■

Guido Heumann wechselt zu EFB-Elektronik

Guido Heumann

Das Bielefelder Unternehmen für Gebäudeinfrastruktur und Sicherheitstechnik sieht den IT-Channel als wichtigen Partner für zukünftiges Wachstum und hat daher mit dem Vertriebs- und Marketingexperten Guido Heumann (41) einen erfahrenen Spezialisten als Business Development Manager IT Distribution eingestellt. In der neuen Position verantwortet der ehemalige Prokurist und General Manager von IC Intracom den Partnerausbau im Channelgeschäft. Heumann soll die Positionierung der EFB-Marken sowie der Partnermarke Techly weiter ausbauen. Zudem übernimmt er die Verantwortung für den Aufbau von speziellen Schulungs- und Betreuungsprogrammen für die Channel-Sales-Teams und soll den Projektschutz sowie die Marketingunterstützung im Print- und Onlinebereich vorantreiben.

www.efb-elektronik.de ■



Entwicklung des Wohnungseinbruchdiebstahls

Mit richtigem Schutz zu weniger Einbrüchen

Investition in den Einbruchschutz lohnt sich – darauf weist der Fachverband Schloss- und Beschlagindustrie (FVSB) hin. Die kürzlich veröffentlichten Zahlen der bundesweiten Polizeilichen Kriminalstatistik (PKS) zeigen, dass die Zahl der Wohnungseinbrüche 2017 stark zurückgegangen ist, trotzdem ist sie weiterhin relativ hoch. Dabei handelt es sich um insgesamt 116.540 Fälle. Somit ist die Anzahl der Wohnungseinbruchdiebstähle im Vergleich zum Vorjahr um 23% gesunken und liegt inzwischen sogar etwas unter dem Stand von 2010 (2010: 121.347 Fälle). Laut PKS handelt es sich bei 45% der Fälle aus 2017 um Versuche. Dies bedeutet einen Anstieg um 1% im Vergleich zum Vorjahr und setzt den seit über 15 Jahren anhaltenden Trend, dass der Anteil der nicht vollendeten Wohnungseinbrüche stetig steigt, fort. Ein Grund könnte hier u.a. die Verbesserung der Sicherungsmaßnahmen gegen Wohnungseinbruchdiebstahl sein.

www.fvsb.de ■

Asecos ist AEO C-zertifiziert

An das vom Bundesministerium der Finanzen/Generalzolldirektion verliehene Zertifikat AEO sind umfangreiche Voraussetzungen hinsichtlich der Zuverlässigkeit, der Zahlungsfähigkeit sowie der Einhaltung rechtlicher Vorgaben gebunden. Seit 1. Januar 2008 können Unternehmen, die in der Europäischen Union ansässig und am Zollgeschehen beteiligt sind, den Status des Zugelassenen Wirtschaftsbeteiligten AEO beantragen. Ziel ist die Absicherung der durchgängigen internationalen Lieferkette (supply chain) vom Hersteller einer Ware bis zum Endverbraucher. Hierzu ist eine weltweite Anerkennung des AEO-Status notwendig. Der Status des Zugelassenen Wirtschaftsbeteiligten ist in allen Mitgliedstaaten gültig und zeitlich nicht befristet. Die Einführung des Zertifikates stellt ein wesentliches Element des EU-Sicherheitskonzepts dar.

www.asecos.com ■

© Foto: Karin Fiedler

Beispielhaftes Personalmanagement und Arbeitsplatzsicherheit – Geze-Mitarbeiter: Azubis und Trainees

Geze erhält zwei Gütesiegel

Zum fünften Mal wurde Geze mit dem Siegel „Top Employer Deutschland" ausgezeichnet und darf sich erneut zu den Top-Arbeitgebern in Deutschland zählen. Das Siegel zertifiziert Unternehmen, die bewiesen haben, dass sie bei ihrer Personalführung und -strategie höchste Standards erfüllen. Die Ergebnisse der umfassenden Auditierung durch das Top Employers Institute zeigen: Geze bietet herausfordernde, verantwortungsvolle Aufgaben, interessante Perspektiven sowie ein breites Ausbildungs- und Studienangebot in einem innovativen international geprägten Umfeld und vereint sie mit den Vorteilen eines mittelständischen Familienunternehmens. Außerdem zeichnete das Wirtschaftsmagazin Focus-Money Geze als einen der Arbeitgeber aus, die in Deutschland die besten und zukunftssichersten Arbeitsplätze anbieten. Basis der Ergebnisse ist die Analyse der Beständigkeit der Kennzahlen eines Unternehmens: der Zuwachs an Mitarbeitern, an Umsatz und an Gewinn. Über einen Zeitraum von fünf aufeinanderfolgenden Jahren mussten alle drei Kriterien kumulativ erfüllt sein.

www.geze.com ■

© Foto: Kliniken Valens

Blick aus der Rehaklinik Valens ins Taminatal

Salto stattet Kliniken Valens mit Zutrittslösung aus

Die Lösung kombiniert nahtlos virtuell und funkvernetzte sowie mobil per Smartphone bedienbare Zutrittspunkte. Insgesamt sind in Valens (Schweiz) derzeit knapp 500 Zutrittspunkte im Klinikgebäude, in den Mitarbeiterwohnungen und den Studios mit der Salto-Anlage ausgestattet. Technologisch basiert die Zutrittslösung auf dem Salto-Virtual-Network (SVN) mit patentierter Schreib-Lese-Funktionalität und verschlüsselter Datenübertragung. Im SVN werden die Informationen zu den Schließberechtigungen auf dem Identmedium gespeichert, wodurch eine Verkabelung der elektronischen Beschläge und Zylinder entfällt. Partiell ergänzt die Salto Wireless-Technologie zur Funkvernetzung von Türen das SVN. Per Mausklick und in Echtzeit lässt sich das Wireless-System konfigurieren, kontrollieren und verwalten.

www.saltosystems.de ■

Securiton: Brandschutz für 350-Jahr-Feier von Merck

Merck, selbst ein Riese unter den Wissenschafts- und Technologieunternehmen, feiert seine 350-jährige Firmengeschichte in einer eigens dafür errichteten gigantischen Zeltkonstruktion, die anschließend wieder abgebaut wird. Das weltweit größte mobile geodätische Kuppelzelt ist 21 Meter hoch, misst 50 Meter im Durchmesser und bietet durch seine ungewöhnliche Bauweise ganz ohne Masten Platz für bis zu 1.700 Menschen. Für die „M-Sphere" genannte, selbsttragende Zeltkonstruktion realisierte Securiton eine individuelle Lösung der Sonderbrandmeldetechnik zum Schutz von Gästen, Mitarbeitern und Besuchern der Jubiläumsfeierlichkeiten von Merck in Darmstadt.

Für die elektronischen Sicherheitslösungen am Unternehmensstandort und nun auch den temporären Brandschutz im Event-Dome und den drei Nebenzelten sorgt Securiton, Spezialist für moderne Brandfrühesterkennung mit intelligenter Systemanbindung. Dabei nutzen die Brandschutzexperten das Gerüst der Wabenkonstruktion zur Installation von Ansaugleitungen. Durch diese unsichtbaren Kanäle wird permanent Raumluft zu den Auswerteeinheiten geleitet, deren hochempfindliche Sensoren sehr schnell einen Anstieg der Rauchkonzentration erkennen. Das ist wichtig, denn je früher Brandherde entdeckt werden, desto mehr Zeit bleibt, das Festzelt zu evakuieren und Menschen in Sicherheit zu bringen. „Ansaugrauchmelder sind ideal für schwierige Umgebungen. Sie werden auch in Hochregallagern, Rechenzentren oder Reinräumen eingesetzt", erklärt Bernd Klock von der Darmstädter Securiton-Niederlassung.

Branderkennung mit System: Im großen Zelt sind gleich mehrere Melder im Boden und Dach der Bühne, Technikgang und Innenraum installiert. Sie liefern die Daten ihrer Auswerteeinheit über eine Ringleitung an die Brandmeldezentrale, die auch die Melder der kleineren Zelte sowie des Technikcontainers erfasst. Die Zentrale ist in einem beheizten Outdoor-Schrank untergebracht, dort befinden sich auch das Bedienfeld und die Laufkarten für die Feuerwehr. Die Brandmeldezentrale informiert über mehrere Hauptmelderlinien die Werksfeuerwehr am Standort. ■

© Foto: Merck

Securiton konzipierte für Merck eine individuelle Sonderbrandmeldelösung im M-Sphere getauften Kuppelzelt.

CCTV IST NICHT MEHR NUR ZU SEHEN, SONDERN ZU FÜHLEN

HDCVI 4.0 IoT

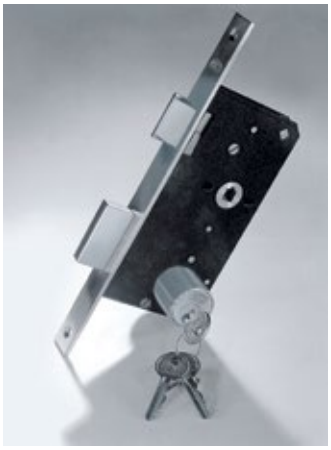
IoT, oder das Internet der Dinge, ist das Konzept der Verknüpfung von Geräten. HDCVI-IoT ist eine auf der HDCVI-Technologie basierende IoT-Infrastruktur. Sie bietet ein umfassendes Ökosystem, das herkömmliche Video- und Audiodaten in HD über Koaxialkabel mit Sensorinformationen wie Temperatur, Luftfeuchtigkeit und Alarmen von mehreren drahtlosen Alarmgebern verbindet. Auf diese Weise erhält der Anwender Warnungen vor potenziellen Risiken, die mit visuellen Beweisen verbunden sind, und kann so Personal und Eigentum über alle Dimensionen hinweg sichern. Die Entwicklung von IoT-Lösungen ist ein wichtiger Meilenstein in der Überwachungsindustrie und HDCVI 4.0 wurde entwickelt, um Systeme an die Spitze dieser spannenden Revolution zu bringen.

DAHUA TECHNOLOGY GMBH
Monschauer Straße 1, 40549 Düsseldorf, Deutschland
http://www.dahuasecurity.com/de/
sales.de@global.dahuatech.com
support.de@global.dahuatech.com

ISO 9001:2000

Die Marke BKS hat Geburtstag

BKS – eine der bekanntesten Marken im Bereich Schließtechnologie und Sicherheit – wurde im Mai dieses Jahres 115 Jahre alt. BKS ist für die Herstellung von Schlössern, Schließzylindern, Schließanlagen, Objekt- und Fluchttürbeschlägen international bekannt. Vom einzelnen Schließzylinder bis zur Großserie konzentriert man sich auf eine wettbewerbsfähige Wertschöpfung und hohe Qualität in der Fertigung. Im Stammwerk im rheinländischen Velbert arbeiten ca. 590 Mitarbeiter in Entwicklung, Produktion und Verwaltung auf einer modernen Produktionsfläche von rund 60.000 m².



Eines der ersten BKS-Schlösser

Am 8. Mai 1903 gründeten der Werkmeister Adolf Boge und der Schlosser Fritz Kasten die Rheinische Türschließerfabrik in Solingen. Sie entwickelten einen Türschließer, mit dem Türen fast geräuschlos ins Schloss fallen, und setzten damit den ersten Meilenstein in der Geschichte des Unternehmens.

www.g-u.com ■

Hikvision begrüßt neuen Distributor

Der Anbieter im Bereich von übergreifenden Videoüberwachungslösungen Hikvision heißt Securetecc in den Reihen seiner Distributoren willkommen. Das Unternehmen erweiterte im ersten Quartal 2018 sein Sortiment um die Produkte des Herstellers aus Hangzhou mit Niederlassung in Deutschland. Unter der Leitung von Geschäftsführer Georg Goffin unterstützt das Team von Securetecc seine Kunden als Solution-Partner, Planer und Errichter bei der Organisation und Projektierung ihrer Aufträge. Hierbei steht im Vordergrund, die optimale Lösung zu generieren, um so die Marktposition und Reputation ihrer Kunden zu stärken. Dabei hat sich Securtecc für Hikvision und seine bewährten Produkte entschieden. Für die ganzheitliche Betreuung bietet Securteccs vertriebliche und technische Schulungen an, die entweder eigenständig, in Zusammenarbeit mit Hikvisions firmeneigenen Fachkräften oder durch VMS-Spezialisten durchgeführt werden.

www.hikvision.com ■

Weniger Einbrüche auch im 1. Quartal 2018

Die sinkende Einbruchstendenz aus dem Vorjahr hält an: Im ersten Quartal 2018 hat das Securitas Operation Center in Berlin 19 % weniger vollendete Einbrüche registriert als in den ersten drei Monaten des Vorjahres. Besonders Banken und Baumärkte bleiben im Visier der Täter. Im Gesamtjahr 2017 waren die Einbruchszahlen, die von den Notruf- und Serviceleitstellen des Sicherheitsdienstleisters bundesweit bei seinen Kunden erfasst worden waren, um 15 % zurückgegangen. Im Jahr 2016 hatte es erstmals einen Rückgang gegeben, damals um rund 20 %, nach neun Jahren mit einer stetig steigenden Zahl von Einbruchsdelikten. „Unsere Arbeit zahlt sich aus: Prävention, Bewachung und Streifen sowie hochwertige Alarmanlagen und technisch ausgefeilte Kamerasysteme helfen, die Werte von Firmen und Privatleuten zu schützen", sagte Manfred Buhl, CEO von Securitas Deutschland. Einbruchsschutz sei eine gesamtgesellschaftliche Aufgabe, dazu gehörten u. a. die verstärkten Maßnahmen der Polizei sowie technisch unterstützte Sicherheitslösungen.

www.securitas.de ■

Dräger mit schwachem Start ins Geschäftsjahr

Im ersten Quartal 2018 hat Drägerwerk den Auftragseingang währungsbereinigt gesteigert. Der Umsatz ging hingegen zurück. Der Auftragseingang ging in den ersten drei Monaten nominal um 2,8 % auf 621,4 Mio. Euro (3 Monate 2017: 639,4 Mio. Euro) zurück, währungsbereinigt legte er hingegen um 2,6 % zu. Dräger konnte die Aufträge in der Region Afrika, Asien und Australien sowie in der Region Amerika währungsbereinigt steigern, während der Auftragseingang in Europa knapp unter dem Niveau des Vorjahrs blieb. Die Aufträge für Produkte der Medizintechnik legten in den ersten drei Monaten währungsbereinigt zu, die Nachfrage bei Produkten der Sicherheitstechnik war hingegen rückläufig. Der Umsatz von Dräger ging im ersten Quartal 2018 nominal um 7,4 % auf 495,6 Mio. Euro zurück (3 Monate 2017: 535,0 Mio. Euro). Währungsbereinigt fiel der Umsatz um 2,5 %.

www.draeger.com ■

Hikvision: Umsatzwachstum von 31,22 %

Seinen jährlichen Bericht für 2017 hat Hikvision, global tätiger Spezialist für Videoüberwachungsprodukte und -lösungen veröffentlicht. Dieser weist ein Wachstum von 31,22 % des Gesamtumsatzes auf, mit einem Anstieg der Erlöse von 31,93 Milliarden RMB im Jahr 2016 auf 41,91 Milliarden RMB in 2017. Insgesamt wird ein Zuwachs der Betriebsgewinne um 26,77 % deutlich. Hikvision konnte diese eindrucksvollen finanziellen Ergebnisse aus mehreren Gründen erreichen. Diese beinhalten u. a. optimierte F&E-Systeme und -Prozesse sowie die Entwicklung von Lösungen für vertikale Branchen in Abstimmung mit den sich verändernden Marktbedürfnissen. Verbesserte Produktanlieferung und intensivierte Vertriebs- und Service-Netzwerke leisteten ebenfalls einen Beitrag zum Unternehmenserfolg 2017.

www.hikvision.com ■

Umsatz und Ergebnis wachsen bei G+D

Der global tätige Konzern für Sicherheitstechnologie Giesecke+Devrient (G+D) hat mit 2,14 Milliarden Euro den hohen Umsatz des Vorjahres mit einem Anstieg um mehr als 2 % erneut ausgebaut. Das angepasste Ergebnis vor Zinsen und Steuern (EBIT) stieg im Vergleich zum Vorjahr um 4 % auf 130 Millionen Euro. Damit hat G+D sein EBIT innerhalb der letzten vier Jahre mehr als verdoppelt. Alle Unternehmensbereiche – Currency Technology, Mobile Security, Veridos und secunet – haben dabei erneut einen positiven Beitrag zum Ergebnis geleistet. G+D verzeichnet einen im Vergleich zum Vorjahr mit 28 % deutlich gesteigerten Jahresüberschuss von 67 Millionen Euro.

www.gi-de.com ■

Rund um das Personal- und Zeitmanagement

Zufrieden blickt das Team der Isgus-Niederlassung Frankfurt am Main auf den Infotag im April zurück. Unter dem Motto „Treibstoff für Ihr Unternehmen" erhielten die Teilnehmer alle aktuellen Informationen rund um die Zeus-Module: Zeiterfassung, Personaleinsatzplanung, Zutrittskontrolle, Betriebs- und Maschinendatenerfassung. Und auch das Thema Datenschutz mit der Umsetzung der neuen Datenschutzgrundverordnung (DSGVO) kam nicht zu kurz. Als toller Veranstaltungsort präsentierte sich die Central Garage – Zentrum für Automobilisten in Bad Homburg. Es blieben keine Wünsche offen, ob als Fan für Oldtimer, Youngtimer oder technikbegeisterte Besucher.

www.isgus.de ■

Genetec vergibt Platinum-Partner-Status an Mobotix

Mobotix, Anbieter von digitalen, hochauflösenden und netzwerkbasierten Video-Sicherheitssystemen, wurde von Genetec, Technologieanbieter für einheitliche Sicherheits-, öffentliche Sicherheits-, Betriebs- und Business-Intelligence-Lösungen, zum Platinum-Partner ernannt. Der Platinum-Partner-Status, der global nur an acht Genetec-Technologiepartner verliehen wird, steht für die Anerkennung der strategischen Beziehung, die Forschung und Entwicklung, Tests, Geschäftsentwicklung und Verkaufsunterstützung für neue und bestehende Unternehmenskunden weltweit. Im Rahmen der Partnerschaft werden die Mobotix-Mx6-Produktlinien der Outdoor-, Indoor-und Thermalkameras nun offiziell in aktuellen und zukünftigen Versionen des Genetec Security-Centers unterstützt. Die Integration umfasst eine weitläufige Unterstützung des Mobotix-Mx-PEG-Codecs sowie wichtige Funktionen wie intelligente Videoanalyse-Tools und Verhaltenserkennung.

www.mobotix.com ■

Weniger Unfälle mit schweren Folgen

Die Zahl der meldepflichtigen Arbeitsunfälle ist im Jahr 2017 um 0,4 % auf 873.562 zurückgegangen. Das ergeben die vorläufigen Arbeitsunfallzahlen, die die Deutsche Gesetzliche Unfallversicherung (DGUV), Spitzenverband der Berufsgenossenschaften und Unfallkassen, veröffentlicht hat. Einen Anstieg gab es hingegen bei den meldepflichtigen Wegeunfällen. Im vergangenen Jahr ereigneten sich 190.095 Unfälle auf dem Weg zur Arbeit und wieder nach Hause. Das sind 2,2 % mehr als im Vorjahr. Einen neuen Tiefstand gab es bei den neuen Unfallrenten insgesamt: Sie gingen um 604 Fälle auf 18.244 neue Unfallrenten zurück. „Kommmitmensch" wirbt für eine gute Präventionskultur in Betrieben und Einrichtungen. Sicherheit und Gesundheit bei allen Handlungen und Entscheidungen mitdenken, das ist das Ziel der Kampagne.

www.kommmitmensch.de,
www.dguv.de ■

Evva verstärkt Konzernbereich Digital Services

Gunther Glawar ist neuer Konzernbereichsleiter Digital Services bei Evva Sicherheitstechnologie.

Das Industrieunternehmen möchte die Digitalisierung weiter offensiv vorantreiben und hat dafür den Konzernbereich Digital Services geschaffen. Executive Vice President/ CDO dieses neuen Bereichs ist seit September letzten Jahres DI Gunther Glawar. Der 46-jährige gebürtige Steirer startete nach erfolgreichem Mathematik-Wirtschaft-Studium an der TU Graz seine Laufbahn im Bereich Logistik und IT bei der Knapp AG. Nach drei Jahren wechselte der Ingenieur zu Magna Steyr in das Prozess-Consulting und konnte dort über den Zeitraum von neun Jahren sein IT- und Digital-Know-how weiterentwickeln. Zuletzt verantwortete Glawar bei der Hirtenberger Gruppe die Aufgabengebiete IT und Digitalisierung und war damit der ideale Kandidat für diese Position.

www.evva.de ■

GIT SICHERHEIT AWARD

Neue Finalisten

Viele Bewerber und zahlreiche Produkte, die für viel Diskussionsstoff in der neutralen Fachjury sorgten. Doch jetzt stehen die Finalisten fest und der GIT SICHERHEIT AWARD geht in die nächste Runde.

Leser stimmen ab

Nachdem unsere Fachjury aus den Bereichen die Finalisten in jeder Kategorie ausgewählt hat, sind nun Sie – unsere Leser – an der Reihe, die Sieger des kommenden GIT SICHERHEIT AWARD zu bestimmen.

Abbildung ähnlich.

Gewinnen Sie den Leser-Preis!

So eine kann jeder gebrauchen: Wir verlosen auch diesmal wieder eine hochwertige, aktuelle Spiegelreflexkamera. Machen Sie mit! Wählen Sie je einen Favoriten aus jeder Kategorie und nehmen Sie an der Verlosung teil.

Die folgenden Seiten zeigen alle Finalisten-Produkte in den Kategorien:

- A – Safety und IT-Security in der Automation, Cyber Security
- B – Brandschutz, Ex- und Arbeitsschutz
- C – Video-Sicherheitssysteme (VSS)
- D – Zutritt, Einbruch- und Perimeterschutz
- E – Sicherheitsmanagement, Lösungen und Dienstleistungen
- F – Sonderkategorie Smart Home

Um ein faires Voting zu gewährleisten, dürfen Unternehmensmitarbeiter nicht für ihre eigenen Produkte stimmen.
Es kann zudem nur mit einer gültigen Firmenadresse abgestimmt werden (Privatpersonen ausgeschlossen).

Stimmen Sie ab – Teilnahmeschluss ist der 24. August 2018!

Stimmabgabe ausschließlich online auf: www.sicherheit-award.de
Dort finden Sie ebenfalls nochmals alle nominierten Finalisten

Bewerteten und analysierten die Bewerber aus den Bereichen Brandschutz, Ex- und Arbeitsschutz: v.l.n.r. Lars Komrowski, TÜV Hessen, Steffen Ebert, Bernd Saßmannshausen, Sicherheits-Chef von Merck, Dr. Heiko Baumgartner, Peter Krapp, Geschäftsführer des ZVEI, Heiner Jerofsky und Andreas Heller vom ZVEI

Prüften die Kandidaten aus den Bereichen Sicherheitsmanagement und -lösungen, Zutrittssysteme, Einbruch- und Perimeterschutz ebenso wie Videosicherheitssysteme auf Herz und Nieren – und nominierten für die Shortlist der Finalisten: v.l.n.r. Steffen Ebert, Manfred Gügel, Chef beim Integrator MNO, Thomas Kunz, Gründer von Vi2Vi, Dr. Peter Schäfer, Leiter der Security-Abteilung bei Merck, Berater und Integrator Heiko Viehweger und Heiko Baumgartner

Kategorie A

Safety und IT-Security in der Automation, Cyber Security

ABB: AFS

AFS Schütze für Sicherheitsanwendungen

Die AFS-Schütze verfügen als Teil der Sicherheitskette über einen fest angebauten Hilfskontaktblock (2 Ö, 2 S) in Safety-Farbe mit zwangsgeführten Hilfskontakten und Mirror-Öffnerkontakten sowie einer Schutzabdeckung und integrierten Entstörgliedern. Zur Integration in Maschinenhersteller-Systeme stehen Daten über Tools wie Sistema oder FSDT von ABB für die Konstruktion gemäß EN ISO 13849 und EN 62061 bereit. Für die Ermittlung des Performance Level (EN ISO 13849) oder von SIL-Werten (EN IEC 62061) sind B10D-Werte verfügbar. Im Fehlerfall reagieren die Schütze mit Ausschaltzeiten von bis zu 30 Millisekunden. Sie verfügen über integrierten Überspannungsschutz und ihre Schützspule verbraucht bis zu 60 % weniger Energie.

Fiessler Elektronik: FMSC

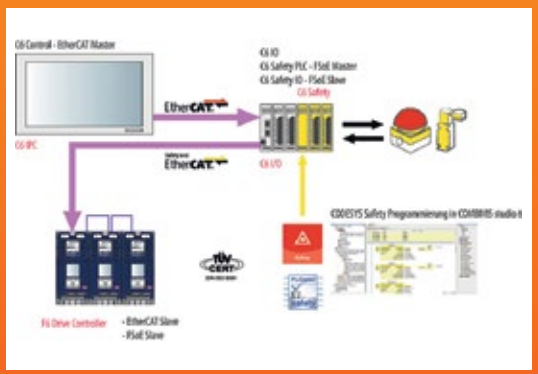
Sicherheitssteuerung

Die Sicherheitssteuerung FMSC, Fiessler Modular Safety Controller, zeichnet sich durch ein modulares Konzept aus. Dazu stehen verschiedene Master – als auch Slavegeräte zur Verfügung. Ein zweistelliges Display für die Erstdiagnose sowie ein USB-Port für die Online-Diagnose runden das Hardwareprofil der Sicherheitssteuerung FMSC ab. Die einfache und intuitive Programmierung der Sicherheitssteuerung FMSC erfolgt mittels der Programmiersoftware FMSC Studio auf zeichnerischem Wege. Je nach Konfiguration stehen bis zu 204 Eingänge, 68 sichere Ausgänge, und 85 Standardausgänge zur Verfügung. Es können bis zu 17 Achsen nach PLe überwacht werden.

KEB: C6 Safety

Sichere Systemlösungen

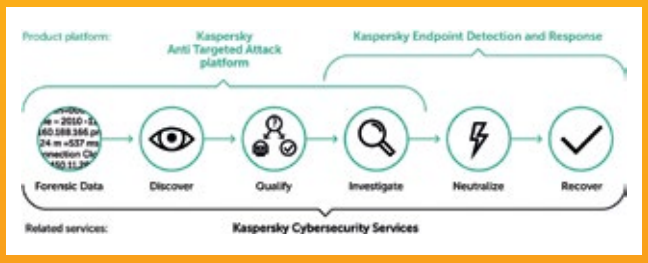
Die Lösungen von KEB Automation bieten eine komplett in das Automatisierungssystem integrierte Sicherheitsarchitektur über drei Ebenen: Neben der C6 Safety PLC als Sicherheitssteuerung gibt es die C6 Safety I/Os zur dezentralen Installation. Hinzukommen die Drive Controller Combivert S6-A und F6-A. Sind sie mit entsprechendem Sicherheitsmodul ausgestattet, bieten sie umfangreiche Funktionen nach IEC- und ISO-Standard mit bewegungsbasierter, sicherer Überwachung direkt im Antrieb. Drittes Element ist die KEB-Automatisierungsplattform Combivis studio 6. Sie vereint die funktionale sowie sicherheitsgerichtete Parametrierung und Programmierung. Vereinfacht wird die Arbeit durch funktionsspezifische Wizards. Die Kommunikation erfolgt über den vorhandenen EtherCAT-Bus mit zertifiziertem Protokoll Safety over EtherCAT (FSoE). Durch die dezentralisierte Struktur ist eine direkte Montage in Maschinen und Anlagen ohne zusätzlichen Verdrahtungsaufwand bei geringstem Platzbedarf möglich. Über die Safety PLC mit FSoE-Master können beliebige FSoE-Slaves (zum Beispiel Safety I/O-Module, KEB Drive Controller mit Sicherheitsmodul) angesprochen werden. ▶



Bernstein: SMART Safety Sensor SRF

Sicherheitssensor für Industrie 4.0

Der berührungslose Smart Safety Sensor SRF unterstützt die Umsetzung einer sicheren Smart Factory: Der SRF (Safety RFID) überwacht beweglich trennende Schutzeinrichtungen, bspw. Klappen oder Türen von Schutzgittern und schützt Mitarbeiter, indem er Maschinen und Anlagen abschaltet oder den Start der Maschine verhindert, bis die trennende Schutzeinrichtung ordnungsgemäß geschlossen ist. Der Fokus liegt auf dem Diagnosesystem DCD: Es liest eine Vielzahl an Daten aus und macht sie zentral verfügbar. Die Diagnosedaten werden bspw. über I/O Link in die Maschinensteuerung eingelesen oder per NFC Technologie auf dem Smartphone angezeigt. So ist eine vorausschauende Wartung (predictive maintenance) durch frühzeitige Fehlererkennung möglich. Das Besondere dieser Neuentwicklung ist das zum Sensor zugehörige Diagnosesystem DCD: Es liest eine Vielzahl an Daten aus jedem einzelnen Sensor aus und macht sie zentral und flexibel im Sinne einer intelligenten Produktion verfügbar. Ein solches Verfahren ist einzigartig am Markt.



Kaspersky: Threat Management and Defense

Cyber-Security Lösung

Die adaptive Unternehmenslösung Kaspersky Threat Management and Defense kombiniert Technologien und Services, die die Implementierung einer adaptiven Sicherheitsstrategie unterstützen. Die Plattform hilft Sicherheitsteams, Angriffe abzuwehren, spezifische Bedrohungen schnell zu erkennen, auf Echtzeit-Vorfälle zu reagieren und zukünftige Bedrohungen zu antizipieren. Die Lösung passt sich laufenden Prozessen der Informationssicherheit an. Die technischen Komponenten werden durch die globale Threat Intelligence sowie spezielle Expertenservices mit Spezialisierung auf Threat Hunting und Vorfallreaktion ergänzt. So ist ein einheitlicher Cybersecurity-Ansatz zum Schutz vor komplexen Bedrohungen und zielgerichteten Angriffen möglich.

Leuze electronic: MLC 500

Sicherheits-Lichtvorhänge mit Smart Process Gating

Die Sicherheits-Lichtvorhänge MLC 500 in der Variante mit Smart Process Gating (SPG) werden für Zugangssicherungen mit Materialtransport eingesetzt. Die Ablaufkontrolle für den Gating-Prozess erfolgt in Verbindung mit der Anlagensteuerung. Dadurch kann auf die sonst notwenigen ‚Muting-Sensoren' verzichtet werden. Der Prozess wird durch zwei Signale gesteuert: das erste Signal kommt von der Steuerung (SPS), während das Zweite durch das Schutzfeld selbst erzeugt wird. Die Kontrolle des zeitlichen Ablaufs erfolgt durch den Lichtvorhang. Das SPS-Signal muss so erzeugt werden, dass beim Einleiten des Gatings das Transportgut nicht mehr als 200mm vom Lichtvorhang entfernt ist. MLC 530 Smart Prozess Gating ist sicherheitstechnisch TÜV-zertifiziert. Das SPG erlaubt eine sehr kompakte Anlagen-Auslegung und spart so wertvollen Platz. Erhöhte Zuverlässigkeit und reduziertes Manipulationsrisiko sichern hohe Anlagen-Verfügbarkeit. Auch Paletten mit ungleichmäßiger Beladung (z. B. Teile nur auf einer Seite oder Lücken zwischen der Beladung) werden zuverlässig transportiert. Zudem ist der Prozess unabhängig von der Art der Oberfläche des Förderguts (matt bzw. stark reflektierend). Geringerer Installations- und Service-Aufwand (einfache Installation, keine Justage von Sensoren bei Änderungen des Förderguts).

Patlite: NHL

Netzwerküberwachungs-Signalturm

Die NHL ermöglicht eine kostengünstige Überwachung komplexer Netzwerkgeräte und stellt die Schnittstelle zwischen dem Anwender und der Sicherheitstechnik da. Die Reaktionszeit des Mitarbeiters wird reduziert, da dieser optisch, akustisch und per E-Mail über ein unübliches Ereignis informiert wird. Der Text der automatisch versendeten E-Mail wird individuell festgelegt und die Informationsdichte auf den Empfängerkreis angepasst. Die NHL geht über den Einsatzbereich einer klassischen Signalsäule hinaus, da das kontinuierliche Ping Monitoring der Netzwerkprodukte und die SNMP Trap Meldung helfen, z.B. einen Serverzusammenbruch zu vermeiden. Die Handhabung im täglichen Einsatz ist intuitiv, die Einrichtung erfolgt durch den Webbrowser und die Software kann selbst bei Fernzugriff aktualisiert werden. Der Anwender profitiert vom Design der NHL, welches sich der Büroumgebung anpasst und drei Befestigungsarten (an der Wand, auf Trennwänden, stehend auf dem Tisch) bietet.

Pepperl+Fuchs: safePXV und safePGV

Positioniersysteme

Safety-Anwendungen nach „SIL 3/PL e" erfordern die Einhaltung höchster Sicherheitsrichtlinien, um Mensch und Maschine jederzeit optimal zu schützen. Während dieses Sicherheitslevel bisher mit einem hohen Kosten- und Zeitaufwand verbunden war, können Anwender dies mit den Positioniersystemen „safePXV" und „safePGV" von Pepperl+Fuchs. Basierend auf einer mehrfach redundanten Technologie ermöglichen diese erstmals die sichere Absolut-Positionierung nach SIL 3/PL e mit nur einem einzigen Sensor. Der safePXV bietet dabei eine Lösung für die lineare Absolut-Positionierung; der safePGV darüber hinaus für das zuverlässige Navigieren von fahrerlosen Transportsystemen. Basis der neuen Sicherheitstechnologie ist die seit Jahren bewährte und besonders zuverlässige Kombination aus einem 2-D-Lesekopf und dem DataMatrix-Code. Allerdings kommt hier ein spezielles Band mit zwei sich überlagernden DataMatrix-Codes in Rot und Blau zum Einsatz. Der 2-D-Lesekopf ist mit zwei unterschiedlich farbigen LED-Ringen – ebenfalls in Rot und Blau – ausgestattet. Durch die zweifarbigen Codes in Verbindung mit der zweifarbigen Beleuchtung entsteht die Sicherheitslösung. In jedem einzelnen Code befinden sich Positions- und Sicherheitsinformationen, die durch die LED-Beleuchtung in Rot beziehungsweise Blau sichtbar gemacht werden und so von der Kamera auslesbar sind. Daher kann die sichere X-Position dort direkt, ohne Prüfung weiterverarbeitet und zur Prozesssteuerung verwendet werden.

Pilz: SecurityBridge

Industrial Security

Mit der SecurityBridge erweitert Pilz sein Produktspektrum um den Bereich Industrial Security. Die Pilz SecurityBridge schützt die Verbindungen zwischen Programmier- bzw. Konfigurationstools und den Hardware-Steuerungen vor Manipulationen, indem sie z.B. unerlaubte Veränderungen am Automatisierungsprojekt aufdeckt. Sie fungiert dabei wie eine Firewall. Anders als generische Firewalls muss sie jedoch nicht aufwändig konfiguriert werden und kann dank anwendungsspezifischer Voreinstellungen nach dem Plug-and-play-Prinzip einfach in Betrieb genommen werden.Anwender profitieren neben der Security auch von einer höheren Verfügbarkeit der Anlage, da nur notwendige Daten (autorisierte Konfiguration und Prozessdaten) übertragen werden.

R3 Communications: EchoRing Evaluation Kit

Kabellose Echtzeit-Übertragungstechnologie

EchoRing wurde als Kabellos-Technologie auf Software-Basis für zeitkritische Anwendungen entwickelt, die gleichzeitig eine hohe Prozesssicherheit (Ausfallwahrscheinlichkeit < 10-8) benötigen. Basierend auf aktuellen Forschungsergebnissen im Bereich massiver Kooperation ermöglicht EchoRing eine deterministische und latenzarme Echtzeitkommunikation (bis zu 1ms), deren Performance an kabelgebundene Systeme heranreicht. Das EchoRing Evaluation Kit ist das erste Produkt von R3 Communications, das auf dem EchoRing basiert. Es wurde entwickelt, um die hochzuverlässige und echtzeitfähige EchoRing-Technologie in Produktionsumgebungen zu testen. Der EchoRing-Ansatz basiert auf einem Token-Ring-Verfahren. Hierbei wird der Token auch als Austauschplattform für Kanalzustände genutzt. Da er jeden Kommunikationsknoten des Netzwerks durchläuft, werden die Kanalzustände aller Übertragungsstrecken des Systems verteilt. Anhand der dadurch vorhandenen vollständigen Kanalkenntnis kann für jede Übertragung ein perfekter Knoten („Buddy") für eine ggf. notwendige Wiederholung bestimmt werden – diese auf räumliche Diversität basierende Technik wird als „massive Kooperation" bezeichnet. Die Implementierung des rein Software-basierten Ansatzes ist auf bereits existierender Hardware möglich.

SSP Safety System Products: HoldX R

Sichere Magnetzuhaltung

Die magnetische Prozesszuhaltung HoldX R kombiniert in kleinster Bauform einen sicheren berührungslosen RFID-Sicherheitssensor mit einem intelligenten Elektromagneten in nur einem Gerät. Über ein- und ausgehende Pigtail-Kabel lassen sich bis zu 17 HoldX R einfach in Reihe schalten. Die Leitung wird einfach durchgeschleift und damit der Verkabelungsaufwand massiv reduziert. Die Besonderheit dabei: Über einen internen Bus, der ganz ohne Gateway zur übergeordneten SPS ausgewertet werden kann, lässt sich jede einzelne Einheit separat auswerten und sogar ansteuern. Eine Bluetooth-Schnittstelle ermöglicht dem Anwender mit einer App sogar mobil auf die Diagnosefunktion der Zuhaltungen zuzugreifen und etwa den Fehlerspeicher einzusehen. Die Kombination aus Magnetzuhaltung und Sicherheitssensor an sich ist nichts Neues. Jedoch handelt es sich bei der S-Variante der HoldX R um die wohl kleinste Bauform am Markt. Was die HoldX R von Wettbewerbsprodukten abhebt, ist die Reihenschaltung, der interne Informations-Bus und die Bluetooth Schnittstelle. Die Reihenschaltung mit ein- und ausgehenden Kabeln von Einheit zu Einheit ist besonders, da sie ohne Y-Stecker oder ähnliches auskommt. Die Adressierung erfolgt über einen manuellen Drehschalter am Gerät selbst, so weiß jede Zuhaltung welcher Teilnehmer sie ist.

Rohde & Schwarz Cybersecurity: TrustedGate

Sicherheitslösung für Clouds

Die Sicherheitslösung TrustedGate verbindet einen Hochsicherheits-Cloud Access Security Broker (CASB) mit einem datenzentrischen Verschlüsselungssystem, um für ausreichenden Schutz zu sorgen (virtuelle Daten in der Cloud und Originaldaten an einem Speicherort der Wahl). Erst beim Download wird das Dokument wieder zusammengesetzt und entschlüsselt. Dabei setzt es auf Sicherheit bei gleichzeitiger Usability. Die Lösung hält zudem Regularien bei der Nutzung von cloudbasierten Systemen ein (z.B. DSGVO). Durch Monitoring der Aktivitäten und Benachrichtigungen beim Eintritt von sicherheitsrelevanten Events bietet es Revisionssicherheit. Im Vergleich zu herkömmlichen CASBs legt TrustedGate nicht nur Wert auf Zugangsberechtigungen in der Cloud, sondern verschlüsselt die Daten gleichzeitig. Dadurch werden die Daten hochsicher gehalten, während gleichzeitig transparent in der Cloud gearbeitet werden kann. Trotz Fragmentierung ist so z.B. eine sichere Volltextsuche in verschlüsselten Texten möglich. Die innovative TrustedGate Office365 Encryption sorgt zudem für Data-Leakage Prevention bei Email-Anhängen. Durch die freie Auswahl vom Speicherplatz, trägt TrustedGate zudem zur Kostenoptimierung bei, indem der günstigere Speicherplatz gewählt werden kann.

Trend Micro: TippingPoint Threat Protection System

Cyber Security

Bei den Trend Micro TippingPoint Threat Protection Systemen handelt es sich um Next-Generation Intrusion-Prevention-Systeme (NGIPS). Sie schützen vor unbefugtem Zugriff auf Netzwerke, indem sie Angriffe auf bekannte und nicht-veröffentlichte Schwachstellen in Echtzeit erkennen und blockieren. Die Systeme nutzen dabei eine Kombination verschiedener Technologien, wie Deep Packet Inspection, Bedrohungs- und URL-Reputation, sowie fortschrittliche Malware-Analyse. Zudem verfügen sie über die ständig aktualisierten globalen Bedrohungsinformationen von Trend Micro. Die Systeme werden in-line in einem Netzwerk installiert und ermöglichen damit unter anderem die Absicherung von vernetzten Industrieanlagen, ohne etwas an diesen Anlagen zu verändern.

Werma Signaltechnik: KombiSIGN 72

Modulare Signalsäule

Die modulare Signalsäule KombiSIGN 72 vereint schnelle Montage, beste Sichtbarkeit und höchste Flexibilität. Da heutige Signalgeräte nicht nur optisch und akustisch vor Ort warnen, leiten und schützen, sondern auch intelligent miteinander kommunizieren, setzt Werma auf modernste Technologien zur Vernetzung. Signalgeräte verfügen über Schnittstellen wie IO-Link, ASi, USB oder Anschluss an das Funknetzwerk und ermöglichen so einen schnellen, flexiblen und unkomplizierten Datenaustausch. Dank OmniView-Kalotte ist sie aus allen Positionen deutlich sichtbar, ohne tote Winkel. TwinLight und TwinFlash vereinen zwei Leuchtbildfunktionen in einem Element, das einfach umgeschalten werden kann

Kategorie B

Brandschutz, Ex- und Arbeitsschutz

Apollo Fire Detectors: Soteria Dimension

Optischer Rauchmelder

Die optischen Rauchmelder Soteria Dimension von Apollo mit deckenbündiger Unterputz-Montage eignen sich für ästhetisch anspruchsvolle Objekte, in denen Architekten einen unauffälligen, von der Gestaltung des Raumes nicht ablenkenden Rauchmelder benötigen sowie für risikoreiche Umgebungen. Die Melder ohne klassische Melderkammer sind mit einer patentierten optischen Sensortechnik ausgestattet, die Rauch außerhalb des Melders detektiert, und dadurch eine Brandfrüherkennung sicherstellt, Falschalarme reduziert und die Wartung vereinfacht. Die nach EN54-7 zugelassen Melder sind in einer Spezialausführung erhältlich, deren Anti-Ligatur Design unabhängig zertifiziert wurde und den Einsatz in Hochsicherheits-Umgebungen wie Gefängnissen, psychiatrischen Kliniken und ähnlichen Umgebungen zulässt. Der Rauchmelder ist durch die Metall-Frontplatte, manipulationssicheren Schrauben und geringer Bauhöhe für Hochrisiko-Umgebungen geeignet.

Bosch Sicherheitssysteme: Remote Services

System zur Ferndiagnose und Fernwartung von Brandmeldeanlagen

Remote Services von Bosch ermöglicht Systemintegratoren, Anlagen aus der Ferne zu warten, rund um die Uhr zu kontrollieren und Störungen frühzeitig zu erkennen. Die IP-basierte Lösung zur Ferndiagnose und Fernwartung erhöht die Zuverlässigkeit von Brandmeldeanlagen und macht den Betrieb effizienter. Remote Services ist ein modulares System bestehend aus drei Komponenten: Remote Connect - Programmierung und Updates der Brandmeldeanlage können jederzeit unabhängig vom Standort vorgenommen werden. Über Remote Maintenance werden die Daten der Brandmeldeanlage laufend erfasst und analysiert, mit dem Ziel, Fehlerquellen zu erkennen, bevor Störungen auftreten und um präventiv einzugreifen. Remote Alert sorgt mit Benachrichtigungen bei Störungen und Alarm für eine bessere Transparenz. Kunden profitieren so von schnellerem Service und kürzeren Ausfallzeiten. Die Wartung wird effizienter und Störungsmeldungen sowie Warnungen werden automatisch über mobile Geräte via SMS und Email versandt. Der Errichter kann durch an die Bosch Cloud übertragene live Daten des Systems und dessen Elemente Wartungseinsätze besser planen und vorbereiten

Dormakaba Germany: G-Ubivis XEA

Batteriebetriebene Feststellanlage

G-Ubivis XEA ist eine batteriebetriebene Feststellanlage zum sicheren Feststellen von Feuer- und Brandschutztüren. Die Energieversorgung durch eine Batterie ermöglicht nicht nur eine unkomplizierte Montage ohne Vorarbeiten anderer Gewerke – sie erlaubt auch eine hohe Flexibilität im Planungsprozess, da kein externer Stromanschluss notwendig ist. Sie wurde konzipiert für einflüglige Türen mit einer Flügelbreite bis 1.250 Millimeter. Als Feststellanlage ist sie für das barrierefreie Bauen nach DIN 18040 geeignet und kann in Bausituationen, die Barrierefreiheit ermöglichen sollen, eingesetzt werden. Die Anlage eignet sich besonders gut für Nachrüstungen in Gebäuden, die keine Eingriffe in die Gebäudesubstanzzulassen, wie etwa bei denkmalgeschützten Bauten. Weil die G-Ubivis keinen Netzanschluss erfordert, wird kein Elektriker gebraucht, um das System anzuschließen.

EPS: FireAngel NG-9B

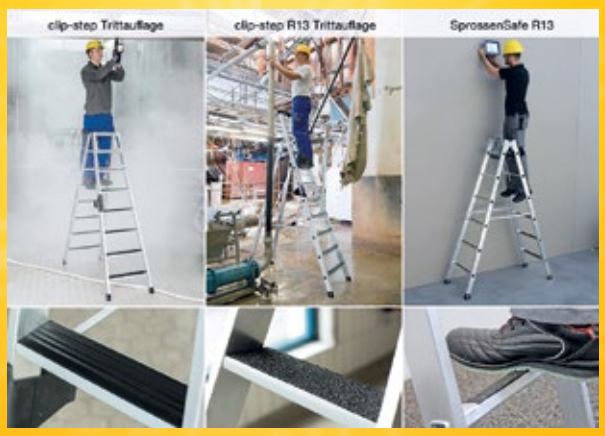
Batteriebetriebener Gasmelder

Der batteriebetriebene Gasmelder NG-9B von FireAngel detektiert sicher und zuverlässig Stadt- und Erdgas (Methan). Der Sensor arbeitet mit einer deutlich verringerten Stromaufnahme, sodass der neue FireAngel Gasmelder ausschließlich mit herkömmlichen Lithiumbatterien betrieben werden kann. Die Warnung erfolgt bereits bei sehr geringen Konzentrationen, die unterhalb eines zündfähigen Gas-Luftgemisches liegen. Die definierte Auslöseschwelle beträgt 10 % des unteren Explosionspunktes. Der FireAngel Gasmelder wurde gemäß der EN 50194-I: 2009 entwickelt und verfügt über intelligente Test-, Silence- und Reset-Tasten für eine erhöhte Benutzerfreundlichkeit. Die Installation des Gerätes kann flexibel und unabhängig von einem verfügbaren Stromanschluss einfach und schnell erfolgen und es kann problemlos in allen Gebäuden mit Gasanschluss nachgerüstet werden.

Dräger: Pac 6000

Eingasmessgerät

Schnelle und zuverlässige Gasmessung ist im industriellen Umfeld enorm wichtig. Das zeitlimitierte, personenbezogene Eingasmessgerät, Dräger Pac 6000, misst auch unter rauesten Bedingungen zuverlässig und präzise CO, H2S, SO2 oder O2. Robustes Design, schnelle Sensoransprechzeiten und eine kraftvolle Batterie sorgen für maximale Sicherheit – zwei Jahre lang und praktisch wartungsfrei. Zudem ist es einfach in der Handhabung. Durch das weite Messspektrum kann das Pac 6000 vielfältig eingesetzt werden: Der CO-Sensor beispielsweise misst Konzentrationen von 1 bis 1.999 ppm, der H2S-Sensor von 0,4 bis 100 ppm.



Günzburger Steigtechnik: clip-step

Rutschsichere Trittflächen für Leitern

Die Trittauflagen clip-step und clip-step R13 sorgen für eine optimierte Rutsch- und Arbeitssicherheit, sicheren Tritt und komfortablen Stand auf Stufenleitern. clip-step besteht aus geriffeltem Kunststoff und sorgt für verbesserte Rutschhemmung bis zu 60 Prozent. clip-step R13 mit Kunststoffprofil und Korundeinstreuung erfüllt die Vorgaben der höchstmöglichen Bewertungsgruppe R13 und sorgt in nassen und öligen Arbeitsbereichen für erhöhte Arbeitssicherheit. Zielsetzung und Anspruch der Produktentwicklungen war die signifikante Verbesserung des Tritt- und Standverhaltens von Nutzern auf Sprossen- und Stufenleitern aus Aluminium und eine deutliche Verbesserung der Arbeitssicherheit.

Honeywell Industrial Safety: Sensepoint XCL / XRL

Bluethooth-fähiger Gasdetektor

Sensepoint XCL/XRL ist ein stationärer, Bluetooth-fähiger Gasdetektor, der den Betrieb und die Mitarbeiter schützt und gleichzeitig die Installation und Wartung durch eine intuitive Smartphone-App vereinfacht. Der Sensepoint XCL misst die gefährliche Konzentration eines ausgewählten Gases und eignet sich dabei für gewerbliche und leichtindustrielle Anwendungen. Der Sensepoint XRL hingegen ist für den Einsatz in explosionsgefährdeten Bereich zertifiziert und daher für den industriellen Einsatz geeignet. Er ist nach IP 66 zertifiziert und verfügt über ein Metallgehäuse, das auch rauen Einsatzbedingungen standhält und gegen regelmäßiges Abspritzen geschützt ist. Die intuitive Sensepoint App führt durch Einrichtung, Kalibrierung, Test und Wartung. Mit der neuen Bluetooth-Konnektivität kann ein einzelner Mitarbeiter alle relevanten Aufgaben sicher vom Boden aus erledigen, von der Einrichtung über die Wartung bis hin zur Berichtserstellung. In Verbindung mit einem Smartphone (oder einem eigensicheren Smartphone in explosionsgefährdeten Bereichen) über eine herunterladbare App ermöglichen Sensepoint XCL/XRL einem einzelnen Mitarbeiter die Einrichtung, Inbetriebnahme, Wartung und Verwaltung des Gasdetektors aus bis zu 10 Metern Entfernung, ohne dass ein zweiter Mitarbeiter in einem Kontrollraum benötigt wird.

Helly Hansen: ICU HI VIS 3 Layer Shell Jacket

Selbstleuchtende Warnschutzjacke

Die Warnschutzjacke aus der ICU Kollektion bietet Sichtbarkeit bei Dunkelheit und Schutz in allen Wetterlagen. Mit der integrierten Light-Flex-Technologie werden Personen sogar ohne direkten Lichteinfall und aus großer Entfernung wahrgenommen: Eine zuverlässige, aktive Lichtquelle aus wasserdichten Leuchtstreifen, die durch einen aufladbaren Akku gespeist werden, verbessern die Sichtbarkeit und Sicherheit bei allen Lichtverhältnissen. Aufgedruckte, passive Reflektoren werden dadurch um eine aktive Lichtquelle ergänzt und erhöhen so die Sichtbarkeit, selbst über weite Entfernungen. Dies macht den Träger nahezu 10-mal sichtbarer – bei Tag und bei Nacht. Die Batterie verfügt über eine Lebensdauer von bis zu zehn Stunden und lässt sich innerhalb von 90 Minuten wieder aufladen. Selbst beim Ladevorgang behält das Light-Flex-System seine reflektierende Eigenschaft bei.

Säbu Morsbach: SAFE Tank Control

Lagercontainer für Gefahrstoffe

Safe Tank Control ist ein Lagercontainer für Gefahrstoffe mit einem serienmäßig verbauten System zu frühzeitigen Erkennung von Explosionsgefahren. Durch die kontinuierliche Messung der Gaskonzentration ist das System in der Lage, eine Warnung der Belegschaft sicherzustellen. Gegenmaßnahmen werden automatisch aktiviert, um die Gaskonzentration zu senken oder die Zündquellen zu eliminieren. Neben einer Erhöhung der Sicherheit wird eine erhebliche Reduzierung der Betriebskosten, besonders im Vergleich zu anderen isolierten und beheizten Gefahrstoffcontainern erreicht. Sobald die Gaskonzentration 10 Prozent der untersten Explosionsgrenze (UEG) des Gas-Luft-Gemisches übersteigt, schaltet sich automatisch der Lüfter ein. Eine Kontrollleuchte an der Außenseite des Gefahrstoffcontainers leuchtet gelb auf. Bei einer Überschreitung des Gas-Luft-Gemisches von 20 % unterbricht die Gaswarnanlage automatisch und umgehend die Stromzufuhr zu allen elektrischen Geräten im Innenraum.

Siqura: XCU Fusion

Edelstahl Dual-Kamera

Die XCU Fusion wurde für den Einsatz in rauen und aggressiven Umgebungen entwickelt. Typische Anwendungen finden sich in der Schwerindustrie, im Verkehr, in Tunneln, auf Wasserstraßen, in der Abfallbehandlung und in der salzhaltigen Meeresumgebung. Die XCU Fusion kombiniert einen Full-HD ultra-low Light Bildaufnehmer mit einem ungekühlten Bolometer für Tag- und Nachtsicht. Die Kamera kann in heißen Klimazonen und in extremer Kälte verwendet werden und korrosionsfördernden Atmosphären widerstehen, die durch Abgase und Salz verursacht werden. Vibrationen, starke Windlasten, Hochdruckwasserstrahlreinigung und allgemein alle Arten von Niederschlag sind für die Kamera kein Problem.

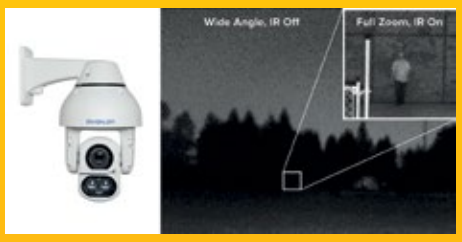
Weiss: smalin

Brand- und Gefahrenmelder

smalin ist eine Kombination aus Rauch-, Kohlenmonoxid- und Thermowarnmelder, entwickelt als Leuchten-Baldachin, zur zentralen Installation an Deckenhängeleuchten. Dabei handelt es sich um einen zur Decke hin geöffneten Baldachin, welcher für nahezu jede Art von Deckenhänge- und Pendelleuchten verwendbar ist. So werden Schutzfunktionen und Design mit einander kombiniert. Die Installation an der vorhandenen und meist zentral gelegenen Deckenleitung ist innerhalb kürzester Zeit möglich. Nach umfangreicher Forschungs- und Entwicklungsarbeit ist es gelungen, einen universellen Gefahrenmelder, auf die ästhetischen Ansprüche der Betreiber hin, herzustellen. smalin steht für SMart ALert INside und kann mit Smart Home Systemen vernetzt werden. Die integrierten und versiegelten Batterien versorgen smalin für bis zu 10 Jahre.

Kategorie C

Video-Sicherheitssysteme (VSS)



Avigilon: H4 IR PTZ-Kamera

PTZ-Kamera mit selbstlernender Videoanalyse

Die Avigilon H4 IR PTZ ist eine HD-PTZ-Kamera für den Außenbereich mit einer IR-Reichweite von 250 Metern, die den IR- Projektionswinkel automatisch dem Zoom und dem Sichtfeld anpasst und so dafür sorgt, dass die Szene der Zoomstufe der Kamera entsprechend ausgeleuchtet ist. In Kombination mit WDR, Bildstabilisierung und der patentierten LightCatcher-Technologie von Avigilon liefert diese Kamera in einer Vielzahl von Anwendungen und Umgebungen hervorragende Bilder. Ein abriebfestes Frontobjektiv und ein integrierter Silikonkautschukwischer sorgen auch bei ungünstiger Witterung für verzerrungsfreie, klare Bilder, sodass sich die Kamera hervorragend für eine Vielzahl von Wetterbedingungen und Überwachungsanwendungen im Außenbereich eignet.

Dahua: IPC-PFW8800-A180

Multi-Sensorkamera

Die Multi-Sensorkamera bietet zusätzliche Flexibilität bei der Erfassung von großflächigen Videoüberwachungen. Mit vier 2-MP-Sensoren, die zusammen einen umfassenden 180°-Überblick schaffen, kann die Kamera mehrere Ein-Sensor-Kameras ersetzen und bietet so einen höheren Mehrwert. Mit der Starlight-Technologie bietet die Kamera ein hochwertiges Schwachlichtbild. Fehlende Infrarot-Unterstützung und Vandalismussicherheit sind eine Einschränkung für herkömmliche Multi-Sensorkameras aufgrund der Komplexität im mechanischen Design. Die neue Panoramakamera mit gekrümmter Kuppel und separater Infrarot-Lichteinstellung überwindet diese Einschränkung und macht die Kamera für die Installation in unterschiedlichen Situationen geeignet. Sie unterstützt die Schutzklassen IP67 und IK10-Schutz und bietet Infrarotlicht. Dank Kontrast-, Gegenlichtkompensations-, Weißabgleich- und Auflösungssteuerung erhält man auch bei schwierigen Lichtverhältnissen ein kristallklares Bild.

Axis: P3717-PLE

Multi-direktionale Kamera

Die multi-direktionale Panorama-Kamera hat eine Gesamtauflösung von 8 Megapixeln, verteilt auf 4 Bildsensoren mit jeweils 1080p Auflösung. Die 4 Sensoren liefern jeweils bis zu 30 Bilder/Sekunde. Die Axis Lightfinder Technologie sowie Forensic WDR garantieren klare Bilder in jeder Situation, Bandbreite und Speicherbedarf werden dank Zipstream-Technologie reduziert. Die Objektive lassen sich via remote justieren, die Ausrichtung und Positionierung innerhalb der Kameraeinheit ist flexibel und einfach. Die kompakte Kamera ist mit der patentierten Axis Kuppel geschützt und IP66/IK09 zertifiziert. Sie kann von -30°C bis +50°C einsetzt werden und verfügt über 4 integrierte IR LEDs, die Videoaufnahmen auch in vollkommener Dunkelheit ermöglichen.

Eneo: eneo Candid

IP-Kamera mit integrierter Anschlusslösung

Die IP-Kamera ist mit einer integrierten Anschlusslösung und einem WLAN-Interface ausgestattet. Sie verfügt über ein motorisiertes Varifokalobjektiv (Brennweite: 2,7–12mm) und erreicht eine maximale Videoauflösung von 3MP. Mit BLC, HLC, D-WDR und Objektiventzerrung bietet sie eine Reihe von Bildoptimierungsfunktionen, die durch die Videoanalysefunktionen Bewegungserkennung, Manipulationsschutz, virtueller Stolperdraht (inkl. Zählfunktion und Richtungserkennung), Bereichsüberwachung sowie Defog ergänzt werden. Muss die Kamera z. B. bei der Korridorüberwachung um 90° oder 270° um die eigene Achse gedreht werden, sorgt VerticalView für die korrekte Bildanzeige. Die Kamera unterstützt ONVIF Profile S sowie ONVIF-Mapping und ist IP67 geschützt.

Eizo: DuraVision FDF2304W-IP

IP-Decoder-Monitor

Der IP-Monitor von EIZO mit integrierter Bildverbesserung ist für den computerlosen Anschluss von Sicherheitskameras konzipiert. Er ist für den 24/7-Einsatz gebaut und bietet höchste Zuverlässigkeit und Langlebigkeit. Bei der Videoüberwachung ist der Einsatz von Computern oft unerwünscht oder aus Platzgründen sogar unmöglich. Häufig stellen auch Thin Clients oder Decoder-Boxen dort aus Performancegründen keine Alternative dar. Speziell dafür bietet EIZO mit dem IP-Decoder-Monitor eine Lösung, die Decodierung und Bildschirmanzeige in einem Gerät vereint. Die nahezu verzögerungsfreie Darstellung von Aufnahmen auf dem Bildschirm ist durch die leistungsstarke, integrierte Hardware-Decodierung garantiert.

Flir Systems: FB-Serie ID

Wärmebildkamera mit integrierter Mensch-Fahrzeug-Erkennungsanalyse

Die FB-Serie ID ist Fixed-Bullet-Wärmebildkamera, die erstklassige Wärmebilddetails mit leistungsstarken Onboard-Analysefunktionen kombiniert und sich daher ideal für die Perimetererkennung im Nah- und Fernbereich sowie für die Überwachung steriler Bereiche eignet. Die FB-Serie ID zeichnet sich durch präzise Videoanalyse aus, die ein Eindringen in vorgegebene Bereiche durch Menschen oder Fahrzeuge detektiert, unterscheidet und klassifiziert. In Kombination mit der automatischen Verstärkungsregelung (AGC) und der Digital Detail Enhancement-Funktion (DDE) von FLIR bietet sie höchsten Bildkontrast und Schärfe, was zu deutlich weniger Fehlalarmen führt und agiert somit als echtes All-in-One-Intrusion-Detection-System. Die Kamera ist für die Integration in Video-Management-Systeme wichtiger Drittanbietern ebenso zertifiziert wie für das FLIR-eigene United VMS.

Hikvision: iDS-2CD8426G0/F-I

Kamera mit Stereo-Optik für 3D Gesichtserkennung

Die DeepinView-Gesichtserkennungskamera ist so konstruiert, dass die beiden Objektive eine Stereo-Sicht der erkannten Personen liefern. Die integrierte Technik ermöglicht Bilder mit einer Auflösung von 1080 Pixel, die auf die Gesichter zugeschnitten werden. Bis zu 30 Personen gleichzeitig werden erfasst und bis zu 90.000 Aufnahmen im Gerät selbst in 4 Bibliotheken gespeichert. Die Kamera ermöglicht dies „standalone" und in Echtzeit, inklusive des Vergleichs der erfassten Personen. So wird bei Auffälligkeiten sofort ein Alarm ausgelöst. Unterstützt durch den Deep-Learning-Algorithmus und einer Hochleistungs-GPU liefert die Kamera genaue und schnelle Ergebnisse. Diese Lösung ist ideal für u.a. Gebäude und Stadien mit hohem Publikumsverkehr.

Hanwha Techwin: XND-6085

IP-Kamera mit Varioobjektiv

Die XND-6085 aus der Wisenet extraLUX Serie ist mit einem hochleistungsfähigen, motorisierten 4,1~16,4 mm Varioobjektiv mit einer Blendenöffnung von nur F0,94 ausgerüstet. Dieses Objektiv ist weltweit einzigartig mit diesem Brennweitenbereich in dieser Lichtstärke. In Kombination mit dem eingebauten ½ -Zoll-CMOS-Sensor gewährleistet diese Optik Farbbilder bis zu 0,004 Lux bzw. 0,0004 Lux im Schwarz-Weiß Betrieb mit hervorragender Qualität ohne die Notwendigkeit von IR-LEDs oder zusätzlicher Beleuchtung. Zur Installationserleichterung ist die XND-6085 ausgestattet mit einem vollmotorisierten Kamerakopf zur lokalen Ausführung der Schwenk-/Neige-/Drehfunktionen über die Wisenet Installations-App oder per Fernzugriff über den Browser.

Mobotix: S16 Thermal

Dual-Thermalkamera

Bei dem S16 Covert Kamerasystem mit ONVIF S-Kompatibilität werden zwei separat verfügbare Thermal-Sensormodule mit bis zu 3 Meter langen Sensorkabeln flexibel an das Kameragehäuse angebunden, um besonders effiziente Installationen und kundenspezifische Sondereinbauten zu ermöglichen. Die Thermal-Sensormodule gibt es in zwei Bauformen mit jeweils drei horizontalen Blickwinkeln (45°, 25° oder 17°), jeweils auch mit Thermal Radiometry Technology für Temperaturereignisse. Sowohl das Kameragehäuse als auch die Sensormodule sind nach IP66 klassifiziert und werden mit einem robusten Sondergehäuse aus Aluminium und Edelstahl ausgeliefert.

Panasonic: WV-X8570N

4 x 4K 360-Grad Multi-Sensor Kamera

Die WV-X8570N kann auch auf Kreuzungen bei Nacht mit geringer Lichtintensität klare Fahrzeugbilder in Farbe erfassen. Die vier repositionierbaren Objektive minimieren tote Winkel und decken flexibel die Verkehrschnittpunkte und Überwachungsbereiche von Städten ab. Intelligent Auto (iA) überwacht Szenendynamik und -Bewegung, um wichtige Kameraeinstellungen automatisch in Echtzeit anzupassen und so Verzerrungen wie Bewegungsunschärfe an sich bewegenden Objekten zu reduzieren. Durch die Verwendung der H.265 Smart Coding-Technologie wird die Bandbreiteneffizienz für eine längere Aufzeichnung und weniger Speicherplatz intelligent erhöht. Die Kamera unterstützt die vollständige Datenverschlüsselung und entspricht den FIPS 140-2 Standards.

Sony: SNC-VB770

4K-Netzwerkkamera

Dank der extrem hohen ISO 409.600-Empfindlichkeit bietet die 4K-Netzwerkkamera SNC-VB770 eine hohe Leistung bei Mindestlichtstärken von weniger als 0,004 Lux. So erfasst sie außergewöhnlich detaillierte 4K-Farbvideos mit 30 Bildern pro Sekunde, auch bei Nacht und in ähnlich extremen Lichtverhältnissen. Die 4K-Netzwerkkamera SNC-VB770 erreicht dies durch Verwendung des extrem empfindlichen 35-mm-Vollformat-Exmor-Sensors, der optimierten E-Mount-Objektive zur Maximierung der Sensorleistung und der Signalverarbeitungs-Engine. Dies ermöglicht der Kamera, gestochen scharfe, klare 4K-Farbvideos mit 30 Bildern pro Sekunde mit viel weniger Bildrauschen bei extrem schlechten Lichtverhältnissen aufzunehmen.

Kategorie D

Zutritt, Einbruch- und Perimeterschutz

Abus: wAppLoxx

Zutrittskontroll-System

Mithilfe des elektronischen wAppLoxx Zutrittskontroll-systems von Abus lassen sich Türen lokal, aber auch weltweit per PC, Tablet und Smartphone öffnen. Sicherheit bietet dabei eine verschlüsselte Peer-to-Peer-Verbindung zur Datenübertragung. Auch Änderungen der Schließrechte lassen sich so in Sekundenschnelle umsetzen und damit bis zu 20 Zylinder und 150 Benutzer verwalten. Für optimalen Bedienkomfort kann wAppLoxx auch mit Alarm und Videoüberwachung zu einem umfassenden Sicherheitssystem vernetzt werden. In dieses können auch Hausautomationsfunktionen integriert werden: Über die elektronischen Schließzylinder aber auch über Hotkeys in der App lassen sich somit z. B. die Garagentür oder Lichtanlagen komfortabel steuern.

Assa Abloy: CLIQ Connect

Mobile Schließanlagen-Verwaltung

Ein Smartphone mit Cliq Connect-App und ein Cliq Connect-Schlüssel – mehr braucht es nicht, um jederzeit mobil und unabhängig die elektronische eCliq-Schließanlage zu verwalten. Alle Daten der Verwaltungssoftware, dem Cliq Web-Manager, werden optional in einer Cloud gespeichert. Sind Smartphone und Schlüssel über Bluetooth miteinander verbunden, kann die neue App aktualisierte oder zeitbegrenzte Zutrittsberechtigungen via Internet direkt vom Server abrufen und auf den Schlüssel laden. Ohne lange Wege zu einem Unternehmensstandort. Um die Sicherheit vor Hackerangriffen zu gewährleisten, werden die Daten bei der Übertragung end-to-end verschlüsselt. Das flexible System mit mobiler Schließanlagenverwaltung beschleunigt nicht nur die Arbeitsabläufe, sondern verbessert auch den Schutz vor Diebstahl, Datenklau oder Industriespionage.

Avigilon: Avigilon Presence Detector

Impulsradargerät für den Perimeterschutz

Der Avigilon Presence Detector (APD) ist ein Impulsradargerät mit kleinem Formfaktor und selbstlernender Radaranalyse, das die Umgebung abtastet, sich mit ihr vertraut macht und sich laufend an die Umgebung anpasst. Dies ermöglicht eine ausgesprochen hohe Genauigkeit bei der Anwesenheitserkennung von Personen bis zu einer Entfernung von neun Metern vom Sensor – auch wenn das Objekt verborgen oder durch andere Objekte wie Decken, Karton, Holz oder Trockenbauwände verdeckt ist. Der APD trägt mit anspruchsvoller Radaranalysetechnologie dazu bei, die Herausforderung der genauen Erkennung von menschlicher Anwesenheit in Innenräumen zu bewältigen, wo herkömmliche Geräte möglicherweise nur eingeschränkt eingesetzt werden können.

CBC: Crucial Trak

Biometrisches Zutrittskontrollsystem

CrucialTrak hat die traditionellen Einschränkungen der biometrischen Erkennungstechnologie durch die Kombination verschiedener biometrischer Technologien in einer Lösung weiterentwickelt und verbessert. Das Multi-Biometrics-Terminal ist eine All-in-One-Integration von vier verschiedenen biometrischen Technologien, die beim Identifizierungs- und Verifizierungsprozess verwendet werden: Fingerabdruck, Gesichtsmerkmale, Irismuster und Venenmuster. Die Verwendung von Multi-Biometrics nutzt die Fähigkeiten jeder Biometrie-Technologie und mindert gleichzeitig Einschränkungen einzelner Technologien.

Dormakaba: Schließzylinder mit SAT-Funktion

Temporären Zutritt gewähren

Mit der neuen SAT-Funktion (Secure Access Temporary) im Schließzylinder Kaba expert plus von Dormakaba wird ein mechanischer Zylinder um eine wichtige Funktion erweitert, die für deutlich mehr Sicherheit, Flexibilität und ein gutes Gefühl sorgen kann, denn sie ermöglicht nur dann Zutritt, wenn es vom Eigentürmer gewollt ist. Wohnungsinhaber können durch einen kleinen Dreh des Schlüssels dritten Personen einfach, schnell und sicher zeitlich begrenzt Zutritt gewähren. Dazu zieht der Inhaber einfach seinen Schlüssel in der Service-Position „8-Uhr" ab. Dann können Personen mit Service-Schlüssel, wie Handwerker, Reinigungskräfte oder Hundesitter, die Tür öffnen. Nach getaner Arbeit schließt die Servicekraft die Tür wieder von außen sicher zu.

Evva: Hybrid-Zylinder

Mechatronischer Schließzylinder

Der Hybrid-Zylinder von Evva kombiniert Mechanik und Elektronik. Kombiniert werden können die elektronischen AirKey- und Xesar-Zylinder mit allen aktuellen modularen mechanischen Evva-Systemen. Ob besser innen oder außen elektronisch oder mechanisch gesichert wird, entscheidet der individuelle Bedarfsfall. Der Hybrid-Zylinder bietet eine Vielzahl an neuen Lösungsvarianten. Der AirKey Hybrid-Zylinder kann eine smarte Ergänzung für alle sein, die der Mechanik treu bleiben, aber die Vorteile der Elektronik nutzen möchten. Der Hybrid-Zylinder, beispielsweise in einer Eingangstür des Privathauses, ist - im Gegensatz zu einem Knauf auf der Innenseite der Eingangstür - von außen nicht manipulierbar. Auf der Außenseite der Eingangstür bietet wiederum der elektronische Zylinder alle Vorzüge einer elektronischen Zutrittssteuerung.

Marshalls: Landscape Protection

Barrikaden für öffentliche Bereiche

Die Schutzbarrikaden von Marshall eröffnen neue Möglichkeiten für Stadtplanner, um Fahrzeugangriffe in öffentlichen Bereichen zu verhindern. Die Produkte folgen den Richtlinien PAS 68/69 und IWA 14.1/14.2 (Publicly Available Specification) – sprich den aktuellen Vorschriften für „Barrikaden, die zur Minderung der Auswirkungen einer Fahrzeugterrorattacke eingesetzt werden". Die Barrikaden von Marshall sind entwickelt worden, um einerseits Fahrzeuge zu stoppen – andererseits bringen sie eine gewisse Ästhetik und Funktionalität mit und können gut in die Umgebung eingegliedert werden. Das Wichtigste jedoch: ein 7-5 Tonnen-LKW mit einer Höchstgeschwindigkeit von 80 km/h kann immer noch gestoppt werden.

Magnetic Autocontrol: mTripod

Dreiarmsperre

Für den neuen mTripod wurde alles bisher Dagewesene auf den Prüfstand gestellt. Mit neuem Material, italienischen Design, neuartiger Beleuchtung, komfortabler Handhabung bei Bedienung und Aufbau sowie zahlreiche Sicherheitseinrichtungen wie Drop-Arm-Funktion, Aufschlagserkennung sowie Übersteig- und Unterkriecherkennung setzt die neue Sperre nicht nur optisch, sondern auch technisch Standards. Viele Funktionen wie eine umfangreiche Ergebnisprotokollierung, ein Impulszähler und ein Zufallsgenerator gehören bereits zur Basisfunktionalität der Steuerung. Die Zutrittskontrolle hat sich durch mTripod vom Funktionselement zum Designobjekt gewandelt.

Nedap: MACE Smart

Lesegerät für sichere Mobile Zutrittskontrolle

Mace Smart nennt sich die jüngste Ergänzung von Nedaps Mace Plattform – der Plattform, die Zugangssysteme ermöglicht, um Smartphones für eine sichere und leistungsfähigere Zutrittskontrolle zu nutzen. Somit können Mace-Kunden ihr Smartphone (iOS & Android) als virtuellen Ausweis verwenden, um Türen und Schranken zu öffnen. Das Mace Smart Lesegerät bietet Personen Zutritt zu Gebäuden, Parkhäusern und Veranstaltungen mit deren Smartphone. Dieses kleine Lesegerät unterstützt gleichzeitig mobile Technologien wie NFC und BLE und traditionelle RFID Smartcard Technologien. Mace Smart bietet viele Standard Kommunikationsschnittstellen, wie Wiegand, Clock & Data und OSDP. Diese erlauben einen einfachen und reibungslosen Einsatz mit bestehenden sowie auch neuen Zugangssystemen.

Optex: Redscan RLS-2020S

Laser-Sensor für Innen und Außen

Der RLS-2020S ist ein kompakter Laser-Sensor für Innen und Außen, der eine anpassbare, ‚virtuelle' Wand oder Decke mit einem Detektionsbereich von bis zu 20m x 20m zur Verfügung stellt, um die Anwesenheit von Personen oder Objekten zu erkennen. Er nutzt die 2D-Lidar-Technologie und detektiert Größe, Geschwindigkeit und Entfernung von Objekten und misst deren genaue X- und Y-Koordinaten. Er ist PoE-konform und wurde entwickelt für Sicherheitsanwendungen wie Einbruchschutz, Erkennung eingeworfener Gegenstände, Decken- und Dach-Absicherung sowie Objektschutz. Er ist in alle wichtigen Video-Managementsysteme und PSIM-Plattformen integriert und verbessert die Zuverlässigkeit videobasierter Sicherheitssysteme.

Paxton: Net2 Entry Premium Monitor

Türsprechmonitor

Der Premium-Türsprechmonitor ist eine Erweiterung des Net2 Entry Programms von Paxton Sprechanlagen. Dieser Monitor kommt mit einem hochwertigen kapazitiven Glas-Touchscreen, 25 schick designten Motiven, die ihm Charakter und dazu noch hochwertige Audio- und Bildqualität verleihen. Kompatibel mit Paxtons vernetzten Net2 Zutrittskontrollsystem ist der Türsprechmonitor durch sein intelligentes, schlankes Design an verschiedene Umgebungen anpassbar. Er verfügt über zahlreiche neue Funktionen, darunter eine Concierge/ Pförtner-Funktion, welche einfache Besucher- und Standortverwaltung ermöglicht. Bewohner, die beschäftigt oder abwesend sind, können ihren Monitor zum Empfang umleiten. Wird ein Besucher verpasst, so erstellt die erweiterte Anrufverwaltung einen Video-Schnappschuss sowie ein Ereignisprotokoll.

Stid: Mobile ID

Mobile Zugangskontrolle per Smartphone

Stid Mobile ID wurde mit RFID- und Bluetooth-Technologien entwickelt und ermöglicht Zugangsausweise auf Smartphones. Die Lösung ist so ergonomisch, dass die Identifikation für den Anwender instinktiv wird. Sie bietet nutzerfreundliche Methoden, die auf die Anwendung zugeschnitten werden können – bei Annäherung, ohne manuelle Eingabe, Fernbedienung, Touchscreen. Man kann Türen öffnen, auch wenn sich das Gerät im Standby-Modus in der Tasche befindet - oder auch beim Telefonieren. Mit den Offline- und Online-Tools lassen sich Daten im Unternehmen speichern, indem lokal oder remote eine virtuelle Karte für Benutzer mit Android-Handys oder iPhone erstellt werden.

Senstar: LM100

Detektion und Beleuchtung für den Perimeterschutz

Die integrierte Lösung für Detektion und Beleuchtung im Perimeter: Als integrierte Lösung für Detektion und Beleuchtung kombiniert das Senstar LM100 System Beschleunigungssensoren mit einer Hochleistungs- LED-Beleuchtung und ermöglicht dabei die Erkennung von Manipulation am Zaun mit einem effizienten Abschreckungseffekt durch sofortige Ausleuchtung. Bei der Entwicklung wurde großen Wert auf Nachhaltigkeit gelegt, da die Beleuchtung nur bei einem Ereignis aktiviert wird und somit gegenüber einer permanenten Ausleuchtung 95% weniger Energie und Lichtverschmutzung bedeutet. Das System ist für fast alle Zaun- und Mauertypen, durch drahtlose Kommunikation äußerst flexibel einsetzbar und dies bei geringsten Installations- und Unterhaltskosten. Es handelt sich um ein neuartiges und innovatives Konzept durch die Kombination Sensor und Licht.

Süd-Metall: ÜLock-B Cable

Sicherheitsschloss mit dünnem zweiadrigem Kabel

Das verkabelte Sicherheitsschloss ÜLock-B Cable von Süd-Metall kombiniert mit einem 2-Ader Kabel und dem I/O Modul EWS Eco (Maß 12,5x12,5cm) Komfort und Sicherheit für jede Türe. Die Innovation besteht in der Vereinfachung des Produktes: Einerseits kann eine Verdrahtung aufgrund des dünnen, zweiadrigen Kabels sehr einfach und schnell erfolgen. Ähnliche am Markt verfügbare Produkte benötigen in der Regel einen 14-adrigen Anschluss. Somit wird der Einbau durch unser Produkt deutlich vereinfacht und die Einbauzeit erheblich verkürzt. Zudem ist eine „Verpolungssicherheit" gegeben, welche Irrtürmern beim Anschluss an das I/O Modul effizient vorbeugt und somit die Fehlernanfälligkeit gegen Null schreiten lässt. Erwähnenswert ist außerdem die deutliche Zeitersparnis, da lediglich zwei Adern an das I/O Modul angeschlossen werden müssen. Eine weitere Besonderheit ist die lange mögliche Distanz zwischen ÜLock und I/O Modul (20 Meter) – somit ist das I/O Modul flexibel montierbar.

Vanderbilt: SPC Connect

Fernüberwachung, Verwaltung und Instandhaltung von Zentralen

SPC Connect ist eine cloudbasierte Lösung, die speziell für Errichter zur Fernüberwachung, Verwaltung und Instandhaltung von SPC-Zentralen über das Internet konzipiert wurde. Die Kommunikation zwischen der SPC-Zentrale und SPC Connect erfolgt über FlexC. Hierbei handelt es sich um ein leistungsstarkes Protokoll, das verschiedene Kommunikationsmethoden, wie Ethernet, GRPS und 3G, unterstützt. So wird sichergestellt, dass die Systemverbindung stets erhalten bleibt. Dank umfassender Optimierungen der Benutzerverwaltung können Benutzer in SPC Connect nun schneller hinzugefügt und konfiguriert werden. Bedeutet, dass der Systemadministrator Benutzern sich umgehend Zugriff auf ein SPC-System verschaffen - und so Zeit und Geld für alle Beteiligten sparen kann. Mit den Push-Benachrichtigungen für iOS-Geräte wird sichergestellt, dass die Benutzer von SPC Connect über neue Ereignisse in ihrem SPC-System benachrichtigt werden – selbst dann, wenn die App nicht geöffnet ist.

Kategorie E

Sicherheitsmanagement, Lösungen und Dienstleistungen

Avigilon Corporation: Unusual Motion Detection (UMD)

Auf KI basierte Management-Lösung

Die Unusual Motion Detection (UMD)-Technologie von Avigilon ist eine fortschrittliche, auf künstlicher Intelligenz (KI) basierende Technologie, die der Überwachung ein völlig neues Maß an Automatisierung verleiht, indem Ereignisse aufgedeckt werden, die andernfalls unentdeckt bleiben würden. Die UMD-Technologie ist ohne vordefinierte Regeln oder Einrichtung in der Lage, zu erfassen, wie typische Aktivitäten in einer Szene aussehen und dann ungewöhnliche Bewegungen zu erkennen und zu melden. UMD-Technologie ermöglicht Betreibern große Mengen des aufgezeichneten Videos schneller durchsuchen, indem Sie automatisch ihre Aufmerksamkeit auf atypische Ereignisse. UMD unterstützt Benutzer durch den Einsatz von KI beim Extrahieren wertvoller Informationen aus ihren Videodaten, um unerwartete Ereignisse schnell zu finden, überprüfen und entsprechende Maßnahmen zu ergreifen.

Bosch Sicherheitssysteme: In-Store Analytics

Videoanalyse-Software für Retail

In-Store Analytics ist eine Software-as-a-service Lösung. Sie ermöglicht es den Zentralen großer Einzelhändler Kundenverhaltensdaten aus den Filialen zu sammeln, um zu verstehen, wie sich die Kunden in den Filialen bewegen und wo Interaktionen stattfinden. So können die Einzelhändler den Kundenservice und betriebliche Prozesse gezielt verbessern. Unter Verwendung von IP Panoramakameras, die mit ihrem 360 Grad Sichtfeld die Verkaufsfläche gut überblicken, werden mit Hilfe der eingebauten intelligenten Videoanalyse-Software anonyme Positionsdaten der Kundenbewegungen im Laden erstellt und in die Cloud übertragen. Dort werden die Daten analysiert und dem Einzelhändler in Form von Kennzahlen und Grafiken über Weboberflächen zur Verfügung gestellt. In-Store Analytics zeichnet sich durch eine Datengenauigkeit von mindestens 95 Prozent sowie die Anonymität der Positionsdaten aus, welche den Schutz der Privatsphäre der Kunden sicherstellt. Darüber hinaus lässt sich die Lösung mühelos skalieren und ist somit auch für die größten Einzelhandelsgeschäfte mit einer hohen Anzahl von Kameras und großen Multi-Store-Ketten geeignet.

Bosch Building Technologies: Praesensa

IP-basiertes Beschallungs- und Sprachalarmierungssystem

Praesensa ist ein Beschallungs- und Sprachalarmierungssystem für mittlere und große Anwendungsbereiche. Aufgrund der IP-Fähigkeit kann das System sowohl zentral als auch dezentral aufgebaut werden. Es ist dabei durch Netzwerk-Redundanz und Rückfallebenen absolut ausfallsicher. Die intelligente Leistungszuweisung der Lautsprecherlinien auf die Mehrkanal-Verstärker macht das System höchst effizient. Die Bedienoberfläche der Sprechstelle mit übersichtlicher Menüführung und Statusrückmeldungen erlauben eine intuitive Bedienung.

Praesensa erfüllt höchste Standards für Sprachalarmanlagen und es bietet für jede Zone eine umfassende Audiosignalverarbeitung. Darum eignet es sich für den kommerziellen Betrieb sowie für Evakuierungsdurchsagen. Die Omneo-IP-Architektur von Bosch unterstützt Dante-Audio-Netzwerke und die AES67- und AES70-Protokolle. Das ausfallsichere Betriebskonzept benötigt nur wenige Geräte, um sämtliche Benutzer-Systemanforderungen zu erfüllen

Deister Electronic: bloxx

Intelligente Objektverwaltung

Equipment und Wertgegenstände sicher zu verwalten, ist mit viel Aufwand und Kosten verbunden. Das vollautomatische und modular konzipierte Objektverwaltungssystem bloxx von der Deister ermöglicht es Wertgegenstände, Equipment und Geräte verlässlich aufzubewahren und zu verwalten. Verschiedene Gehäuse und Modulblöcke mit unterschiedlichen Fachgrößen können miteinander kombiniert werden, wodurch beliebiges Equipment in demselben System verwaltet werden kann. Die intelligente Software des Systems weiß zu jeder Zeit, welches Equipment durch wen im Einsatz ist und garantiert so mehr Transparenz und Aufschluss hinsichtlich des tatsächlichen Bedarfs an Equipment. Das gewährleistet mehr Sicherheit und Effektivität am Arbeitsplatz.

HID: Location Services for Item Management

Überwachungslösung von Orten und Objekten

HID Location Services for Item Management ermöglichen eine Überwachung von Ort und Bewegung von Objekten. Zudem bieten die HID Condition Monitoring Services eine Echtzeitanalyse von Gerätezustand und -performance. Darüber hinaus unterstützen die Lösungen bei der Prognostizierung von Fehlern und Ausfällen bei Motoren, Generatoren und anderen Maschinen. Eine leistungsstarke Policy-Engine bietet eine schnelle Identifizierung potenzieller Risiken und Alarmierung, so dass Unternehmen Ausfallzeiten reduzieren können. Die neuen Services basieren auf einer Standard-Plattform von Bluvision, die eine nahtlose Bereitstellung ohne hohe Kosten ermöglicht. Für präzise Echtzeit-Location-Services wird Bluetooth Low Energy (BLE) genutzt. Unternehmen haben mit den Condition Monitoring Services zudem die Möglichkeit, sofort auf Gerätefehler zu reagieren beziehungsweise diese durch prädiktive Analyseverfahren vorab zu prognostizieren. Dadurch können Gerätebetreiber beispielsweise Wartungsmaßnahmen auf Basis von Algorithmen und Datenanalysen proaktiv planen, anstatt auf einen Fehler zu einer möglicherweise ungünstigen Zeit reagieren zu müssen.

Kentix: MultiSensor-LAN

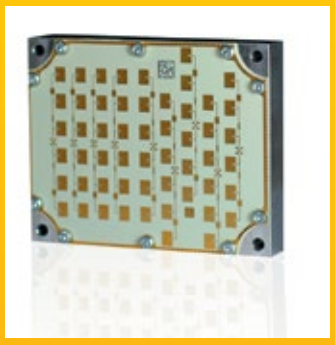
Lösung zur Serverraum-Überwachung

Der MultiSensor-LAN ist eine sehr einfache und doch umfassende Lösung zur Serverraum-Überwachung. Er überwacht IT-Infrastrukturen auf 19 physikalische Gefahren wie kritische Klimafaktoren, Brand oder Einbruch mit nur einem Gerät. Das legt den Grundstein zur Absicherung nach BSI Grundschutz und der ISO 27001. Durch den integrierten Webserver werden alle nötigen Einstellungen über den Web-Browser direkt auf dem Gerät vorgenommen. Alarme werden unmittelbar per E-Mail mit allen wichtigen Informationen gemeldet. Der MultiSensor bietet zudem eine SNMP-Schnittstelle zur Integration in die gängigen Network Monitoring Systeme. Der Kentix MultiSensor-LAN integriert 8 Sensoren. Es wird keine externe Software benötigt, was Kosten und Aufwand spart. Dank des dezentralen Technikansatzes wird die Ausfallsicherheit erhöht und eine sehr hohe Skalierbarkeit von kleinen bis hin zu großen Systemen ermöglicht. IP-Videokameras lassen sich bei Bedarf ebenfalls nahtlos integrieren. So entsteht kein Systembruch und der Systemadministrator erhält immer zuverlässig alarmsynchrone Daten. Lizenzkosten fallen keine an.

InnoSenT: iSYS-5010

Radarsystem zur Sicherheitsüberwachung

Das Radarsystem iSYS-5010 optimiert die Videoüberwachung von Außenanlagen. Das Produkt wurde speziell für die Integration in ein Kamerasystem entwickelt. Diese Kombination gleicht die Problematik der Videotechnik im Hinblick ungünstiger Lichtverhältnisse oder Wetterbedingung aus. Durch die Ergänzung der Radartechnik werden Fehlalarme reduziert sowie die Effizienz und Zuverlässigkeit des Sicherheitssystems gesteigert. Außerdem bietet die Nutzung der Radartechnologie anonyme Informationen über Entfernung, Bewegung, Winkel, Präsenz, Richtung oder Geschwindigkeit eines erfassten Objekts. Des Weiteren ermöglicht das Radarsystem eine Definierung von Gefahrenzonen und das Filtern relevanter Detektionen.



Raytec: VARIO2 IP Hybrid

Hybrid Netzwerk Scheinwerfer

Vario2 IP Hybrid ist ein IP-fähiger Hybrid-Netzwerk-scheinwerfer und stellt die neueste Raytec-Technologie auf einer einzigen Plattform dar. Er kombiniert 4 wichtige Komponenten, nämlich Infrarot-, Weißlicht-, PoE- und IP-Anbindungen in einem einzigen netzwerkfähigen Scheinwerfer. Mit den Platinum Elite Twin-Core SMT LEDs, die im Vergleich zur vorherigen Generation um 200 Prozent leistungsfähiger sind, vereint Vario2 IP Hybrid die gesamte Leistungsfähigkeit von zwei vollwertigen Strahlern (eine Infrarot- und eine Weißlichtquelle) in einer wesentlich kleineren Hybridplattform. Mit vollständiger IP-Adressierbarkeit ermöglicht es die sofortige Kontrolle, auf Live-Ereignisse zu reagieren, Ferneinstellungen vorzunehmen und die vollständige Integration mit Geräten von Drittanbietern, um so auf Ereignisse automatisch zu reagieren.

Seagate: SkyHawk AI

Festplatte für KI-Videoüberwachungslösungen

Die SkyHawk AI ist eine speziell für die Anwendungen im Bereich künstlicher Intelligenz (KI) entwickelte Videoüberwachungslösung. Die Festplatte fußt auf der zehnjährigen Erfahrung von Seagate in der Bereitstellung von videoüberwachungsoptimierten Speicherlösungen und bietet eine zuvor unerreichte Bandbreite sowie Rechenleistung für die Verwaltung von kontinuierlichen datenintensiven Workloads. Die SkyHawk AI eignet sich ideal für rechenintensive Workloads von KI-Workflows. Der hohe Durchsatz und das verbesserte Caching sorgen für niedrige Latenzzeiten und eine hervorragende Random-Read-Performance, um Bilder schnell zu lokalisieren und Videomaterial für die Analyse bereitzustellen. Dies eliminiert die Latenzzeit bei Austausch und Verarbeitung Cloud-basierter Daten. Mit der enthaltenen ImagePerfect KI-Firmware lassen sich qualitativ hochwertiges, scharfes Videomaterial mit hoher Framezahl zuverlässig erfassen und gleichzeitig KI-fähige NVR-Analysen vereinfachen. Dadurch wird sichergestellt, dass die durch Aufnahmen gewonnenen Informationen nicht verloren gehen

Panasonic: WV-ASF950

Gesichtserkennung

WV-ASF950 bietet erstklassige Gesichtserkennungs-Performance. Ein maschineller, selbst-lernender Algorithmus wird implementiert, um eine hohe Genauigkeit bei der Gesichtserkennung zu realisieren. Von Panasonic-Kameras werden Gesichtsdaten als Metadaten an den Face-Server gesendet, was weniger Serverspeicher als das Senden des reinen Streams erfordert. Mit der neuen Deep-Learning Funktion ist die Genauigkeit der Gesichtserkennung für Personen, die eine Sonnenbrille tragen oder nach unten sowie zur Seite schauen, stark verbessert (links / rechts ± 45 °, hoch / runter ± 30 ° abgewandte Gesichter). Dies wird durch die Kombination mehrerer Deep-Learning-Technologien realisiert. WV-ASF950 hilft auch, Gesichter von Personen zu erkennen, wenn sie jung sind (z.B. in Pässen). Mit der Intelligent Auto (iA) -Technologie können die besten Gesichtsbilder automatisch erfasst und an die Server gesendet werden. Die Daten selbst und die Kommunikation zwischen Kamera, Server und Client werden verschlüsselt, um die Privatsphäre zu schützen, sodass die DSGVO eingehalten werden kann.

UTC Fire & Security: UltraSync

Smart Home App

UltraSync ist eine internetbasierte Lösung zur interaktiven Steuerung eines ZeroWire oder Advisor Advanced SmartHome- und Sicherheitssystems. Mittels UltraSync App auf dem Smartphone oder Tablet und einer sicheren UltraSync Internet Verbindung wird das System aus der Ferne von überall und jederzeit gesteuert. Das Ergebnis ist ein sicheres System-Management mit nur einer intuitiven Smartphone App. Intuitive Funktionen für den Endanwender: Scharf-/Unscharfschaltung des Systems, Empfang von Alarm-/Ereignismeldungen, Geo-Fensing basierte Aktionen, Vergabe von Zugriffsberechtigungen, Steuerung von Z-Wave Komponenten für Licht und Klimatisierung, Ansicht von Live-Video und Aufzeichnung, Erstellung und Aktivierung von automatisierten Abläufen. Wird ein sicherheitsrelevantes Ereignis detektiert, kann UltraSync eine Reihe von Maßnahmen starten, die eine schnelle Intervention ermöglichen: Alarmmeldung an Notrufzentrale senden, Ereignis basierende Videoaufzeichnung starten, Push-Benachrichtigung auf Smartphone senden.

Kategorie F

Sonderkategorie Smart Home

Hekatron: Genius Port

Smarter Brandschutz

Mit dem Genius Port und der kostenfreien Genius Control App lassen sich Alarm, Status- und Störungsmeldungen aus allen bestehenden Genius Funksystemen auf mobilen Endgeräten empfangen – jederzeit und weltweit. So können Sie im Ernstfall auch aus der Ferne schnell reagieren, die Feuerwehr alarmieren, Melder die keinen Rauch detektiert haben stumm schalten und Leben und Sachwerte schützen. Weiter lassen sich Genius Funksysteme mit dem Genius Port in Smart-Home-Systeme von Digitalstrom (ab Juni 2018) und demnächst auch Smartfrog integrieren. Weitere Kooperationspartner folgen in den kommenden Monaten.

Johnson Controls: iotega

Drahtloses Sicherheits- und Automationssystem:

Diese innovative drahtlose Sicherheits- und Automationslösung soll Eigenheime und Kleinunternehmen intelligenter und sicherer machen. In das komplett verschlüsselte iotega-System ist die PowerG-Funktechnologie bereits integriert. Die elegante iotega-Zentrale verfügt über ein unauffälliges Touch-Bedienfeld, einen optionalen 7"-Touchscreen (WLAN-fähig) sowie ein Funkbedienteil zum Scharfschalten und ist mit diversen Apps kompatibel.

Ksenia Security: auxi-H

Security und Heimautomations-Modul

auxi-H ist ein Modul, das nicht nur für reine Sicherheits-, sondern auch für Heimautomationsanwendungen entwickelt wurde. Über einen speziellen Jumper an Bord können zwei Betriebsmodi eingestellt werden: einer für die komplette Steuerung von motorisierten Rollläden (mit zwei verriegelten Relaisausgängen), der andere für die Lichtsteuerung (frei konfigurierbare Ausgänge). Aus den in lares 4.0 konfigurierten Szenarien können sowohl die Rollläden geöffnet als auch geschlossen und in vier verschiedenen Öffnungsstellungen eingestellt werden. Es ist möglich, die lokalen Switches als klassischen Totmannschalter zu verwalten und das komplette Öffnen und Schließen mit einem einfachen Doppelklick zu verwalten.

Lupus: XT3

Professionelle Smarthome Alarmanlage

Die Lupus XT3 ist ein System für Gebäudesicherheit, Videoüberwachung und Smarthome-Steuerung. Ohne bauliche Veränderungen schützt sie effizient gegen Einbruch, Überfall, Feuer, Wasser, Gas und medizinische Notfälle. Sie kann die Steuerung von Heizung, Leuchten, Rollläden und Elektrogeräte übernehmen und schafft Transparenz, per Live-Video-Verbindung zu fest installierten Kameras. Sie verwaltet bis zu 160 Sensoren. Mit über 70 smarten Komponenten bietet Lupus ein großes Sortiment aus einer Hand. Die Alarmanlage ist nach dem europäischen Qualitätsstandard EN50131 Grad 2 zertifiziert, KfW-förderfähig und Teil des Notfallmanagements der Provinzial-Versicherung.

Telenot: FBT 250

Funk-Bedienteil

Smart Home – auch auf einzelne Komponenten kann es ankommen. Das Funk-Bedienteil FBT 250 ist eine Komponente des Telenot Funk-Alarmsystem DSS2. Die kapazitative Touch-Oberfläche und das OLED-Display mit integrierter Tastatur ermöglichen eine komfortable und gezielte Bedienung aller Sicherungsbereiche per Funk. Umfangreiche Schaltfunktionen des FBT 250 ermöglichen zudem die Steuerung von Komponenten der Gebäudeautomatisierungstechnik – sowie Smart-Home-Funktionen. Ein RFID-Leser mit verschlüsselter Übertragung und ein Signalgeber mit flexibler Nutzung, z.B. für Internalarm, sind ebenfalls integriert. Durch den Batteriebetrieb ist eine flexible Montage des Funk-Bedienteil FBT 250 am gewünschten Ort möglich. Der Meldungsspeicher der Einbruchmelderzentrale kann jederzeit angezeigt werden.

Panasonic: 1 by multi VIC

Video-Intercom System

Das Video-Intercom System von Panasonic wurde für kleine und mittlere Wohnungen entwickelt und bietet eine Verkabelungstopologie für Neubauten und Ersatzprojekte. Das System bietet volle Sicherheit durch das Weitwinkelobjektiv (horizontal 170 ° und vertikal 110 °), welches unbefugten Zugriff durch Erweiterung des Sichtfelds verhindert. Das flexible System ist erweiterbar von zwei auf 32 Räume mit verschiedenen Monitoren. Darüber hinaus verfügt das VIC über die beiden Hauptverdrahtungsmethoden, Bus- und Sternverdrahtung. Die „Lobby Station" steht zudem für elegante Schlichtheit und Benutzerfreundlichkeit mit zeitlosem Design. Das System will daneben punkten mit einfacher Installation und Wartung.

UTC Fire Security: ZeroWire

Smart Home Sicherheitssystem

ZeroWire ist ein funkbasiertes Sicherheits- und Hausautomationssystem mit integriertem Z-Wave Gateway und WiFi, das nach der Sicherheitsklassifizierung EN 50131 Grade 2 zertifiziert ist. Mit 64 Meldegruppen für Sensoren und Kontakte stehen ausreichend Überwachungspunkte zur Verfügung, um Wohnung, Praxis oder kleinere Gewerbeeinheiten, ganz gleich welcher Bauart, außen und innen zu überwachen. Mittels der „UltraSync" App kann das Smart Home Security System programmiert, konfiguriert und kontrolliert werden sowie per Push-Nachricht, E-Mail und SMS mit ihm kommuniziert werden. Und Dank integrierter IP-Kameras können Live-Videos und Aufzeichnungen, ausgelöst durch Alarme oder Ereignisse, angezeigt und bei Bedarf erneut abgespielt werden.

THE NEXT GENERATION OF SECURITY

Wir schaffen Mehrwert für unsere Kunden indem wir als zuverlässiger Berater Menschen, Wissen und Technologie so miteinander kombinieren, dass wir wirksame Sicherheitslösungen liefern.

Somit tragen wir aktiv zu einer sicheren Gesellschaft bei und gestalten die globale Sicherheit von morgen mit: Schutz von Privatem, Wirtschaft und Öffentlichkeit.

Tel. 0800-22 000 23
securitas.de

SECURITAS

Dirk Jacobs, Prokurist und Sicherheitschef bei Freudenberg Service

KONZERNSICHERHEIT

Service im Park

Sicherheitsdienstleistungen für den Industriepark Weinheim

Freudenberg ist ein globales Technologieunternehmen. Gemeinsam mit Partnern, Kunden und der Wissenschaft entwickelt die Unternehmensgruppe Lösungen und Services für mehr als 30 Marktsegmente und für Tausende von Anwendungen: Dichtungen, schwingungstechnische Komponenten, Vliesstoffe, Filter, Spezialchemie, medizintechnische Produkte, IT-Dienstleistungen und modernste Reinigungsprodukte. Der Geschäftsbereich Freudenberg Service betreibt die Industrieparks in Weinheim, Neuenburg und Laudenbach. Unser wissenschaftlicher Schriftleiter Heiner Jerofsky sprach mit Dirk Jacobs, Prokurist und Sicherheitschef bei Freudenberg Service, über Aufgaben, Sicherheitsplanung und Notfallmanagement.

> „Unser Dienstleistungsportfolio umfasst mehr als 140 Leistungen, …“

GIT SICHERHEIT: Herr Jacobs, Sie sind mit Ihrer Firma Dienstleister in Sachen Sicherheit. Können Sie unseren Lesern Ihre Hauptaufgaben umreißen?

Dirk Jacobs: Auf den ersten Blick hört sich das exotisch an, und tatsächlich, das ist es auch. Als Industrieparkbetreiber für die Industrieparks in Weinheim, Neuenburg und Laudenbach ist die Freudenberg Service KG Dienstleister für über 60 Unternehmen, die sich an diesen Standorten mit Verwaltung, Forschung und/oder Produktion niedergelassen haben. Das umfangreiche Leistungsspektrum beinhaltet unter anderem den Betrieb eines eigenen Kraft-Wärme-Kälte-Kraftwerkes, die Verpflegungsbetriebe, das Bildungszentrum von Freudenberg, Informations- und Kommunikationstechnik, den Arbeitsmedizinischen Dienst, die Betreuung der Freudenberg Liegenschaften außerhalb des Industrieparks sowie die Sicherheitsorganisation, die wir Werk-/Brandschutz nennen. Mehr als die Hälfte der Mieter im Industriepark Weinheim sind Unternehmen, die nicht zur Freudenberg Gruppe gehören. Das Thema Sicherheit ist für alle Mieter am Standort eine Mandatsleistung, das bedeutet, dass mit Unterschrift unter den Mietvertrag alle Kunden die Regulierungen am Standort akzeptieren und den definierten Sicherheitsstandard

in Form von sogenannten Basisleistungen von der Geschäftseinheit Werk-/Brandschutz abrufen. Aufgrund der Kundenstruktur ist diese Einheit zugelassenes Sicherheitsunternehmen nach §34 GewO, also im Prinzip ein klassischer Sicherheitsdienstleister. Unser Dienstleistungsportfolio umfasst mehr als 140 Leistungen, die wir nach Basis- und Zusatzleistungen unterscheiden. Grob gesagt gehören zu den Basisleistungen alle Sicherheitsdienstleistungen, die unsere Kunden am Standort gleichermaßen in Anspruch nehmen, wie z.B. die Werkschutzleistungen am Empfang und an den Toren, die operative Gefahrenabwehr, den Betrieb eines Zutrittskontrollsystems, die eigene Ausweisstelle, die Parkplatzverwaltung sowie die Besetzung einer ständig besetzten Notruf- und Serviceleitstelle. Zusatzleistungen können von unseren Kunden individuell abgerufen werden. Hierzu gehören unter anderem die Stellung von Brandschutzbeauftragten, Durchführung von Schulungen, Planung und Erstellung von Sicherheitskonzepten im Rahmen von Neubauten oder Nutzungsänderungen inklusive der Begleitung der Genehmigungsverfahren, das Veranstaltungsmanagement und vieles mehr.

> „Alle neuen Mitarbeiter durchlaufen eine umfassende Ausbildung, …“

ganze Jahr im 24/7-Betrieb verfügbar. Hier übernehmen die Mitarbeiter die Aufgaben des Werkschutzes innerhalb des Werkszaunes und stellen die gesetzlichen Aufgaben der anerkannten Werkfeuerwehr sicher. Die Werkschutzaufgaben an den Werkszufahrten und Empfängen übernehmen Mitarbeiter von einem Partnerunternehmen. Für die Gefahrenabwehr im Industriepark Neuenburg ist eine anerkannte Werkfeuerwehr zuständig, die Werkschutzaufgaben werden dort von unserem Partnerunternehmen übernommen.

Wieviel eigenes oder fremdes Personal steht Ihnen dafür zur Verfügung und welche Qualifikationen verlangen Sie bei Feuerwehr und Werkschutz? Gibt es interne Aus- und Fortbildung?

Einsatzübung mit dem Sonderlöschfahrzeug

Wie hat sich Ihre Sicherheitsorganisation aufgestellt, um dieses Leistungsspektrum umsetzen zu können?

Dirk Jacobs: Organisatorisch führen wir in der Geschäftseinheit Werk-/Brandschutz fünf Bereiche, die zum Teil als Cost Center, zum Teil als Profit Center operieren. Als Cost Center führen wir die Bereiche Werkschutz, Werkfeuerwehr und Fahrbereitschaft, während die Planungs- und Technikteams als Profit Center fungieren. Das Team der operativen Gefahrenabwehr im Industriepark Weinheim ist als Matrixorganisation aufgebaut und das

Dirk Jacobs: Für die Kernaufgaben sind in der Geschäftseinheit Werk-/Brandschutz 61 eigene Mitarbeiter sowie im Rahmen von Werkverträgen 20 externe Mitarbeiter tätig. Hinzu kommen rund 90 Mitarbeiter der nebenberuflichen Werkfeuerwehr, also Kolleginnen und Kollegen, die bei unseren Kunden beschäftigt sind und im Rahmen der Gefahrenabwehr zu feuerwehrtechnischen Einsätzen angefordert werden können. Je nach Aufgabenstellung verlangen wir entsprechende Qualifikationen. In den Leitungsfunktionen setzen wir eine akademische Ausbildung sowie die Laufbahnprü-

Bitte umblättern ▶

Lkw-Abwicklung im neuen Tor 3

Dirk Jacobs in einem Planungsgespräch

fung für den höheren oder gehobenen feuerwehrtechnischen Dienst in Verbindung mit der Ausbildung Security Manager voraus. In den Bereichen Sicherheitsplanung und Gefahrenmeldetechnik/Zutrittskontrollsystem erstreckt sich das Spektrum vom Ingenieur der Elektrotechnik über den Techniker bis hin zur CAD – Spezialistin. Für einen Arbeitsplatz im Team der Gefahrenabwehr muss ein Bewerber eine abgeschlossene Berufsausbildung und im Idealfall die Laufbahnprüfung für den mittleren feuerwehrtechnischen Dienst sowie den Lkw – Führerschein mitbringen. In diesem Team findet man die klassischen Einstiegsberufe für Berufsfeuerwehren wie Kfz-Mechaniker, Zimmerleute und Elektroniker, aber auch den Maschinenbauingenieur, den Vertriebsspezialisten, den IT-Spezialisten oder die Hotelfachfrau. Alle neuen Mitarbeiter durchlaufen eine umfassende Ausbildung, die je nach Umfang der Vorausbildung bis zu drei Jahre in Anspruch nehmen kann. Am Ende der Basisqualifizierung haben die Mitarbeiter ihren ursprünglichen Berufsabschluss, eine absolvierte Laufbahnprüfung für den mittleren feuerwehrtechnischen Dienst, eine IHK-Prüfung als Geprüfte Fachkraft für Schutz und Sicherheit, die Rettungssanitäter Ausbildung sowie eine Spezialisierung auf mindestens einem Fachgebiet als Sachkundiger erworben. Während der Ausbildung muss sich jeder Mitarbeiter zudem sehr fundierte Orts- und Prozesskenntnisse aneignen, was aufgrund der dynamischen Veränderungen im Industriepark ein nie endender Lernprozess ist. Die kontinuierliche Weiterbildung wird in Form von sogenannten Qualifizierungsschichten durchgeführt. Einmal monatlich durchläuft jede der vier Schichtgruppen ein auf sechs Stunden ausgelegtes Trainingsmodul aus dem Bereich Gefahrenabwehr. Zusätzlich gibt es in jeder Nachtschicht noch ein Zeitfenster für die Wachausbildung. Die nebenberuflichen Werkfeuerwehrangehörigen werden über das gesamte Spektrum der Ausbildung für Freiwillige Feuerwehren ausgebildet. Im Rahmen der gesetzlichen Forderungen finden hier regelmäßig Unterrichte und Übungsdienste statt, die von den hauptamtlichen Kollegen organisiert und durchgeführt werden. Das Personal unseres Partnerunternehmens besteht überwiegend aus geprüften IHK Werkschutzfachkräften, bzw. IHK Geprüften Sicherheits- und Schutzkräften.

Der Objektschutz ist für Ihre Kunden von großer Bedeutung. Wie und mit welchen Sicherheitstechniken schützen Sie die Menschen, Anlagen und Gebäude Ihrer Kunden? Wie würden Sie Ihr Sicherheitskonzept beschreiben?

Dirk Jacobs: Im Prinzip unterscheiden wir im Industriepark zwei Sicherheitsbereiche, den äußeren und den inneren. Der äußere Sicherheitsbereich ist in drei Zonen unterteilt, der Werksumfahrung, dem Werkszaun mit seinen Toren und automatisierten Zugängen sowie der Zone zwischen Zaun und dem von den einzelnen Mietern gemieteten Bereich, der aus Außenflächen/Freiflächen und Gebäuden bestehen kann. Für den äußeren Sicherheitsbereich gibt es einen bei Freudenberg definierten Standard. Die jeweiligen Mieter sind für den Objektschutz des angemieteten Objektes, den inneren Sicherheitsbereich, verantwortlich, d.h. jedes Unternehmen definiert dort seinen Bedarf bzw. Sicherheitslevel. Aufgrund der unterschiedlichen Unternehmensziele gibt es alle vorstellbaren Varianten. Vom normal gesicherten Büro bis hin zum hochgeschützten Sicherheitsbereich ist alles zu finden. Bei der

> „Der Schwerpunkt unseres Handelns liegt auf der Prävention."

Definition der jeweiligen Schutzziele und der Entwicklung des daraus abgeleiteten Sicherheitskonzeptes sowie der Implementierung und dem Betrieb der eingesetzten Sicherheitstechnik unterstützen die Spezialisten aus den einzelnen Teams der Geschäftseinheit Werk-/Brandschutz.

Mit welchem technischen- und personellen Aufwand regeln Sie die Zutrittskontrolle bei Freudenberg? Hat der Industriepark ein einheitliches Ausweiswesen?

Dirk Jacobs: Die Zutrittskontrolle für die Industrieparks ist weitestgehend automatisiert. Die Zugänge über Drehkreuze, Drehsperren und Zweiradschleusen sind über Ausweisleser gesteuert und werden von den rund 6.500 Beschäftigten und Fremdfirmenmitarbeitern genutzt. Je nach Kundenanforderung wird das Zutrittskontrollsystem bis zur letzten Bürotür fortgeführt. Damit ist dann auch die Frage nach dem einheitlichen Ausweiswesen beantwortet, denn das System funktioniert nur dann, wenn alle Berechtigten dasselbe

Ausweissystem verwenden. Die Ausweise sind vom Layout einheitlich ausgeführt und unterscheiden sich lediglich durch das Firmenlogo des Unternehmens, bei dem der Ausweisinhaber beschäftigt ist. Das Ausweismanagement wird zentral in der Ausweisstelle durchgeführt. Hier werden nicht nur die Zutrittsdaten für die Industrieparks verwaltet, sondern auch weitere Freudenbergstandorte in Deutschland – von Hamburg bis in den Schwarzwald betreut. Für die Systempflege, Wartung und Instandhaltung des Zutrittskontrollsystems, aber auch der Schrankenanlagen und Vereinzelungsanlagen sowie der Videoüberwachung hält die Geschäftseinheit ein Technikteam vor. Für die Besucher- und Lkw-Abwicklung betreibt der Industriepark Weinheim zwei Tore und einen Empfang mit personeller Besetzung, in Neuenburg und Laudenbach jeweils ein Tor.

Führen Sie auch interne Ermittlungen für Ihre Kunden durch? Was können Sie vorbeugend tun, um strafbare Handlungen zu verhindern?

Dirk Jacobs: Bei internen Ermittlungen gelten die allgemeinen gesetzlich vorgegebenen Rahmenbedingungen, in denen sich eine private Sicherheitsorganisation bewegen darf, bzw. kann. In diesem Rahmen bewegen wir uns mit unseren Spezialisten, die bei konkreten oder bestätigten Hinweisen umgehend die zuständigen Behörden einschalten. Der Schwerpunkt unseres Handelns liegt auf der Prävention. Zur Verhinderung von strafbaren Handlungen setzen wir auf regelmäßige Kommunikation, Beratung und Sensibilisierung, operative Unterstützung durch Bestreifungen, Zutrittskontrollen, Durchführung oder Begleitung von Sicherheitsaudits sowie Planung und Einsatz von technischen Mitteln zur Gefahrenabwehr.

Sie unterhalten eine eigene Werkfeuerwehr im Industriepark Weinheim. Welche Einsatzkräfte und -fahrzeuge sind dazu einsatzbereit? Mit wie vielen Einsätzen rechnen Sie jährlich?

Dirk Jacobs: Für die operative Gefahrenabwehr halten wir insgesamt sieben Einsatzfunktionen 24/7 in einem zwei mal zwölf Stunden Schichtmodell vor, das von vier Schichtgruppen übernommen wird. Werktags sind sieben weitere Funktionen in der Tagschicht vorhanden. Zur Sicherstellung der technischen Einsatzleitung gibt es einen Leitungsdienst, der in Form einer 24/7 Bereitschaft arbeitet. Auf Basis einer Alarm- und Ausrückordnung werden die hauptberuflichen Kräfte von der eigenen Leitstelle zu den Einsätzen angefordert und, je nach Eskalationsstufe, durch weitere

> „Der vorbeugende Brandschutz ist eines unserer Kerngeschäfte."

nachalarmierte dienstfreie hauptberufliche sowie nebenberufliche Einsatzkräfte ergänzt. Bei Bedarf werden Einsatzkräfte der Freiwilligen Feuerwehr Weinheim oder anderer benachbarter Wehren nachalarmiert. Der Fuhrpark wird aktuell neu aufgestellt, um den geänderten Strukturen im Industriepark Rechnung zu tragen. Ein normaler Einsatz besteht aus einem Sonderlöschfahrzeug, der Teleskopmastbühne und dem Einsatzleitwagen. Im Bereich der Technischen Hilfeleistung kommt dann noch

24/7 besetzte Notruf- und Serviceleitstelle der Geschäftseinheit Werk-/Brandschutz

Bitte umblättern ▶

ein Rüstwagen hinzu. Des Weiteren stehen zwei Wechselladerträgerfahrzeuge mit insgesamt acht Abrollbehältern zur Verfügung, auf denen unterschiedlichste Komponenten wie Sonderlöschmittel oder Großlüfter verlastet sind. Das Einsatzaufkommen der Werkfeuerwehr liegt bei durchschnittlich 900 Einsätzen pro Jahr.

Ein derart komplexes Gebilde wie der Industriepark Weinheim unterliegt ständigen Veränderungen, nicht nur hinsichtlich der ansässigen Unternehmen, sondern auch unterschiedlichsten industriellen Nutzungen. Wie hat sich die Sicherheitsorganisation entwickelt, und wie stellen Sie sicher, dass sie mit dieser dynamischen Veränderung Schritt hält?

Dirk Jacobs: Die ersten Aufzeichnungen in den Archiven deuten auf einen Gründungstermin der Werkfeuerwehr im Jahr 1940 hin. Aus einer kleinen Löschgruppe entstand nach und nach eine anerkannte Werkfeuerwehr, die heute für die Gefahrenabwehr im Industriepark verantwortlich ist. Neben dem Schutz aller Mitarbeitenden gilt es, die Gebäude und Produktionseinrichtungen auf dem über 80 Hektar großen Areal zu schützen und durch hochspezialisierte Einsatzkräfte und geeignete Ausrüstung Produktionsunterbrechungen sowie Auswirkungen von Schadensereignissen auf Umwelt und Nachbarschaft zu verhindern. Um diese Ziele zu erreichen, haben wir mit den Mitarbeitern der Geschäftseinheit Werk-/Brandschutz einen Business Case entwickelt, der sich dynamisch an sich verändernde Strukturen anpassen kann. In einer konventionellen Brandschutzbedarfsplanung wurde zunächst ein Abgleich der heutigen Gefährdungspotentiale mit den Auflagen aus dem derzeit gültigen behördlichen Anerkennungsbescheid durchgeführt. Daraus wurde der Bedarf an Personal und Technik für die klassischen Gefahrenabwehraufgaben ermittelt und eine langfristige Qualifizierungs- und Investitionsplanung ausgearbeitet. In einem weiteren Schritt wurden das Dienstleistungsportfolio und die Organisationsstruktur untersucht. Hier galt es zu prüfen, welche Leistungen für den Industriepark notwendig und wirtschaftlich vertretbar sind. Über 120 neue Geschäftsideen wurden von den Mitarbeitern entwickelt und zu fünf neuen strategischen Geschäftsfeldern zusammengefasst. Schließlich wurde die Organisation noch einer wirtschaftlichen Prüfung unterzogen. Hierzu gehörten ein umfangreiches Prozess- und Kosten-Benchmark sowie eine Make or Buy Analyse. Unser neues Geschäftsmodell wird zukünftig in der Lage sein, mit sehr kurzen Reaktionszeiten auf Veränderungen in den Industrieparks reagieren zu können.

Welche Bedeutung hat der vorbeugende Brandschutz in ihren Werken und wie gestaltet sich die Zusammenarbeit mit den örtlichen Feuerwehren?

Dirk Jacobs: Der vorbeugende Brandschutz ist eines unserer Kerngeschäfte. Schon im Rahmen der Vorplanung neuer Gebäude oder bei produktionsbedingten Nutzungsänderungen versuchen wir, mit unseren Ingenieuren zu beraten. Hierbei unterstützen wir Produktionsplaner und Fachplaner aus dem FM-Bereich bei der Entwicklung von Brandschutzkonzepten und Gefährdungsanalysen. Die Fachfunktion vorbeugender Brandschutz stellt sicher, dass die Einsatzmannschaft über alle relevanten Veränderungen informiert wird, spätestens dann, wenn ein Projekt aus der „Planwelt" in die „Bestandswelt" überführt wird. Anders herum kanalisiert diese Schnittstelle alle Erkenntnisse aus Gebäudebegehungen, Risikobesichtigungen und Bestreifungen der Einsatzmannschaft in Richtung der Planungsbereiche. Vorbeugender Brandschutz im Sinne der Prävention ist aber nicht nur Ingenieuraufgabe, sondern Tagesgeschäft vieler Mitarbeiter der Geschäftseinheit. Dazu gehören im anlagentechnischen Brandschutz Revisionsarbeiten an Lösch- und Gefahrenmeldeanlagen, Freigabeverfahren für feuergefährliche Arbeiten, Brandschutzbegehungen, Wartung der Feuerlöscher und Wandhydranten und vieles mehr. Im Bereich unseres Freudenberg Learning Management Systems bieten wir zudem Schulungen zum Brandschutzhelfer, Evakuierungshelfer und Brandschutzkoordinator an, Letzteres ist eine Freudenberg-spezifische Lösung zur Verbesserung des Vorbeugenden Brandschutzes in kleineren Standorten. Die Zusammenarbeit mit den örtlichen Feuerwehren ist eng und funktioniert gut. Bereits bei der Erstellung des Brandschutzkonzeptes, spätestens jedoch im Rahmen der Einsatzplanung werden neue Objekte oder Anlagen gemeinsam diskutiert und Eskalationsmodelle zur Gefahrenabwehr entwickelt. Die dabei festgelegten Maßnahmen werden in der Alarm- und Ausrückordnung des Landkreises hinterlegt, sodass im Ernstfall eine zeitnahe Alarmierung der erforderlichen Einsatzmittel möglich ist. Zudem sprechen sich die Wehren bei der Beschaffung neuer Einsatztechnik ab, um mit einem aufeinander abgestimmten Einsatzkonzept für alle Beteiligten wirtschaftlich vertretbare Investitionslösungen herbeizuführen.

Wie muss man sich Ihr Krisen- bzw. Notfallmanagement vorstellen?

Dirk Jacobs: Das Krisenmanagement ist auf Ebene der Führungsgesellschaft standardisiert. Wie in anderen global operierenden oder größeren Unternehmen auch sind in diesem Standard Maßnahmen für bestimmten Szenarien hinterlegt sowie Eskalationsmodelle definiert. Im Krisenfall entscheidet ein lokaler Krisenstab nach vorgegebenen Kriterien, ab wann der Vorfall einen Krisencharakter erhält und weiter eskaliert werden muss. Die lokalen Einheiten arbeiten die Krise im Rahmen des Notfallmanagements ab.

> „Die Zufriedenheit unserer Kunden im Industriepark ist für uns das primäre Ziel,..."

Welche moderne Sicherheitstechnik zur Schadensabwehr halten Sie für besonders wichtig und innovativ?

Dirk Jacobs: Sicherlich liegt ein Schwerpunkt auf der Gestaltung des Gefahrenmanagementsystems. Hierunter fallen sämtliche Bereiche der Gefahrenmeldetechnik wie Brandmeldesysteme, Einbruchmeldeanlagen, aber auch die Sprinkler- und Gaslöschanlagen sowie die Videotechnik. Aus unserer Sicht ist der Einsatz eines Leitrechners das wesentliche Element, alle eingehenden Informationen zeitnah abarbeiten und die richtigen Dispositionsentscheidungen treffen zu können. Denn jede Sekunde zählt, wenn Hilfsfristen unter fünf Minuten eingehalten werden sollen. In der Fahrzeug- und Einsatztechnik geht es darum, zeitnah mit möglichst geringem Aufwand auf Veränderungen in den Produktionsbereichen, was eingesetzte Materialien oder neue Produktionsverfahren betrifft, reagieren zu können. Hierzu stellen wir derzeit unser Equipment auf modulare Systeme um, die bei Bedarf ausgetauscht werden können, ohne jedes Mal wieder ein neues Einsatzfahrzeug kaufen zu müssen. Dabei achten wir auch darauf, den Mitarbeitern mit einheitlichen Standards die Arbeit im Einsatz zu erleichtern und potentielle Fehlerquellen auszuschalten.

Sie erarbeiten auch Sicherheitskonzepte für andere Kunden. Wie muss man sich solche Planungen vorstellen und wie erreichen Sie wirtschaftlich vertretbare Lösungen?

Dirk Jacobs: Die Zufriedenheit unserer Kunden im Industriepark ist für uns das primäre Ziel, unabhängig davon, ob es sich um Kunden unserer Unternehmensgruppe oder andere Kunden handelt. Viele Kunden haben noch andere Niederlassungen oder Produktionsstandorte, für die wir den Auftrag erhalten, Sicherheitskonzepte zu erstellen. Hinzu kommen weitere Kunden im regionalen Umfeld, die über andere Geschäftsbeziehungen zum Industriepark auf unser Leistungsspektrum aufmerksam geworden sind und mit uns Kontakt aufnehmen. Im Prinzip können wir das gesamte Spektrum im Bereich der Sicherheitskonzeption anbieten. Ein Schwerpunkt liegt jedoch im Bereich der Flucht- und Rettungswegplanung sowie in der Ausarbeitung von Brandschutzkonzepten und Gefährdungsanalysen. Eine hohe Nachfrage genießen auch unsere Schulungen zum Brandschutzhelfer. Wirtschaftlich vertretbaren Lösungen erreichen wir durch intensive Diskussion mit unseren Kunden über die zu erreichenden Schutzziele. Hier werden die entscheidenden Weichen für das Endergebnis gestellt. Gepaart mit unserer Erfahrung als Dienstleister innerhalb eines Industrieparks und der breiten Qualifikation unserer Spezialisten entstehen dann Konzepte, die wir, wenn der Kunde das wünscht, bis zur behördlichen Genehmigung begleiten und implementieren. Dieser durchgängige Prozess aus einer Hand reduziert aufwändige Schnittstellendiskussionen und damit letztendlich den wirtschaftlichen Aufwand beim Kunden.

Wie schätzen Sie die aktuelle Sicherheitslage für den Industriestandort Deutschland ein?

Dirk Jacobs: Die Beurteilung der aktuellen Sicherheitslage ist Aufgabe der Politik und Verbände. Klar ist allerdings, dass private Sicherheitsorganisationen mit einer stetig steigenden Dynamik konfrontiert werden, was Bedrohungsszenarien sowie technologische und prozessuale Veränderungen betrifft. Globalisierung, Digitalisierung, IT-Sicherheit, Knowhow-Schutz, Supply Chain Management, Infrastrukturen, Wirtschaftsgrundschutz, aber auch Demographie sind nur einige der Aufgabenstellungen, mit denen sich eine moderne Unternehmenssicherheit heute täglich auseinandersetzen muss. Wer situationsgerecht nutzerspezifische Sicherheitskonzepte anbieten will, muss erhebliche Ressourcen für die Weiterentwicklung der Organisation und deren Mitarbeiter investieren. Das im Kontext zu der berechtigten Forderung nach wirtschaftlich vertretbaren Lösungen ist eine anspruchsvolle Herausforderung, der wir uns stellen müssen.

Vielen Dank für das Gespräch.

Das Interview führte:
Dipl.-Verw. Heiner Jerofsky
Kriminalrat a. D.

Vertriebspartnerschaft geschlossen

Videor vertreibt jetzt Produkte von Slat. Der Hersteller unterbrechungsfreier Gleichstromversorgungen steht für den zuverlässigen Betrieb von Anlagen kritischer Infrastrukturen und technischer Netzwerke aus den Bereichen Sicherheits- und Videotechnik, Gebäude- und Automationstechnik. Dank der Mitarbeit in europäischen Normenausschüssen und der Herstellerzertifizierung durch den VdS sowie nach ISO 9001/14001 (2015) optimiert Slat seine Prozesstechnik ständig und hält damit die Qualität seiner Produkte auf einem stets hohen Level.

Christian Janßen, Leiter der deutschen Niederlassung von Slat, kommentiert die Zusammenarbeit so: „Wir freuen uns, mit Videor einen starken Distributionspartner gefunden zu haben, mit dem wir bestehende Märkte der Video- und Sicherheitstechnik weiter durchdringen und neue dazugewinnen können. Wir bauen auf den Erfolg und die Kompetenz unseres Partners, um gemeinsam zu wachsen und mit Videor eine dauerhaft führende Rolle auf dem Markt einzunehmen." Beate Meyer-Young, Leiterin Product Management bei Videor: „Die Zusammenarbeit mit Slat versetzt uns in die Lage, unseren Kunden bewährte kompakte USV-Lösungen anzubieten. Damit sind sie die perfekte Ergänzung für unsere Integratoren und Installateure, die eine Hochverfügbarkeit der Videoanlagen gewährleisten müssen. Wir freuen uns über das Vertrauen dieses etablierten Anbieters und sind sicher, mit dieser Partnerschaft zusätzliche Applikationen abdecken zu können."

www.videor.com ■

ZUTRITTSSTEUERUNG

Läuft nicht gibt's nicht!

Zum 40. Jubiläum von Deister Electronic

40 Jahre – für mittelständische Unternehmen ist das ein Alter, in dem man sich schon mal einen kleinen Rückblick erlauben kann. Matthias Erler von GIT SICHERHEIT sprach aus diesem Anlass mit Firmengründer Anatoli Stobbe und seinem Sohn und Nachfolger in der Geschäftsführung Nicolas Stobbe über Etappen und Erfolge – inklusive Blick auf die jüngsten Produkte aus dem Hause Deister Electronic.

GIT SICHERHEIT: Meine Herren, Anatoli Stobbe und Nicolas Stobbe, zunächst einmal: Herzlichen Glückwunsch! Deister Electronic wird in diesem Jahr sage und schreibe 40 Jahre alt. Wie werden Sie das Jubiläum begehen?

Nicolas Stobbe: Das werden wir gebührend feiern – mit einigen internen Festen und Veranstaltungen im Verlauf des Jahres. Das ist eine gute Gelegenheit, einmal die Meilensteine aufzuarbeiten, die hinter uns liegen. Es trägt nicht nur zur Identifikation unserer Mitarbeiter mit dem Unternehmen bei, sondern hilft auch dabei, unsere nächsten Schritte in die Zukunft besser zu verstehen.

Wenn Sie deister heute in einigen knappen Sätzen definieren wollten – wie würde diese Definition aussehen?

Nicolas Stobbe: Wir sind ein Unternehmen mit einem sehr vielfältigem Lösungsangebot im Sicherheitsbereich, und das für sehr unterschiedliche Kunden. Unsere treibenden Kräfte sind Innovation, Qualität und Sicherheit – letzteres umfasst die ganze Lösung, End-to-end-Sicherheit von der Software bis in die Hardware. Wir entwickeln diesbezüglich ja alles selbst, so dass wir auch die Sicherheitskonzepte von A bis Z selbst in der Hand haben. Abgesehen davon, haben wir uns bei allem was wir tun, Kundenzufriedenheit und Kundenservice auf die Fahnen geschrieben. Wir haben uns dadurch den Ruf erarbeitet, dass unsere Produkte ausnahmslos funktionieren – und wenn wir bei Kunden eine schwierige Infrastruktur vorfinden, bieten wir auch hier unsere Unterstützung für die Inbetriebnahme und Integration an. Das Projekt ist für uns erst abgeschlossen, wenn unser Kunde uns sein Okay gibt, dass alles auch so wie gewünscht funktioniert.

Anatoli Stobbe: Was uns von Anfang an ausgemacht hat, waren technische Leistungen, die wir als begeisterte Ingenieure entwickelt haben. Ich selbst war immer mehr Ingenieur als Unternehmer – das Vertriebliche musste ich erst lernen. Angeregt und vorangetrieben hat uns immer die Arbeit an Dingen die es vorher nicht gab – und in Bereichen, die für uns oft völlig fremd waren. Ein frühes Beispiel dafür ist unsere elektronische Lösung für die Wächterkontrolle für Wachgesellschaften. Anders als bei der traditionellen Stechuhr konnte man unsere Geräte am PC auswerten und Kontrollgänge verlässlich elektronisch erfassen – diese Vorteile haben uns damals schnell zum Marktführer für Wächterkontrollsysteme in Deutschland gemacht und die Anwender nannten unseren Datensammler dann einfach nur noch „den Deister"…

…und bald kam die RFID-Technik dazu?

Anatoli Stobbe: Die erste rudimentäre RFID Technik wurde in den USA eingesetzt, wo auch wir damals darauf aufmerksam wurden und das Potential erkannten – aber die dort genutzte Frequenz durfte bei uns nur von U-Booten eingesetzt werden, also nicht in der Zutrittskontrolle, wo wir sie brauchten. Das war für uns der Anlass, zusammen mit Studenten und mit Hilfe von Mittelstands-Fördergeldern von Bund und Land ein eigenes System zu entwickeln – so fingen wir mit der Chipentwicklung an. Schwierig war vor allem, eine performante und sichere Lösung für die Zutrittskontrolle zu entwickeln – es war alles andere als leicht, einen Transponderchip zum Schreiben und Beschreiben zu bauen. Aber letztlich entwickelten wir auf diesem Weg ein Basispatent für sämtliche RFID-Schreibvorgänge – so ist übrigens die entsprechende Technik von Mifare ein Deister-Patent.

Wie ging es weiter?

Anatoli Stobbe: Wir haben mehrere eigene Chips entwickelt. Der Transponderchip war damals unser Hauptumsatzträger. Unser Readerchip wurde dann nach der Wende sehr wichtig. Damals stieg die Zahl der Autodiebstähle und die von uns entwickelten ersten Wegfahrsperren sollten dem entgegenwirken. Wir lieferten erst Lösungen für Luxuswagen wie die E-Klasse oder den Maybach. Wir haben immer die Passion, etwas völlig Neues hinzukriegen – so entstand bei uns die Lösung für das automatische Öffnen und Schließen des Autos mit dem Autoschlüssel in der Hosentasche. Und von Projekt zu Projekt wurden in der Folge viele völlig unterschiedliche Produkte und Lösungen aus ganz verschiedenen Sektoren entwickelt, die heute noch in unserem Lösungsportfolio sind – von der Fahrzeugerkennung via UHF Technologie bis hin zum Schutzsystem für Patienten und Neugeborene im Krankenhaus oder demenzkranker Bewohner im Altenpflegeheim. Was soll ich sagen, RFID ist eine tolle Technologie, die überall ihren Einsatz findet.

Das führt Sie zuweilen auch über klassische Sicherheitsanwendungen hinaus?

Anatoli Stobbe: Unser Textilmanagement System zum Beispiel. Wir haben einen Wäscheschrank für Berufskleidung erfunden, der bei jeder Benutzung Inventur über die Bekleidungsstücke macht. Dies basiert auf textilen RFID-Transpondern und wird in Wäschereien und in der Bekleidungsindustrie eingesetzt. Auch hier haben wir das scheinbar Unmögliche technisch realisiert: Wir haben die ersten textilen Transponder erfunden – und diese funktionieren sogar noch pitschnass. Für die Entwicklung mussten einige unserer Ingeni-

eure Weben lernen und wir haben dazu sogar eine eigene Webmaschine angeschafft. Bei aller Buntheit der Sektoren in denen wir uns bewegen, muss man aber sagen, dass wir unsere Kernwerte Innovation, Qualität und Sicherheit immer im Fokus halten.

Sie sind schon lange nicht nur in Deutschland, sondern weltweit mit Niederlassungen vertreten – unter anderem in den USA, UK, Frankreich, in Japan und in Singapur. Was macht Ihr Unternehmen für diese Länder attraktiv? Profitieren Sie hier auch von dem bei uns häufig als Prädikat verstandenen „Made in Germany"?

Nicolas Stobbe: Unsere unternehmerischen Stärken kommen im internationalen Wettbewerb sehr gut zur Geltung – dazu kommt in der Tat auch die Tatsache, dass Deutschland weltweit einen sehr guten Ruf hat, von dem auch wir profitieren. Wir tun allerdings mit unserem intensiven, jederzeit ansprechbaren Support sehr viel dazu, unseren Kunden Vertrauen und das geradezu geborgene Gefühl zu vermitteln, bei uns gute aufgehoben zu sein. Entsprechende Rückmeldungen bekommen wir auch. Man sagt über uns, dass es kein Deister-System gibt, das nicht funktioniert. Und das ist auch so: Oft ist ja die Herausforderung, dass viele Kunden bereits eine komplexe Infrastruktur an Systemen haben, in die wir uns integrieren müssen – und wir gehen nicht eher, bis unser System perfekt integriert ist und läuft. Was immer von uns eingekauft wird, funktioniert auch – das ist für uns Ehrensache. All das gilt nicht nur für unser eigenes Unternehmen, sondern auch für unsere sämtlichen Partner. Wir suchen sie entsprechend strategisch aus, auch wenn wir dafür hin und wieder länger suchen müssen.

> „Was immer von uns eingekauft wird, funktioniert auch – das ist für uns Ehrensache."

Wie entwickeln Sie sich im internationalen Umfeld – bzw. in welchen Regionen wollen Sie noch weiter wachsen?

Nicolas Stobbe: Unser Exportgeschäft nehmen wir weltweit als sehr stark wahr. Die Wirtschaft wächst weltweit und auch in Deutschland. Gerade auch die USA sind und bleiben für uns

Firmengründer und Geschäftsführer Anatoli Stobbe und sein Sohn und Nachfolger in der Geschäftsführung Nicolas Stobbe

trotz der politischen Turbulenzen sehr attraktiv. Das Gleiche gilt für Europa – und auch für die von der Finanzkrise stärker betroffenen Länder. Dementsprechend bauen wir den Vertrieb weiter aus, denn die Nachfrage steigt stetig und wir werden auch dieses Jahr die Mannschaft weiter verstärken.

Kommt Ihnen dabei der viel besprochene Fachkräftemangel in die Quere?

Nicolas Stobbe: Nein. Das mag daran liegen, dass wir hier eine andere Philosophie vertreten. Wir glauben, dass man zusätzlich zu dem Ausbau der Belegschaft durch Weiterbildung und Motivation der eigenen Leute die wachsenden Anforderungen mit abdecken kann. Ein motivierter Mitarbeiter, der wirklich Lust hat kann viel mehr bewegen als ein Top-Überflieger mit den besten Noten, der aber nicht ins Team passt. Die menschliche Komponente ist nach unserer Erfahrung ein entscheidender Punkt. Wir glauben an die Entwicklung von Mitarbeitern. Das gilt quer durch alle Bereiche unseres Unternehmens – vom Vertrieb bis zur Entwicklung. Natürlich suchen wir auch neue Leute – aber auch hier muss ich sagen, dass es sich für uns eigentlich kaum verändert hat über die letzten Jahre. Die richtigen Mitarbeiter zu finden, ist, glaube ich, immer eine Aufgabe, der man viel Aufmerksamkeit schenken muss. Positiv für uns ist, dass wir ein Familienunternehmen sind, was viele unserer Mitarbeiter schätzen und unser Firmensitz in einer günstigen Lage zwischen Landleben und Großstadtnähe in einer attraktiven Region liegt.

▲ **Auf der Security in Essen wird es unter vielem anderen zu sehen sein: Das Übergabesystem „Bloxx" mit einem Portfolio aus Schubladen- und Fächermodulen**

Sie sind mit Ihren Lösungen ja in vielen Branchen zuhause. Wo sehen Sie für deister die größten Zukunftschancen?

Nicolas Stobbe: Deister ist tatsächlich in vielen Branchen mit Lösungen präsent – und wir entdecken immer wieder neue Branchen für uns. Eine Fokussierung auf bestimmte ausgewählte Branchenlösungen würde nicht zu uns passen – das würde uns eher einengen und uns Chancen verbauen, denn unsere Entwicklungen sind meist sehr vielseitig einsetzbar. Es besteht für uns auch nicht die Notwendigkeit dafür, zumal sich bereits viele unserer Partner ihrerseits aus anderen Gründen eher spezialisieren. Wir schränken unsere Partner auch nicht mir etwaigen Vorgaben ein, sondern unterstützen sie jeweils mit intensivem Support. Viele unserer Projekte sind anspruchsvolle Hochsicherheitsanwendungen, beispielsweise von Banken oder Regierungen. Hier haben wir das notwendige Know-how, das wir unseren Partner gerne zu Verfügung stellen. Wir beraten, betreuen und unterstützen unsere Partner so intensiv, als wären es Tochterunternehmen. Und unsere Partner entsenden ihre Mitarbeiter umgekehrt mehrfach im Jahr zu uns nach Barsinghausen zum Training.

Lassen Sie uns etwas näher über aktuelle Treiber der Sicherheitsmärkte sprechen – etwa das große Thema Smart Building. Wie ist Deister hier aufgestellt, mit welcher Philosophie und welchen Lösungen?

Nicolas Stobbe: Aus unserer Sicht zeigt die steigende Bedeutung von Themen wie Smart Building, Building Automation etc., dass zunehmend verstanden wird, welche Vorteile sich bieten, wenn man Themen als zusammenhängend versteht und Gewerke zusammen betreibt. Wir haben mit unserer „Connected"-Linie ja schon sehr früh in dieser Richtung gearbeitet. Für uns liegt das gerade wegen der Vielfalt der Deister-Systeme besonders nahe. Anwender fragen immer häufiger nach den Vorteilen dieser Verbindung – hier wird etwa die Vereinfachung von Vorgängen genannt. Der eigentliche Mehrwert wird allerdings noch zu wenig gesehen, da viele Kunden auch noch gar nicht wissen, was alles möglich ist, und dass viele Anforderungen auch einfacher umgesetzt werden können.

…das wird im Zusammenhang mit dem Schlagwort Künstliche Intelligenz wohl eher der Fall sein?

Nicolas Stobbe: Das ist noch in der Entwicklung, so dass sich bislang noch die Frage stellt, wo Künstliche Intelligenz anfängt und wo sie aufhört. KI hat mit Analytik und komplexerer Entscheidungsfindung zu tun. Sie kann beispielsweise Kosten für die Infrastruktur verringern. Ihr liegt Rechenpower zugrunde – und es geht darum, wie Geräte voneinander lernen können. Wir sind der Ansicht, dass Geräte und Systeme intelligenter werden – durch zunehmende Rechenleistung und Vernetzung. Es werden mehr und mehr Informationen zwischen den einzelnen Komponenten ausgetauscht, so dass das Gesamtsystem intelligenter wird.

▲ **Viel Platz zum Denken und Entwickeln: Der Deister-Firmensitz in Barsinghausen**

…einhergehend mit noch weitergehender Einbindung mobiler Endgeräte?

Nicolas Stobbe: Smartphones, Wearables – alles was im Alltag immer stärker integriert ist, wird auch in der Arbeitswelt und den Unternehmen integriert. Das bringt neue Aufgaben mit sich, die vor allem darin bestehen, Sicherheit und Komfort auf einen Nenner zu bringen. Das nimmt nicht jedes Unternehmen ernst – teils auch deshalb, weil es ja oft auch um Anwendungen geht, die keinen besonders hohen Sicherheitsbedarf haben. Für uns haben höchste Sicherheitsstandards allerdings überall uneingeschränkte Priorität. Wir entwerfen komplexe und performante Architekturen mit sicherer Einbindung von Fremdgeräten.

2018 ist ja ein Security-Essen-Jahr – Sie werden ja wieder mit einem Stand vertreten sein?

Nicolas Stobbe: Selbstverständlich. Wir gehören ja gewissermaßen zu den Security-Dinosauriern. Sie ist aus unserer Sicht nach wie vor eine der wichtigsten, wenn nicht die wichtigste Messe der Branche weltweit. Mit den neuen Hallenplänen wurden wir zwar alle recht stark durcheinandergewirbelt – aber wir sind mit unserem neuen Stand sehr zufrieden. Wir werden das Thema „Connected" weitertreiben, und einige neue Produkte vorstellen.

Könnten Sie uns einmal Ihr Programm vorstellen? Was wird es bei Deister an Innovationen zu sehen geben in Essen?

Nicolas Stobbe: Wir werden diesmal unser komplettes Lösungs-Portfolio zeigen, also auch Lösungen aus dem Automationsbereich. „Connected" wollen wir nicht mehr nur auf Sicherheit reduzieren, sondern zeigen, dass bei uns wirklich alles aus einer Hand kommt und zusammen funktioniert. Wir werden im Bereich Asset-Management neue Lösungen zeigen, damit Kunden Ihr Arbeitsequipment und Utensilien optimal einsetzen und transparent verwalten können. Daher werden bei uns auf dem Stand auch unsere Textilmanagement Lösung und unser neues Übergabesystem „Bloxx" mit einem Portfolio aus Schubladen- und Fächermodulen zu sehen sein. Zudem werden wir auch das neue Asset- und Personenschutzsystem „Aman-Tag" vorstellen, mit dem sich ebenfalls Arbeitsequipment, wertvolle Geräte, aber eben auch Personen schützen lassen.

Was halten Sie, zusammengefasst, für die wichtigsten Faktoren des Erfolgs auch für die Zukunft Ihres Unternehmens?

Nicolas Stobbe: Wir sind hier bei Deister ganz einhellig der Meinung, dass das Wichtigste in der Tat die Kollegen sind, denen wir es ermöglichen, so zu arbeiten, dass sie Freude haben. Wenn das gelingt, passieren mitunter ganz seltsame und überraschende Dinge. Sämtliche Hierarchien werden obsolet, Vorgaben spielen keine Rolle, der Spaß treibt die Dinge voran, alles läuft auf einmal wie von alleine. So sind schon die besten Ideen und Produkte entstanden. Unsere 117 Patente sind also nicht durch Einzelgänger entstanden, sondern weil wir Leute haben, die Lust haben, an spannenden Projekten zu arbeiten und denen wir den notwendigen Freiraum dafür lassen. Dazu kommt Folgendes: Wir haben immer wieder alles selbst entwickelt – auch wenn es zum Beispiel um Fragen der Cloud-Kommunikation oder Bluetooth-Anwendung ging, die auf uns zukamen. Wir haben immer wieder festgestellt, dass wir Dinge doch lieber verbessern wollten, weil wir das Vorgefundene als nicht gut genug empfanden. Und eben dies ergab dann letztlich den entscheidenden Kaufgrund für die Kunden. Wir haben bei Deister den Drang entwickelt, immer tief zu bohren und nicht an der Oberfläche stehen zu bleiben. Das kostet natürlich oft erhebliche Ressourcen, die der Kunde oft gar nicht mitbekommt – aber für uns ist es das Wichtigste, mit Herz und Seele gute Sachen zu machen. Schließlich wäre als Erfolgsfaktor zu nennen, dass wir immer mehrere Standbeine haben, die sich auch untereinander sehr gut kombinieren lassen, um unseren Kunden einen Mehrwert bieten zu können. Ich glaube, dass wir gut und sturmfest aufgestellt sind für die Zukunft unseres Unternehmens. ■

Kontakt

Deister Electronic GmbH
Barsinghausen
Tel.: +49 5105 51601
info.de@deister.com
www.deister.com

Robert Köhler (kniend) von Avigilon: SOT 2018 an allen Tourstationen gut besucht

SOT 2019

Startschuss für die Security on Tour 2019

Roadshow der Sicherheitsbranche nimmt Berlin und Ingolstadt in das Tour-Programm auf

Die Roadshow Security on Tour, organisiert von Eucamp, etabliert sich für viele renommierte Security-Hersteller als wichtiges Branchenevent neben den Fachmessen. Anfang des Jahres tourten, nach 17 Ausstellern in 2017, bereits 22 führende Hersteller von Sicherheitsprodukten und -lösungen durch Deutschland und Österreich. Rund 1.100 Fachdienstleister tauschten sich in den besuchten Regionen zu den gezeigten über 50 Sicherheitslösungen mit den Fachexperten der Unternehmen aus. Die Pläne für 2019 stehen jetzt fest.

Termine der Security on Tour 2019:

- 24.01.2019 – Hamburg
- 29.01.2019 – Berlin
- 31.01.2019 – Leipzig
- 05.02.2019 – Frankfurt a.M.
- 07.02.2019 – Ingolstadt
- 12.02.2019 – Wien, Österreich

Hersteller können sich hier als Aussteller anmelden: http://securityontour.com/aussteller/pakete-preise/

Aussteller der SOT 2018 waren: Advancis, Avigilon, Dahua, Dom, Eizo, Eneo, Erdkreis Video, Euromicron, Gehrke, Hanwha Techwin Europe, Hikvision, Idis, Iseo, Kemas, Mobotix, PCS, Promise Technology und Solvido.

Auch in 2019 sind Fachvorträge der Aussteller zu Trends und Innovationen an jeder Roadshow-Station geplant

2019 noch breiter aufgestellt

Das SOT-Team bereitet sich bereits jetzt auf eine noch breiter aufgestellte Security-Roadshow vor. Stationen der vom 24.01. - 12.02.2019 stattfindenden Security on Tour 2019 sind Hamburg, Berlin, Leipzig, Frankfurt a.M., Ingolstadt und Wien. Die Hauptstadt und Ingolstadt wurden neu im Tour-Programm aufgenommen. Fachbesucher erwartet die gesamte Vielfalt von Videoüberwachung bis -Software, Zutrittskontrolle und Zeiterfassung, Brandschutz-, Alarm- und Sicherheits-Management. Ein zentrales Thema nimmt die im Markt fortschreitende Digitalisierung ein, die Fachbetrieben neues Potenzial bei Installation und Servicegrad an die Hand gibt. Ergänzt werden die Hersteller- Präsentationen durch hochkarätige Fachvorträge an jeder Roadshow-Station. Um einen freien Dialog zu fördern, ist für die Fachbesucher aus Fachdienstleister, Errichter bis Fachhandel der Eintritt zur Security on Tour weiterhin kostenlos.

Kompetenz vor Ort

„Die SOT hat sich für Hersteller, Fachdienstleister und Fachhandel zu einer wichtigen Plattform zum Fachaustausch entwickelt, die durch den Regionalfokus beide Seiten enger als bisher zusammenbringt", sagt SOT-Veranstalter Isaac Lee von Eucamp. „Für Fachbesucher verbinden sich Sortimentseinsicht und Wissenstransfer zu einem einmaligen Informationsangebot, das in ihrer Region seines Gleichen sucht. Hersteller erhalten direkten Kontakt zu vielen potenziellen Neukunden, können Kundenbeziehungen durch persönliche Treffen weiter stärken und erfahren ungefiltert, welche Herausforderungen aktuell im Markt besonders präsent sind. Für beide Seiten bietet die Security on Tour damit direkten Mehrwert und konkreten Nutzen." ■

> „Ein zentrales Thema nimmt die im Markt fortschreitende Digitalisierung ein, die Fachbetrieben neues Potenzial bei Installation und Servicegrad an die Hand gibt."

Kontakt

Eucamp
Bad Homburg v. d. H.
Tel.: +49 6172 3818262
info@securityontour.com
www.securityontour.com

PROZESSOPTIMIERUNG

Blick über den Tellerrand

Videomanagement-Software schützt und unterstützt Lebensmittelproduktion bei Feinkost-Hersteller Wernsing

Fruchtdesserts und Eintöpfe, Salate und Suppen die Feinkostprodukte der niedersächsischen Firma Wernsing sind in aller Munde. Vertrieben werden sie über den Fachgroßhandel, zahlreiche Lebensmitteleinzelhändler und die großen Discounter – in Deutschland und darüber hinaus. Das Familienunternehmen setzt auf Nachhaltigkeit und baut sowohl das angebotene Sortiment als auch die Reichweite ständig aus. Seit kurzem setzt das Unternehmen in seiner Produktion eine Videolösung von SeeTec ein.

▲ **Videotechnik von SeeTec dienen bei Wernsing auch der operativen Unterstützung der Prozessabläufe**

Als modernes, wachsendes Familienunternehmen hat Wernsing schon vor einigen Jahren die Vorteile einer Videolösung zur Unterstützung des Produktionsablaufs erkannt. Denn natürlich benötigt ein Lebensmittel produzierender Betrieb eine Außenhautüberwachung, welche die Produktionsstätten und -anlagen zuverlässig schützt. Doch bei Wernsing erkannte man schnell auch das zusätzliche Potenzial, das die Videotechnologie jenseits klassischer Sicherheitsanwendungen bietet. So sollten IP-Kameras auch in weiteren Einsatzgebieten wie etwa zur operativen Unterstützung der Prozessabläufe genutzt werden.

Der lange Weg der Pommes Frites

Eine Produktionsstraße bei einem Lebensmittelhersteller kann eine beachtliche Fläche einnehmen: Bei der Herstellung von Pommes Frites besteht sie z. B. aus einer Reihe von Einzelkomponenten wie einer Kartoffelwaschanlage und nachfolgenden Stationen zum Schälen, Schneiden, Veredeln und Verpacken.

Auch die Transportsysteme zwischen den einzelnen Stationen überwinden mitunter nicht gerade kleine Strecken. Manche Abschnitte der Produktionsstraße sind schon aufgrund baulicher Gegebenheiten nur schwer einseh- oder erreichbar. Kurz: Ein idealer Einsatzbereich für Videotechnik, denn der Personaleinsatz, um eine solche Anlage während der Betriebszeiten lückenlos vor Ort zu überwachen, wäre immens. Bei Wernsing entschied man sich deshalb für die Montage von Kameras an den Produktionslinien sowie für die Einrichtung von dezentralen, videogestützten Monitoring-Stationen im Produktionsbereich zur Überwachung der Verarbeitungsprozesse.

An ihnen kann sich der Prozessverantwortliche per Live-Bild am Bildschirm von der ordnungsgemäßen Funktion der Anlage überzeugen. Der Vorteil: Der zuständige Mit-

▲ **In aller Munde: Die Produkte des niedersächsischen Feinkost-Herstellers Wernsing. In Lager und Produktion setzt das Unternehmen auf Videotechnik von SeeTec**

arbeiter bekommt sofort mit, sollte es in der Anlage zu Störungen kommen. Neben den Monitoring-Stationen innerhalb der Produktion können die Bilder natürlich auch zentral in einer Leitwarte aufgeschaltet werden. Dort gibt es neben dem Live-Bildstrom auch die Möglichkeit, das aufgezeichnete Videomaterial nach Ereignissen oder Auffälligkeiten zu durchsuchen. Bis zu 45 Nutzer greifen heute gleichzeitig auf die Bilddaten der über 350 verbauten Kameras zu.

Komplettlösung der Partner SeeTec, Gadcon und Advancis

Die Planung und Installation eines Videosystems dieser Größe, das auch für die Produktionsüberwachung eingesetzt wird, erfordert die Unterstützung durch kompetente Partner. Hier setzte man bei Wernsing auf die Firma Gadcon.

Von Anfang an hatte man bei Wernsing eine Komplettlösung im Blick, die neben dem Videosystem auch das Gebäudemanagement (Advancis Winguard) und Zutrittskontrolle umfasst und dem Kunden so zusätzliche Mehrwerte für seine Infrastruktur-Investitionen bietet. Als zertifizierter SeeTec-Partner konnte Gadcon zudem eine weitere Lösung präsentieren: die Verknüpfung der Kamerabilder mit Prozessdaten, die z. B. in Auftragsabwicklung und Versand anfallen. Dieser Ansatz, der vor allem in der Logistik zunehmend verbreitet ist, konnte auch die Entscheider von Wernsing überzeugen. Deshalb kommt im Versand nun mit SeeTec BVI eine intelligente Softwareplattform zum Einsatz, die Videodaten mit weiteren relevanten Produktionsdaten verknüpft. Im Falle von Wernsing geschieht dies so: Für die Auftragsabwicklung, den Versand und die Verladung gibt es auf dem Werksgelände verteilt mehrere Scanplätze. An diesen wird die ausgehende Ware im Zuge des Versand- und Verladeprozesses mehrfach gescannt und mit den im Warenwirtschaftssystem hinterlegten Auftragsdaten verglichen. Jeder Scanvorgang wird nun mit den Videoaufnahmen „verheiratet", die zum Zeitpunkt des Scanvorgangs entstanden sind. So lässt sich im Schadensfall analysieren, wo im automatisierten Logistikprozess ein Fehler aufgetreten ist. Darüber hinaus können die Videobilder aber auch bei Reklamationen eingesetzt werden, um z. B. nachzuweisen, dass die versendete Ware unbeschädigt war und zur korrekten Ladebucht gelangt ist.

Das System hat sich bereits in kürzester Zeit bewährt, weil auf diese Weise Mängel im Logistikprozess besonders einfach aufgedeckt und sofortige Verbesserungen vorgenommen werden können. Somit steigern die durch die Videobilder optimierten Prozesse die Kundenzufriedenheit sozusagen im Vorbeifahren nachhaltig und Wernsing kann sein Qualitätsversprechen, das weit über die eigentliche Produktqualität hinausgeht, noch besser erfüllen.

Mehr als 350 Kameras im Einsatz

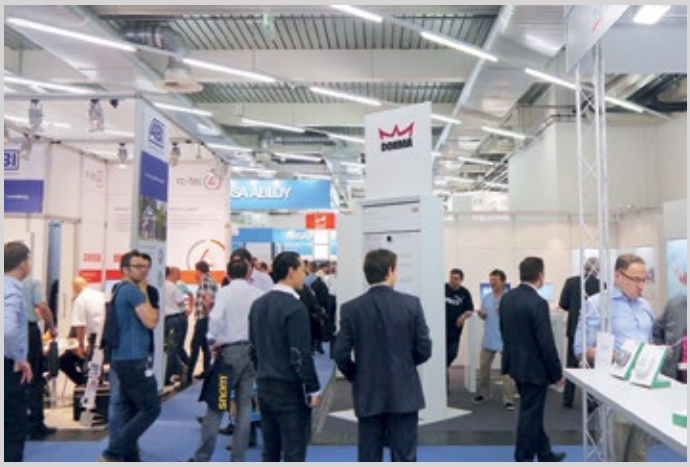
Das Projekt bei Wernsing nahm bereits während der Planungsphase eine neue Dimension an. Ging man zunächst von 110 zu installierenden Kameras aus, wurde sehr schnell klar, dass diese Zahl aufgrund des in der Projektierung gemeinsam erarbeiteten Optimierungspotenzials nicht ausreichen würde.

Deshalb sind heute bereits mehr als 350 Kameras im Einsatz und auch für zukünftige Erweiterungen in der Produktion wird bei Wernsing auf SeeTec gesetzt. Seckin Bayindir, der Projektverantwortliche bei Wernsing, erklärt das so: „Das System wurde von den Mitarbeiterinnen und Mitarbeitern in der Produktion sehr gut angenommen, denn für sie bietet die dezentrale Überwachung der Produktionsanlagen eine große Arbeitserleichterung. Außerdem wurden sie von Anfang an in die Planung mit einbezogen, da sie aufgrund der täglichen Arbeit in der Produktion am besten die kritischen Stellen kennen, wo Probleme auftreten können." Aber auch für die Projektpartnern Gadcon und SeeTec hat Herr Bayindir lobende Worte: „Die Erfahrung, die beide Firmen bei uns eingebracht haben, ermöglichte es uns, das Projekt zu einem erfolgreichen Abschluss zu bringen. Und auch bei der Entwicklung von Speziallösungen war die Zusammenarbeit mit SeeTec und Gadcon stets partnerschaftlich und auf Augenhöhe." Mit einem Augenzwinkern merkt er an: „Durch die intensive Nutzung des Systems haben wir immer wieder Wünsche für neue Funktionen – ich bin allerdings sehr guter Dinge, dass unser Feedback dazu beiträgt, dass auch andere Kunden in Zukunft von unseren Vorschlägen profitieren können." ■

Kontakt

SeeTec GmbH, Bruchsal
Tel.: +49 7251 9290 0
info@seetec.de
www.seetec.de

JEROFSKYS SICHERHEITS-FORUM



Sicherheitsexpo: Messeimpressionen von der Sicherheits-Expo

15. SicherheitsExpo 2018

Die SicherheitsExpo in München vom 27. bis 28. Juni 2018 zeigt u. a. Neues aus den Bereichen NFC, RFID, Biometrie und Identity-Management sowie Zutrittskontrolle, Videoüberwachung, Leitstellen und Mobilfunk. Im Forum 1 und 2 präsentieren Aussteller die neuesten Trends und Enwicklungen in der Sicherheitstechnik, und Sicherheitsexperten referieren zu aktuellen Themen. Der Zutritt ist für alle Messebesucher frei. Der Bayerischer Staatsminister des Innern, Joachim Herrmann, eröffnet die Messe mit einem Vortrag zur aktuellen Sicherheitslage in Bayern und Europa. U. a. referiert unser wissenschaftlicher Schriftleiter Heiner Jerofsky zum Thema „Einbruchschutz für Industrie, Handel und Gewerbe aus kriminalistischer Sicht". Die paralell laufende Brandschutz-Tagung unter der Leitung des Brandschutz-Experten Dr.Wolfgang Friedl informiert über die aktuellen gesetzlichen und technischen Anforderungen an den Brandschutz in Deutschland. Es werden die wichtigsten Vorschriften und Normen für den betrieblichen Brandschutz vorgestellt.■

Zutrittssteuerung und Identifikationsmanagement

Vom 13.09. bis 14.09.2018 veranstaltet der Bundesverband Sicherheitstechnik (BHE) in Hünfeld zum Thema Zutrittsteuerung und Identifikationsmanagement ein Fachseminar. Im Rahmen dieser Veranstaltung werden alle für die Thematik relevanten Inhalte vermittelt und vertieft. Den Teilnehmern werden in dieser produkt- und herstellerneutralen Veranstaltung neben der Beschreibung der technischen Komponenten die wichtigen Bereiche Planung, Projektierung, Installation, Inbetriebnahme und Instandhaltung von Zutrittssteuerung erläutert. Das Seminar ist für kundenorientierte Mitarbeiter von Firmen geeignet, die solche Systeme anbieten, errichten, installieren und in Betrieb nehmen (z. B. auch Berater und Mitarbeiter im Support und Vertrieb usw.). Neben der Zutritts-Technik werden auch Informationen zu Verordnungen, Normen und rechtlichen Fragen gegeben. Insbesondere zur neuen Datenschutz-Grundverordnung (DS-GVO). Es wird geklärt, was beim Einsatz von biometrischen Daten zu beachten ist, da sie zu den „besonderen Kategorien personenbezogener Daten" gehören, die gemäß Art. 9 DS-GVO einem besonderen Schutz unterliegen. Am Ende der Veranstaltung können interessierte Seminarteilnehmer eine Prüfung ablegen. Bei Bestehen wird eine Fachkompetenz-Urkunde ausgestellt. BHE-Mitglieder können somit eine der Voraussetzungen für die Auszeichnung „BHE-zertifizierter Fachbetrieb Zutrittssteuerungsanlagen" erfüllen.■

Definitionen

› Sicherheitskennzeichen

Sicherheitskennzeichen nach DIN EN ISO 7010 und DIN 4844-2 werden entsprechend ihrer Funktion bzw. Sicherheitsaussage wie folgt kategorisiert:

- Rettungszeichen – Sicherheitszeichen, das einen Fluchtweg, den Ort einer Erste-Hilfe-Einrichtung oder ein sicheres Verhalten kennzeichnet,
- Brandschutzzeichen – Sicherheitszeichen, das den Standort von Brandmelde- und Feuerlöscheinrichtungen kennzeichnet,
- Gebotszeichen, das ein bestimmtes Verhalten vorschreibt,
- Verbotszeichen – das ein bestimmtes Verhalten untersagt und
- Warnzeichen – Sicherheitszeichen, das vor einer bestimmten Gefahr warnt.

› Mechanische Schlüsseldepots

Für die sichere Verwahrung von Gebäudeschlüsseln für den Notfall stehen unterschiedliche Arten von mechanisch wirkenden Schlüsseldepots zur Verfügung, wie z. B.: Schlüsselrohr mit einem oder zwei Zylindern und Schlüsseldepot mit Gehäuse mit separatem Zylinder. Schlüsseldepots können z. B. in der Fassade eingebaut werden. Sie können im Notfall mit einem übergeordneten Notschüssel (z. B. von der Feuerwehr oder anderen autorisierten Personen) geöffnet werden.

› Sicherheitstechnik

steht für alle technischen Einrichtungen, die zum Schutz von Personen und Werten in Gebäuden installiert und betrieben werden. Es handelt sich laut „Baunetz Wissen" um die technische Gebäudesicherheit einschließlich der technischen und organisatorischen Schnittstellen zu

Cyber Security Konferenz auf der Security 2018 in Essen

Cyber-Security-Konferenz auf der Security

Im Rahmen der Security Essen veranstaltet die Messe Essen gemeinsam mit dem BHE Bundesverband für Sicherheitstechnik sowie mit fachlicher Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) die Cyber-Security-Konferenz. Wissenstransfer und Erfahrungsaustausch stehen hier an allen vier Tagen der Security Essen im Mittelpunkt. Experten können ihre Bewerbung für einen Vortrag rund um die Themenbereiche „Chancen & Risiken von Cyber Security", „Connected Building – Sicherheit im Gebäude der Zukunft" sowie „Zugang, Zutritt, Zugriff – Möglichkeiten der Identifikation" einreichen. .■

DB-Sicherheitsbericht

Die Deutsche Bahn hat ihren Sicherheitsbericht für das Jahr 2017 vorgelegt. Um ein Viertel zurückgegangen ist demnach der Taschendiebstahl (rund 31.000 Fälle). Es gab 38 Prozent weniger aufgebrochene Fahrkartenautomaten (ca. 250) sowie jeweils knapp sieben Prozent weniger Fälle von Vandalismus (rund 9.000) und Metalldiebstahl (ca. 570). Dagegen stieg die Zahl der Graffiti-Beschädigungen (ca. 18.120) um ca. 4 Prozent. Die Zahl der Übergriffe auf Reisende ist mit ca. 12.680 in etwa gleich geblieben. 2017 nutzten insgesamt deutlich über zwei Milliarden Reisende die Züge der DB in Deutschland. Noch immer verzeichnet die DB einen Anstieg der Angriffe auf Mitarbeiter und hier insbesondere auf die Sicherheitskräfte. 2.550 DB-Mitarbeiter sahen sich 2017 mit Übergriffen konfrontiert; das sind 176 bzw. sieben Prozent mehr als 2016. Von 2015 auf 2016 hatte der Anstieg noch 30 Prozent betragen.

Hans-Hilmar Rischke, Leiter Konzernsicherheit: „Der Umgangston in der Gesellschaft wird rauer, das spüren unsere Mitarbeiter genauso wie die Polizei oder Feuerwehr. Unsere Reaktion: personelle Verstärkung in den Ballungsräumen, entschiedenes Vorgehen gegen Störer, deutlicher Ausbau und Modernisierung der Videotechnik, Einsatz von Bodycams sowie der Einsatz von mehr Hundestaffeln."

Um sich für gefährliche Situationen zu wappnen, absolvieren Zugbegleiter, Lokführer und Sicherheitskräfte der DB bereits seit Jahren Deeskalations- und Verhaltenstrainings. Es ist ab 2018 für die Mitarbeiter im Kundenkontakt verpflichtend, an dem Training teilzunehmen. Die DB ist zudem auch mit den Gewerkschaften und Betriebsräten im Gespräch, um gemeinsame Lösungen für mehr Sicherheit zu entwickeln.■

angrenzenden Systemen wie Gebäudeleit- und -managementsystemen (HLK), Personal- und Betriebsdatenerfassung, IT-Sicherheit, Notfallplanung und Katastrophenmanagement, Aufzugssteuerungen, Energie- und Regeltechnik, Lichtregelung und Beschattungstechnik. Sicherheitstechnik hat grundsätzlich drei Wirkungsziele: technische Prävention, frühzeitige Erkennung und Meldung von Schutzverletzungen und intelligente Vernetzung mit angrenzender Haus- und Gebäudetechnik.

› Generalhauptschlüssel

Als Generalhauptschlüssel bezeichnet man den ranghöchsten übergeordneten Schlüssel einer Generalhauptschlüsselanlage. Der Generalhauptschlüssel schließt sämtliche Zylinder aller Schließgruppen einer Generalhauptschlüsselanlage, mit Ausnahme spezieller Sperrschließungen.

› Fundamentalismus

ist seit dem 11. September 2011 zu einem politischen Schlagwort insbesondere für islamistische Bestrebungen geworden. Durch fundamentalistische Gruppen wird das Wiederaufgreifen von bestimmten religiösen oder politischen Ideologien eingefordert, wobei sie sich streng von der modernen Lebensweise abgrenzen. Dabei richten die Fundamentalisten ihr Leben voll und ganz nach ihren traditionellen Vorstellungen aus, welche notfalls mit radikalen und intoleranten Mitteln – auch mit Gewalt – durchgesetzt werden sollen.

› Rettungsweg

ist ein Begriff aus dem Bauordnungsrecht und dem Brandschutz. Er kennzeichnet den Zugang für die Einsatzkräfte, der für Brandbekämpfung, Rettung oder Verletztenbergung stets freigehalten werden muss (§ 14 MBO).

Kameras für Außenbereich gewerblicher Unternehmen

Flir Systems kündigt die Saros-Reihe an, eine neue Generation von Sicherheitskameras für den Außenbereich, die mehrere herkömmliche Perimeterschutztechnologien in einer einheitlichen Lösung verbindet. Dieser Ansatz wurde entwickelt, um genaue, umsetzbare Warnmeldungen und verifizierte Alarmdaten bereitzustellen. Die Kameraserie ermöglicht es gewerblichen Unternehmen, ein hochmodernes Einbrucherkennungssystem für den Außenbereich auf kostengünstige Weise einzusetzen. Herkömmliche Perimetersicherungssysteme können erhebliche Investitionen erfordern, sowohl in die Infrastruktur als auch in laufende Kosten aufgrund von Fehlalarmen. Flir Saros senkt nicht nur die Kosten für die Erstinstallation durch Minimierung der erforderlichen Ausrüstung, sondern reduziert auch Fehlalarme durch integrierte, fortschrittliche Analysen und erweitert damit für Sicherheitsalarmüberwachungsunternehmen den Markt für Perimeterschutz im Außenbereich.

www.flir.com/security ■

Herstellerneutrales Gefahrenmanagementsystem

Advancis ist im Juni auf mehreren Messen und Veranstaltungen präsent. Vom 12. bis 13. Juni findet das 6. Symposium „Leitstelle aktuell" in Bremerhaven statt. Die Leitstelle ist Dreh- und Angelpunkt – kommt es hier zu Problemen, hat dies Auswirkungen auf die Arbeit von Feuerwehr, Polizei und Rettungsdienst. Mit dem herstellerneutralen Gefahrenmanagementsystem WinGuard bietet Advancis eine umfassende Lösung, um Anwender in der Sicherheitsleitstelle optimal zu unterstützen. Die Messe IFSEC International in London vom 19. bis 21. Juni steht unter dem Motto „Wege zum Erreichen globaler Sicherheit". Die Besucher können sich am Stand-Nr. E110 über das Lösungsangebot im Bereich Gefahrenmanagement von Advancis informieren und die neuen Funktionalitäten von WinGuard testen.

HxGN Local veranstaltet vom 26. bis 27. Juni in der Kongresshalle am Zoo Leipzig die Anwenderkonferenz HxGN Local Safety & Infrastructure D-A-CH. Das Themenspektrum umfasst Einsatzleittechnologien, Lageinformations- und Stabsysteme, Netzinformationssysteme, geografische Informationssysteme und Server-/Cloud-Lösungen mit Geo-Bezug. WinGuard kann direkt mit Einsatzleitsystemen unter Einbindung von Geo-Informationsdaten verknüpft werden. Ziel der SicherheitsExpo in München vom 27. bis 28. Juni ist es, Sicherheitstechnik vorzustellen, die vor kriminellen Angriffen von innen und außen schützt. Hier sind die neuesten Entwicklungen u. a. in den Bereichen Zutrittskontrolle, Videoüberwachung, Leitstellen und Mobilfunk entscheidend. Am Stand Nr. D01 zeigt Advancis, wie die offene Softwareplattform WinGuard ein zuverlässiges Gefahrenmanagement für alle Branchen ermöglicht.

www.advancis.net ■

Audio- und I/O-Erweiterung für IP-Kameras

Sobald die Geräte der neuen Axis T61-Serie zwischen der Kamera und dem Switch installiert sind, können mit der Portcast-Funktion Audio- und I/O-Daten digital über das Netzwerkkabel zwischen der Kamera und der Schnittstelle übertragen werden. Mit der Axis T6101 und Axis T6112 Audio- und I/O-Schnittstelle kann eine Reihe beliebter Axis-Kameras, die selbst noch keine integrierte Audio- und I/O-Funktion aufweisen, nahtlos erweitert werden. Da die Kamera von der Audio- und I/O-Schnittstelle getrennt angeordnet ist, können die Kunden beides optimal anordnen: zum Beispiel eine kleine Kamera an einer diskreten Position und eine Audioerfassung näher an der überwachten Stelle. Mit zusätzlichem Zwei-Wege-Audio können die Kunden beispielsweise bei Vorfällen oder Ereignissen mithören oder Eindringlinge warnen. In Zukunft wird auch eine Audioanalyse beispielsweise zur Aggressionserkennung unterstützt.

www.axis.com ■

Türschließer im neuen Design

Die Optik eines Türschließers gewinnt bei der Kaufentscheidung zunehmend an Bedeutung. Mit einem neuen Look zollt Assa Abloy dieser Entwicklung Tribut. Abgerundete Kanten, edle Oberflächen und eine schmale Ziernut prägen das Erscheinungsbild des neuen Türschließer-Sortiments. In der Anmutung klar und zeitlos elegant lassen sich die Produkte nahtlos in praktisch jedes gestalterische Gesamtkonzept integrieren. Dank der vielfältigen Oberflächenausführungen und einer großen Farbpalette können Architekten und Planer optisch exakt auf die Tür abgestimmte Lösungen wählen. Ebenso Verlass ist auf die hohe Funktionalität und die verfügbaren Umweltproduktdeklarationen. In Kombination mit weiteren Produkten von Assa Abloy bieten die Türschließer im neuen Look nicht nur unzählige Möglichkeiten für viele Anwendungen, sondern vervollständigen Schließlösungen rund um die Tür durch ihr ansprechendes Design.

www.assaabloy.de ■

Eigenständig und doch vernetzt

G-SIM/Global ist die Weiterentwicklung von G-SIM, dem Sicherheits-Informations-Management von Geutebrück – nur, dass es sich über räumliche Grenzen hinwegsetzt. Mit G-SIM können komplexe Video-Systeme und Abläufe einfach verwaltet und bedient werden. Es bündelt und überblickt sämtliche Informationen und Daten der Geutebrück-Welt und aller angebundenen Drittsysteme. Unabhängige G-SIM Installationen werden zu einem großen Gesamtsystem miteinander verknüpft. Ausgelöste Alarme und notwendige Rechercheschen können zentral von jedem beliebigen Ort überprüft bzw. ausgeführt werden. User können sogar über Länder und Kontinente hinweg auf Kameras, Lagepläne oder Prozessdaten ihrer Anlagen zugreifen. Die hochsensiblen Systeme bleiben eigenständig, sind aber miteinander vernetzt. Der gleichzeitige Zugriff in die Setup-Oberfläche zur Optimierung bzw. Reduzierung der Konfigurationsdauer ist möglich. G-SIM/Global eignet sich für den flexiblen Einsatz im Security Bereich, in der Logistik oder im Katastrophenfall.

www.geutebrueck.com ■

IP-Router schützt Gebäudedaten mit KNX

Der neue i-bus KNX IP-Router Secure* (IPR/S 3.5.1) von ABB schützt KNX-Anlagen vor Cyberattacken und verbessert die Stabilität des KNX-Netzes. Um die Sicherheit des Industrieprotokolls KNX-Standard zu verbessern, verschlüsselt der Router die gesamte Kommunikation über das IP-Netz des Gebäudes und sichert auch die Inbetriebnahme. Dies mindert die Gefahr eines Angriffs über das IP-Netzwerk. Auf der Grundlage des Verschlüsselungsstandards ISO/IEC 18033-3 AES 128 bietet er höchstmögliche Sicherheit. Im Bereich Smart Building ist die Datensicherheit einer der Schlüsselfaktoren. Ein potentieller Angriff auf eine KNX-Anlage erfolgt mit hoher Wahrscheinlichkeit über das IP-Netzwerk. In Hotel- oder Bürogebäuden sind die Bedrohungen meist auf unerlaubten Zugriff auf das IP-Netzwerk zurückzuführen. Die Quellen für diese Bedrohung können sowohl innerhalb des Gebäudes (Intranet) als auch außerhalb (Internet) liegen und erheblichen, kostspieligen Schaden anrichten.

www.abb.de ■

Jetzt mit Pin-Code-Einbindung

Simons Voss hat sein System „Mobile Key" weiterentwickelt. Mit der Einbindung der neuen Pin-Code-Tastatur Online für Mobile Key kann die Tastatur mit integrierter Vernetzung nicht nur über das Netzwerk programmiert werden. Ab dem 3. Quartal dieses Jahres können die PINs auch online geändert und verwaltet werden. Der Funktionsumfang umfasst: Drei Benutzer-PINs; vier- bis achtstelliger Code; Programmierung über Mobile Key Online; Verwaltung der Benutzer-PINs über Mobile Key Online. Die Eingabe der richtigen PIN löst eine Fernöffnung einer vernetzten Schließung aus. Den PINs kann wie bei Transpondern ein Zeitplan hinterlegt werden. Außerdem: Kabelfreie und batteriebetriebene Pin-Code-Tastatur mit extrem langer Batterielebensdauer (bis zu zwölf Jahre Stand-by); für den Innen- und Außenbereich (IP 65). Die Einbindung der Tastatur erfolgt über das Hinzufügen eines neuen Schlüssels, wie bei der aktuellen Tastatur oder gleich über die bekannte Netzwerkverwaltung. Bei der Anlage der Pin-Code-Tastatur durch die Auswahl „Online-Version" erscheint ein Eingabebereich für die auf der Verpackung aufgedruckte Chip-ID. In diesem Schritt wird auch gleich die zugewiesene Schließung (muss vernetzt sein!) definiert. Anschließend erfolgt die Vernetzung über die bekannte Netzwerkverwaltung unter Netzwerk. Neben den Auswahlmöglichkeiten Smartbridge und Schlösser findet sich nun dort auch der Abschnitt Pin-Code-Tastatur.

www.simons-voss.com ■

Server mit vorinstallierter VMS

Systemintegratoren können jetzt die Wisenet Wave Videomanagementsoftware (VMS) von Hanwha Techwin praktisch vorinstalliert auf ausgewählten hochleistungsfähigen BCDVideo Servern bestellen. Wisenet Wave VMS-Server basieren auf BCDVideos aktuellsten Apollo- und Neptune-Serien „Powered by Dell EMC". Beide Serien kommen mit der aktuellsten Generation an Intel Xeon-Prozessoren, mit Dual-RAID, redundanter Stromversorgung, sicherem globalen Fern-Systemmanagement und einer fünfjährigen Vor-Ort-Gewährleistung. Für erweiterte Datensicherheit umfasst die Gewährleistung darüber hinaus die Retention von Datenmedien. Ersetzte Festplatten werden auf dem Betriebsgelände für die sachgerechte Entsorgung durch den Kunden gehalten. Alle Server mit vorinstallierter Wisenet Wave VMS sind ausgestattet mit hochleistungsfähigen Intel Vierkernprozessoren für eine schnelle, leistungsstarke und zuverlässige Videoverarbeitung für einsatzkritische Anwendungen.

www.hanwha-security.eu/de ■

Wandleser für den Außenbereich

Elektronische Lesegeräte müssen gerade im Außenbereich teils hohen Belastungen durch starke Witterungseinflüsse standhalten. Uhlmann & Zacher hat daher den wetterbeständigen Wandleser CX6134 speziell für den Outdoor-Einsatz entwickelt. Er ist staub- und wasserdicht nach Schutzklasse IP67 und somit geschützt vor eindringendem Wasser bis hin zu zeitweiligem Untertauchen. Durch die hohe Schutzklasse bietet der Wandleser einen zuverlässigen Betrieb im Außenbereich. Er ist daher speziell geeignet für die Steuerung von Außenanlagen wie Schranken, elektrischen Tür- und Torsystemen und Drehkreuzanlagen. Der CX6134 kann sowohl offline als auch online an das System angeschlossen werden. Durch die Online-Anbindung kann der neue Wandleser für den Außenbereich auch als Online-Programmierterminal CX6554 genutzt werden. Hierdurch ist es möglich Berechtigungen, die beispielsweise nur tageweise gelten, über den Wandleser auf den Transponder zu schreiben.

Für den Einsatz im ungesicherten Außenbereich kann der Wandleser in Verbindung mit einem Sicherheitsrelaismodul im Innenbereich als Sicherheitsvariante eingesetzt werden. Außerdem ermöglicht die Verbindung mit einem Fernmodul die Verwendung des Produkts zur Ansteuerung von z. B. Aufzügen, Postfächern und Umkleideanlagen. Durch die optische und akustische Signalisierung ist eine intuitive Bedienung möglich. Als Identifikationstechnologien stehen Mifare und EM/Hitag zur Verfügung. Der neue Outdoor-Wandleser CX6134 wird inklusive anthrazitfarbenem Aufputz-Gehäuse geliefert und ist mit allen Produkten von U&Z kombinierbar.

www.UundZ.de ■

Vielseitige elektronische Zutrittslösungen

Auf der SicherheitsExpo im MOC München präsentiert Salto Systems (Halle 3, Stand B15) erstmals die Version 5.0 seiner Managementsoftware ProAccess Space. Diese punktet mit einer Vielzahl an neuen Funktionen. Dazu zählen u. a. ein neuer Report über unbenutzte Zutrittspunkte, neue Auslöser für das Add-on „Alarm Events" auf Basis von Ereignissen aus den Türsteuerungen, mehrstufige Warnmeldungen, wenn sich die Blacklist-Einträge dem Limit nähern, sowie Vereinfachungen bei der Vergabe von mobilen Schlüsseln und der Nutzerverwaltung. Weiterhin ist BlueNet Saltos neue Wireless-Technologie für die Funkvernetzung von kabellosen Türkomponenten. Sie nutzt die Bluetooth-Schnittstelle zur Kommunikation. Der Aufbau der Infrastruktur gleicht jenem der bisherigen Wireless-Technologie Salto RFnet. Beide Technologien, RFnet und BlueNet, können in einer Installation parallel betrieben werden. Die JustIn Mobile App von Salto unterstützt in der neuesten Version auch HCE (Host Card Emulation). Das Verfahren ist für die Kommunikation über NFC (Near Field Communication) relevant. Damit können mit der gleichen App sowohl NFC- als auch BLE-kompatible Salto Türkomponenten angesprochen werden.

www.saltosystems.de ■

Vectorprofile mit hoher Manipulationssicherheit

Assa Abloy Sicherheitstechnik hat neue Schließanlagenprofile für seine Sonderklasse SK6 auf den Markt gebracht. Die Versionen Vectorprofil Rippe und Vectorprofil Rippe Extra der Marke Ikon sind technisch ausgefeilte Weiterentwicklungen der bisherigen Vectorprofile: Durch ihre besondere Konstruktion sind die Zylinder außerordentlich schwer zu manipulieren und gewährleisten einen besonders hohen Einbruchschutz. Mit den neuen Profilen bietet Assa Abloy ein hochwertiges und patentiertes Schlüsselsystem, das sich für den Einsatz in komplexen Schließanlagen größerer und kleinerer Objekte eignet. Auch das neue System verfügt wieder über zwei Sicherheitsstufen. Sie lassen sich in einer Schließanlage miteinander kombinieren, denn Schlüssel der zweiten Sicherheitsstufe schließen auch Zylinder der ersten Stufe. Beide Profile zeichnen sich gegenüber herkömmlichen Schlüsselprofilen durch eine sehr hohe Manipulationssicherheit gegen Aufsperr- und Abtastwerkzeuge sowie unautorisierte Nachschlüssel aus.

www.assaabloy.de ■

„Smart-Bedienung“

Von Abi-Sicherheitssysteme steht die erweiterte Version der MCVisu.cloud-App im Apple-App-Store (iOS) und Google-Play-Store (Android) zum kostenlosen Download bereit. Mit der App werden Smartphones und Tablets, wie z. B. iPad mini, zum „Smart-Bedienteil“ für die Bedienung der ABI-MC-1500-Gefahrenmeldeanlage von zu Hause oder unterwegs. Die einfache und intuitive Menüführung ermöglicht jederzeit das Anzeigen und Bedienen der Gefahrenmeldeanlage, zudem stehen umfangreiche Funktionen für Smart-Home-Anwendungen zur Verfügung. Die MCVisu.cloud-App bietet die Möglichkeit, häufig benötigte Funktionen als Favoriten zu definieren. Mit nur einer Displayberührung startet die App sofort im Favoritenmenü. Dies ermöglicht das schnelle und unkomplizierte Anzeigen und Bedienen.

www.abi-sicherheitssysteme.de ■

Upgrade für Zentralen

Neben der kompletten Erneuerung der Gefahrenmeldeanlage bietet ABI-Sicherheitssysteme ein Upgrade für die Zentralen MC 1100, MC 1200-S und MC 1200-M an. Das Gehäuse und das Netzladeteil (MC 1200-M) können in der Regel weiter verwendet werden. Die Anforderungen der Nutzer an Komfort und Funktionalität der Systeme haben sich weiterentwickelt. So rückt z.B. die Nutzung von Smartphone und Tablet PC für die Bedienung der Gefahrenmeldeanlagen immer mehr in den Vordergrund. Zur Nutzung neuer Funktionalitäten und/oder des Smartphones zur Bedienung ist ein Austausch der Zentrale und deren Hauptkomponenten oder ein Upgrade der vorhandenen Anlage notwendig. Durch Nutzung der vorhandenen Verkabelung können schnell und preiswert Anlagen getauscht oder durch ein kostengünstiges Upgrade für die gestiegenen Anforderungen „fit“ gemacht werden.

www.abi-sicherheitssysteme.de ■

Zertifizierungstraining für Audio-over-IP-Technik

Um professionellen Anwendern einen vollständigen Überblick über die umfassenden Features und komfortablen Anwendungsmöglichkeiten von Audio-over-IP zu verschaffen, veranstaltete Monacor in Kooperation mit Audinate ein dreitägiges Dante-Zertifizierungstraining. Das Schulungsprogramm richtete sich sowohl an Einsteiger, die erste Basiskenntnisse in der Audio-over-IP-Technik erwerben wollten, als auch an fortgeschrittene und erfahrene Anwender.

www.monacor-international.de ■

Aktuelles Service-Release

Digivod stellt das Release 3.5.0.40071 zur Verfügung. Unter anderem wurden die 360°-Kameras des Herstellers Oncam – ein unabhängiges und spezialisiertes IP-Video- und Technologieunternehmen – implementiert. Oncams einziger Fokus liegt auf 360°-Smart-IP-Video – in Zusammenarbeit mit Partnern, hochwertige Lösungen für Kunden bereitzustellen, die die preisgekrönte Technologie von Oncam nutzen. Das Unternehmen verfügt über fundiertes Branchenwissen in Kombination mit Spezialkenntnissen in den Bereichen Gesundheitswesen, Einzelhandel, Transport, See- und Häfen, Banken, Casinos und Gastgewerbe. Neben dieser Integration beinhaltet das aktuelle Service-Release wie gewohnt Fehlerbehebungen und Performanceverbesserungen.

www.digivod.de ■

Flexible Schließlösungen

Auf der diesjährigen SicherheitsExpo vom 27. bis 28. Juni im Münchener Veranstaltungscenter MOC präsentiert Uhlmann & Zacher sein vielfältiges Produktsortiment im Bereich der elektronischen Zutrittskontrolle (Halle 3, Stand A06).

Auf diesem Branchentreff zeigt das Unternehmen seine umfassende Produktpalette aus der Welt der elektronischen Schließsysteme. Ein besonderer Fokus liegt hierbei auf dem elektronischen Türdrücker CX6172 und dem elektronischen Türbeschlag CX6174. Die einzigartige Bauweise dieser Produktreihe, bei der die gesamte Elektronik, Mechanik, Stromversorgung und LED-Signalisierung auf kleinstem Raum im Türdrücker verbaut ist, wurde bereits mehrfach prämiert. Das Portfolio umfasst eine Vielzahl an Varianten, beispielsweise unterschiedliche Beschläge und Rosetten, die Auswahl verschiedener Drückerformen, Versionen für den Einsatz im Außenbereich und Varianten für die Montage in Feuerschutz- und Rauchschutztüren sowie in Notausgangsverschlüsse. Durch das minimalistische Design in zeitloser Edelstahl-Optik lassen sich der elektronische Türdrücker und Türbeschlag in nahezu jedes Interieur-Design integrieren. Die vielfältigen Produktvariationen bieten eine große Flexibilität für die Anwendung in den unterschiedlichsten Objekten.

www.UundZ.de ■

Gira-Neuheiten auf der Light+Building

Als Komplettanbieter intelligenter Systemlösungen für die Gebäudesteuerung stellte Gira auf der Light+Building 2018 zahlreiche Neuheiten vor – Produkte und Lösungen rund ums Smart Home, aber auch zu den Themen Alarm und Sicherheit. Beispiel: Sicherer Fernzugriff mit Gira S1. Wer heute ein Smart Home plant oder baut, will es von unterwegs aus einsehen und steuern können, etwa Kamerabilder überprüfen, die Heizung einschalten oder Jalousien herablassen. Das Problem dabei: Unbefugte könnten diesen Fernzugriff ebenfalls nutzen. Für kritische Nutzer ist das der entscheidende Vorbehalt gegenüber smarten Technologien. Doch dieser Einwand gilt nicht länger, denn mit dem Fernzugriffsmodul S1 kann Gira die Kommunikation zuverlässig verschlüsseln. Mit dem Gira S1 ist erstmals eine geschützte Fernwartung und Fernbedienung des gesamten KNX Smart Homes möglich. Zudem erlaubt das Modul den sicheren Fernzugriff auf webbasierte Visualisierungen. Umgekehrt lassen sich Vorgänge im Gebäude direkt aufs Smartphone übertragen, wenn etwa der Rauchmelder auslöst. Besonders erfreulich für den Elektromeister: Das Fernzugriffsmodul Gira S1 lässt sich sehr einfach und intuitiv in Betrieb nehmen. Zudem ist sichergestellt, dass bei Verwendung von zugehöriger App und Fernzugriffe die strengen deutschen Datenschutzstandards gewahrt sind.

www.gira.de ■

Eindämmung der Einbruchkriminalität

In einer durch die Funke Mediengruppe in Auftrag gegebenen Umfrage durch Emnid wurde danach gefragt, welche Themen die neue Bundesregierung aus Sicht der Deutschen mit höchster Priorität angehen sollte. Dabei wurde die „Eindämmung der Einbruchkriminalität" mit 91 % als zweitwichtigstes Thema benannt – nach „Sicherung der Rente" (95 %). Da es aktuell keine verpflichtenden Richtlinien für den Einbau von Sicherheitstechnik bei Neubauten oder im Bestand gibt, ist also die Initiative von Eigentümern gefordert, wenn für das Plus an Sicherheit gesorgt werden soll. Ganz alleine lässt der Staat seine Bürger bei dem Thema dennoch nicht: Wer sich für den Einbau von Sicherheitstechnik durch einen Fachmann entscheidet, der erhält aktuell bis zu 20 % Zuschuss vom Staat. Die KfW-Förderbank unterstützt Eigentümer und Mieter beim Einbau von Sicherheitstechnik mit der Übernahme von 20 % der Kosten bis 1.000 Euro. Darüberhinausgehende Investitionen in Sicherheitstechnik werden bis zu einer Summe von 15.000 Euro mit 10 % bezuschusst.

Hierzu bietet der Markt ein umfangreiches Sortiment an Sicherheitslösungen wie z. B. Sicherungen an Fenster und Türen. Dabei gilt – auch aufgrund der Empfehlungspraxis der Polizei – zertifizierte mechanische Sicherungen bilden die Basis eines sinnvollen Einbruchschutzes. Der Trend geht dabei immer mehr zu vernetzten Lösungen. Vor allem das Thema Mechatronik, wo massive Schlösser mit intelligenter Elektronik ausgestattet und zu Alarmsystemen vernetzt werden, ist hier zu nennen. Systeme, wie z. B. die Funkalarmanlage Secvest von Abus, bieten ein Plus an Funktionalität und vereinen die Bereiche Mechanik, Alarm, Video, Brandschutz sowie Notfall in einer Lösung.

www.abus.com ■

Führerscheinkontrolle am Terminal

Bei der Dienstwagenüberlassung an Mitarbeiter ist der Arbeitgeber zur regelmäßigen Führerscheinkontrolle verpflichtet. Manuelle Kontrollen bedeuten einen erheblichen Aufwand, welcher bei der elektronischen Führerscheinkontrolle von IntraKey auf ein Minimum reduziert wird und maximale Rechtssicherheit schafft. Auf dem Führerschein wird ein fälschungs- und manipulationssicheres RFID-Label angebracht, welches sich rückstandsfrei auch wieder entfernen lässt. Der Fahrer wird zyklisch per E-mail, Smartphone-App oder am Zeiterfassungsterminal an seinen Kontrolltermin erinnert und kann am touch.ON-Terminal selbstständig nachweisen, dass er im Besitz seines Führerscheins ist. Die Nachweise werden revisionssicher im System gespeichert. Bleiben Nachweise aus, erfolgt eine Meldung an den Verantwortlichen. Die Führerscheinkontrolle kann in ein bestehendes Zeiterfassungssystem integriert oder als Standalone-Lösung verwendet werden.

www.intrakey.de ■

Smarte Haustür ohne Umbau

Der IP-Konverter DoorBird D301 von Bird Home Automation verwandelt herkömmliche Türsprechanlagen in IP-Türsprechanlagen. So können Bewohner die Vorteile einer intelligenten Türsprechanlage nutzen, ohne das vorhandene analoge Gerät tauschen zu müssen. Die mehrfach ausgezeichneten Produkte des Berliner Unternehmens ermöglichen dem Nutzer mit jedem, der vor seiner Hauseingangstür steht, via Smartphone oder Tablet zu kommunizieren. Wenn es klingelt, erhält der Nutzer eine Push-Mitteilung. So kann er sofort mit dem Besucher sprechen und ihn auch sehen, abhängig vom Modell und sofern die vorhandene Türsprechanlage mit einer Kamera ausgestattet ist. Dank der guten Tonqualität ist es für den Besucher nicht hörbar, ob der Bewohner tatsächlich zu Hause ist oder nicht. Dieser Sicherheitsaspekt ist für viele Menschen besonders wichtig. Per App kann der Nutzer die Hauseingangstür oder das Gartentor öffnen.

www.doorbird.com ■

Produktkatalog für Netzwerktechnik

Als Print- oder Downloadversion ist der neue Katalog Netzwerktechnik 2018 von EFB-Elektronik verfügbar. Auf über 450 Seiten wird das individuell zugeschnittene Produktsortiment im Bereich Lichtwellenleiter, Kupferverkabelung, Schranksysteme, Multimedia sowie Aktive Komponenten vorgestellt. Die Eigenmarke Infralan wird in einem eigenen Kapitel präsentiert. So sind alle Informationen und Produkte rund um das ganzheitliche System gebündelt im Katalog. Zudem wird eine Vielzahl neuer Produkte angeboten, wie z. B.: IP68-Buchsengehäuse für Keystone-Module und Bajonettverschluss; FTTH IP65 Anschlussbox 8 Ports; 19" Netzwerkschrank 42HE 800x1.000, IP55.

www.efb-elektronik.de ■

Fachseminar zum Parkraum-Management

Parkhäuser rufen je nach Standort und Modernität bei Autofahrern unterschiedliche Gefühle hervor. Insbesondere bei älteren Parkhäusern sind die Betreiber dazu aufgerufen, veraltete Konzepte und Ausstattungen hinsichtlich Beleuchtung, Brandmelde- und Videosicherheitsanlagen zu überdenken und auf die heutigen Anforderungen anzupassen. Auch der vermehrte Bedarf an Ladesäulen für Elektrofahrzeuge bedeutet ein Umdenken im Parkraum-Management. Das von Automatic Systems gemeinsam mit Axis und Securiton durchgeführte kostenlose Fachseminar „Intelligentes Parkraum-Management" am 21. Juni 2018 im Staatsbad Salzuflen widmet sich genau diesen Themen und ist auf die Anforderungen von Parkhausbetreibern, Security-Consultants sowie Planungs- und Ingenieurbüros zugeschnitten.

www.automatic-systems.com ■

Plug-and-Play-Videosicherheitslösung

Gerade im Mittelstand sind eine schnelle Installation und ein reibungsloser Betrieb der Videosicherheitstechnik wichtig. Für diese Zielgruppe bietet Dallmeier die VideoNetBox 3, mit der sich schnell und einfach eine komplette Videosicherheitslösung für bis zu 16 HD-Video-Streams aufbauen lässt. Die Appliance kombiniert die bewährte Smavia Aufzeichnungs- und Analysesoftware mit einer kompakten, lüfterlosen und energieeffizienten Server-Hardware. Mit der VideoNetBox 3 können z. B. Geschäfte, Tankstellen oder kleine Produktionsbetriebe schnell und einfach Lösungen basierend auf den bewährten Dallmeier-Kameras abbilden. Auch die führenden Multifocal-Panomera-Systeme des Herstellers werden unterstützt. Umfassende Analyse- und Betriebsfunktionen erfüllen die Sicherheitsziele des Kunden beim Aufbau auch umfassender Sicherheitslösungen. Der „Plug-and-Play"-Ansatz und hohe Energieeffizienz sparen Kosten und Aufwand. Falls gewünscht, lassen sich ebenso Kameras von Drittherstellern über ONVIF integrieren. Hardware-seitig sorgen bestens abgestimmte Komponenten für geringen Platzbedarf, minimale Geräuschentwicklung und eine hervorragende passive Kühlung bei maximal 15 Watt Leistungsaufnahme.

www.dallmeier.com ■

VIDEOTECHNIK

Koaxiale Vielfalt

Technologisch vielseitige Multisignalprodukte von Eneo

Unter dem Seriennamen „Eneo Coaxize“ bietet Eneo Facherrichtern und Betreibern die nötige Bandbreite an Produkten für HD-Analog- oder Hybridlösungen – Videoqualität, Robustheit und Wirtschaftlichkeit inklusive.

HD-TVI, CVI und AHD haben sich im Videosicherheitsmarkt etabliert. Gleiches gilt für digitales HD-SDI und EX-SDI. Der große gemeinsame Vorteil dieser Technologien: sie können mit den hohen Videoauflösungen von IP mithalten und erlauben zugleich die Weiterverwendung der bestehenden Koaxialverkabelung. Kein kleiner Vorteil angesichts der vielen Tausend Kilometer Koaxialkabel, die nach wie vor weltweit verlegt sind. Zumal sie – über ihre hohe Wirtschaftlichkeit und geringe Fehleranfälligkeit hinaus – weitere Vorteile zu bieten haben, allen voran die hohen Übertragungsreichweiten von bis zu 500m, die je nach Qualität der Bestandsverkabelung mit oder ohne Signalverstärker möglich sind.
Hinzu kommen Null-Latenz und artefaktfreie, äußerst detailreiche Videobilder. Das empfiehlt sie für Anwendungen, in denen Echtzeitaufnahmen in HD oder Full-HD von missionskritischer Bedeutung sind, etwa in Kasinos oder Banken. Das macht sie aber auch für diejenigen Endkunden attraktiv, die sich aufgrund von Nachhaltigkeitserwägungen für die Möglichkeit einer umweltfreundlichen, weil ressourcenschonenden Modernisierung ihres Videosicherheitssystems interessieren. Facherrichter wiederum wissen zu schätzen, dass für die Installation keine Netzwerkkenntnisse erforderlich sind und die Montage im komfortablen Plug-and-Play-Verfahren möglich ist.

Vielfältige Signaloptionen

Bei Eneo begleitet man diese Entwicklung seit 2012. Nach der Einführung der ersten HD-SDI-Kameras und Rekorder erfolgte 2015 die Einführung der Produktfamilie Eneo Coaxize, in der zunächst AHD- und HD-TVI-Produkte vertreten waren. Heute handelt es sich durchgängig um Multisignalkameras und -rekorder, die bis zu sechs verschiedene Signalformate unterstützen, vom klassischen Analogsignal über HD-TVI, AHD,

Eneo Coaxize: Die Multisignalkameras und -Rekorder unterstützen bis zu sechs verschiedene Signalformate, vom klassischen Analogsignal über HD-TVI, AHD und CVI bis hin zu HD-SDI und EX-SDI

Auch die für die Videoaufzeichnung erforderlichen Rekorder finden sich im Portfolio – die Kanäle können zusätzlich zu HD-TVI, CVI, AHD, FBAS, HD-SDI und EX-SDI auch mit IP-Signalen belegt werden

und CVI bis hin zu HD-SDI und EX-SDI. Dies bietet Betreibern und Anwendern eine große Flexibilität für die Modernisierung von Bestandssystemen.

Auflösungen von bis zu 4MP

Auch in Sachen Videoauflösung haben sich die analogen HD-Kameras enorm weiterentwickelt. Modelle wie die Autofokus-Zoom-Domes MPD-64A0003P0A und MPD-74A0003M0A oder die ebenfalls mit Autofokus-Zoom-Objektiv ausgestattete Bullet-Kamera MCB-64A0003M0A liefern maximale Auflösungen von 4 MP in Echtzeit und eignen sich damit insbesondere für Anwendungen, in denen detailreiche Videobilder aus forensischen Gründen missionskritisch sind. Das Spektrum von Eneo Coaxize reicht von extrem robusten Modellen für den Innen- und Außeneinsatz in industriellen Sicherheitsumgebungen bis hin zu Kameras, die ausschließlich für den Betrieb in Gebäuden ausgelegt sind, etwa für Videoüberwachungsanwendungen im Einzelhandel.

Modelle mit integrierter Anschlusslösung

Unter den neuesten Multisignalmodellen verdienen zwei Bullet-Kameras vom Typ Eneo Candid, die mit einer integrierten Anschlusslösung ausgestattet sind, besondere Erwähnung. Hier werden die Vorteile der Multisignaltechnologie durch eine Design-Innovation im Zeichen von Errichterfreundlichkeit ergänzt. Die Anschlussbox, die bislang nur als optionales Zubehör unter dem Namen Eneo Easy Installation Box erhältlich war, ist hier mit Kamera und Wandarm zu einer kompakten Einheit verbunden, die sich noch schneller und bequemer montieren und anschließen lässt als die Kombination aus Kamera und separater Anschlussbox. So bietet die Multisignalkamera MCB-64A0003M0A über den Zeitvorteil hinaus eine Reihe von Merkmalen, durch die sich die Leistungsfähigkeit koaxbasierter Videosicherheitssysteme deutlich erhöht.

Die Kamera kommt mit einem 1/2,9" 6,64 Megapixel Sony Starvis CMOS-Sensor und liefert eine maximale Videoauflösung von 4 MP. Das Autofokus-Zoom-Objektiv (3,2–9mm) ist mit einem dreifachen optischen Zoom ausgestattet. Die DOL-WDR-Funktion sorgt durch einen dreifachen Scan der Bilder für optimierte Bildqualität auch unter sehr schwierigen Lichtverhältnissen. Darüber hinaus verfügt die MCB-64A0003M0A über Point-of-Interest- und Smart-Motion-Zoom, der festinstallierten Kameras erlaubt, einen optischen Schwenk auszuführen, um relevante Objekte oder Personen an beliebiger Position des Bildbereiches zu vergrößern.

Bei MCB-72M2712M0A handelt es sich um eine Full-HD-Kamera (1920 x 1080 Pixel). Auch bei dieser Bullet-Kamera können Anwender unter HD-TVI, AHD, CVI, FBAS sowie EX-SDI und HD-SDI wählen. Das motorisierte Objektiv hat eine Brennweite von 2,7–12mm. Die Kamera unterstützt Privatzonenmaskierung, ist mit Defog (automatische Korrektur atmosphärisch bedingter Bildbeeinträchtigungen) ausgestattet und verfügt über einen integrierten Bewegungsmelder.

Hybridlösungen mit IP-fähigen Multisignalrekordern möglich

Auch die für die Videoaufzeichnung erforderlichen Rekorder finden sich im Portfolio. Aktuell stehen mit MER-24R040200A, MER-24R080200A und MER-34R160300A 4-, 8- und 16-Kanal-Multisignalrekorder bereit, deren Kanäle zusätzlich zu HD-TVI, CVI, AHD, FBAS, HD-SDI und EX-SDI auch mit IP-Signalen belegt werden können und die für den Mischbetrieb ausgelegt sind. Mit den Produkten können also auch ohne Probleme hybride Systeme aufgebaut werden, die Analog- und Netzwerktechnologie kombinieren. Die Steuerungs-Software kann bis zu 144 Kameras simultan verbinden und ist für den Multimonitorbetrieb geeignet. ■

Kontakt

Videor E. Hartig GmbH
Rödermark
Tel.: +49 6074 888 0
info@videor.com
www.eneo-security.com

Kameras mit neuen Möglichkeiten für Sicherungssysteme. Das System erstellt automatisch eine einminütige Aufzeichnung jedes durch die Alarmanlage Jablotron 100 erfassten Ereignisses und bietet dadurch einen sofortigen Überblick ▶

▲ Kameras zur Videoverifikation: Die JI-111c mit Dome-Objektiv …

… und das Modell JI-112C mit Bullet-Objektiv ▼

Die EPS Vertriebs GmbH und Jablotron stellen IP-Kameras zur Videoverifikation vor, die mit dem Alarmsystem Jablotron 100 kompatibel sind. Die einfach und schnell installierbaren Kameras dienen der automatischen Aufzeichnung jedes Ereignisses im Objekt. Mit „My Jablotron" kann der Nutzer alles überprüfen, einsehen und Fehlalarme eliminieren.

ALARMIERUNG

Alarm in Farbe

Firmengebäude sichern, Wochenendhaus schützen: Videoverifikation für Alarmsystem

Zusammen mit der Erweiterung der Smartphones oder Tablets, die zunehmend auch zur Sicherung oder Steuerung des Haushalts eingesetzt werden, wächst auch der Bedarf an der visuellen Kontrolle des Geschehens. Viele Hersteller haben ihr Angebot diesem Aspekt angepasst, sodass wir z.B. auf dem Handy-Display überprüfen können, wer gerade vor der Tür unseres Hauses steht. Jablotron geht noch einen Schritt weiter – mit Kameras zur Videoverifikation, die sich mit einer Alarmanalage verbinden lassen. Die Modelle JI-111c (mit Dome-Objektiv) und JI-112C (mit Bullet-Objektiv) sind mit dem Alarmsystem Jablortron 100 voll kompatibel, sodass sie den Benut-

Kamera	Pixelzahl	Auflösung	Erfassungs-winkel	IR-Zusatzlicht Reichweite	Sensor	Stromversorgung	Kommunikations-schnittstelle
JI-111C	2 MPx	Full HD	115°	30 m	1/2,8 CMOS	PoE (802.3af)/12V	RJ-45 10M/100M Ethernet
JI-112C	2 MPx	Full HD	90°	50 m	1/2,8 CMOS	PoE (802.3af)/12V	RJ-45 10M/100M Ethernet

Spezifikation neuer IP-Kameras zur Videoverifikation

zern anstatt einer bloßen Bildkontrolle gleich eine komplexe Lösung für die Sicherung der Haushalte oder Firmengebäude bieten.

Wie funktioniert das System?

Melder, Sensoren oder Kameras überwachen die Situation in den bewachten Räumen und liefern dem Eigentümer Echtzeit-Informationen in Form von SMS-Benachrichtigungen oder über die Anwendung My Jablotron. Bei einem Alarmereignis informieren die Kameras den Benutzer und senden ihm zusätzlich eine einminütige Aufzeichnung, in der erfasst ist, was vor dem Alarm und unmittelbar nach dem Alarm passiert ist.

Die Videoaufnahme ist nur die Vorstufe für eine Überwachung und Sicherung von Gebäuden. Nicht weniger wichtig ist auch, wann die Aufnahme den Benutzer erreicht, wie er sie behandeln kann und wie er sie zeitsparend sichten kann. Außerdem muss sichergestellt sein, dass es immer genügend Speicherkapazität gibt, damit die ganzen Bemühungen um den Vermögensschutz überhaupt sinnvoll sind. Die Antworten darauf sind in Form dreier Schwerpunktfunktionen der Kameras gelöst: Videosequenz, Aufzeichnung und Livestream (Live-Übertragung).

Livestream bietet eine Echtzeitübertragung des Bildes aus dem überwachten Ort. Der Benutzer kann darauf über jedes Smart-Gerät zugreifen. Er kann somit das Geschehen im Objekt in der Echtzeit bequem überprüfen und sich vergewissern, dass sich keine unbefugten Personen im Objekt befinden, die Leuchten ausgeschaltet sind oder dass die Kinder sicher zu Hause angekommen sind.

Wenn der Benutzer beispielsweise zum Wochenendhaus oder in den Urlaub fährt oder er die Firma über das Wochenende überwachen will, kann er den Extra-Service der drei- oder siebentägigen Aufzeichnung in Anspruch nehmen. Dadurch wird das Geschehen bei seiner Abwesenheit aufgenommen und er kann jeden beliebigen Zeitpunkt der Aufzeichnung einsehen.

Die Funktion Videosequenz bietet eine einminütige Aufnahme, die aus dreißig Sekunden des überwachten Bereichs vor und nach der Alarmauslösung, dem Unscharfschalten des Objektes usw. besteht. Der Benutzer hat sofort den Überblick über die Ursache der Alarmauslösung und die darauffolgenden Ereignisse, ohne das Telefon ständig beobachten zu müssen - das System macht den Benutzer automatisch aufmerksam, sobald etwas passiert. Die Aufzeichnung ist von jedem beliebigen Ort aus im Smartphone oder über die Web-Schnittstelle in der Anwendung My Jablotron verfügbar. Alle Informationen sind also übersichtlich und an einer Stelle verfügbar.

Moderner Speicherplatz in der Cloud

Ein weiterer Vorteil liegt darin, dass die Kamera, und somit auch der aufgenommene Bereich, von der Aufzeichnung physisch abgetrennt ist. Selbst bei einem Angriff des Täters auf das Aufzeichnungsgerät wird die Aufzeichnung nicht beschädigt, weil sie in der Cloud an einem sicheren Ort aufbewahrt wird. Die Kameras nutzen die eigene Jablotron-Cloud als Speicherplatz, der für den Benutzer über ein beliebiges Gerät – Computer, Notebook, Tablet oder Smartphone – zugänglich ist. Er kann immer überprüfen, was durch die Kamera gerade aufgenommen wird, oder sich die bereits aufgenommenen Ereignisse ansehen. Alle Daten sind zudem verschlüsselt, wodurch der Schutz vor ihrem Missbrauch oder Vernichtung sichergestellt ist.

Durch eine Benachrichtigung über den Verlust der Verbindung weiß der Benutzer sofort, dass der Schutz nicht hundertprozentig ist und dass die Verbindung wiederhergestellt werden muss.

**Besuchen Sie die EPS-Schulungen und erfahren Sie alle Details zu der neuen Videoverifizierung und Jablotron 100.
Die EPS Schulungs-Akademie bietet folgende Termine an (siehe QR-Code oder Link in Browser eingeben):**

https://bit.ly/2Iu9x0N

Anbindung an Notrufserviceleitstelle

Für die Inbetriebsetzung der schnell und einfach zu installierenden Kameras braucht der Errichter keine speziellen Erfahrungen oder teuren Schulungen. Die Kameras werden zusammen mit der Halterung und PoE (Stromversorgung über Datenkabel) geliefert; benötigt werden nur Werkzeuge zum Befestigen der Kamera und ein Smartphone mit der Anwendung My Company.

Ebenso schnell und einfach ist die Anbindung an eine Notrufserviceleitstelle, die für das Überwachen des Objektes und die Hilfe bei einem außerordentlichen Ereignis rund um die Uhr sorgt. Geschulte Mitarbeiter prüfen bei einem Alarm die Lage im Objekt visuell und kontaktieren den Eigentümer. Bei Bedarf senden Sie ein Einsatzteam ins Objekt unverzüglich und benachrichtigen die Polizei.

Full-HD und Nachtsichtmodus mit IR-Zusatzlicht

Beide Kameramodelle nehmen das Farbvideo mit HD- oder Full-HD-Qualität mit der Auflösung 1920*1080 Bildpunkte auf. Bei schlechten Lichtverhältnissen wechseln sie zum Nachtsichtmodus, in dem sie das Infrarot-Zusatzlicht mit 12 IR-LEDs mit maximaler Reichweite von 30 bis 50 Meter nutzen. Die Kameraobjektive verfügen über einen Erfassungswinkel von 90° bis 115°, sind für den Außenbereich vorgesehen und erfüllen die Schutzart IP67. Der erste Typ JI-111C (DOME) verfügt über die Abmessungen 111 x 111 x 82 mm, der zweite Typ JI-112C (BULLET) dann 300 x 90 x 90 mm. ■

Kontakt

EPS Vertriebs GmbH
Havixbeck
Tel.: 02507 98750-14
ko@eps-vertrieb.de
www.eps-vertrieb.de

Hinter den Kulissen des Freizeitpark Puy du Fou sorgt Genetecs Security Center für Sicherheit

VIDEOMANAGEMENT

Historische Themen, aktuelle Sicherheit

Themenpark verbessert Sicherheit und Service mit Genetec Security Center

Der Freizeitpark Puy du Fou liegt im Westen Frankreichs und ist mit jährlich über zwei Millionen Besuchern der zweitgrößte Themenpark des Landes – nach dem Disneyland Paris. Im Jahre 1978 startete Puy du Fou mit nur einer Show. Heute erweckt der Park über 26 historische Ereignisse zum Leben. Allein im Rahmen der Hauptveranstaltung kommen 1.200 Schauspieler, mehrere Hundert Pferde und 800 Feuerwerkskörper auf der größten Bühne der Welt zum Einsatz. Hinter den Kulissen sorgt das Team für reibungslose Übergänge und eine sichere Show.

Puy du Fou fördert Kultur der Exzellenz mit Security Center

Eine einfach zu bedienende Plattform ermöglicht es Nutzern, effektiver zu arbeiten. Diese Erfahrung machte auch Puy du Fou seit der Installation von Genetec Security Center. Die Nutzeroberfläche ist übersichtlich und leicht verständlich. Videoaufnahmen können schon mit zwei Mausklicks exportiert werden. Intuitive Features erlauben es den Verantwortlichen, schnell von einer Kamera zur nächsten zu wechseln.

„Die Sicherheitsteams haben die volle Kontrolle bei der Überwachung übernommen, indem sie das Videosystem einfach navigieren, in Details hineinzoomen und von einer Kamera zur nächsten wechseln können“, sagt Laurent Martin, Security Manager im Puy du Fou. „Dadurch konnten wir unsere Abläufe professionalisieren und lernen, die Überwachungsmethoden zu beherrschen. Brauchten wir früher noch 15 Leute, um einen Verdäch-

Security Center unterstützt die neueste Komprimierungstechnik für eine Videoüberwachung ohne Verzögerungen

tigen im Park zu finden, benötigen wir jetzt nur noch zwei."

Hinter jeder Bühne arbeitet ein Stage-Manager. Dieser verfügt über eine Kontrollstation mit zwei Monitoren, die bis zu 32 Videobilder gleichzeitig anzeigen können. Im zentralen Sicherheitskontrollraum zeigt die aus acht Bildschirmen bestehende Videoleinwand bis zu 128 Bilder gleichzeitig. Von dort aus übernehmen fünf Sicherheitsverantwortliche die Videoüberwachung des gesamten Parks.

Belastbare Lösung spart Zeit

Auch das IT-Team profitiert vom intuitiven Design der Sicherheitslösung. „Es gibt eine zentrale Datenbank für das Kameramanagement. Es ist ein virtuelles System, das wir auf jedem Server betreiben können, was die Wartung vereinfacht", sagt Mathias Jauffrit, IT-Leiter im Puy du Fou.

Security Center unterstützt die neuesten, breitbandbandeffizienten Komprimierungsformate, einschließlich H.264-Videostreaming. Dadurch kommt es auch bei der Videoüberwachung zu keinen Verzögerungen. Das ermöglicht dem Freizeitpark einen naht- und problemlosen Zugang zur Videoüberwachung. Ein zentraler Datenbankserver empfängt alle Video-Feeds sowie Metadaten. Die Videoarchive werden auf einem Cluster von vier Dell-Servern mit insgesamt 90 TB Speicherplatz gespeichert. Damit können die gesamten Aufnahmen mehrerer Tage gesichert werden. Zudem kann das IT-Team die Speicherkapazität bei Bedarf erweitern.

„Wir müssen uns nicht mehr darum kümmern, welche Kamera-Archive auf welchem Server gespeichert werden. Die Speicherzuweisung funktioniert dynamisch. Security Center entscheidet selbst, welcher Server am besten geeignet ist. Das spart unserem technischen Team Zeit", erklärt Jauffrit.

Optimaler Service rund um die Uhr

Obwohl der Freizeitpark in den Wintermonaten geschlossen ist, bleibt Security Center das ganze Jahr über in Betrieb. Sicherheitsverantwortliche überwachen den Park auch während der Nebensaison und schützen ihn vor unbefugtem Zutritt. Darüber hinaus beaufsichtigen sie alle Service- und Lagerbereiche, in denen elektrische sowie mechanische Geräte und hochexplosive Feuerwerkskörper aufbewahrt werden. Dafür wurden auch Intercom- und Einbruchmeldesysteme in die einheitliche Sicherheitsplattform integriert. Erkennt das System eine Bewegung, wird ein stiller Alarm ausgelöst. Über das Intercom-Modul können dann sowohl Eindringlinge als auch Mitarbeiter direkt angesprochen werden.

Zukünftig will der Puy du Fou seinen Kundenservice noch weiter ausbauen. So erwägt das Team, ein automatisches Kennzeichenerkennungssystem in Security Centers hinzuzufügen, um Gästen, Schauspielern und Auftragnehmern das Parken zu erleichtern und den Standort besser absichern zu können.

Eine Kultur der Exzellenz ist für den Puy du Fou in allen Bereichen unerlässlich. Laurent Martin ist daher stolz, dass sein Team mit der neuen Plattform erfolgreich arbeitet. „Ich möchte, dass mein Team sein größtmögliches Potenzial entfaltet. Seit wir Genetec Security Center einsetzen, ist uns das gelungen. Wir haben dafür jetzt die richtigen Werkzeuge." ■

Kontakt

Genetec Deutschland GmbH
Düsseldorf
Tel.: +49 211 13866 575
info@genetec.com
www.genetec.com/de

INTERNET OF THINGS

Smart IoT Industriepark

Dahua bringt Produktivität und Qualität auf ein neues Niveau.

Im neuen IoT-Industriepark in Hangzhou fertigt Dahua seit Juni 2017 seine Produkte

Auf Basis aktueller Fertigungstrends und im Zeitgeist von Industrie 4.0 wurde von Dahua Technology im Juni 2017 ein neuer intelligenter IoT Industriepark in Hangzhou in Betrieb genommen. Der Industriepark umfasst insgesamt 207 Hektar im Fuyang Distrikt von Hangzhou, ca. 20 Autominuten vom Dahua Hauptquartier entfernt, und ist für 6.000 Mitarbeiter ausgelegt. Wir werfen einen Blick auf die Fertigungstechnologien mit denen der intelligente Industriepark darauf angelegt ist, die Produktivität und Qualität der Dahua Sicherheitsprodukte zu verbessern.

Schnellere Produktion und Anpassung

Die automatische Produktionslösung auf Basis eines integrierten Informationssystems garantiert nicht nur eine höhere Produktivität, welche die Lieferzeiten für Dahua-Kunden deutlich verkürzt, sondern auch eine größere Flexibilität für spezielle Anforderungen und eine sich ständig ändernde Realität.

Der Einsatz von Software wie ERP, PLM, PDM, MES, APS und WMS hilft bei der Informationsintegration, die in Kombination mit Industriekameras, RFID-Sensorik und Automatisierungstechnologien Personal, Logistik, Arbeiten, Engineering-

Projekte und Finanzen aus den jeweiligen Bereichen der Produktion (Vorbereitung, Montage, Prüfung, Verpackung, Inspektion, Versand) integriert und den gesamten Prozess sichtbar, nachvollziehbar und digital macht.

Schnell und sparsam

Der Mounter als Herzstück der Produktion zeigt anschaulich die Effizienz des gesamten Produktionssystems: Die von ASM (ursprünglich Siemens) gelieferten High-End-Geräte (u.a. Bestücker, Drucker, automatische optische Inspektionsgeräte und Lötwerkzeuge) erreichen eine Geschwindigkeit, die zu den schnellsten der Welt gehört. Nach dem IPC-Standard X4iS kann der neueste High-Speed-Mounter 125.000 Bauteile pro Stunde oder 35 pro Sekunde verarbeiten. Der Multifunktions-Mounter X35 kann 54.000 Komponenten pro Stunde oder 15 pro Sekunde verarbeiten. Eine Produktionslinie der X-Serie kann die Produktivität um das 2,7-fache steigern und gleichzeitig den Energieverbrauch, verglichen mit der ursprünglichen Produktionslinie der D-Serie unter den gleichen Bedingungen, um 52 % senken.

Die höhere Geschwindigkeit gilt auch für die Entwicklung neuer Formen, da der intelligente Industriepark Dahua den großen Vorteil interner Synergien bietet, die eine durchgängige vertikale Lieferkette mit effizienter Integration von Marketing, Forschung und Entwicklung und Fertigung ermöglichen. Das hochentwickelte Organisationssystem wird von erstklassigen Geräten wie Makino Hochgeschwindigkeits-Graphitbearbeitungsmaschinen, GF CNC, GF WEDM-LS Maschinen, Hexagon 3D Nikon Projektoren und elektronischen Displays unterstützt. Mit einer Bearbeitungsgenauigkeit von +/-0,002 bis +/-0,005 mm und der Unterstützung von CAD/CAM/CAE-Kooperationen und gleichzeitiger Fertigung ermöglichen diese Maschinen Dahua die Entwicklung neuer mechanischer Formen in nur 7 Tagen.

Höhere Qualität

Höhere Qualität spart dem Kunden viel Zeit und wirtschaftliche Kosten. Noch wichtiger ist, dass eine höhere Qualität die Wahrscheinlichkeit von Fehlfunktionen der Produkte verringert, insbesondere wenn sie in absolut kritischen Situationen eingesetzt werden. Dahuas Produkte werden aus zwei Gründen mit einer höheren Qualität garantiert: Erstens hat Dahua einen hohen Standard an Genauigkeit in der Produktion gesetzt; zweitens hat wurde mit einem Zuverlässigkeitslabor auf der Produktionsseite ein effektiver geschlossenen Kreislauf für die Qualitätskontrolle im Herstellungsprozess aufgebaut.

Verbesserte Genauigkeit

Die Genauigkeit war schon immer ein wichtiger Indikator für die Fertigungsfähigkeit, da sie die Qualität und die Bandbreite der zu produzierenden Produkte direkt begrenzt. Nehmen wir noch einmal den oben genannten Bestücker: Er kann Bauteile in metrischen Abmessungen bis zu einer Größe von 03015 (0,3 x 0,15 mm) mit einer SMD-Präzision von +/-0,025 mm (innerhalb des 3-Sigma-Bereichs) verarbeiten, die sich durch eine weltweit führende Leistung auszeichnen und kann praktisch alle in der Industrie verwendeten Bauteile abdecken.

Dahua-Industriekameras spielt eine wichtige Rolle bei der optischen Inspektion und der IdD, einemn geschlossenen Regelkreis für die Qualitätskontrolle im Herstellungsprozess, in dem alle Materialien, Personen und Geräte miteinander verbunden sind und die Produkte auf die spezifische Produktionslinie und den genauen Zeitpunkt ihrer Herstellung zurückverfolgt werden können. Mit einer Vielzahl von Funktionen werden Dahua Industriekameras in verschiedenen Produktionsbereichen eingesetzt, die eine automatische Montage, hochpräzise grafische Inspektion und Produktfehlerprüfung ermöglichen. Durch die hochauflösende Bildverarbeitung lokalisieren sie automatisch und präzise die Komponenten und begrenzen so den Montagefehler auf Mikrometerebene.

Verbesserte Zuverlässigkeit

Das Zuverlässigkeitslabor dient dazu, die Qualität zu sichern, indem die Produkte nach dem Zufallsprinzip aus den Produktionslinien entnommen und in Zuverlässigkeitstests unter Simulation von Fall, hohen/niedrigen Temperaturen und Verschleiß getestet werden, die von branchenführenden Prüfeinrichtungen im Labor durchgeführt werden. So wird das, was in der Forschung und Entwicklung vorgedacht ist, von der Produktionslinie bestätigt, die Synergie beider Enden verspricht bessere Produkte. Dieses Labor ist auch für die Prüfung aller Rohstoffe zuständig. Dank der vorgenannten Informationsintegration werden alle Tests automatisch durchgeführt, aufgezeichnet und sind nachvollziehbar.

Der Dahua Smart IoT-Industriepark ist mit den neuesten und weltweit führenden Produktionsanlagen ausgestattet, die sich durch ein hohes Maß an Automatisierung und Intelligenz auszeichnen, um die immer höheren Anforderungen der Kunden in Bezug auf Lieferzeit, Spezialeinsatz und Qualität zu erfüllen. In diesem neuen intelligenten Industriepark steckt noch viel Potenzial. Er ist buchstäblich nur in seiner ersten Phase. Und in der Zukunft soll er noch intelligenter werden, eine kundenorientierte, flexible Produktion realisieren und eine sicherere Gesellschaft und ein intelligenteres Leben ermöglichen. ■

Kontakt

Dahua Technology GmbH
Düsseldorf
sales.de@global.dahuatech.com
www.dahuasecurity.com/de

VIDEOÜBERWACHUNG

Gleich in die Luft gehen?

Zur Grundstückssicherung gehört inzwischen auch die Absicherung des Luftraums

▲ Zuverlässiger Perimeterschutz muss zukünftig den Luftraum miteinschließen

Es ist nicht mehr nur der klassische Einbrecher (oder Ausbrecher), der über den Zaun steigt: Egal ob produzierender Industriebetrieb, Energieversorger oder auch Justizvollzugsanstalt – die Bedrohungsszenarien und die Anforderungen an den Perimeterschutz sind deutlich vielfältiger geworden. Moderne Bedrohungen kommen jedoch zunehmend auch aus der Luft.

Drohnen stehen durch Massenproduktion, günstige Preise und vereinfachtem Bedienaufwand einer immer breiteren Öffentlichkeit zur Verfügung. Im Vordergrund der Berichterstattung stehen häufig Angstszenarien für kritische Infrastrukturen, bei denen Terroristen Kernkraftwerke angreifen, Wasserreservoirs vergiften oder auch Kliniken über die Luftschächte kontaminieren. Gefängnisse kämpfen gegen Drogen- und Warenlieferungen, die mittels Drohne schnell und bequem direkt an die Zellenfenster geflogen werden.

Abseits dieser Extremfälle sind die Probleme jedoch viel alltäglicher: Grundstücksgrenzen werden häufig auf der Suche nach dem perfekten Foto nicht respektiert, Industrieunternehmen und Areale werden aus der Luft ausgespäht, weil man beispielsweise den neuesten Erlkönig sehen möchte und an anderer Stelle, am Flughafen, können riesige Passagiermaschinen nicht landen, da Drohnen direkt über der Landebahn platziert und dadurch die Triebwerke gefährdet werden. In diesen Fällen handeln keine ausgebildeten Terroristen, sondern vielleicht sogar der arglose Familienvater von nebenan.

Absicherung des Luftraums

Moderne Sicherheitskonzepte müssen sich zukünftig auch um die Absicherung des Luftraums über einem Grundstück kümmern. Es gilt, Lösungen für eine zuverlässige Detektion und nachgelagert auch für den Umgang, im Rahmen der gesetzlichen Möglichkeiten, mit einer erkannten Drohne zu finden. Man muss jedoch auch zwischen Gefahr und Nutzen unterscheiden, denn nicht jede Drohne

führt zwangsläufig immer Böses im Schilde. Unternehmen nutzen die Technologie zunehmend für friedliche Zwecke. Sie forschen an der Nutzung als Transportmittel, überwachen Ernteerträge oder setzen Wärmebildkameras bei der Suche nach verschütteten Personen ein. Auf lange Sicht müssen sich Detektionssysteme diesen Anforderungen anpassen.

Status quo

Die heutige Realität sieht anders aus: Viele Unternehmen haben bis jetzt keine vernünftige Basis, also kein ausgereiftes Perimeterschutzkonzept zur Absicherung des Firmenareals auf dem Boden. Wenn dies nicht geregelt ist, fällt es schwer sich um den betroffenen Luftraum zu kümmern.

heitssystems. Spezialisten erarbeiten individuelle Lösungen für den jeweiligen Einsatzort und Einsatzzweck. Dazu werden alle notwendigen Daten erfasst, gesammelt und evaluiert, um letztlich das bestmögliche und wirtschaftlichste Ergebnis zu präsentieren. Bestehende Systeme und bereits installierte Bauteile finden ebenso Beachtung, wie vorhandene Netzwerkinfrastrukturen. Nach der qualifizierten Prüfung dieser Strukturen werden konkrete Konzepte zur Umsetzung erarbeitet.

Optimales Schutzniveau

Alle eingesetzten Bauteile sollten zuvor getestet werden. Sie müssen aktuelle Normen erfüllen, um das optimale Schutzniveau gewährleisten zu können. Zu einem

Intelligente Videobildanalyse – Der IPS VideoManager erkennt Eindringlinge automatisch

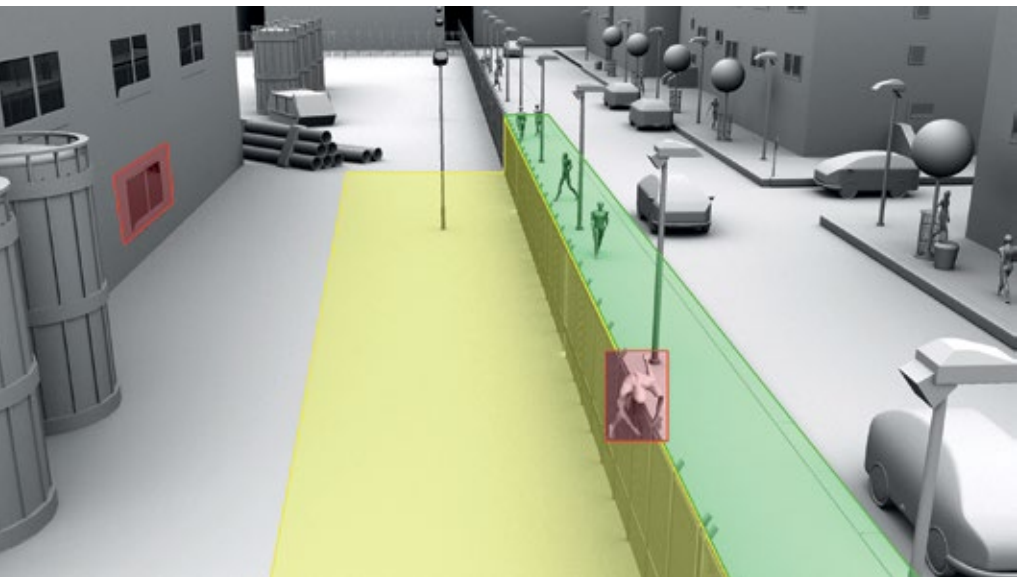
Kameras um ein Grundstück positionieren, Videobilder auf Monitoren in einer Zentrale anzeigen und aufzeichnen: Die Meinung, dass solch eine Ausstattung und dieser Prozess für einen effektiven Schutz ausreichen, ist noch immer weit verbreitet. Heutige High-end-Videosicherheitssysteme leisten darüber hinaus vieles mehr. Qualitative Unterschiede beginnen dabei bereits bei der Planung.

Professionelle Beratung durch geschultes Personal ist der Grundpfeiler einer erfolgreichen Zusammenarbeit mit zufriedenen Kunden und eines am Ende gut funktionierenden Videosicher-

hochwertigen Sortiment gehören Qualitätskameras verschiedenster Ausprägungen, von Fixkameras über Schwenk-Neige-Kameras bis hin zu 360-Grad-Dome-Kameras. Die Wahl der Kamera muss im Einklang mit der Beleuchtung stehen.

Um Eindringlingen keine zusätzliche Hilfe zu bieten, ist es ratsam, Infrarotstrahler einzusetzen. Sie leuchten das Gelände vollständig aus, was jedoch nur für die Kamera und nicht für das menschliche Auge wahrnehmbar ist. Die Anbringung der Kameras und der Strahler sollte an einem stabilen Ort erfolgen. Letztlich taugen die beste Kamera und die beste Lichtquelle für keine

Bitte umblättern ▶



Die Basis ist ein durchdachtes Perimeterschutzkonzept am Boden

Videobildanalyse, wenn sie durch Erschütterungen beeinflusst werden. Dabei spielen stabile Masten eine entscheidende Rolle. Sie müssen Wind und Wetter trotzen.

Ist die Positionierung der Kameras geklärt, werden Kabelwege und die Netzwerkinfrastruktur effizient auf die Örtlichkeiten abgestimmt. Ob große oder kleine Serverlandschaft – die Möglichkeit zur Skalierung einer Anlage sollte von einem modernen System jederzeit gewährleistet sein, um dem Anwender auch zu einem späteren Zeitpunkt die Nachrüstung und Erweiterung zu garantieren. Mit durchdachten Lösungen für die Netzwerkinfrastruktur ist eine Aufschaltung zu einer externen Notruf- und Serviceleitstelle jederzeit möglich und selbst eine Ferneinwahl über das Internet stellt kein Problem dar. Der Kunde ist mobil und kann rund um die Uhr seine Anlage kontrollieren. Eigene, direkt beim Kunden angesiedelte Leitstände, sind ebenfalls möglich.

Mehrwert intelligente Videobildanalyse

Die wahre Herausforderung für die Hersteller beginnt bei den Videobildanalysen, die unerwünschte Ereignisse automatisch detektieren können. Videobilder intelligent durch Softwarealgorithmen auswerten – das klingt einfach, ist es aber nicht. Störgrößen, also Umwelteinflüsse wie vorbeiziehende Wolken, sich bewegende Blätter der Bäume oder auch Wasseroberflächen stellen die Entwickler vor große Herausforderungen. Das Ziel ist stets diese Störgrößen herauszufiltern, um eine möglichst geringe Täuschungsalarmrate zu erwirken.

Des Weiteren beanspruchen diese Analysen die IT-Struktur und damit das Budget. Je effizienter ein Algorithmus arbeitet, desto kleiner kann die Serverlandschaft geplant werden – das spart Kosten für Anschaffung, Betrieb und Wartung. Intelligente Videobildanalysen überwachen Objekte nicht einfach nur – sie schützen sie, erkennen unerwünschte Ereignisse automatisch und gewinnen dadurch die Zeit zur schnellen oder unmittelbaren Intervention.

Im Falle von Securiton werden die intelligenten Videobildanalysen in eigenen Unternehmen in Deutschland entwickelt. Für das Videomanagementsystem IPS VideoManager und den zugehörigen Analysemodulen bedeutet dies ein Team, das sich ausschließlich um die Weiterentwicklung dieser Software kümmert. Abgestimmt auf Kundenwünsche wird die Software kontinuierlich verbessert und erhält mit jedem neuen Release Aktualisierungen und neue Funktionen.

> „Die wahre Herausforderung für die Hersteller beginnt bei den Videobildanalysen, die unerwünschte Ereignisse automatisch detektieren können.“

Mit der Übergabe einer ausgereiften und funktionstüchtigen Anlage ist die Arbeit eines spezialisierten Sicherheitsunternehmens noch immer nicht beendet. Service-Techniker gewährleisten durch regelmäßige Wartung der Hard- und Software eine ordnungsgemäße Funktion der Anlage. Sollten dennoch Probleme auftreten, darf der Kunden nicht im Regen stehen. Eine 24-Stunden-Hotline bietet selbst am Wochenende schnelle Hilfe und liefert kompetente Antworten und Unterstützung zu auftretenden Fragen und Problemen.

Videobildanalyse und Drohnendetektion – ein starkes Duo

So entsteht eine umfassende und durchdachte Videosicherheitslösung, die den Perimeter am Boden rund um die Uhr und stets mit höchster Aufmerksamkeit sichert. Wird diese Analyse nun mit modernen Drohnendetektionssystemen kombiniert, entsteht ein starkes Duo. Doch das Thema Drohnendetektion ist nicht ganz trivial. Der Anwender muss wissen was er tatsächlich detektieren möchte. Es stehen unterschiedliche Technologien zur Auswahl und die optimale Lösung bedeutet für jeden Kunden etwas anderes. Die eingesetzte Technik entscheidet die maximale Detektionsdistanz und auch die Detektionsgenauigkeit sowie die mitgelieferten Informationen. Manche Detektionssysteme können den genauen Typ einer Drohne identifizieren und geben so Auskunft über Größe, Gewicht und Tragfähigkeit. Wichtig sind auch die zur Verfügung stehenden Frequenzen. Beim Einsatz von Radarsystemen sind nicht alle Frequenzen für eine zivile Nutzung freigegeben.

Im Idealfall lassen sich Drohnen bereits vor dem Start in die Luft detektieren – und zwar in mehreren Kilometern Entfernung. Dazu empfängt das Detektionssystem den ersten Funkverbindungsaufbau zwischen Drohne und Steuereinheit. Empfindliche Antennen können dies bereits in Entfernungen über 15 Kilometern erfassen, detektieren mit einer 360-Grad-Rundumsicht und orten dazu noch die exakte Richtung. Kleinere Systeme haben Detektionsentfernung von etwa zwei Kilometern. Ihr Erfassungswinkel ist eingeschränkter. Dafür gibt es transportable Varianten, die sogar am Körper getragen werden können. ■

Kontakt

Securiton GmbH
Alarm- und Sicherheitssysteme
Achern
Tel.: +49 7841 62 23 0
info@securiton.de
www.securiton.de

ZUTRITTSSTEUERUNG

Beständig durch Zeit und Raum

Stabilus investiert in Zutrittskontrolle und Zeiterfassung

▲ Mit dem System IF-6020 von Interflex benötigen die Mitarbeiter von Stabilus nur noch einen einzigen multifunktionalen Firmenausweis

Das Unternehmen gehört weltweit zu den führenden Anbietern von Gasfedern, Dämpfern und elektromechanischen Antrieben. Das Stammwerk von Stabilus ist in Koblenz – und es gibt ein globales Produktionsnetzwerk in neun Ländern. Jetzt hat das Unternehmen für seine rund 6.000 Mitarbeiter in ein ganzheitliches Zutritts- und Zeiterfassungssystem von Interflex Datensysteme investiert. Die Spezialisten von Interflex passten das System IF-6020 individuell an den aktuellen Bedarf und an das Wachstum der Unternehmensstrukturen an.

Die Mitarbeiter von Stabilus brauchen jetzt nur noch einen einzigen multifunktionalen Firmenausweis. Damit können sie die Zugänge zu ihrem Arbeitsplatz passieren und ihre Arbeitszeiten buchen. Die passenden Zutrittsrechte speichert das System IF-6020 von Interflex für jeden Angestellten auf einem Chip seines Mitarbeiterausweises. Die elektronischen Beschläge an den Türen sind über die NetworkOnCard-Technologie zuverlässig mit dem zentralen System verbunden.

SAP-Schnittstelle

Ein wichtiges Novum in der Zeiterfassung ist die Übertragung der Zeitbuchungen über eine zertifizierte Schnittstelle direkt in das SAP-System von Stabilus. Die Anpassung der Gesamtlösung erfolgte nach einer sorgfältigen Bedarfsanalyse direkt durch die Teams von Interflex. Der Anbieter entwickelt maßgeschneiderte Hard- und Softwarelösungen für moderne Sicherheitskonzepte sowie Workforce-Management.

„Dank der Skalierbarkeit unserer Lösungen profitiert Stabilus mit dem neuen Zutritts- und Zeiterfassungssystem von langjähriger Investitionssicherheit. Denn natürlich ist es in einem internationalen Konzern von Zeit zu Zeit erforderlich, Erweiterungen einzurichten. Das ist aus der Hand unserer Spezialisten in aller Regel schnell und kosteneffizient erledigt“, so Dr. Jörg Wissdorf, General Manager von Interflex. Zudem entspricht das neue Zutritts- und Zeitmanagement von Stabilus umfassenden Sicherheitsanforderungen und bietet ein hohes Maß an Benutzerfreundlichkeit. ■

Kontakt

Interflex Datensysteme GmbH
Stuttgart
Tel.: +49 711 13 22 0
interflex.info@allegion.com
www.interflex.den

▲ Stabilus mit seinem Stammsitz in Koblenz gehört weltweit zu den führenden Anbietern von Gasfedern, Dämpfern und elektromechanischen Antrieben

▲ Die Anpassung der Gesamtlösung erfolgte nach einer Bedarfsanalyse direkt durch die Teams von Interflex

In der Zutrittskontrolle, Zeiterfassung, Sicherheitstechnik und Besucherverwaltung helfen Workflow-Szenarien, Genehmigungs- und Freigabe-Verfahren zu optimieren

ZUTRITTSSTEUERUNG

Im Fluss

Workflow-Szenarien in der Zutrittskontrolle und Zeiterfassung

Automatisierte Prozesse für bestimmte Routine-Aufgaben können Abläufe in Unternehmen vereinfachen und die Effektivität steigern. In der Zutrittskontrolle, Zeiterfassung, Sicherheitstechnik und Besucherverwaltung helfen Workflow-Szenarien, Genehmigungs- und Freigabe-Verfahren zu optimieren.

Workflow-Szenarien in der Zeiterfassung können beispielsweise Folgendes beinhalten: Der Mitarbeiter kann am Zeiterfassungsterminal – per Smartphone oder am PC – Beginn und Ende seiner Arbeitszeit buchen, seine Zeitsalden einsehen, Urlaubsanträge stellen sowie vergessene Einzelbuchungen und Anträge auf Mehrarbeit oder Dienstreisen genehmigen lassen. Über eine webbasierte Anwendung ist dies auch von unterwegs möglich, was Außendienstmitarbeitern lästige Nachbuchungen oder Anträge erspart. Schnittstellen in die Lohn- und Gehaltsprogramme verarbeiten die so erfassten Zeiten und berücksichtigen spezielle Arbeitszeitmodelle (Bereitschaftszeiten, Feiertags- und Nachtarbeit, etc.).

Das Genehmigungsverfahren kann hierarchisch strukturiert werden, so dass mehrere Personen dem Antrag zustimmen müssen. Dieser Prozess läuft automatisiert, der Antrag wird nach Freigabe automatisch an die nächste Ebene zur Genehmigung weitergeleitet, bis am Ende der Antragsteller schließlich die Freigabe erhält. Alle Ereignisse werden automatisch protokolliert und sind jederzeit nachvollziehbar. Der Workflow nimmt außerdem Prüfungen vor. So kann etwa ein Mitarbeiter nur Gleitzeitausgleich beantragen, wenn die dafür erforderliche Anzahl an Stunden auf seinem Konto vorhanden ist. Es werden keine

unlogischen Anträge ausgelöst, die manuelle Prüfung ist überflüssig und die Personalabteilung wird deutlich entlastet.

Zutrittskontrolle

In der Zutrittskontrolle dienen Workflow-Szenarien der Vergabe von Zutrittsrechten für Personen und Identifikationsmedien. So kann etwa ein Mitarbeiter beantragen, dass er für einen definierten Zeitraum Zugang zu einem bestimmten Bereich erhält. Beispiel: Der Mitarbeiter aus Berlin beantragt per Workflow eine Dienstreise in die Niederlassung nach Barcelona und damit gleichzeitig die Berechtigung für die Zufahrt durch die Schranke aufs Firmengelände (via Kennzeichen-Erkennung) und den Zutritt zum Firmengebäude durch Buchung mit seinem Chip am Zutrittskontroll-Leser sowie in das dortige Labor, für das spezielle Zutrittsrechte für Hochsicherheitsbereiche gelten.

Die Zutrittsberechtigungen erlöschen automatisch nach Ablauf der definierten Frist. Die Ereignisse werden genau protokolliert, es ist jederzeit nachvollziehbar wer, wann welche Berechtigungen erteilt oder verweigert hat. Die Sicherheitsanforderungen sind gewährleistet.

> „Alle Ereignisse werden automatisch protokolliert und sind jederzeit nachvollziehbar."

Besucherverwaltung

Im Bereich Besuchververwaltung erleichtern Workflow-Szenarien die Planung und sorgen für einen professionellen Empfang. Der Besucher erhält im Vorfeld eine E-Mail zur Erfassung seiner Daten. Nachdem er diese übermittelt hat, erhält er einen QR-Code auf sein Smartphone. Am Tag des Besuches kann der Besucher über den QR-Code einen Ausweis mit den für ihn definierten Zutrittsberechtigungen erhalten. Bei Buchung erhält die Person, die ihn eingeladen hat, automatisch eine E-Mail, dass der Besucher eingetroffen ist. Parallel wird dann bspw. die Tür am reservierten Besprechungsraum entriegelt.

Ist die Gebäude-Automation in den Workflow-Prozess mit eingebunden, wird automatisch das Licht eingeschalten, die Jalousie hochgefahren, die Heizung oder Klima-Anlage in Betrieb genommen. Der Besucher kann sich alternativ ohne vorherige Anmeldung direkt im Unternehmen an einem sog. Kiosk-Terminal oder durch einen Scan seiner Visitenkarte bei seinem Gastgeber anmelden. Die Freigabe bzw. Genehmigung für diesen Besuch erfolgt ebenfalls über die im Workflow hinterlegten Hierarchie-Ebenen. ■

Kontakt

Primion Technology AG
Stetten am kalten Markt
Tel.: +49 75 73 95 20
info@primion.de
www.primion.de

Die Zutrittssteuerung ist ein wichtiger Baustein für die IFS-Food-Zertifizierung

ZUTRITTSSTEUERUNG

Im Dampf der Brühwurstküche

Zutrittssteuerung in der Lebensmittelproduktion – ein Baustein für die IFS-Food-Zertifizierung

Fleisch, Wurst und Milch gehören zu den Grundnahrungsmitteln in Deutschland. Sie werden in der Regel weiterverarbeitet, zum Beispiel zu Fleischfertigprodukten, Wurst, Joghurt, Käse. Damit unsere Lebensmittel hygienisch unbedenklich und einwandfrei produziert werden können, hat sich die Lebensmittelindustrie zusammengeschlossen und sorgt mit der IFS Food Zertifizierung für Standards bei den sensiblen Prozessen in der Lebensmittelproduktion. Dazu gehören auch geeignete Zutrittslösungen wie die von PCS Systemtechnik.

Die freiwillige Verpflichtung nach den IFS-Regeln des „Food Defense" gilt als Gütesiegel für die hygienische Lebensmittelproduktion. Sie ist eine vertrauensbildende Maßnahme bei Handelspartnern und Endverbrauchern. Die Richtlinien schreiben unter anderem vor, dass der Prozessablauf von der Warenannahme bis zum Versand so eingerichtet ist, dass eine Kontamination vermieden wird.

Zonen für Schutzmaßnahmen

Mit dem jeweiligen Sicherheitsbeauftragten sollten für jeden Standort die notwendigen Schutzmaßnahmen geplant und die Bereiche definiert werden, die besonderen Hygiene- und Schutzmaßnahmen erfordern. So sollte definiert werden, welche Zonen mit normaler Straßenkleidung betreten werden oder in welchen Räumlichkeiten, ein direkter Kontakt zu Lebensmitteln besteht. Dort hat nicht in der Regel jeder Mitarbeiter Zutritt, das Personal muss regelmäßig im Umgang mit den Nahrungsmitteln geschult werden.

Oft dürfen diese Bereiche nur über Hygieneschleusen betreten werden, Schutzkleidung wie Kittel und Haube sorgen für einwandfreie Hygiene. Auch die klimatischen Bedingungen dieser Produktionsumgebungen sind zu beachten. Störungen durch unbefugte Besucher

Die Zutrittsleser müssen IP65-wasserdicht sein, die Gehäuse komplett geschlossen und unter Umständen mit Heizung ausgestattet sein

Hygieneschleuse in der Lebensmittelproduktion

sind hier mit einer Zutrittskontrolle am besten zu vermeiden.

Sicherheit beginnt bei Zufahrt auf Werksgelände

Der erste Baustein für eine sichere Nahrungsmittel-Produktion beginnt mit dem Perimeterschutz an allen lebensmittelverarbeitenden Standorten. Am Werkeingang regeln Vereinzelungsanlagen und Drehkreuze mit kombinierten Intus-Zutrittslesern von PCS Systemtechnik, dass nur Mitarbeiter das Gelände betreten können. Den einfahrenden Lieferantenverkehr kontrolliert in der Regel ein Wachmann. Nicht bekannte Fahrer müssen sich beim Wachmann erst registrieren. Damit die Einfahrtskontrolle schneller geht, können angemeldete LKWs mit einem aktiven Transponder in den Stoßfängern durchs Tor fahren. Dafür sorgen zum Beispiel Longrange-Leser, die auch über eine Entfernung von acht Metern RFID-Ausweise lesen.

Feuchtigkeit und Kälte

In der Lebensmittelindustrie herrschen vorwiegend schwierige Milieus für elektronische Geräte, denn Feuchtigkeit, Kälte oder Nässe sind eine Herausforderung. Die Zutrittsleser müssen sich auch in diesen Umgebungsbedingungen betreiben lassen, dafür müssen sie IP65-wasserdicht sein, die Gehäuse komplett geschlossen und unter Umständen mit Heizung ausgestattet sein, damit sie in den besonderen Bedingungen der Lebensmittelindustrie zum Beispiel bei der Brühwurstherstellung installiert werden können.

Auch die Reinigung mit Dampfstrahlgeräten und ähnlichem müssen sie überstehen. Zusätzlich können mechatronische Türzylinder und Beschläge zum Beispiel für Verwaltungsbereiche und Metalltüren zum Einsatz. Vernetzte Leser für Innen- und Außenbereiche kontrollieren dann Türen, Drehkreuze, Tore und Schranken und trennen so sauber die Zonen der verschiedenen Produktionsbereiche. Denn es kann in der Wurstproduktion in einem Sektor zum Beispiel in der Salamiherstellung ein Bakterium benötigt werden, mit dem aber im anderen Bereich die Wurstwaren auf keinen Fall in Berührung kommen sollen. Die Zutrittskontrolle verhindert das Verbreiten des Keims durch unbedachtes Handeln.

Nur registrierte Besucher

Mit der Nutzung der Zutritts- und Zufahrtskontrolle stellt man sicher, dass sich nur Mitarbeiter und registrierte Besucher auf dem Werksgelände befinden. Dazu sollten alle Komponenten aus der Software heraus gesteuert werden. Ein Besuchermanagement mit Sicherheitsbelehrung bezieht auch die Besucher in das Sicherheitssystem mit ein. Im Notfall helfen Anwesenheitstableaus und Notfall-Listen bei der Evakuierung.

Für ein Sicherheitskonzept im Rahmen der Zertifizierung nach IFS Food V6 unterstützt PCS Nahrungsmittelproduzenten mit Planung, Beratung, Produkten, Installation und Wartung. Das Unternehmen liefert die komplette Zutrittskontroll-Hardware sowie eine leistungsstarke Zutrittskontroll-Software zur lückenlosen Absicherung von Produktions- und Lagerbereichen in der Lebensmittelherstellung. Zu den vielen anderen Herstellern oder Händlern, die die PCS-Produkte im Einsatz haben, zählen z.B. die Getränkehersteller Adelholzener und Radeberger, die Molkerei-Produzenten Bauer und Müller-Milch oder die Fleischproduzenten Hans Kupfer und Handelshof. ■

Kontakt

PCS Systemtechnik GmbH
München
Tel.: +49 89 68004 0
intus@pcs.de
www.pcs.de

Ein hoher Zaun mit Stacheldraht? Für den Schutz eines Geländes braucht es mehr: Mehrere Schichten, verstärkt mit robusten Sicherheitslösungen bilden die Basis für einen guten und auch sicheren Schutz. Einige Unternehmen kämpfen noch immer mit der Entwicklung und Umsetzung eines umfassenden Perimeterschutzplans. Für sie hat Jochen Sauer von Axis Communications sechs Fragen zusammengestellt, die bei der Erstellung eines solchen Plans gestellt werden müssen.

In der Regel sind größere Mengen an Zaun- und Sicherheitslösungen erforderlich, um einen Perimeter abzusichern

PERIMETERSCHUTZ

6 Fragen . . .

. . . die sich stellen sollte, wer einen Gebäudeschutz-Plan entwickeln will

1. Definition: Was ist der „Perimeter"?

Perimeter sind alle Grenzen, die ein Gebiet umfrieden oder von einem anderen schützen. Perimeterschutz beinhaltet die Sicherung gefährdeter Standorte oder Strukturen innerhalb dieser Umfriedungen. Bei der Entwicklung eines Perimeterschutzplans sollte man zunächst einmal die Größe des Perimeters berücksichtigen. In der Regel sind größere Mengen an Zaun- und Sicherheitslösungen erforderlich, um einen Perimeter abzusichern.

Der zu entwickelnde Plan soll jeden Meter einer kilometerlangen Umfriedung mit gleicher Aufmerksamkeit behandeln. Hier hilft es, folgende Punkte zu berücksichtigen:

- Identifikation aller Ein- und Ausgänge

Typischerweise dringen Eindringlinge zuerst in diese Bereiche ein, weil sie oft am leichtesten zu durchbrechen sind.

- Physische Perimeter

Physische Perimeter können aus Mauern, Zäunen oder anderen Umweltstrukturen oder -barrieren und manchmal auch aus natürlicher Vegetation bestehen:

- Auswirkungen, wenn der Schutz durchbrochen wird

Wird ein Alarm ausgelöst, wenn ein Eindringling einbricht, oder ist die Entfernung oder Richtung der Bewegung des Eindringlings wichtiger? Es ist entscheidend, die kritische bis unkritische Natur des Grundstücks als konzentrische Kreise zu betrachten, wobei das Zentrum die kritischsten Punkte beinhaltet und die Gefahr von innen nach außen abnimmt.

2. Ist die Technologie auf dem neuesten Stand?

Viele Gründe sprechen für die Verwendung der aktuellsten Sicherheitslösungen:

- Einhaltung gesetzlicher Vorschriften:

Organisationen im Gesundheitswesen oder Unternehmen, die für Bundesbehörden arbeiten, sind häufig gesetzlich verpflichtet, ihre Sicherheitslösungen auf dem neuesten Stand zu halten, um Sanktionen zu vermeiden.

- Verbesserung der Produkteffizienz:

Technologien zur Video-Bewegungserkennung haben sich von einer pixelbasierten Analyse zu einer intelligenteren, objektbasierten Erkennung entwickelt, die je nach Objektgröße und -geschwindigkeit einen Alarm auslösen kann. IP-Geräte werden immer leistungsfähiger und können eine fortschrittliche Analyse durchführen, um Fehlalarme zu erkennen und zu reduzieren.

Technik sollte grundsätzlich auf dem neuesten Stand sein: So bleibt man normengerecht, effizient und besser vor Cyber-Angriffen geschützt

■ Schutz vor Cyber-Angriffen:
Die Internet of Things (IoT)-Technologie, die IP-Kameras und andere Devices verwenden, ist von Natur aus mit Netzwerken verbunden und kann daher anfällig für Cyber-Angriffe sein. Laut einem aktuellen Deloitte-Bericht werden verteilte Denial-of-Service-Angriffe (DDoS = Distributed Denial of Service) immer zahlreicher und größer. Diese können Sicherheitslösungen lähmen, indem sie entweder Systeme zum Absturz bringen oder den Zugriff auf Videomaterial blockieren. Durch das Herunterladen der neuesten Updates und Patches können sich Unternehmen besser vor Cyber-Bedrohungen schützen.

3. Beeinträchtigen Klima oder Umweltbedingungen die Erkennung?

Klima- und Umweltbedingungen können sich auf die Sicherheitsausrüstung und deren Detektionsgrad auswirken. Beispielsweise können bei Szenen mit extremer Beleuchtung oder Gegenlicht – z. B. bei auf-oder untergehender Sonne oder bei Nachtbetrieb – analoge Kameras Schwierigkeiten haben, klare Bilder zu erzeugen. Hier sind IP-Kameras mit weitem Dynamikbereich oder mit thermischer Technologie besser geeignet.

Neben der Beleuchtung kann auch die Bildstabilisierung zu einem Problem werden, wenn die Kameras starken Winden ausgesetzt sind. Elektronische Bildstabilisierung (EIS) kann Erschütterungen durch hohe und niedrige Schwingungen und Windeinflüsse reduzieren.

Bei Anlagen, die unter extremen Bedingungen arbeiten, muss der Betreiber mehr als nur die Funktionen von Sicherheitslösungen berücksichtigen: weitere Aspekte:

■ Luftfeuchtigkeit: Wenn sich Kondensation im Innern eines Kameraobjektivs bildet, kann es sowohl Bilder verwischen als auch die Elektronik stören. Bei Kameras, die ständigen Luftdruckschwankungen und starken Regenfällen ausgesetzt sind, können Dichtungen und andere Bauteile reißen und sich Feuchtigkeit im Innern ansammeln. Die besten Kameras haben interne Lüfter und schnelle Trocknungstechnik.

■ Umweltbedingungen: Ein hoher Salzgehalt in der Luft oder hochaggressive Reinigungschemikalien in einer Produktion von Lebensmitteln, Medizin- und Reinraumanlagen können die Sicherheitsausrüstung mit der Zeit korrodieren. Dabei empfiehlt sich die Verwendung von außentauglichen Kameras mit Edelstahl oder Vollpolycarbonat-Gehäusen.

■ Temperatur: Extrem kühle Temperaturen können die einwandfreie Funktion der einzelnen Kamerateile verhindern. Wenn die Kamera keine Speed-Dry-Technologie oder Temperaturregelung hat, kann sich Eis auf dem Objektiv bilden, was zu unscharfen Bildern führen kann, oder die Kamera schaltet sich nicht korrekt ein - wenn sie überhaupt funktioniert.

■ Montage: Nicht jede Fläche ist gleich. Beispielsweise können Kameras, die an porösen Wänden montiert sind oder die einen extremen Temperaturtransfer (warm bis kalt) ermöglichen, mehr Feuchtigkeit ausgesetzt sein. Durch eine Montage vor der Installation können Kameras besser vor rauen Umgebungsbedingungen und extremen Temperaturschwankungen geschützt werden.

4. Wer erhält den Alarm und wie?

Um Perimeter jederzeit und an mehreren Standorten überwachen zu können, wird häufig IP-Videoüberwachungstechnologie mit Remote-Zugriff eingesetzt. Mit diesen Lösungen kann das Sicherheitspersonal die Außengrenzen über Überwachungsmonitore oder die Außenstellen mit mobilen Geräten überwachen.

Durch Perimeterschutzlösungen lassen sich Situationen bewerten. Zum Beispiel wird Sicherheitspersonal nur dann benachrichtigt, wenn eine echte Bedrohung vorliegt. Indem Mitarbeiter über den Bedrohungsgrad informiert werden, haben sie die Möglichkeit, die Art des Risikos zu überprüfen und angemessen zu reagieren.

Dieses Sicherheitsniveau hilft Unternehmen auf dreifache Weise:

- Reduktion von Strafen und Gebühren: Unerwünschte Alarme kann für Unternehmen hohe Kosten verursachen. Die besten Überwachungslösungen reduzieren unerwünschte Meldungen, indem sie nur echte Bedrohungen identifizieren.
- Verringert Sachschäden und Verluste: Schnelle Reaktion auf einen Einbruch hilft, Sachschäden zu vermeiden.
- Weniger Betriebsunterbrechungen: Lösungen für den Perimeterschutz können die Anzahl der durch Fehlalarme verursachten Unterbrechungen des Betriebs und der Produktion verringern oder deren Auswirkungen vermindern.

5. Wie lässt sich feststellen, was den Alarm verursacht hat?

Mit den richtigen Lösungen für den Perimeterschutz wird es einfacher zu erkennen, was einen Alarm ausgelöst hat oder was die Bedrohung ist.

Komplexer als es aussieht: Ein effizienter Gebäudeschutz setzt die Entwicklung eines umfassenden Perimeterschutzplans voraus

Wärmebildkameras mit intelligenter Videoanalyse produzieren beispielsweise nicht nur deutlich weniger Fehlalarme als optische Kameras, sondern sind auch unempfindlicher gegen Umweltbedingungen wie Regen, Schnee und Nebel. Einige Wärmebildkameras sind auch mit EIS ausgestattet, um sie bei Schwankungen durch, zum Beispiel Wind ruhig und stabil zu halten.

In Umgebungen mit schlechter oder extremer Beleuchtung können Sicherheitseinrichtungen Eindringlinge nur schwer identifizieren. Lösungen mit einem großen Dynamikumfang können Szenen grundlegend umstrukturieren, so dass Objekte in Umgebungen mit unterschiedlichsten Lichtverhältnissen besser betrachtet werden können. Auch eignet sich die Verwendung von Kameras mit 950nm-Infrarotlicht, da sie dunkle Bereiche in Szenen besser ausleuchten. Schließlich kann das einfache Hinzufügen von Zusatzbeleuchtungen in dunklen Bereichen einer Szene dazu beitragen, Eindringlinge besser zu identifizieren.

6. Was ist die Lösung?

Ein zentrales Anliegen des Sicherheitspersonals sollte es sein, tote Winkel entlang der Begrenzungslinie zu beseitigen. Dazu gilt es die Bedrohung genau einzuschätzen, um die beste Lösung zu finden.

Alle Produkte können fehlschlagen, wenn sie nicht korrekt installiert und implementiert sind. Die Kenntnis der praktischen Anwendung der Perimeter-Schutztechnologie in der Praxis und ihrer Erfassungsgrenzbereiche kann dem Personal helfen, bessere Lösungen zu entwickeln. ■

Kontakt

Axis Communications GmbH, Ismaning
Tel.: +49 89 358817 0
info-de@axis.com
www.axis.com

Data-on-Card – Aktualisierung am Terminal

Neben den vielseitigen Funktionen als Terminal zur Zeiterfassung, zur Raumvergabe oder zum Management von Schrankschlössern unterstützt das touch.On-Terminal von IntraKey auch die Data-on-Card-Funktion für die Offline-Zutrittskontrolle. Nach Vorhalten der Karte bzw. des Transponders zeigt das Farbdisplay alle für den Nutzer aktuell gesetzten Offline-Rechte im Klartext an. Sowohl Einzeltüren als auch Türgruppen und zeitliche Beschränkungen lassen sich so bequem im Self-Service überprüfen. Veränderte Offline-Berechtigungen sowie Gültigkeitsdaten werden zeitgleich auf die Karte geschrieben. Die intuitive Bedienung ermöglicht es auch ungeübten Benutzern, das Terminal z. B. als Check-in-Terminal im Hotel zu verwenden. Neben der sekundenschnellen Aktualisierung von Offline-Berechtigungen erhält der Nutzer sofort einen Überblick, zu welchen Räumen er Zutritt hat.

www.intrakey.de ■

Robuste Bahnnetzwerke für reibungslosen Betrieb

Auf der diesjährigen Fachmesse IT-Trans in Karlsruhe präsentierte der Value-Added-Distributor Vitel Lösungen für die fortschrittliche Schienenverkehrskommunikation mit Produkten des Herstellers Moxa. Vitels Komplettpaket von IP-basierten, für den Schienenverkehr optimierten Kommunikationslösungen umfasst verkabelte und drahtlose Netzwerktechnik, Computing-Plattformen, Automatisierungslösungen und CCVT. Sie lassen sich in den Bereichen passagiernahe Dienste, Fahrgast-Wi-Fi, CBTC (Communication-Based Train Control), ATO (Automatic Train Operation), Strecken-DCS (Data Communications Subsystems) und weiteren Schienenverkehrssystemen einsetzen.

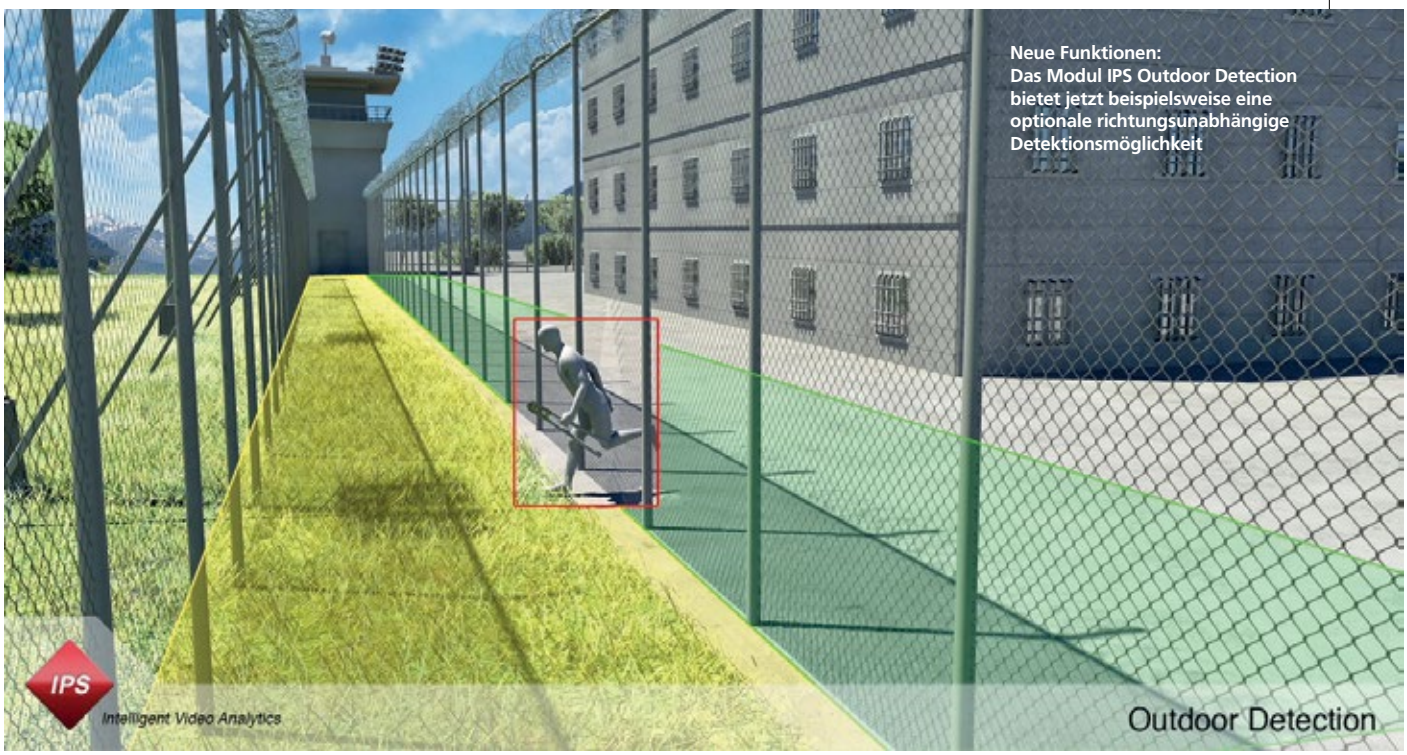
www.vitel.de ■

VIDEOÜBERWACHUNG

Kein Herz für Hacker

IPS veröffentlicht Software-Release 9.0

Mit dem Software-Release 9.0 stellt IPS Intelligent Video Analytics neue und optimierte Features in seinem IPS Video-Manager, dem IPS Analytics-Manager und IPS Video-Analytics zur Verfügung. Im Mittelpunkt stehen eine erhöhte IT-Security, mehrere neue und vereinfachte Schnittstellenfunktionen zur Anbindung an Fremdsysteme sowie erweiterte Funktionen bei verschiedenen Videoanalysen.



Neue Funktionen:
Das Modul IPS Outdoor Detection bietet jetzt beispielsweise eine optionale richtungsunabhängige Detektionsmöglichkeit

Zur IT-Sicherheit in der Videoüberwachung zählt vor allem eine lückenlose End-to-end-Verschlüsselung von der Bildquelle bis zum Client, um die übertragenen Daten vor jeglichem Missbrauch zu schützen. Aufgrund wachsender Bedrohungen und einer mehr und mehr vernetzten Infrastruktur stärkt das Unternehmen das Thema Verschlüsselungen und die Verwendung von Zertifikaten. Durch die Anwendung sicherer und aktueller Übertragungsprotokolle sowie einer zeitweisen Sperrung der Passwortanmeldung nach mehrfachen Falscheingaben ist somit Hackerangriffen noch effektiver vorgebeugt. So werden zum Beispiel Video-Streams über das sichere Übertragungsprotokoll HTTPS zwischen Kamera (Axis) und Device-Server übertragen.

Für zusätzliche Sicherheit sorgt IPS zudem durch die Unterstützung des Protokolls TLS1.2.Neben der vollumfänglichen SOAP-Schnittstelle stellt das Unternehmen mit der Software-Version 9.0 drei neue TCP-Schnittstellen zur Verfügung, die die Anbindung an Fremdsysteme erheblich vereinfachen und die der Anwender je nach Umfang und Komplexität seines Systems wählen kann.

Videoanalysen mit erweiterten Funktionen

Mit der Version 9.0 wurden auch die Funktionen einiger der server- und kamerabasierten Videoanalysen ausgebaut – dazu kommt eine Verbesserung der Anzeige. So wurde das Modul Public Transport um eine weitere Überwachungszone ergänzt: Neben Gleisbettüberwachung detektiert das Modul nun auch, ob sich Personen auf dem Sicherheitsstreifen an Bahngleisen aufhalten, was zu einem Sicherheitsrisiko bei ein- und ausfahrenden Zügen führen kann. Auch das Modul IPS Outdoor Detection erhielt eine neue Funktion. Es verfügt nun auch über eine optionale richtungsunabhängige Detektionsmöglichkeit.

Stark erweitert wurde das kamera- als auch serverbasierte Modul IPS Loitering Detection, welches nun mit einer deutlich längeren einstellbaren Zeit bis zur Auslösung eines Alarms ausgestattet wurde. Dies ist zum Beispiel bei der Überwachung von Bankautomaten sehr hilfreich, um sich hier ungewöhnlich lange aufhaltende Personen zu detektieren. ■

Kontakt

Securiton GmbH, IPS Intelligent Video Analytics
München
Tel.: +49 89 451590 0
info@securiton.de
www.ips-analytics.com

VERANSTALTUNG

Brandschutz für die Chemie

Zum Dechema-Praxisforum „Brandschutz in der chemischen Industrie“

Feuer ist laut Guido Wehmeier, BASF Lampertheim, nach der Stofffreisetzung die häufigste Schadensursache bei meldepflichtigen Ereignissen. Besonders im Bereich von chemischen Anlagen birgt das ein hohes Risiko, das schwer zu verhindern erscheint: Brennbare, leicht- bis selbstentzündliche, reaktionsstarke, leicht flüchtige Stoffe in Reinform sowohl in festem, flüssigem als auch gasförmigem Zustand erschweren teilweise die Risikominimierung. Insbesondere dem abwehrenden und vorbeugenden, organisatorischen und anlagentechnischen Brandschutz kommt hier eine hohe Bedeutung zu.

Ein Brand in einem chemischen Betrieb vernichtet nicht nur Sachwerte und führt zu Produktionsausfall, sondern stellt auch eine zusätzliche Bedrohung für Mensch und Umwelt dar. „Durch die immer näher heranrückende Wohnbebauung in Ballungsräumen entsteht zunehmend Handlungsbedarf bei den Unternehmen“, sagt Ralf Schröder, Regierungspräsidium Darmstadt.

Mit ausgebildeten und berufserfahrenen Experten sowie einer Werksfeuerwehr auf einem Industriegelände lassen sich diese Probleme im Griff behalten. Doch wie können sich klein- und mittelständige Unternehmen (KMUs) absichern?

Beim Dechema-Praxisforum „Brandschutz in der chemischen Industrie“ kommen Experten aus der Industrie, aber auch aus Versicherungen, Behörden, Hochschulen und Forschungseinrichtungen zusammen, um sich praxisnah und lösungsorientiert zum optimalen Brandschutz in der chemischen Prozessindustrie auszutauschen.

Schwerpunktthemen der Veranstaltung sind Schadenfälle in der chemischen Industrie, abwehrender und vorbeugender Brandschutz, Simulationen von Brandszenarien, die neue Seveso III-Richtlinie sowie Ausbreitungsmodelle zur Stoff- und Energiefreisetzung.

In Best-Practices- und Expertenvorträgen wird den Teilnehmern ein umfassender Überblick über den Brandschutzalltag in einem chemischen Betrieb gegeben. Ein Highlight der Veranstaltung ist der Praxisnachmittag in Zusammenarbeit mit dem Landesfeuerwehrverband Hessen und den Werksfeuerwehren.

Das Praxisforum wird in Kooperation mit VdS durchgeführt und wechselt sich im jährlichen Rhythmus mit der VdS-Fachtagung „Brandschutz in chemischen Anlagen“ ab. ■

> „Die Zukunft liegt in der Vernetzung von Brandschutz, Explosionsschutz und Anlagensicherheit der Prozessindustrie“
>
> **Jochen Schäfer, Sanofi-Aventis**

Link zur Veranstaltung:
http://dechema.de/Brandschutz
Termin: 29.–30.08.2018

SICHERHEITSEXPO

27.-28. Juni 2018
im MOC München

Die Fachmesse für

Zutrittskontrolle
Videoüberwachung
Brandschutz
Perimeter Protection
IT-Security

www.sicherheitsexpo.de

©famveldman - stock.adobe.com

BRAND- UND RAUCHMELDUNG

Kinder, Gäste und Senioren

Branderkennung und -warnung für „kleine Sonderbauten“ wie Kitas, Pensionen und Seniorenwohnheime

Sie schließt eine zentrale Sicherheitslücke: Eine neue DIN-Norm tritt dieses Jahr in Kraft und schafft Rechtssicherheit für den Bereich der Branderkennung und Brandwarnung für Kindertagesstätten, Heime und Beherbergungsstätten mit bis zu 60 Betten sowie für besondere gemeinsame Wohnformen für Senioren und Behinderte. Um das Schutzziel „Personenschutz durch Evakuierung“ und eine dauerhafte Betriebssicherheit für Bewohner, Eigentümer, Betreiber, Planer und Errichter sogenannter „kleiner Sonderbauten“ zu gewährleisten, gilt künftig die DIN VDE 0826-2 in Verbindung mit den Normen der Reihe DIN EN 54. Ein Beitrag von Stephan Kreutzer, Geschäftsführer bei Atral-Secal – der zu diesem Thema auch beim Intersec Forum 2018 vortrug.

Viele Kindergärten, Heime, Pensionen und kleinere Hotels setzen bislang meist vernetzte Rauchwarnmelder ein – sie sind deshalb beim vorbeugenden Brand- und Gefahrenschutz in bauaufsichtlich unzureichender Weise und deswegen nicht ausreichend gesichert. Zwar regelt die EN 14604, dass im Brandfall in weniger als 30 Sekunden an alle anderen Rauchwarnmelder eine Alarminformation erfolgen muss – hinsichtlich der Übertragungswege werden jedoch keine Anforderungen definiert. Dementsprechend erfolgt – im Fall einer Störung oder eines Ausfalls der Übertragungsstrecke – auch keine Information darüber, dass eine Störung oder ein Ausfall vorliegt. Die Folgen einer verzögerten Alarmierung und Evakuierung können für die Betroffenen verheerend sein. Im Schadensfall kann dies zu rechtlichen Problemen führen.

Richtlinie für Brandwarnanlagen

Um diese Rechtsunsicherheit zu beenden, wurde auf Basis der bereits eingeführten BHE-Hausalarmrichtlinie eine Schutzziel-orientierte Richtlinie für den Einsatz sogenannter Brandwarnanlagen entwickelt. Sie dient ausschließlich der Warnung der Gebäudenutzer. Im Unterschied zur Brandmeldeanlage meldet sie nicht an die Feuerwehr oder eine andere, außenstehende Stelle. Die dauerhafte Betriebssicherheit wird durch die Verwendung und Einhaltung der Anforderungen der Normenreihe DIN EN 54 gewährleistet. Zur sicheren Funk-Übertragung muss mindestens ein Redundanzkanal vorhanden sein. Darüber hinaus hat alle 300 Sekunden ein Statussignal mit Bestätigung zu erfolgen. Unterbleibt dies, erfolgt eine Störungsmeldung und Störungsanzeige.

Da die Überwachung der Vernetzung fortlaufend sichergestellt wird, ist eine Brandwarnanlage nach DIN VDE V 0826-2 geeignet, die zwingenden Vorgaben der Landesbauordnungen zu erfüllen. Zudem sind die bauaufsichtlichen Anforderungen nach einer auf die gesamte

© Foto: Daitem

Die Einsatzbereiche für Brandwarnanlagen sind vielfältig: Als rechtssichere Lösung ist eine Brandwarnanlage nach DIN VDE V 0826-2 – speziell für kleine bis mittelgroße Objekte ohne gesetzliche Brandschutzauflagen – die ideale Alternative zur bisherigen Praxis mit dem Einsatz vernetzter Rauchwarnmelder. Auch zur Nachrüstung bieten sich Brandwarnanlagen auf Funkbasis an. Allerdings müssen die Funk-Brandkomponenten nach Normen der EN 54 zugelassen sein ▶

Nutzungseinheit bezogenen, frühzeitigen und automatischen Branddetektion ausschließlich mithilfe CE-gekennzeichneter, harmonisierter oder national zugelassener Bauprodukte zu realisieren. Es ist eine interne Warnung im Brandfall ohne automatische Alarmierung der Feuerwehr oder einer anderen behördlich benannten alarmauslösenden Stelle vorgesehen.

EN-54-Komponenten

In der DIN VDE V 0826-2, die bis zum Inkrafttreten noch den Status einer Vornorm hat, wird eine Anlagenkonfiguration mit ausgesuchten EN-54-Komponenten beschrieben. Die einzelnen Komponenten weisen die Leistungsdetails auf, die für das Schutzziel relevant sind: Frühzeitige Warnung von anwesenden Personen oder geschulten Evakuierungshelfern vor Brandrauch und Bränden, sodass diese Personen auf das Gefahrenereignis rechtzeitig und angemessen reagieren können.

Eine Meldung mit empfohlener Quittierung wird mit klar verständlichen Informationen (Art und Ort der Meldung) an einer oder mehreren hausinternen Stellen (z.B. Pförtner, Schwesternzimmer) signalisiert und angezeigt. Hier können automatisch oder mit einfacher Bedienung die nächsten Aktionen (Alarmierung, Evakuierung) eingeleitet werden.

Eine externe Weiterleitung zu einer ständig besetzten, hilfeleistenden Stelle ist nicht zwingend erforderlich, aber optional möglich.

Besondere Anforderungen

Gemäß DIN VDE V 0826-2 ist eine Brandwarnanlage eine sicherheitstechnische Einrichtung. Als Bestandteil des gesamten Sicherungskonzepts für den Personenschutz in Gebäuden oder Gebäudeteilen muss eine Brandwarnanlage daher – hinsichtlich der technischen Spezifikation, Planung, Projektierung, Inbetriebnahme, Abnahmeprüfung sowie dem Betrieb und der Instandhaltung – grundlegende Anforderungen erfüllen. So müssen Brandwarnanlagen durch eine Fachfirma geplant, installiert und instand gehalten werden.

Der Tätigkeitserfüllung der Elektrofachkraft für Gefahrenmeldeanlagen liegt die Qualifikationsanforderung nach DQR-Niveau 5 zugrunde. Der Überwachungsumfang ist mit dem Betreiber und gegebenenfalls mit den aufsichtführenden Behörden anhand einer Risikoanalyse in einem Sicherungskonzept – oder, falls im Einzelfall gefordert, gegenüber der Bauaufsicht im Brandschutzkonzept beziehungsweise in der Brandschutzfachplanung – festzulegen. Bewertet werden muss: 1. Welche Flächen werden von der Brandwarnanlage überwacht? 2. Wie erfolgt die Detektion? 3. Welche Aktionen werden ausgelöst?

Besonderheit „Stille Signalisierung"

Um bei kranken und hilfsbedürftigen Menschen Panik und unkontrollierte Reaktionen zu vermeiden, kann eine „Stille Signalisierung" sinnvoll sein. Diese ist in der DIN VDE V 0826-2 explizit vorgesehen. Grundvoraussetzung ist, dass gezielte Informationen über ein detektiertes Brandereignis von der Brandwarnanlage an Helfer weitergeleitet und von diesen innerhalb von 60 Sekunden quittiert werden. Dazu ist die technische Verbindung mit einer Lichtrufanlage nach DIN VDE 0834, einem Pagersystem oder einer Telefonanlage erforderlich. Bleibt die Quittierung aus, muss eine Warnung des Bereichs erfolgen.

Sicherheit und Rechtssicherheit gestärkt

Soweit die DIN VDE 0826-2 in den „Verwaltungsvorschriften Technische Baubestimmungen" der Landesbauordnungen künftig aufgeführt ist, ist die Norm verbindlich anzuwenden. Betreiber und Träger, Planer, Behörden und Schutzbefohlene profitieren – beim Schutzziel „Personenschutz durch Evakuierung" – von mehr (Rechts)Sicherheit. Ziel des Einsatzes von Brandwarnanlagen ist eine Alarmierung aller Gebäudenutzer zur Ermöglichung der Selbstrettung und die zeitnahe Aktivierung von Brandschutz- und Evakuierungshelfern. Die Einsatzgebiete sind der vorbeugende Brand- und Gefahrenschutz vor allem bei Bauten mit speziellem Personenrisiko, wie beispielsweise Kindergärten und Kindertagesstätten, Heime, Schulen, Beherbergungsstätten mit bis zu 60 Betten sowie besondere gemeinsame Wohnformen für Senioren und Behinderte. ■

intersec
forum
CONFERENCE REVIEW
Artikel war Thema beim Intersec Forum 2018

Kontakt
Atral-Secal GmbH
Weinheim
Tel.: +49 6201 6005 0
info@daitem.de
www.daitem.de

BRANDBEKÄMPFUNG UND PRÄVENTION

Die Bio-Milch macht's

Brandschutz in der Milchproduktion

Der multifunktionale Brandmelder IQ8Quad mit vier integrierten Funktionen in einem Gehäuse: Detektion, Blitzleuchte, akustischer Alarm und Sprachausgabe

Die Nachfrage nach Milchprodukten nimmt weltweit zu. Arla Foods ist der weltweit größte Hersteller von Molkereiprodukten in Bio-Qualität. Das Werk Arla Foods Deutschland in Pronsfeld zählt zu den wichtigsten Wirtschaftsfaktoren in der Eifel-Region. Forschung und Entwicklung sind für das Unternehmen von zentraler Bedeutung. Die ganze Bandbreite der Esser-Brandmeldetechnik kommt hier zum Einsatz und schützt das Werk vor Produktionsausfall.

Wer Radiowerbung nicht regelmäßig ausblendet, wird vermutlich irgendwann schon mal einen Werbespot zu Arla Kærgården wahrgenommen haben. Hinter dieser Bezeichnung verbirgt sich eines der vielen Produkte von Arla Foods, einer europäischen Molkereigenossenschaft, die zu 100 Prozent den rund 11.200 Arla Landwirten aus Schweden, Dänemark, Deutschland, Großbritannien, Belgien, Luxemburg und den Niederlanden gehört. Die Produkte werden unter bekannten Markennamen in mehr als 100 Ländern der Erde vertrieben. Das Unternehmen verfügt über Produktionsstätten in zwölf Ländern und Vertriebsniederlassungen in insgesamt 30 Ländern.

Mit einer Gesamtfläche von 55 Hektar ist der Standort in Pronsfeld der weltweit größte des Unternehmens. Am Rand der Vulkaneifel in Rheinland-Pfalz sind bei der Arla Foods Deutschland über 1.100 Mitarbeiter/innen beschäftigt, darunter 60 Auszubildende in zwölf Berufen.

Auf neuestem technischen Stand

Der Standort im Eifelkreis Bitburg-Prüm zählt zu den modernsten Produktionsstätten der Milchindustrie weltweit und feierte jüngst seinen 50. Geburtstag. In den vergangenen sechs Jahren wurden mehr als 130 Millionen Euro in das Pronsfelder Werk investiert. Dank dieser Investitionen ist der Betrieb heute auf dem neuesten technischen Stand und arbeitet besonders energieeffizient und umweltschonend.

Um diesen wichtigen Standort vor Produktionsausfall zu schützen, ist nicht zuletzt

auch eine optimale, brandschutztechnische Überwachung erforderlich. Diese anspruchsvolle Aufgabe wurde dem Unternehmen Kurth Elektro aus Bitburg übertragen, das für die Sparte Sicherheitstechnik bei der VdS Schadensverhütung für die Errichtung von Brandmelde-, Sprachalarmierungs- und Einbruchmeldeanlagen zertifiziert ist. Kurth Innovative Elektrotechnik arbeitet erfolgreich in allen Bereichen der Sicherheits- und Kommunikationstechnik. Dazu gehören u.a. Brandmelde- und Einbruchmeldeanlagen, Videoüberwachung, Sprachalarmanlagen und 24 Stunden Rufbereitschaft für Wartungskunden. Als Partnerunternehmen der Novar setzt es seit Jahren im Bereich Brandmeldetechnik die Produkte der Traditionsmarke Esser ein.

Besonderheiten der Applikation

Produktionsbereiche verlangen nicht selten aufgrund der unterschiedlichen Umgebungsbedingungen eine gezielte und auf die jeweiligen Anforderungen abgestimmte, brandschutztechnische Überwachung. So erschwert z. B. durch Milchpulver bedingter Feinstaub die Überwachung. Auch Reinigungsdämpfe können zu Falschalarmen führen, wenn diese nicht als Störgröße erkannt werden. Der Brandmelder „IQ8Quad" ist für diese Störgrößen-Erkennung besonders ausgelegt. Zu den zu überwachenden Flächen zählen neben dem Produktionsbereich auch Hochregallager, Bürogebäude, Werkstätten, eine Kläranlage sowie explosionsgefährdete Areale.

Für die gesamte Überwachungsfläche von über 100.000 m² sind 13 Brandmelderzentralen vorgesehen, an die insgesamt 82 Ringleitungen angeschlossen sind. Die Vernetzung der Zentralen erfolgt über 500 kB Essernet-Module.

Die installierten Brandmelder decken nahezu die gesamte Palette der verfügbaren Typen ab. Neben rein optischen Brandmeldern erfüllen auch knapp 2000 O²T-Melder mit ihrer zur Falschalarmunterdrückung entwickelten Zweiwinkeltechnik die anspruchsvollen Aufgaben. Multifunktionale Melder schließlich, die zusätzlich über eine integrierte Alarmierung verfügen, vervollständigen die Überwachung. Neben knapp 200 konventionellen Signalgebern, die entweder akustisch oder optisch alarmieren, kommen weitere kombinierte Signalgeber der neuen Generation zum Einsatz.

In den Ex-Bereichen sind speziell hierfür zugelassene Melder mit ATEX-Zulassung eingesetzt. Über 80 Rauchansaugsysteme der FAAST XM-Serie mit fünf konfigurierbaren Alarmstufen und dem sogenannten Acclimate-Modus sind dafür geeignet, auch bei abgestuften Alarmkonzepten verwendet zu werden. 310 Handfeuermelder ergänzen die technischen Komponenten hinsichtlich einer optimalen Überwachung und ermöglichen so den am Standort beschäftigen Mitarbeitern, sich beruhigt auf Ihre Tätigkeiten zu konzentrieren. ■

Kontakt

Honeywell Building Products Fire
Novar GmbH
Neuss
Tel.: +49 2131 40615 600
info@esser-systems.com
www.esser-systems.com

© Sara Winter/Getty Images

Errichterimpulse 2018

Die Veranstaltungsreihe „Errichterimpulse“, die im vergangenen Jahr ins Leben gerufen wurde, ist bei vielen Entscheidern der Brandschutz- und Sicherheitstechnik gut angekommen. Das erfolgreiche Programmformat wird daher 2018 mit zahlreichen Seminaren für Fachplaner und Facherrichter fortgesetzt. Auch in diesem Jahr stehen hochkarätige Netzwerk- und Weiterbildungsangebote auf dem Programm. Geplant ist auch eine Exkursion ins Herz der Digitalisierung, dem Silicon Valley. „Bei der Auswahl der Themen und Referenten haben wir uns an den Wünschen und Bedürfnissen der Facherrichter orientiert“, so Stefan Schraner, Initiator der Veranstaltungsreihe. „Deshalb stehen auch die Trendthemen Fachkräftemangel und Digitalisierung im Fokus.“ Weitere Themen, Termine und Anmeldung unter:

www.errichter-impulse.de, www.schraner.de ■

Rauchwarnmelder-Schnittstelle zur Elektroinstallation

Das Ausgangsmodul Ei428H von Ei Electronics lässt sich auf der Hutschiene von Verteilerschränken und damit in unmittelbarer Nähe zu Steuereinheiten der Haus- und Gebäudeautomation installieren. Im Brandfall wird die Gefahrenwarnung von funkvernetzten Rauch-, Wärme- und Kohlenmonoxidwarnmeldern über den potentialfreien Kontakt zuverlässig und direkt weitergegeben. Zusätzlich zur lokalen Gefahrenwarnung können Aktionen ausgelöst werden, wie z. B. das Einschalten des Lichts, das Abschalten des Herds oder die Anwahl einer Telefonnummer über ein Telefonwählgerät. Durch weitere akustische bzw. optische Signalgeber wird ein Alarm auch für nicht unmittelbar anwesende Personen hör- und sichtbar gemacht.

www.eielectronics.de ■

Brandschutz neu gedacht

Die Cebit 2018, Messe für Informationstechnik, wandelt sich und wird vom 11. bis 15. Juni als Business-Festival für Innovation und Digitalisierung auf Hannovers Messegelände ausgetragen. Als Unternehmen, das sich stets neuen Anforderungen stellt, präsentiert sich die Wagner Group am 360°dc-Gemeinschaftsstand D99 in Halle 12. Im Fokus: Brandschutzlösungen der Zukunft für Rechenzentren. Als Anlagenbauer mit eigener Forschungs- und Entwicklungsabteilung hat sich der Brandschutzexperte Wagner auf innovative Lösungen für wertkonzentrierte und prozesssensible Bereiche spezialisiert. Rechenzentren, EDV- und IT-Räume benötigen als solche einen besonderen Brandschutz. Damit im Brandfall nicht stromlos geschaltet werden muss – Datenverluste sind da vorprogrammiert –, bietet Wagner Brandbekämpfungssysteme an, die auf Gaslöschung basieren. FirExting bekämpft Brände effektiv und rückstandsfrei. Je nach Anforderungen der Betreiber und der individuellen Gegebenheiten vor Ort, werden als Löschgase Stickstoff sowie Kohlendioxid und Novec 1230 eingesetzt.

Eine andere Möglichkeit, Bränden in Rechenzentren aktiv vorzubeugen, bietet das Brandvermeidungssystem OxyReduct. Es setzt an, bevor sich ein Brand entwickeln kann, und schützt vor brandbedingten Verlusten von Daten und betriebsgefährdenden Unterbrechungen. Der Sauerstoffgehalt im zu schützenden Bereich wird dafür unter die Entzündungsgrenze der dort vorherrschenden Materialien abgesenkt und kontrolliert auf diesem Niveau gehalten. Der benötigte Stickstoff wird bedarfsgerecht aus der Umgebungsluft generiert. In Kombination mit FirExting sind mehrstufige Brandschutzkonzepte mit Schnellabsenkung möglich. Wie Sauerstoffreduktion funktioniert, erleben Besucher am Stand von Wagner live vor Ort in einer OxyReduct-Kabine.

Die Basis jeder Brandschutzlösung bildet immer ein Brandfrüherkennungssystem. Titanus-Ansaugrauchmelder erkennen Brandursachen bis zu 2.000-mal schneller als herkömmliche Punktmelder. Speziell für Serverschränke ist der Titanus Rack·Sens entwickelt worden. Der 44,45 mm hohe Brandmelder (eine Höheneinheit) lässt sich problemlos implementieren und kann optional um eine Brandbekämpfung erweitert werden.

www.wagnergroup.com ■

GIT CYBER SECURITY

2018

EIN SPECIAL VON GIT SICHERHEIT + MANAGEMENT

DIE RICHTIGEN SCHUTZMASSNAHMEN GEGEN CYBER-ATTACKEN

WILEY

ZVEI-UMFRAGE

Sicherheitslagebild auf Grundlage der ZVEI-Umfrage

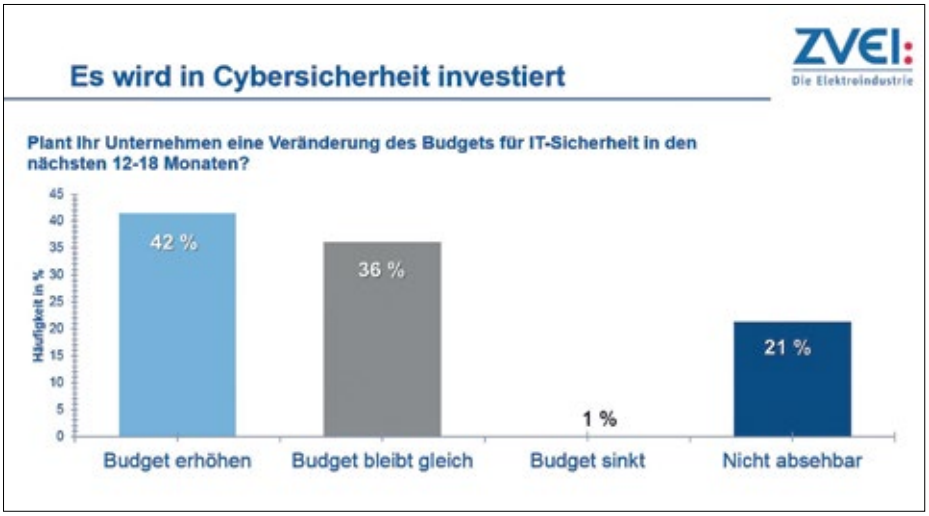
ZVEI-Sicherheitslagebild: Wie steht es um die Cybersicherheit in der Elektroindustrie?

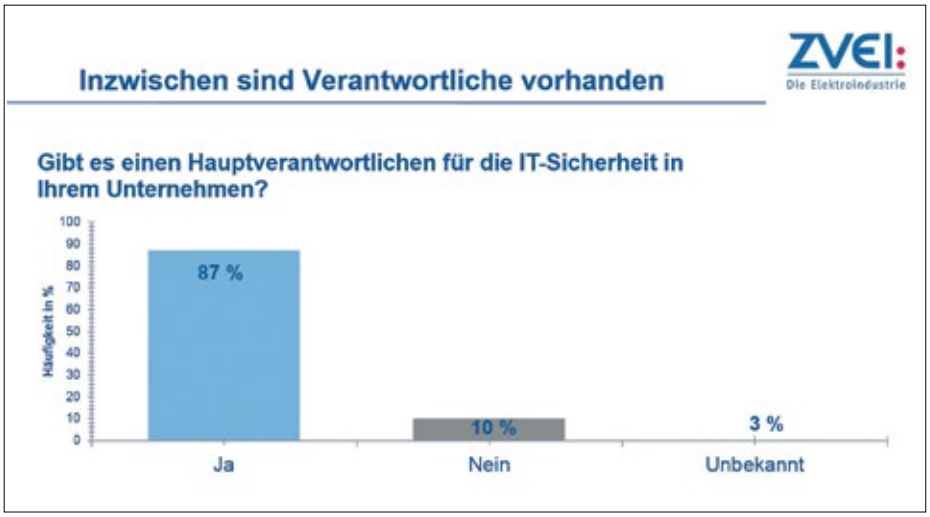
In einer Zeit, in der die Anzahl der Cyberangriffe in allen Lebensbereichen steigt, lohnt es sich, die aktuelle Cybersicherheitslage genau zu kennen. Denn nur so lassen sich die richtigen Schritte für mehr Cybersicherheit einleiten. Um diese Basis zu schaffen, hat der ZVEI - Zentralverband Elektrotechnik und Elektronikindustrie bereits im Jahr 2016 das Pilotprojekt „Sicherheitslagebild im Fachverband Automation" erfolgreich abgeschlossen. Es zeigt: Nahezu jedes Unternehmen in der Automationsbranche ist mit kleineren und mittleren Angriffen konfrontiert, drei von zehn Unternehmen müssen regelmäßig schwere Vorfälle bewältigen.

Nun hat der ZVEI das Sicherheitslagebild auf die gesamte Elektroindustrie erweitert: Gemeinsam mit dem BSI (Bundesamt für Sicherheit in der Informationstechnik) hat der Verband eine Mitgliederumfrage zur Cybersicherheit in den Unternehmen durchgeführt. Insgesamt nahmen daran 101 Unternehmen aus 21 unterschiedlichen Industriesektoren teil, von denen die meisten KMUs mit bis zu 1.000 Mitarbeiter waren. Die Fragen umfassten sowohl Office- als auch Produktions-IT.

Cybersicherheit in der Elektroindustrie: Wie ist die Branche aufgestellt?

Zu den wichtigsten Erkenntnissen aus der Befragung gehört, dass das Thema Cybersicherheit definitiv in der Branche angekommen ist. So bezeichnen es 88 Prozent der Teilnehmenden als Topthema der Geschäftsführung. Die große Mehrheit der befragen Unternehmen (87 %) beschäftigen zudem einen Hauptverantwortlichen für IT-Sicherheit.





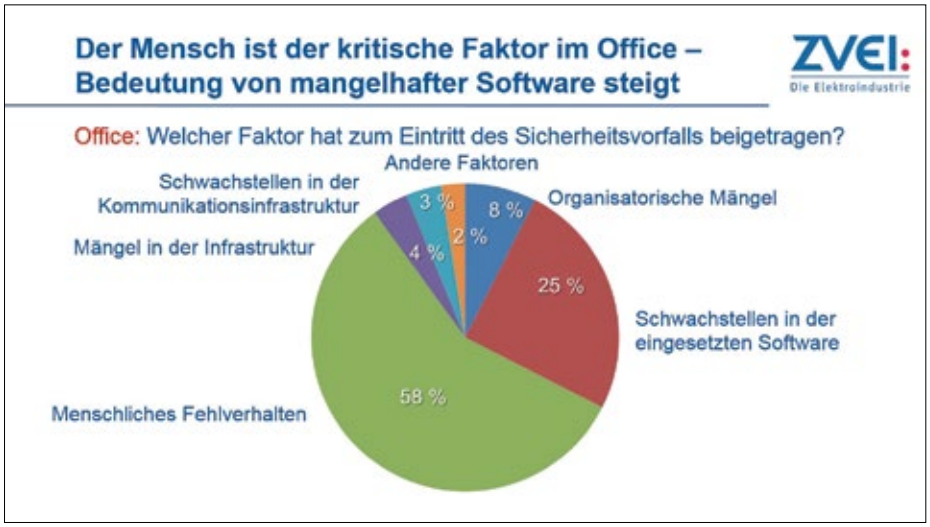
© Quelle: ZVEI/Frederik Böttche

Ein Security-Engineering für Produkte, d. h. ein Fokus auf Cybersicherheitsaspekte schon im Entwicklungsprozess, ist noch nicht die Regel, wird aber durch die Unternehmen aufgebaut, um „Security-by-Design" umsetzen zu können. Standardmaßnahmen wie Prozesse für Vorfälle, Passwort- und Rechtemanagement und Backups sind dagegen in den meisten Unternehmen implementiert. Ein gutes Drittel (33 %) führt Risikoanalysen für alle Bereiche ihrer Firma durch, weitere 23 Prozent im Bürobereich sowie 15 Prozent für die Produktions-IT. Deutlich wird außerdem, dass mit der erhöhten Relevanz von Cybersicherheit auch mehr finanzielle Mittel für diesen Bereich einhergehen: 42 Prozent der Befragten planen, ihr Budget zu erhöhen, weniger will fast niemand (1 %) für Cybersicherheit ausgeben. Positiv zu sehen ist, dass das Geld ganzheitlich in IT-Sicherheit investiert wird: Neben Technik (37 %), fließen auch in Prozesse (32 %) und Neuanstellungen und/oder Schulungen (20 %) finanzielle Mittel. Hindernisse für Investitionen stellen neben der Qualifizierung des Personals (25 %) vor allem die Inkompatibilität der Lösung mit dem Bestand (17 %) sowie die Intransparenz des Markts (16 %) dar. Hier müssen aus Sicht des ZVEI die Anbieter an Verbesserungen arbeiten.

Sicherheitsvorfälle und Ursachen: Woran liegt es, wenn Cyberangriffe erfolgreich verlaufen?

Cyberangriffe gehören zum Alltag. Das bestätigen die befragten Unternehmen: In den vergangenen zwei Jahren waren 60 Prozent von ihnen von Trojanern und Ransomware betroffen. 9 Prozent geben an, dadurch einen Schaden von mindestens 100.000 Euro erlitten zu haben. Aber was sind die Hauptursachen für geglückte Cyberangriffe? Im Bürobereich ist menschliches Fehlverhalten mit 58 Prozent Hauptfaktor für Sicherheitsvorfälle, danach kommen Schwachstellen in der eingesetzten Software (25 %). In der Produktion sind letztere die häufigste Ursache für Vorfälle (29 %), dicht gefolgt von menschlichem Fehlverhalten (22 %) sowie organisatorischen Mängeln (19 %). Damit gewinnt die Bewertung und Prüfung von eingekaufter Soft- und Hardware in der Branche an Bedeutung. 39 Prozent der Befragten haben das erkannt und geben an,

Bitte umblättern ▶



© Quelle: ZVEI/Frederik Böttche

dass das Thema Vertrauenswürdigkeit von eingekauften Komponenten relevant für das Supply-Chain-Management ist. 28 Prozent messen dem noch keine hohe Bedeutung zu. Nach Auffassung des ZVEI herrscht hier Verbesserungsbedarf: Neben Know-how-Aufbau in puncto Cybersicherheit ist die Vertrauenswürdigkeit von eigenen und Drittprodukten aus Sicht des Verbands ein entscheidender Faktor, um Cyberangriffen zu begegnen. Aus diesem Grund bietet der ZVEI am 19. Juni 2018 einen „ZVEI-Expertentag Vertrauenswürdigkeit" an, der Verantwortlichen für Supply-Chain-, Produkt- und Qualitätsmanagement sowie Produktsecurity Informationen zu rechtlichen Aspekten, Möglichkeiten bei der Bewertung und Prüfung sowie Lösungsansätzen für Industrie- und Konsumgüter vermittelt. Trotz der hohen Anzahl an Cybersicherheitsvorfällen, halten sich die daraus entstandenen Schäden bisher in Grenzen. So geben 39 Prozent an, keinen Schaden erlitten zu haben, 27 Prozent nennen Finanzschäden, 13 Prozent Datenverlust. Auffallend ist aus Sicht des ZVEI, dass Imageschäden nur fünf Prozent der entstandenen Schäden ausmachen.

Unterstützung im Kampf gegen Cyberkriminalität

Trotz häufiger Cyberattacken und der hohen Zahl an Betroffenen verläuft die Zusammenarbeit zwischen Unternehmen und Ermittlungsbehörden noch nicht optimal. Hauptursache dafür ist fehlendes Vertrauen in die Arbeit der Behörden. So haben 83 Prozent der Teilnehmer angegeben, einen mutwillig verursachten Vorfall nicht zur Anzeige gebracht zu haben, da die Erfolgsaussichten als gering eingestuft (21 %) oder die Täter im Ausland, und damit außerhalb der Zugriffsmöglichkeiten nationaler Behörden, vermutet werden (weitere 20 %). Das ist insofern von Bedeutung, als dass das vermutete Argument „Angst vor Reputationsschäden" nicht der entscheidende Faktor zu sein scheint (die sehen nur 2 % als Hindernis). Dies bestärkt den ZVEI darin, sich weiterhin für eine verstärkte europäische und internationale Zusammenarbeit bei der Verfolgung von Cyberkriminalität einzusetzen. Neben staatlichen Stellen bietet auch die Allianz für Cyber-Sicherheit kostenlos Hilfestellung für Unternehmen. Ihre Mitglieder unterstützt die Allianz mit BSI-Warnungen, aktuellen Lagebildern, Lösungshinweisen und verschiedenen Schulungsangeboten. Laut der Umfrage ist sie allerdings nur knapp der Hälfte der Befragten bekannt.

intersec
forum
CONFERENCE REVIEW
Artikel war Thema beim Intersec Forum 2018

Fazit

Das Sicherheitslagebild zeigt, dass die Branche beim Aufbau von Cybersicherheits-Kompetenz vorangekommen ist. Ihre Bedeutung als Voraussetzung für die Digitalisierung ist erkannt worden. Eine Baustelle bleibt das Zusammenspiel mit den Security-Anbietern und Dienstleistern. Hier finden die Unternehmen noch nicht das Maß an Flexibilität und Anpassungsfähigkeit an ihre Bedürfnisse, das sie brauchen. Gleichzeitig wird klar sichtbar, wo noch Verbesserungsbedarf besteht: Security-Engineering muss konsequent eingeführt und Security-Standards (z. B. IEC 62443) angewendet werden. Bei der Bekämpfung von Cybercrime müssen die Behörden mehr leisten, um das Vertrauen in die staatliche Handlungsfähigkeit zu erhalten. Schließlich ist die Zusammenarbeit von Industrie, Behörden und Kunden – zum Beispiel über die Allianz für Cyber-Sicherheit – der Schlüssel zu mehr Cybersicherheit in der Elektroindustrie. ■

Kontakt:
Lukas Linke
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
Senior Manager Cybersecurity
Project Manager (IPMA-GPM)
Frankfurt am Main
Fon: +49 69 6302-432
linke@zvei.org
www.zvei.org

INDUSTRIAL SECURITY

Sicher in die digitale Zukunft – Industrial Security

Industrial Security sichert industrielle Kommunikations- und Produktionssysteme, damit die Industrie sicher und zuverlässig produzieren kann. Dabei hat der Maschinen- und Anlagenbau eine Doppelrolle inne. Einerseits setzt er als Betreiber der Anlagen darauf, Produktionsprozesse zu digitalisieren. Andererseits entwickelt er als Integrator neue Maschinen, Anlagen, Dienste sowie Geschäftsmodelle im Rahmen von Industrie 4.0 für seine Kunden. So trägt der Maschinen- und Anlagenbauer eine große Verantwortung, wenn er Security-Anforderungen formuliert und die darauf basierenden Maßnahmen entwickelt, implementiert und aktualisiert.

Steffen Zimmermann, Leiter Competence Center Industrial Security beim VDMA

Warum Security so wichtig ist

Bei der Security-Umfrage des VDMA aus dem Jahr 2017 berichteten 59 Prozent der befragten Mitglieder davon, dass sich die Anzahl der Security-Vorfälle in ihrem Unternehmen erhöhen wird. Viele Unternehmen im Maschinen- und Anlagenbau setzen zeitgleich auf neue Dienstleistungen, zum Beispiel Predictive Maintenance. Die vorausschauende Wartung ist auf Betriebsdaten angewiesen, die jederzeit korrekt und zur richtigen Zeit am richtigen Ort verfügbar sein müssen. Werden diese Anforderungen nicht erfüllt, können Maschinen- und Anlagenbauer Predictive Maintenance als Dienstleistung nicht zuverlässig mit hoher Qualität anbieten. Zwei der wichtigen Ziele der Industrial Security lauten demzufolge Integrität und Verfügbarkeit.

Der Maschinen- und Anlagenbau muss Vertraulichkeit gewährleisten, damit kein anderer diese Dienstleistung erbringen kann. So stehen Unternehmen vor der Herausforderung, die Integrität, Verfügbarkeit und Vertraulichkeit über den gesamten Zeitraum der Dienstleistung gewährleisten zu müssen – angefangen bei der Planung des Service über die Bereitstellung der Maschine bis hin zum Dauerbetrieb. Gleichzeitig müssen Betreiber ihre bestehenden, meist autarken und statischen Systeme in agile Kommunikationsstrukturen einbetten. Die dafür nicht geschaffenen Maschinen und Anlagen werden oft mit Zeitdruck auf- und umgerüstet, ohne die aus rechtlicher und technischer Sicht notwendigen Anforderungen der Standardisierung und Datensicherheit ebenfalls anzupassen.

Wissensaufbau statt Aktionismus

Je früher Unternehmen Wissen über mögliche Bedrohungen, notwendige Maßnahmen und hilfreiche Informationsquellen im Produktlebenszyklus integrieren, desto nachhaltiger und zuverlässiger werden die tatsächlichen Umsetzungsmaßnahmen sein. Der „Leitfaden Industrie 4.0 Security" des VDMA gibt hierbei zentrale Handlungsempfehlungen für die Integration von Security in Produkten und Systemen.

Geballtes Know-how für Mitglieder

Der VDMA hat verschiedene Gremien zu den Themen Industrial Security und Informationssicherheit ins Leben gerufen: Das VDMA Competence Center Industrial Security wurde Anfang 2017 gegründet und fungiert als zentraler Ansprechpartner für Politik, Wissenschaft, Normung und Mitgliedsunternehmen. Daneben bildet der VDMA-Arbeitskreis Industrial Security das zentrale Netzwerk von Herstellern, Integratoren, Betreibern, Dienstleistern, Forschung und Behörden. Er dient dem Wissensaustausch zur Security in Produktion und Automation. ■

intersec
forum
CONFERENCE REVIEW
Artikel war Thema beim Intersec Forum 2018

Kontakt

VDMA Verband Deutscher Maschinen- und Anlanbau e.V.
Frankfurt

Steffen Zimmermann
Leiter Competence Center Industrial Security
Tel.: +49 69 6603 1978
steffen.zimmermann@vdma.org

VIDEOSICHERHEITSTECHNIK

Cyber Security bei Videoanlagen

BHE liefert wichtige Hinweise für Errichter, Planer und Betreiber

Digitalisierung und Vernetzung verändern auch die Videosicherheitstechnik grundlegend: Klassische analoge Videokameras mit direkt zugeordneten (dedizierten) Videoaufzeichnungsgeräten (Recordern) werden ersetzt durch immer leistungsfähigere IP-Kameras, die in einer komplexen IT-Infrastruktur betrieben werden. Damit wachsen auch die Herausforderungen, die für einen sicheren Betrieb dieser Anlagen zu meistern sind.

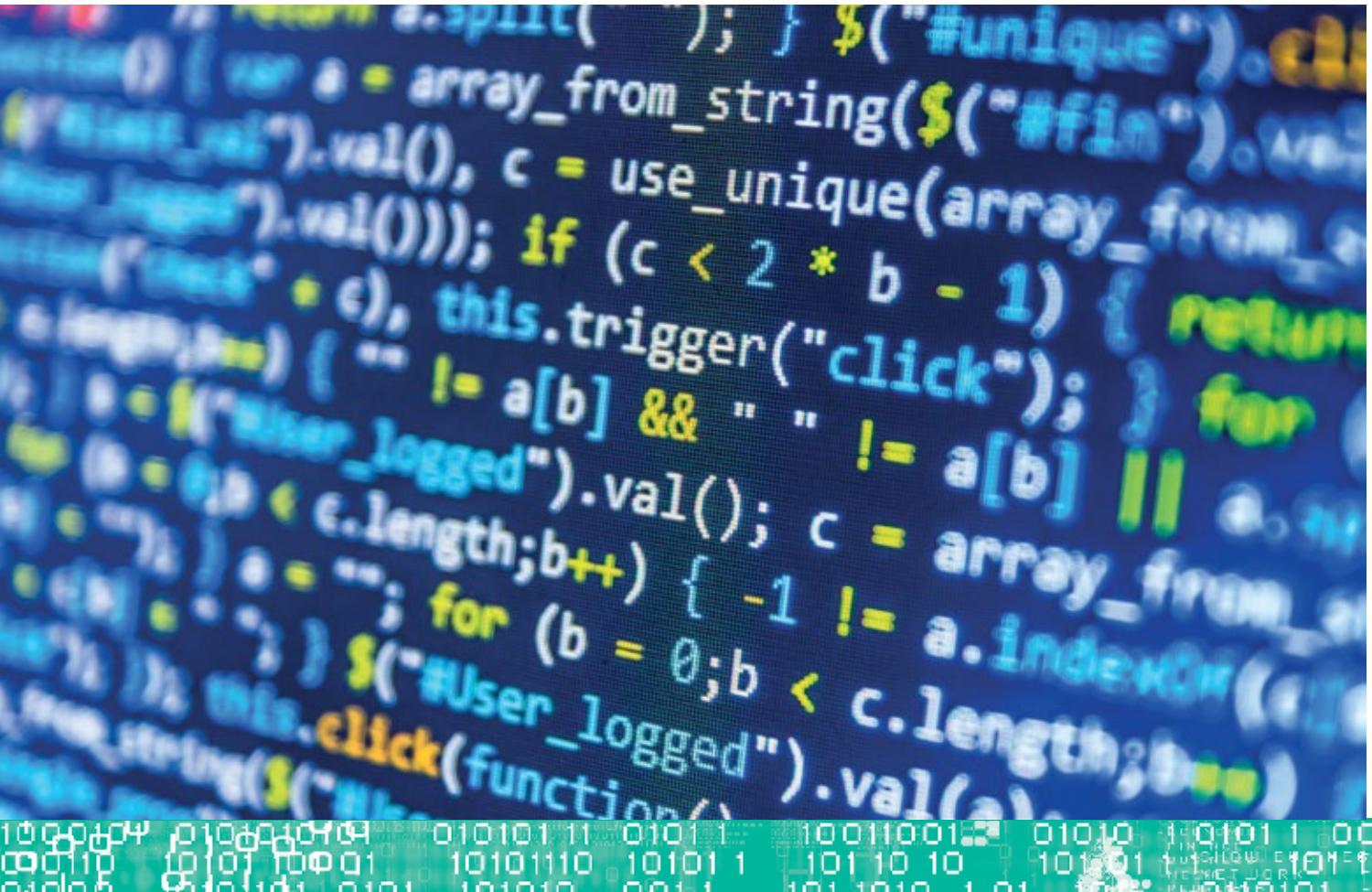
Das Thema Sicherheit wird meist intuitiv mit Angriffen von außen in Verbindung gebracht. Folgerichtig unterliegen bei den üblichen Firewall-Einstellungen vor allem jene Verbindungen strengen Regeln, die von außen (aus dem Internet) nach innen (in das private Netz, LAN) aufgebaut werden.

Hingegen wird der Aufbau von Verbindungen von innen nach außen meist nicht oder nur wenig reglementiert, um den Zugriff der Anwender auf die verschiedenen weltweiten Internet- Anwendungen und Dienste nicht zu beeinträchtigen.

Unterschätztes Risiko „Embedded Systems"

Embedded Systems bergen Risiken, weil sie durch die Firewall von innen nach außen Verbindungen aufbauen können. Ist eine solche Verbindung erst einmal hergestellt, können Angreifer darüber das Gerät steuern und somit das private Netz (LAN) von innen angreifen. Server und PCs sind als sicherheitsrelevante Technik klar zu erkennen und werden entsprechend sorgfältig in Sicherheitskonzepten berücksichtigt. Risiken, die von eingebetteten Systemen ausgehen, werden dagegen häufig unterschätzt, weil bei diesen Geräten die Hauptfunktion im Mittelpunkt steht und nicht auf den ersten Blick zu erkennen ist, was alles im Gehäuse steckt. Eine IP-Kamera ist aber eben nicht nur eine Kamera, sondern ein voll vernetzter Computer mit allen Möglichkeiten und Risiken, die diese komplexe Technik bietet.

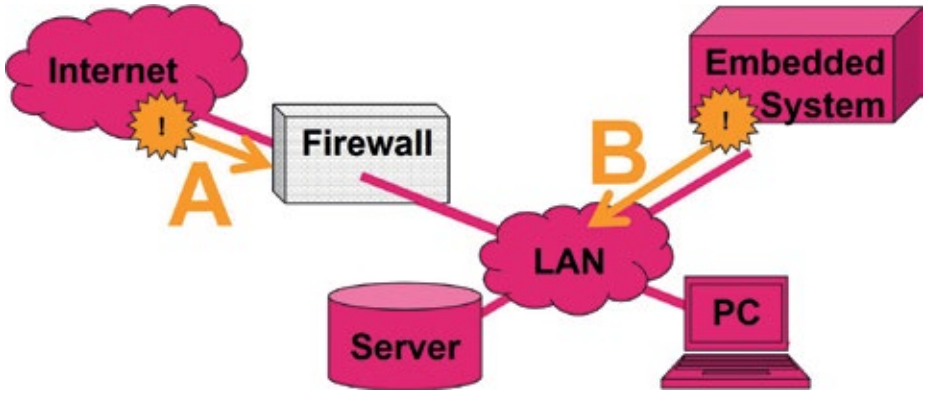
Bei Entwicklung und Auswahl von Embedded Systems stehen meist Funktion und Preis im Vordergrund. Das hat zur Folge, dass die Datensicherheit oft vernachlässigt wird.



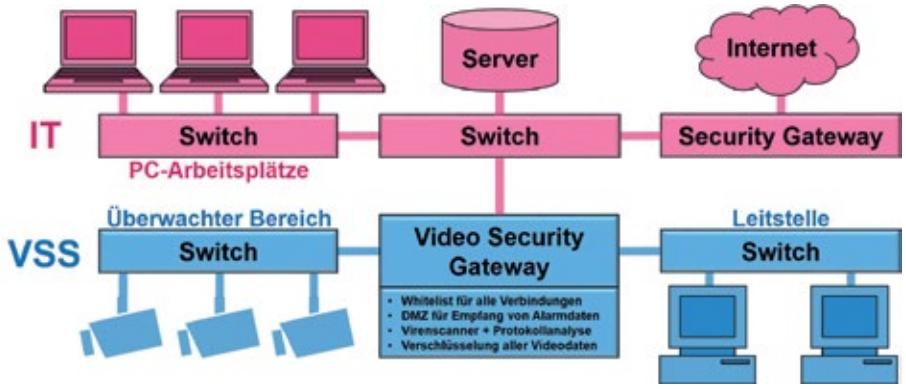
© Mclek/Shutterstock

Embedded Systems

Embedded Systems (eingebettete Systeme) sind Computer, die für einen bestimmten technischen Zweck in ein Gerät eingebaut werden und dort – für den Anwender oft unsichtbar – ihren Dienst tun. Mit Produkten aus dem Smart- Home-Bereich, „intelligenten" Lautsprechern, Alarmanlagen und auch IP-Kameras halten sie Einzug in viele private Netze, ohne dass den Anwendern die damit verbundenen Gefahren bewusst sind.



Netze sind oft nur gegen Angriffe von außen (A) geschützt. Die Erfahrung zeigt jedoch, dass Angriffe auch von innen (B) erfolgen. Viele Videoanlagen sind dagegen unzureichend geschützt. Statt zu mehr Sicherheit führen solche Anlagen zu mehr Risiko. Hier besteht dringender Handlungsbedarf für Errichter und Betreiber



Videonetz im Kundennetz – Kaskadierter Schutz: Strenge Sicherheitsregeln des VSS können möglicherweise nicht an der beim Kunden bereits vorhandenen Firewall umgesetzt werden, weil dort noch anderer Datenverkehr fließt, der flexibler gehandhabt werden muss. Lösung: Zweites Security Gateway zwischen Kunden- LAN und Video-LAN

Viele Embedded Systems bauen bereits ab Werk automatisch Verbindungen zu externen Servern auf, etwa für Updates, Fernwartung oder zum Speichern von Daten in der „Cloud". Diese Verbindungen unterlaufen die Firewall; der Anwender hat in der Regel keine Kontrolle darüber, welche Daten über diese Verbindungen transportiert werden. Bei manchen Geräten sind Hintertüren bekannt geworden, die versehentlich oder absichtlich eingebaut wurden. Mitunter werden Geräte auch gezielt von Geheimdiensten, Industriespionen oder der organisierten Kriminalität manipuliert. Solche kompromittierten Systeme stellen ein erhebliches Sicherheitsrisiko für das gesamte betroffene Netzwerk und Unternehmen dar.

Dieses Risiko ist nicht abstrakt und theoretisch, sondern ganz konkret und hat in der Praxis bereits zu erheblichem wirtschaftlichen Schaden geführt. Das zeigen folgende Beispiele:

- Eine russische Hackergruppe hat im Zuge der Kampagne „Carbanak" u.a. Überwachungskameras in Banken kompromittiert und konnte Millionenbeträge erbeuten.
- Die Schadsoftware „Mirai" hat u.a. zahlreiche Überwachungskameras für einen DDoS-Angriff genutzt.
- Überwachungskameras des amerikanischen Herstellers „NetBotz" waren jahrelang mit einer Hintertür in vielen Unternehmen und kritischen Bereichen eingesetzt, u.a. in Serverräumen.

Auch aus Gründen der Informationssicherheit und des Datenschutzes müssen Errichter und Betreiber von Videosicherheitssystemen sicherstellen, dass nur berechtigte Nutzer auf die Geräte und Daten zugreifen können.

Herausforderung IP

Für klassische Videoüberwachungsanlagen hat sich die Abkürzung „CCTV" etabliert. Das CC steht für „Closed Circuit". Damit ist gemeint, dass nur ein geschlossener Benutzerkreis auf diese Anlage und ihre Daten zugreifen kann. Mit der Umstellung auf IP ist grundsätzlich ein weltweiter Zugriff möglich. Deshalb muss durch geeignete technische Vorkehrungen dafür gesorgt werden, dass auch IP-basierte Videoanlagen wieder zu geschlossenen Systemen werden.

Während Anwender von ihrem IT-Endgerät (PC, Smartphone) weltweit uneingeschränkten Zugriff auf alle Anwendungen und Dienste wünschen, sollen bei Video Sicherheits Systemen (VSS) die Bilder einer begrenzten Anzahl Kameras nur auf einer wohldefinierten Auswahl von Monitoren dargestellt werden. VSS erlauben und erfordern deshalb engere Regeln als allgemeine IT-Systeme.

Die oberste Sicherheitsregel lautet: Das Netzwerk darf ausschließlich nur die explizit gewünschten Verbindungen zulassen; dann können embedded Systeme keine Verbindung zu einem Angreifer aufbauen. Das Risiko unerwünschter Verbindungen lässt sich durch geeignete technische Vorkehrungen vermeiden. Die so gewonnene Sicherheit rechtfertigt den größeren Aufwand und die höheren Kosten. Zumal die ohne Vorkehrungen zu befürchtenden Schäden sehr viel höher wären. Der Sicherheit stehen oft entgegen

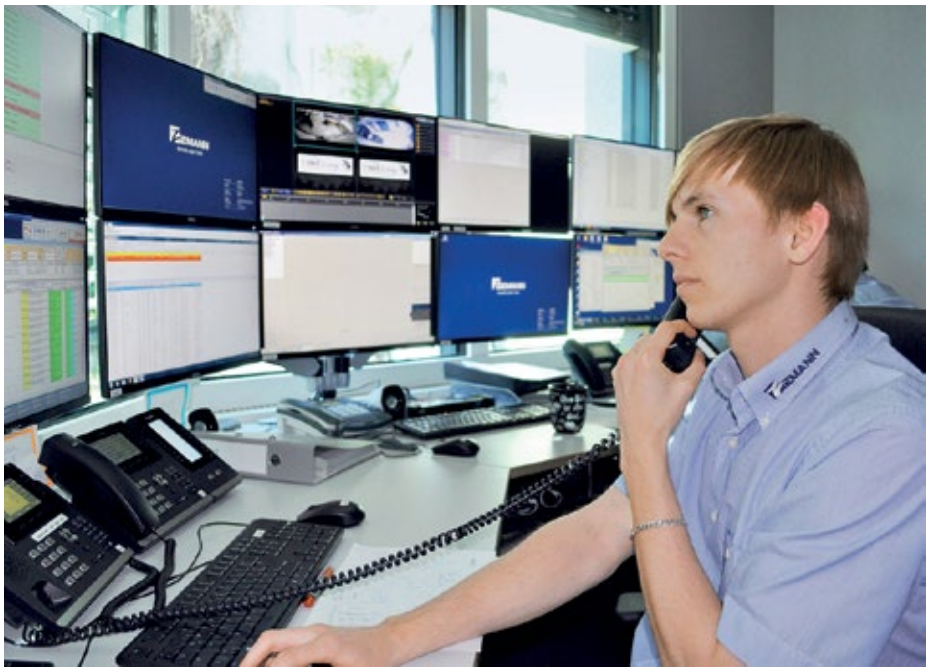
- Bequemlichkeit
- mangelnde Kenntnisse
- Kosten sparen „um jeden Preis"

Von Vorteil ist, bereits bei der Planung einer Videoanlage ein passendes Sicherheitskonzept zu wählen.

Mögliche Ursachen für Angriffe von innen

- von Anwendern eingebrachte Schadsoftware / Plugins
- Backdoors der Hersteller, z.B. für Support, Behörden etc.
- Sicherheitslücken (fehlende Updates, Standard- Passworte)
- Verbindungen für Updates, Video-Hosting, Fernwartung etc.
- für Spionagezwecke präparierte Geräte

Bitte umblättern ▶



© Ziemann Sicherheit GmbH

Vernetzung mit Leitstellen: besondere Ansprüche an IT-Sicherheit. Enge Zusammenarbeit zwischen Errichter und Leitstelle ist wichtig

Im beim BHE erhältlichen Papier „Cyber Security bei Videoanlagen" werden verschiedene Lösungsalternativen in der Reihenfolge von „ganz sicher" bis „voll vernetzt" aufgezeigt, die je nach gegebener Aufgabenstellung auch miteinander kombiniert werden können.

Lösungsalternativen

- 1. Einfach und sicher – separate Netze: Ein separates Netz für Video bringt die größte Sicherheit und wird deshalb vom BHE empfohlen. Die physikalische Trennung der Leitungen kann von keiner Software überwunden werden. Höhere Kosten oder fehlende Kabeltrassen zwingen aber oft dazu, Video über vorhandene Kabel zu transportieren.
- 2. Mehrere Netze auf einem Kabel – VLAN: Mit einem Virtual Local Area Network (VLAN) kann vorhandene Verkabelung genutzt werden, um darauf mehrere logisch getrennte Netze zu realisieren. Dies erfordert durchgängig VLAN-fähige aktive Netzwerkkomponenten (statisches oder tagged VLAN nach IEEE 802.1Q) und eine konsequente fachgerechte Konfiguration.
- 3. Ein sicherer Tunnel für Daten auf ihrem Weg durch das Internet – VPN: VPN ist das Mittel der Wahl wenn sensible Daten über das Internet übertragen werden sollen. Es ist darauf zu achten, dass alle Videodaten stets im LAN, VLAN und VPN verbleiben. Alle internen und externen Verbindungen außerhalb dieser geschützten Bereiche sind zu unterbinden.
- 4. Sichere Verbindung nach außen – Video Security Gateway: Wenn doch Verbindungen zu anderen Netzen benötigt werden, sollten diese durch einen speziellen Netzwerkübergang (Gateway) geschützt werden. Ein Video Security Gateway überwacht alle ein- und ausgehenden Verbindungen und kombiniert dabei verschiedene Sicherheitsmaßnahmen, die speziell auf die Belange der Videosicherheitstechnik abgestimmt werden.
- 5. Konsequente Verschlüsselung für alle vertraulichen Videodaten: Eine durchgängige „Ende-zu-Ende-Verschlüsselung" von der Kamera bis zum Monitor gewährleistet, dass niemand unbefugt auf die Videodaten zugreifen kann. Dies ist insbesondere dann geboten, wenn Videodaten z.B. in der „Cloud" gespeichert werden sollen. Entscheidend: Wer besitzt den Schlüssel?

Video-Security-Gateway

Wichtig ist bei allen Lösungen, dass auf mögliche Netzwerkkopplungen geachtet wird: Alle Geräte, die an mehrere Netze angeschlossen sind, können (ggf. auch ungewollt) Verbindungen zwischen diesen Netzen herstellen. Deshalb dürfen alle Geräte jeweils nur an ein Netz angeschlossen werden. Sind weitere Kommunikationsbeziehungen nötig, so dürfen diese nur über ein Security Gateway erfolgen.

Ein Video-Security-Gateway enthält u.a. folgende Sicherheitsfunktionen:

- Firewall: Lässt nur explizit gewünschte Verbindungen zu
- Router: Stellt nach vorgegebenen Regeln Verbindungen her
- NAT: Verbirgt die IP-Adressen des internen Netzes
- DMZ: Pufferzone zwischen äußerem und innerem Netz
- Protokollanalyse: Verdächtigen Datenverkehr erkennen
- Virenscanner: Prüft alle Daten auf verdächtige Strukturen

Firewall

An der Firewall sollten zunächst alle ein- und ausgehenden Verbindungen gesperrt werden. Dann werden gezielt ausschließlich nur die explizit vom Kunden gewünschten und benötigten Verbindungen freigegeben. Diese Whitelist sollte regelmäßig geprüft und nicht mehr benötigte Einträge entfernt werden.

Welche Sicherheitseinstellungen eine Firewall bietet und wie diese konfiguriert werden, hängt vom jeweiligen Hersteller und Produkt ab. Neben fundierten Kenntnissen über digitale Netze ist deshalb auch eine Schulung speziell zu den verwendeten Produkten nötig, damit ein Errichter seine Arbeit ordnungsgemäß ausführen kann.

Wichtig ist ein ganzheitlicher Ansatz: Auch wenn die Videoübertragung z.B. nur für TCP/IPv4 ausgelegt ist, könnte Schadsoftware auch IPv6, ICMP, DNS oder den UDP-Protokollstack nutzen. Schadsoftware zweckentfremdet gern Standardports und unverdächtige Protokolle. Da sie nur spontan aktiv wird, muss das Gateway dauerhaft alle Verbindungen überwachen, nicht nur die vom VSS genutzten.

Auswahl des passenden Lösungsansatzes

Welche Lösung für welchen Anwendungsfall optimal ist, hängt von den Anforderungen und Randbedingungen der jeweiligen Projekte ab. Einige Beispiele sollen dies verdeutlichen:

- Wenn die Entfernungen zwischen Kameras und Monitoren nicht zu groß und geeignete Kabeltrassen frei zugänglich sind, ist die Einrichtung eines separaten Videonetzes die einfachste, sicherste und auch kostengünstigste Lösung.
- Wenn auf bestimmten Strecken eine eventuell bereits vorhandene IP-Verkabelung mitgenutzt werden soll, bietet sich VLAN als Lösung an.
- Für den Fernzugriff auf Videobilder durch das Internet stellt VPN die passende Lösung dar.
- Werden weitere Verbindungen benötigt (etwa zu einem Management-System) oder soll das Videosystem in ein Kundennetz integriert werden, sollte ein Video-Security-Gateway zwischengeschaltet werden.

■ Sollen vertrauliche Videodaten im Internet übertragen oder gespeichert werden (z.B. bei „Cloud- Lösungen"), ist eine zuverlässige durchgehende Verschlüsselung geboten.

Kein Formalismus kann ersetzen, dass Planer und Errichter von Fall zu Fall sorgfältig abwägen, wie die jeweiligen Anforderungen des Kunden am besten umgesetzt werden können, denn hier spielen noch eine Fülle weiterer Parameter eine Rolle. Fachkundigen Rat bietet beispielsweise der BHE.

Authentifizierung

Es muss damit gerechnet werden, dass Angreifer und Schadsoftware die Standard-Passwörter (default passwords) vieler Produkte kennen, denn Listen dieser Passwörter sind im Internet frei zugänglich. Unmittelbar bei der Erstinbetriebnahme müssen deshalb auf jedem Gerät eigene „starke" Passwörter konfiguriert und die vom Hersteller vorkonfigurierten Benutzerkonten gelöscht werden.

Hersteller sollten verhindern, dass ihre Produkte mit Standard- Passwörtern im Wirkbetrieb genutzt werden, etwa durch wiederholte Hinweise und indem die Gültigkeit der initialen Zugangsdaten begrenzt wird.

Feste IP-Adressen verwenden

Um variable (dynamische) IP-Adressen nutzen zu können, wird ein Domain Name System (DNS) benötigt. Dieses ist jedoch angreifbar (z.B. mit DDoS). Manipulierte DNS-Einträge können Verbindungen zu ungewollten Gegenstellen bewirken. Nach der täglichen Zwangstrennung und Neuzuweisung einer dynamischen IP-Adresse ist eine Aktualisierung der DNS-Einträge notwendig. Während dieses Vorgangs, der mehrere Minuten dauern kann, ist keine Verbindung möglich. Dynamische IP-Adressen sind deshalb nicht für sicherheitsrelevante Anwendungen geeignet!

Vom BSI empfohlene Maßnahmen

Das „Bundesamt für Sicherheit in der Informationstechnik" (BSI) empfiehlt in seinem Dokument „Sicherheit von IP-basierten Überwachungskameras" (Version 1.10 vom 08.11.2016) die folgenden Maßnahmen:

- Ungeschützte Erreichbarkeit über das Internet vermeiden
- Ausgehende Kommunikation durch Firewall einschränken
- Selbstgewählte hinreichend starke Passwörter verwenden
- Fernzugriff nur über VPN ermöglichen
- Nur benötigte Dienste aktivieren
- Nur verschlüsselt kommunizieren
- Beachtung des EOS Zeitraums
- Einsatz ausreichend starker Authentisierungsmechanismen
- Netzwerkseparation einsetzen a
- Zeitnahes Einspielen von Updates
- Monitoring der Kommunikation (Logfiles)
- Cloud-Konzepte vermeiden
- Wi-Fi/WLAN in kritischen Bereichen vermeiden
- Optionale Verwendung von Rechte- und Rollenkonzepte
- Optional Verwendung physikalischer Zugriffsschutz

Achtung: Haftungsrisiko

Wenn Errichter von Sicherheitssystemen bei ihren Projekten den anerkannten Stand der Technik nicht kennen bzw. nicht anwenden, gehen sie möglicherweise ein erhebliches Haftungsrisiko ein, falls ihre Kunden durch die von ihm installierte Technik Schaden erleiden.

Als „anerkannter Stand der Technik" können beispielsweise die Empfehlungen des BSI gelten.

Möglicherweise können in einzelnen Projekten nicht alle empfohlenen Sicherheitsmaßnahmen umgesetzt werden. Dies sollte dann mit den Kunden detailliert besprochen und die Kunden sorgfältig beraten werden. Außerdem sollten sich die Errichter ggf. schriftlich bestätigen lassen, wenn der Kunde beispielsweise aus Kostengründen bewusst auf bestimmte Schutzmaßnahmen verzichtet.

Aufschaltung von Videosystemen auf Leitstellen

Videokameras bringen nur dann einen Sicherheitsgewinn, wenn auf alle relevanten Ereignisse schnell reagiert wird. Deshalb ist die Aufschaltung von Videosicherheitssystemen auf rund um die Uhr besetzte, professionelle Leitstellen ein wichtiger Zusatznutzen, den Errichter ihren Kunden anbieten bzw. den Betreiber, Kunden bei ihren Dienstleistern nachfragen sollten. Mit diesem Thema beschäftigt sich auch das BHE-Papier „Notruf- und Service-Leitstellen (NSL): Gute Gründe für eine Videoaufschaltung".

Fazit: Neue Herausforderungen

Die Technik entwickelt sich rasant weiter, die Angreifer wenden immer raffiniertere Methoden an. Auf diese Weise entstehen neue Bedrohungen, auf die reagiert werden muss. Moderne Videoanlagen sind komplexe IT-Systeme, die für einen sicheren Betrieb eine kontinuierliche fachgerechte Wartung erfordern. Dazu gehört, dass sämtliche Systemkomponenten regelmäßig mit Updates auf den neuesten Stand gebracht werden. Errichter sollten deshalb vor Auswahl und Einsatz aller Systemkomponenten (PCs, Software, Router, IPKameras etc.) klären, ob und wie lange der jeweilige Hersteller Softwarepflege für seine Produkte gewährleistet, in deren Rahmen auch alle neu erkannten Sicherheitslücken geschlossen werden. In Zukunft ist mit weiteren, neuartigen Bedrohungen zu rechnen. Aktuell werden beispielsweise Risiken durch „Air Gap Hacking" in Betracht gezogen: IP-Kameras könnten über einen angeschlossenen IR-Scheinwerfer mittels einer Art „Morsezeichen" vertrauliche Informationen nach außen senden, ohne dass dazu eine Netzwerkverbindung nötig ist. Errichter sollten sich deshalb über neue Entwicklungen stets auf dem Laufenden halten.

> „Als „anerkannter Stand der Technik" können beispielsweise die Empfehlungen des BSI gelten. "

Das Informationspapier, Quellen und weiterführende Infos zum Thema sind über den BHE erhältlich. ■

Autoren
Michael Meissner,
Vorsitzender des FA Video im BHE Bundesverband Sicherheitstechnik e.V.

Hardo Naumann,
Mitglied im FA Video

Kontakt

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

Peter Martin Schroer, Geschäftsführer von ene't: „Wir waren positiv überrascht, wie schnell Rittal vom Angebot bis zum Projektstart reagierte und zudem eine auf unsere Anforderungen angepasste individuelle Lösung präsentierte"

TITELTHEMA

IT auf Nummer sicher

Rechenzentrum-Container von Rittal für höchste Ausfallsicherheit bei IT-Systemhaus ene't

ene't ist ein auf die Energiebranche spezialisiertes IT-Systemhaus, das seinen Kunden branchenspezifische Anwendungen als Service und stets aktuelle Daten zum Strom- und Gasmarkt liefert. Hierfür betreibt das Unternehmen ein eigenes Rechenzentrum mit höchsten Sicherheitsstandards. Und das muss ausfallsicher sein. Unser Titelthema zu Cyber-Security, physikalische und organisatorische Sicherungsmaßnahmen – und ein effizientes Rechenzentrum.

Aufgebaut wie ein modernes Inhouse-Rechenzentrum: Kaltgangeinhausung für IT-Racks ermöglicht die energieeffiziente Klimatisierung der IT-Systeme

Bereits im Jahr 2002 erkannten die Firmengründer der ene't GmbH die hohe Komplexität rund um die Kalkulation von Strom- und Gaskosten im Energiemarkt und wollten hierfür entsprechende Software-Lösungen anbieten. Denn: Die zur Preisfindung benötigten Kosten präzise zu bestimmen, ist für die Marktteilnehmer wie Erzeuger, Netzbetreiber und Stadtwerke keine leichte Aufgabe, da die Anbieterlandschaft in viele regionale Versorger unterteilt ist. Eine Lösung bieten die intelligenten Software-Anwendungen und stets aktuelle Tarifdatenbanken zu den aktuellen Netzentgelten von ene't.

Heute zählt ene't zu einem der führenden Systemhäuser für die deutsche Energiewirtschaft. Software und Services sind hierbei die Eckpfeiler des Geschäftsmodells. Ein leistungsfähiges und ausfallsicheres Rechenzentrum ist daher entscheidend, um den wirtschaftlichen Erfolg des Unternehmens abzusichern. Auch die mehr als 500 Kunden aus der Energiewirtschaft, darunter etwa 300 Strom- und 200 Gasversorger, vertrauen auf die hohe Verfügbarkeit der IT-Services, die ene't über ein eigenes Rechenzentrum zur Verfügung stellt.

Wachstum erfordert neue IT-Kapazitäten

Wie erfolgreich das Geschäftsmodell tatsächlich ist, zeigt sich an dem rasanten Wachstum von ene't: In nur fünfzehn Jahren kletterte die Zahl der Mitarbeiter von drei auf über 100. Gleichzeitig haben viele Unternehmen der Energiewirtschaft ihre eigene digitale Transformation gestartet und immer mehr IT-Services in ihre Prozesse zur Kalkulation integriert – auch die Leistungen von ene't. So stellt ene't heute viele Applikationen als Software-as-a-Service (SaaS) zur Verfügung, damit die Kunden schnell und unkompliziert über das Internet auf die Applikationen zugreifen können. Damit haben sich die Anforderungen an die interne IT-Infrastruktur bei ene't immer weiter erhöht.

Im Jahr 2016 wurde schließlich ein Geschäftsvolumen erreicht, das ein neues Rechenzentrum notwendig machte. Ein Ausbau der bestehenden Räume war nicht möglich und eine größere Integration von Public Cloud-Ressourcen war nicht gewollt. Das neue Rechenzentrum sollte sehr schnell realisiert werden und höchsten Ansprüchen an IT-Sicherheit und Ausfallsicherheit genügen. So fiel die Entscheidung auf einen Rechenzentrums-Container, der auf dem Firmengelände im Freien positioniert werden sollte.

Container-Rechenzentrum mit höchsten Sicherheitsstandards

Im September 2016 begann das Projekt – mit ersten Gesprächen bei möglichen Lieferanten. Zu den Anforderungen zählten höchste physische Sicherheit, eine redundant ausgelegte Infrastruktur, bestmögliche Energieeffizienz und vor allem kurze Lieferzeiten. Das Ziel: Im Mai 2017 mit der neuen IT-Umgebung durchzustarten. Ein solcher Zeitrahmen ist nur machbar, wenn hierbei vorkonfigurierte Komponenten für ein Container-Rechenzentrum zum Einsatz kommen, die einen risikofreien und raschen Aufbau der Infrastruktur ermöglichen.

Den Zuschlag für das Projekt hat nach einem Auswahlverfahren schließlich Rittal erhalten. „Wir waren positiv überrascht, wie schnell Rittal vom Angebot bis zum Projektstart reagierte und zudem eine auf unsere Anforderungen angepasste individuelle Lösung präsentierte", sagt Peter Martin Schroer, Geschäftsführer, ene't. Die Rechenzentrums-Experten konfigurierten auf Basis der von ene't gelieferten Leistungsdaten zwei Container, die die komplette IT beinhalten können und heute auf dem Firmengelände stehen. Aus modularen Komponenten ist eine Lösung entstanden, die voll und ganz den individuellen Kundenanforderungen entspricht.

Aufgebaut sind die Container wie ein modernes Inhouse-Rechenzentrum. Eine Kaltgangeinhausung für die IT-Racks ermöglicht die energieeffiziente Klimatisierung der IT-Systeme. Solar-Panele auf dem Dach verbessern nochmals die Energiebilanz der Gesamtanlage. Die Kühlung übernehmen sechs Rittal Liquid Cooling Packages (LCP) – Luft-Wasser-Wärmetauscher an den Racks – in redundanter Auslegung. Diese wurden großzügig dimensioniert, damit sie nicht an der Kapazitätsgrenze laufen und um eine bestmögliche Energieeffizienz sowie eine künftige Erweiterung zu unterstützen.

In den beiden Containern ist Platz für zwölf IT-Racks, von denen aktuell vier ausgebaut sind. Hier hat ene't ausreichend Kapazität, um das künftige Firmenwachstum auch IT-technisch zu verarbeiten. Aktuell befinden sich die gesamten Entwicklungs- und Produktivumgebungen in den IT-Containern.

Umfassende Sicherheitsvorkehrungen

In einem separaten Technikraum innerhalb der Container sind die USV-Systeme untergebracht. Diese sind ebenfalls redundant ausgelegt und sichern den IT-Betrieb bis zu drei Stunden über Batterien. Das System ist so konzipiert, dass jeder Server und jeder Switch über zwei Netzteile versorgt wird, die jeweils über eine voneinander unabhängige Stromeinspeisung verfügen. Sollte der Strom über längere Zeit ausfallen, versorgt ein Notstromaggregat mit einer Dieselreserve für 24 Stunden das gesamte System.

Der Container wurde im Außenbereich des Firmengeländes auf einem massiven Betonsockel platziert und ist für Besucher des Unternehmens nicht sofort sichtbar. Zudem ist das Rechenzentrum auf den ersten Blick nicht als technische Installation erkennbar, da zum Beispiel auf auffällige Beschriftungen verzichtet wurde. Darüber hinaus sind die Türen in stabiler Bauweise ausgelegt und die Zugänge sind dreifach abgesichert. Das gesamte System ist zudem über eine Alarmanlage gesichert.

Bitte umblättern ▶

ene't, auf die Energiebranche spezialisiertes IT-Systemhaus: mit selbst entwickelter Software und aktuellen Daten zu Strom- und Gasmarkt kalkulieren Erzeuger, Netzbetreiber und Versorger bestmögliche Endverbraucherpreise

Lösung aus modularen Komponenten: Rechenzentrums-Experten von Rittal konfigurierten auf Basis der von ene't gelieferten Leistungsdaten zwei IT-Container, die die komplette IT beinhalten können und heute auf dem Firmengelände stehen

Sauerstoffgehalt unter 14 Prozent: Oxy-Reduct-Anlage sorgt für eine dauerhafte Sauerstoffreduktion der Luft innerhalb des Containers, sodass keine offenen Brände entstehen können – schon bei einer Konzentration von 17 Volumenprozent können Elektronikbauteile nicht mehr Feuer fangen

IT-Verantwortlicher Falk Heinen: „Laufende Detailentscheidungen konnten wir gemeinsam mit den Experten von Rittal jederzeit rasch und sehr zielführend beantworten, wodurch sich Abläufe insgesamt beschleunigten"

In einem separaten Technikraum innerhalb der Container sind die USV-Systeme untergebracht. Diese sind ebenfalls redundant ausgelegt und sichern den IT-Betrieb bis zu drei Stunden über Batterien

Eine Oxy-Reduct-Anlage sorgt für eine dauerhafte Sauerstoffreduktion der Luft innerhalb des Containers, sodass praktisch keine offenen Brände entstehen können. Hierfür wird der Sauerstoffgehalt auf 14 Prozent gesenkt. Schon bei einer Konzentration von 17 Volumenprozent können Elektronikbauteile nicht mehr Feuer fangen – normale Luft enthält in einer Standardumgebung 20,9 Prozent Sauerstoff. Sowohl im Bereich der Racks, als auch im Technikraum ist eine Brandfrüherkennung untergebracht. Zusätzlich ist im Technikraum eine Löschanlage installiert.

Alles im Blick

Dem umfassenden Monitoring-System innerhalb des Containers entgeht kein Detail: Es erfasst die Meldungen von physikalischen Sensoren und meldet jede noch so geringe Abweichung vom Normalbetrieb. Ergänzend hierzu erfasst die Rittal CMC III-Monitoring-Lösung zentrale Parameter innerhalb der IT-Schränke, wie Temperatur, Luftfeuchte, Sauerstoffgehalt, Rauchentwicklung oder geöffnete Türen und gibt diese Meldungen an den zentralen IT-Leitstand weiter. Eine weitere Besonderheit ist eine von ene't entwickelte Übersichtskarte des Containers, in die der Status aller Sensoren eingeblendet wird. Somit erfassen die IT-Administratoren rein visuell sofort den aktuellen Betriebszustand der Gesamtanlage.

„Mit unseren Alarmsystemen und Sensoren haben wir alle relevanten Details innerhalb und außerhalb des Containers stets im Blick. Damit ist unser Container überwacht wie ein Patient auf einer Intensivstation", sagt Falk Heinen, IT-Verantwortlicher, ene't.

Auf Nummer sicher gehen

Die Datensicherheit und Hochverfügbarkeit spielen bei dem Geschäftsmodell von ene't eine wichtige Rolle. Daher sind alle Komponenten des Rechenzentrums redundant ausgelegt, inklusive der Stromeinspeisung und der Internet-Anbindung.

„Unsere Kunden verlangen stets verfügbare IT-Services, daher benötigen wir eine absolut ausfallsichere IT-Infrastruktur. Fällt das Rechenzentrum aus, haben wir ein echtes Problem", sagt Roland Hambach, ene't-Geschäftsführer. „Mit der von Rittal gelieferten Container-Lösung sind wir höchst zufrieden, da wir hiermit unsere High Availability-Anforderungen für die Rechenzentrum-Infrastruktur bestens erfüllen können".

Hand in Hand für den Projekterfolg

Aus Sicht von ene't war ein wichtiger Aspekt bei diesem Projekt, dass die Zusammenarbeit mit externen Partnern und Lieferanten reibungslos funktioniert – insbesondere bei dem engen Zeitplan. „Laufende Detailentscheidungen konnten wir gemeinsam mit den Experten von Rittal jederzeit rasch und sehr zielführend beantworten, wodurch sich Abläufe insgesamt beschleunigten", kommentiert Falk Heinen.

Autor
Michael Nicolai
Leiter Technischer Projektvertrieb
Deutschland bei Rittal

Autorin
Patricia Späth
Referentin Referenzmarketing bei Rittal

Kontakt

Rittal
Herborn
Tel.: +49 2772 505 0
info@rittal.de
www.rittal.de

WILEY

Anbieter? Dann jetzt Sponsor werden!

GIT CYBER SECURITY

GIT Cyber Security

Die richtigen Schutzmaßnahmen gegen Cyber-Attacken.

GIT Cyber Security erscheint 2018 als Special in GIT SICHERHEIT, als **gedruckte Ausgabe,** als **e-Paper,** als speziell auf dieses Thema zugeschnittene **digitale Microsite** – und in ganz neuem Format als **Smart Magazine.** Mit den wichtigsten Informationen, Lösungen und Konzepten für alle Entscheider in Sachen IT-Security. Die Management-Ebene mit CEO, COO und CIO – und die für Sicherheit verantwortlichen Fachebenen in Organisationen, Behörden und Industrie.

Wenn Sie Anbieter von Lösungen, Produkten und Konzepten für Cyber Security sind, dann kontaktieren Sie uns jetzt. **Werden Sie Partner und Sponsor.**

Kontakt:
heiko.baumgartner@wiley.com
steffen.ebert@wiley.com

Das Thema: Cyber Security – welchen Cyber-Gefahren sind Unternehmen und Organisationen ausgesetzt, welche Security-Services, Trainings, Schulungen helfen bei der Abwehr. Konzepte gegen Ransomware und DDoS-Attacken. Cloud, Government und Industrial Cyber Security. Konzepte für sicheres Industrie 4.0, Embedded Systems, virtualisierte Umgebungen und Data Center.

Die Zielgruppe: Obere Management-Ebene und Sicherheits-Chefs in Organisationen, Behörden und Industrie. Sicherheitsverantwortliche für IT und physikalische Sicherheit. Sicherheitsprofis, die Schutzkonzepte planen, errichten und integrieren.

Das Konzept: Wir stellen die wichtigsten Erkenntnisse, Lösungen und bereits verfügbare Services und Produkte in Sachen Cyber Security für die Zielgruppe übersichtlich und kompakt zusammen.

Der Cross-Media-Ansatz: Verfügbar als Smart Magazine, Microsite, e-Paper und als gedruckte Printausgabe. Bespielung aller digitalen und klassischen Informationskanäle.

Vorteil für Anbieter: Wir vermarkten das Thema und die Inhalte sechs Monate lang mit jeweils passenden Intensitäten, Instrumenten und Kanälen.

Vorteil für Anwender: Informationsvorsprung für die Leser und Entscheider.

http://www.git-sicherheit.de/whitepaper/it-und-it-security/git-cyber-security-2018-heft-e-paper-und-microsite

Die besten Cyber-Security-Konzepte für die Entscheider in Organisationen, Behörden und Industrie.

GIT SICHERHEIT + MANAGEMENT
MAGAZIN FÜR SAFETY UND SECURITY

www.GIT-SICHERHEIT.de

INDUSTRIE 4.0

Cyberangriffe gegen Industrie-Rechner

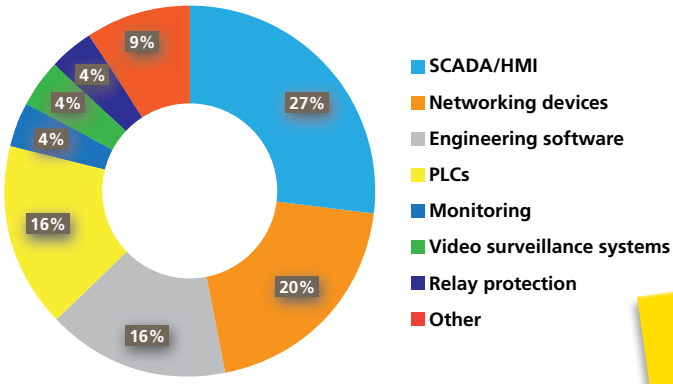
Verstärkter Krypto-Malware-Befall bei Industrierechnern nach Bitcoin-Boom

In Zeiten von Industrie 4.0 haben viele Branchen mit Cyberattacken zu kämpfen – allen voran Unternehmen der Sektoren Energie, Maschinenbau und ICS-Integration – aber auch in anderen Branchen nimmt die Zahl der Angriffe zu. Das zeigt eine vor kurzem veröffentlichte Studie: Im Kaspersky-CERT-Bericht zu Cyberbedrohungen für industrielle Automationssysteme wurden Angriffe analysiert, die sich gegen Automationssysteme und speziell gegen Rechner für industrielle Kontrollsysteme (ICS, Industrial Control Systems) richten. In der zweiten Jahreshälfte 2017 gab es demnach überwiegend viele Cyberattacken auf Organisationen aus diesen Bereichen.

Mangelnde Cybersicherheit von Industrieanlagen kann zu erheblichen Konsequenzen für Industrieprozesse und den Umsatz führen. Die Experten des Kaspersky ICS CERT haben die derzeitigen Cybergefahren und Trends für industrielle Systeme untersucht. Demnach wurden 38,7 Prozent der analysierten ICS-Rechner der Energiebranche und 35,3 Prozent der industriellen Rechner in den Bereichen Maschinenbau und ICS-Integration in der zweiten Jahreshälfte 2017 mindestens einmal von Malware angegriffen.

Die Baubranche verzeichnete im Vergleich zum ersten Halbjahr den höchsten Anstieg. Hier waren 31,1 Prozent aller ICS-Rechner von einem Angriff betroffen. Automatisierung ist für diese Branche ein noch neues Gebiet und der Cybersicherheit wird damit noch nicht die

© WrightStudio - stock.adobe.com



© Grafik: Kaspersky Lab

Vielfältig verletzlich: Systeme im Industrieumfeld

Mehr Informationen zu den Cyberbedrohungen für industrielle Automationssysteme enthält der aktuelle Kaspersky-Bericht unter

https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h2-2017/85053/

nötige Aufmerksamkeit gewidmet. In anderen Branchen wie Nahrungsmittel, Bildung, Gesundheitswesen, Telekommunikation, Industriebeteiligungen, Versorgung und Fertigung lag der Anteil bei knapp unter 30 Prozent. Eine große Mehrheit der Angriffe kann dabei als Zufallstreffer gewertet werden.

Die Energiebranche ist Vorreiter beim breiten Einsatz von Automatisierungslösungen, und zählt zu den Branchen mit dem höchsten Rechnereinsatz. Moderne Stromnetze gehören zu den ausgedehntesten Systemen miteinander verbundener Industrieanlagen mit vielen Rechnern, die zugleich relativ gefährdet sind. Die Cybersicherheitsvorfälle der vergangenen Jahre sowie verschärfte Auflagen zwingen Strom- und Energiekonzerne zu einer Anpassung der Cybersicherheit ihrer Systeme im Bereich Operative Technologie (OT). Weitere, ernste Probleme der letzten Jahre wurden hier von Zulieferern versursacht.

„Die Ergebnisse unsere Untersuchung attackierter ICS-Rechner aus verschiedenen Branchen haben uns überrascht. So zeigt zum Beispiel der große Prozentsatz angegriffener ICS-Rechner bei Unternehmen der Strom- und Energiebranche, dass deren Bemühungen um die Cybersicherheit ihrer Automationssysteme nach einigen schweren Vorfällen nicht ausreichen. Noch sind zahlreiche Schlupflöcher offen für Cyberangreifer", sagt Evgeny Goncharov, Leiter des Kaspersky Lab ICS CERT.

Bitte umblättern ▶

Report: Trends bei Angriffen

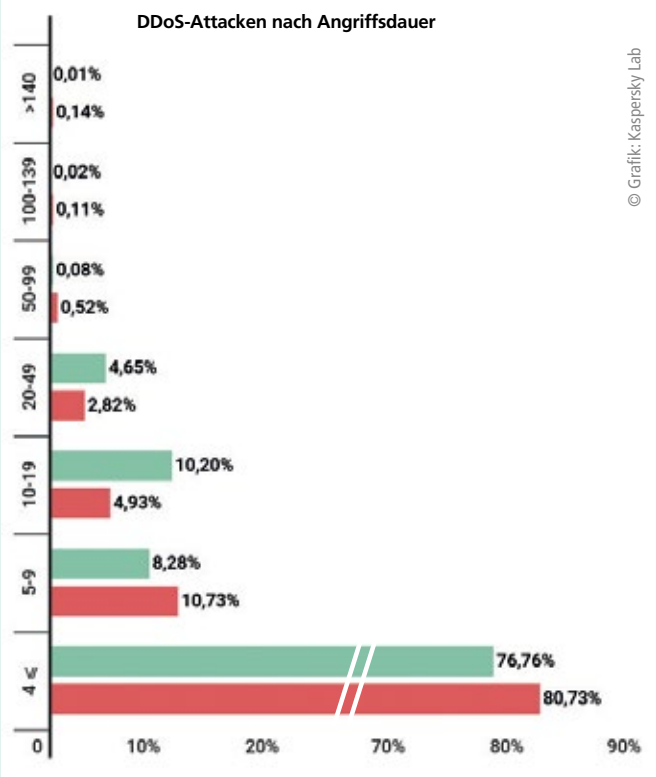
Im ersten Quartal 2018 hat Kasperky Lab die am längsten andauernde DDoS-Attacke seit Ende des Jahres 2015 gemessen – mit einer Dauer von 297 Stunden (mehr als 12 Tage). Weitere Trends: ein Anstieg bei Verstärkungsangriffen und der Aktivität alter und neuer Botnetze, sowie die Rückkehr von Deutschland in die Top-10 derjenigen Länder, die die meisten für DDoS-Angriffe verwendeten C&C-Server hosten.

Laut Kaspersky-Report haben DDoS-Botnetze im ersten Quartal 2018 Web-Ressourcen in 79 Ländern weltweit attackiert. Erneut führen China, die USA und Südkorea die Liste der am stärksten betroffenen Länder an. Das gilt sowohl für die Anzahl der Server, die den Angreifern zur Verfügung stehen, als auch für die Anzahl der dort gehosteten Websites und Services. Hongkong und Japan haben inzwischen die Niederlande und Vietnam aus den Top-10 der am stärksten betroffenen Länder verdrängt. Deutschland liegt hier auf dem achten Platz.

Noch markantere Veränderungen gebe es unter den Top-10 der Länder, in denen sich die meisten für DDoS-Attacken genutzte Command-and-Control-Server (C&C-Server) befinden, so die Studie. Neben Italien, Hong Kong und Großbritannien ist dort jetzt Deutschland auf Platz sieben vertreten. Das gehe vermutlich auf die Anzahl aktiver C&C-Server von Darkai (einem Klon des berüchtigten Mirai-Botnetzes) und den erheblichen Anstieg bei AESDDoS-Bots zurück. Zudem hätten die bekannten Botnetze Xor und Yoyo ihre Aktivität wieder aufgenommen. Obwohl es sich bei den meisten um Linux-Botnetze handele, sei deren Anteil gegenüber dem vierten Quartal 2017 leicht zurückgegangen, nämlich von 71 auf 66 Prozent.

Verstärkungsangriffe wieder populär?

Die in ihrer Mächtigkeit beispiellosen Memcached-Verstärkungsangriffe prägten das Ende des ersten Quartals 2018. Die Kaspersky-Experten gehen davon aus, dass diese Angriffe nur sehr kurzzeitig populär sein dürften, denn neben den eigentlichen Zielobjekten



werden auch die Unternehmen geschädigt, die unwissentlich an der Durchführung der Angriffe beteiligt sind. Insgesamt gewannen Verstärkungsangriffe im ersten Quartal 2018 wieder an Fahrt, nachdem sie vorher zurückgegangen waren.

„Cyberkriminelle, die sich auf DDoS-Botnetze spezialisiert haben, nutzen bevorzugt Schwachstellen aus", erklärt Alexey Kiselev, Project Manager im DDoS Protection Team bei Kaspersky Lab. „Bereits die ersten Monate des Jahres 2018 haben gezeigt, dass von DDoS-Angriffen nicht nur die eigentlichen Ziele betroffen waren, sondern auch jene Unternehmen, deren Infrastruktur Schwachstellen birgt. Das bestätigt einmal mehr, dass jedes Unternehmen zur Implementierung mehrschichtiger Cybersicherheit auch die regelmäßige Beseitigung von Schwachstellen und einen dauerhaften Schutz gegen DDoS-Angriffe integriert haben sollte."

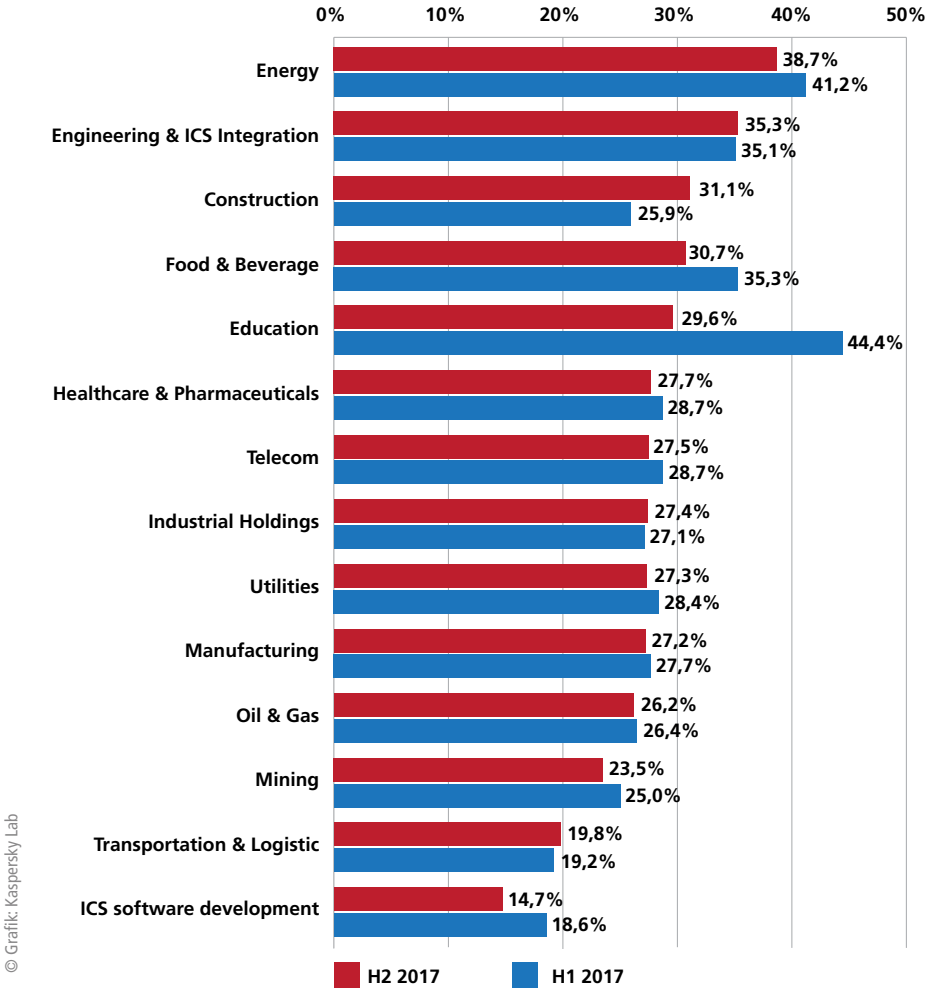
Krypto-Malware bei Industrierechnern angekommen

Auch ICS-Rechner erfahren seit September 2017 verstärkt Angriffe mit Krypto-Malware. Die Experten von Kaspersky ICS CERT führen dies auf den allgemeinen Trend Hype von Bitcom und Co. zurück. Haben schädliche Mining-Aktivitäten zum heimlichen Schürfen digitaler Währungen auf Rechnern im industriellen Umfeld einen bestimmten Umfang erreicht, hat dies negative Auswirkungen auf die Leistung und Stabilität der ICS-Rechner. Von Februar 2017 bis Januar 2018 griff Mining-Malware 3,3 Prozent aller Rechner zur industriellen Automation an. In den meisten Fällen erfolgten die Attacken rein zufällig.

Zahlen aus dem aktuellen Kaspersky-Bericht:

- Bei 37,8 Prozent aller ICS-Rechner, die über Kaspersky-Lösungen geschützt waren, wurden Infektionsversuche blockiert (1,4 Prozentpunkte weniger als im Vorjahreszeitraum).
- Das Internet bleibt mit 22,7 Prozent Hauptquelle für ICS-Infektionen. Die Angriffe stiegen gegenüber der ersten Jahreshälfte 2017 um 2,3 Prozent.
- Die Zahl der in der zweiten Jahreshälfte gefundenen Malware-Modifikationen auf ICS-Rechnern stieg von 18.000 auf über 18.900.

2017 wurden 10,8 Prozent aller ICS-Rechner von Botnetz-Agenten angegriffen. Die Attacken erfolgten über das Internet, aber auch über Wechseldatenträger und E-Mails.



© Grafik: Kaspersky Lab

Angegriffene ICS-Rechner nach Industriezweigen

■ Die Experten von Kaspersky ICS CERT fanden im Jahr 2017 63 Schwachstellen in Industrie- und IoT-Systemen, von den 26 durch die Hersteller beseitigt wurden.

„Generell verzeichnen wir im Vergleich zum Jahr 2016 einen leichten Rückgang bei den ICS-Angriffen – vermutlich ein Zeichen dafür, dass Unternehmen der ICS-Cybersicherheit mehr Aufmerksamkeit widmen, beispielsweise mittels Mitarbeiterschulungen und von Audits (Überprüfungen) der industriellen Segmente ihrer Netzwerke. Das ist ein gutes Zeichen, denn für Unternehmen ist es von größter Bedeutung, proaktiv Maßnahmen zu ergreifen, mit denen zukünftige Cybervoralleinsätze vermieden werden können", sagt Evgeny Goncharov.

Schutzempfehlungen

■ Regelmäßige Updates von Betriebssystem, Anwendungs-Software und Sicherheitslösungen auf allen Systemen, die zum industriellen Netzwerk im Unternehmen gehören.

■ Einschränkung des Netzwerk-Verkehrs über Ports und Protokolle auf Edge-Routern und innerhalb des OT-Netzwerks.

■ Audits der Zugangskontrollen auf die ICS-Komponenten im industriellen Netz des Unternehmens einschließlich seiner Grenzen.

■ Einsatz von Endpoint-Sicherheitslösungen für ICS-Server, Workstations und HMIs, um OT und industrielle Infrastruktur vor zufälligen Cyberangriffen zu schützen.

■ Einsatz von Lösungen zum Monitoring des Netzwerkverkehrs sowie zur Analyse und zur Erkennung gezielter Angriffe. ■

Kontakt

Kaspersky Labs GmbH
Ingolstadt
Tel.: +49 841 98 18 90
info@kaspersky.de
www.kaspersky.de

VIDEOTECHNIK

Angriff durch die Hintertür

Schutz gegen Cyber-Angriffe: Auch an die Absicherung der Videosysteme denken!

Die Zahl der über das Internet geführten Cyber-Attacken gegen Hard- und Software wächst täglich. Um an hochsensible Daten zu gelangen, konzentrieren sich Hacker in der jüngsten Vergangenheit auf ansonsten wenig beachtete Geräte im Firmennetzwerk wie Netzwerkdrucker oder Video-Sicherheitssysteme. Ein Beitrag von Pascal Heinkele, Sales Director DACH bei Mobotix.

Hier lässt sich der Cyber Protection Guide herunterladen:
Download unter https://www.mobotix.com/sites/default/files/2018-02-08-17-52/Mx_CyberProtection-Guide_de_20180208.pdf

Es ist ein Einfallstor, das vom Unternehmen selbst geöffnet wird – denn heutige Sicherheitstechnologie ist IP-fähig und mit größeren Netzwerken beziehungsweise direkt mit der Cloud verbunden. Das erlaubt zwar eine größere Funktionalität und Flexibilität, das Sicherheitssystem wird so jedoch zum schwächsten Glied in der IT-Sicherheitskette. Aus diesen Gründen haben gezielte Angriffe auf Video-Sicherheitssysteme deutlich zugenommen und enorme Risiken für Unternehmen in den Fokus gerückt.

Beispielsweise können Kriminelle nicht nur den Video-Livestream abfangen, sondern über die IP-Kamera in das Firmen-Netzwerk eindringen, auf die IT-Infrastruktur eines Unternehmens zugreifen und zu einem umfassenden Cyber-Angriff übergehen. Einmal drinnen, können Hacker erhebliche Schäden verursachen, die weit über einen physischen Vorfall wie Diebstahl oder Sabotage hinausgehen. Selbst ein sicheres Netzwerk kann durch vorinstallierte Malware gefährdet werden, die aus der Ferne und verdeckt aktiviert werden kann.

Häufig werden diese Geräte für Botnets und den Versand von Spam eingesetzt, wodurch die Organisation potenziell für kriminelle Aktivitäten haftbar gemacht werden kann, ohne es überhaupt zu wissen. Zudem kann IoT (Internet of Things) -spezifische Malware Geräte wie z.B. die physische Zugangskontrolle oder Überwachungskameras mit einem Code infizieren, der sie unbrauchbar macht. Die nutzlosen Geräte müssen durch neue und funktionsfähige ersetzt werden. In der Zwischenzeit gewähren sie unbefugten Personen Zugang zu geschützten Bereichen. Diese Risiken zeigen, dass wenig beachtete Geräte im IoT-Verbund eines Unternehmens genau der gleichen Sorgfalt bedürfen wie Server, Rechner und Co.

Sicherheit umfassend gedacht

Von Vorteil ist es deshalb, wenn Lösungsanbieter Cyber-Sicherheit bereits in die Produkt-Philosophie integriert haben. So hat beispielsweise Mobotix mit dem „Cactus Concept" eine umfassende Lösung entwickelt, das jedes Gerät während der Entwicklung, Fertigung und Bedienung umfassend schützt und eine End-to-end-Verschlüsselung im gesamten Nutzungs- und Verwaltungszyklus bietet. Das Konzept stellt einen ganzheitlichen Ansatz zum Schutz von Mobotix-Produkten vor drohenden Cyber-Angriffen in Kombination mit Aufklärung und Tools dar. Die darin enthaltenen Maßnahmen unterstützen gezielt Kunden und Partner dabei, Umgebungen durch Videoüberwachung und Zutrittskontrolle langfristig zu schützen.

Hardware als Bollwerk

So sind bereits hardwareseitig etliche Sicherheitsvorkehrungen getroffen, die sowohl ein sicheres, modifiziertes Linux-Betriebssystem, fortschrittliche Authentifizierungs- und Berechtigungsverfahren wie auch Datenverschlüsselung oder Intrusion Detection abdecken. Für ein Höchstmaß an Cyber-Sicherheit nutzen IT-Administratoren deshalb die auf allen Mobotix-Systemebenen serienmäßig integrierten Sicherungs- und Konfigurationstools. Die Nutzung dieser Tools – im Verbund mit grundlegenden Sicherheitsmaßnahmen wie Firewalls und Netzwerksegmentierungen – reduziert die möglichen Hacker-Angriffsflächen auf ein Minimum.

Optimal konfiguriert

Um die sicherere Systemkonfiguration zu ermöglichen, hat der Hersteller einen Leitfaden erstellt. Dieser „Cyber Protection Guide" enthält alle entscheidenden Admin-Konfigurationsschritte der Einzelkomponenten (Kamera, VMS, NAS), um die gesamte Videoinfrastruktur optimal vor Fremdzugriffen zu schützen. Dazu zählen unter anderem die Aktualisierung der Firmware, Änderung der Passwörter, Anlegen von Benutzergruppen, Deaktivierung oder Beschränkung von Zugriffsrechten, Aktivierung der Intrusion Detection, Einschränkung von Web-Robots, Anpassung von Authentifizierungs- und Verschlüsselungs- oder Port-Parametern sowie die Einrichtung einer OpenVPN-Verbindung für den Fernzugriff. ■

Pascal Heinkele, Sales Director DACH bei Mobotix

Kontakt

Mobotix AG
Langmeil
Tel.: 06302-9816 0
info@mobotix.com
www.mobotix.com

ISOLATIONSTECHNIK

Browser in der Box

So wird das Internet zum sichersten Ort der Welt

Sicherer im Internet unterwegs – dank einer Isolationstechnik, die Malware den Nährboden entzieht

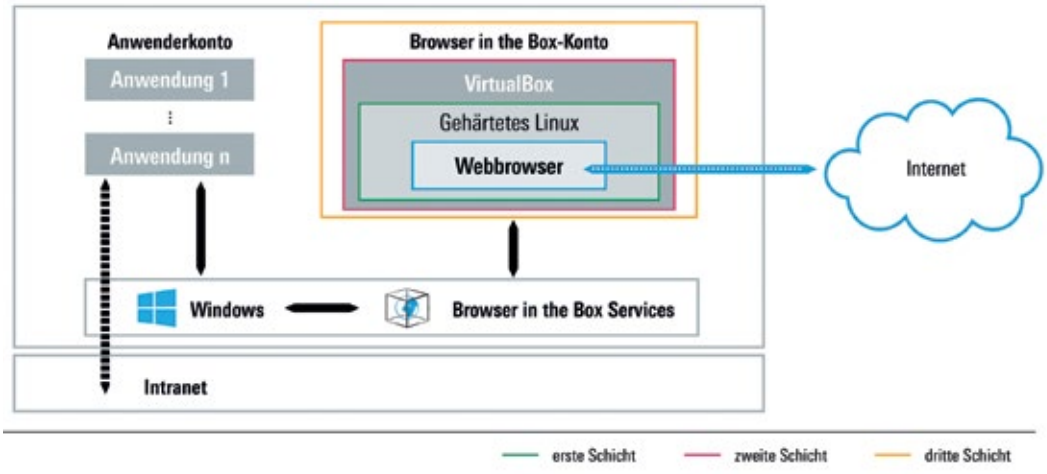
Das Surfen im Internet gehört zum Arbeitsalltag wie der Morgenkaffee. Doch ausgerechnet der dafür benötigte Browser dient Cyberkriminellen zunehmend als Einfallstor für Schadsoftware. Dafür gibt es eine Lösung: Moderne Isolationstechnik entzieht Malware den Nährboden.

Heutige Schadcodes funktionieren immer über eine Verbindung zum Internet – so laden Makroviren weiteren Schadcode nach. Dabei erfolgen 70 Prozent aller Cyberangriffe – wie Zero-Day-Exploits, Ransomware, Viren und Trojaner – über einen Browser bzw. die besuchte Webseite. Problematisch sind dabei vor allem aktive Inhalte auf Internetseiten wie Flash, Java, JavaScript, ActiveX oder HTML. Diese gängigen Programmierschnittstellen erlauben Hackern den Zugriff auf den PC des Users und die Kontrolle über dessen Anwenderumgebung.

Leider bieten traditionelle Sicherheitsbarrieren, wie Antivirensoftware, hier wenig Schutz: Viele Viren durchbrechen diese oft mühelos, weil sie unerkannt bleiben. Wirklichen Schutz bietet jetzt eine neuartige Lösung: die „Vollvirtualisierung".

Virtuelle Surf-Umgebung

Vollvirtualisierte Browser, wie der gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) für den Behördeneinsatz entwickelte Browser in the Box von Rohde & Schwarz Cybersecurity, verfolgen ein „proaktives" Modell: Als Erweiterung zur hardware-basierten Komponente wird eine software-basierte, virtuelle Surf-Umgebung geschaffen. Auf diese Weise wird eine zusätzliche Verbindungs- und Ausführungsschicht etabliert. Konkret: Anstatt – wie bei Antivirenpro-



„Proaktives" Modell: Als Erweiterung zur hardwarebasierten Komponente wird eine software-basierte, virtuelle Surf-Umgebung geschaffen. Auf diese Weise wird eine zusätzliche Verbindungs- und Ausführungsschicht etabliert ▶

grammen – Schadcodes zu erkennen, werden von vorneherein deren Auswirkungen verhindert, indem alle potenziell gefährlichen Aktivitäten in einem geschlossenen virtuellen Browser isoliert werden.

Der Vorteil: Netzwerke werden konsequent getrennt und der Aufbau einer unbekannten und möglicherweise gefährlichen Internetverbindung zur „Nachladung" von Schadcode wird verhindert. Durch eine Isolation des Intranets kann Schadcode selbst im Falle eines Angriffes, beispielsweise bei unabsichtlichem Download von Malware, nicht in das interne Netz vordringen. Gleichzeitig kann die Schadsoftware wie zum Beispiel Ransomware oder Makroviren keine Verbindung zum Internet herstellen, um die eigentliche Schadsoftware herunterzuladen. Statt eines separaten PCs für den Webzugriff wird ein virtueller PC auf dem Arbeitsplatz-PC erzeugt. Betriebssystem und Browser haben keinen direkten Zugriff auf die Hardware, sondern lediglich auf die virtuelle Hardware, die wie eine zusätzliche Schutzmauer agiert.

Eindringende Viren, Trojaner und anderer Schadcode bleiben in dieser Umgebung eingeschlossen und können sich nicht auf dem Rechner und im lokalen Netzwerk verbreiten. Ein Neustart des Browsers erfolgt mit einem virenfreien Zustand.

Unabhängigkeit von Windows-Betriebssystemen

Ein weiterer wesentlicher Sicherheitsfaktor ist das Betriebssystem, das die Vollvirtualisierung nutzt. Denn: Knapp 90 Prozent aller Angriffe sind Windows-basierend. Schwächen innerhalb dieses Betriebssystems – etwa bekannt gewordene Fehler, Bugs, etc. – stellen dann ein hohes Risiko dar. Die Gefahr, sich mit Schadcode zu infizieren, ist daher groß und könnte durch ein anderes Betriebssystem, beispielsweise Linux, bereits deutlich reduziert werden. Browser in the Box setzt daher auf Diversität und ist unabhängig vom Windows-Betriebssystem.

Durch die VPN-Technologie mit einem von Microsoft unabhängigen Netzwerk schafft Browser in the Box eine umfassende Netzwerktrennung. Dadurch kann nur der Browser in the Box via VPN-Tunnel eine Verbindung zum Internet herstellen.

Softwareseitig wird Linux-OS und die Linux-Version des Google Chrome oder Mozilla Firefox ESR Browsers sowie zusätzlich ein gehärtetes Linux mit einem zusätzlichen Sicherheits-Framework „AppAmor"- Whitelisting verwendet. Damit laufen Angriffe auf das Windows-Host-System, unabhängig ihrer Art, immer ins Leere. Im Gegensatz zu mikrovirtualisierten Browsern verfügen vollvirtualisierte Browser über ein eigenes Betriebssystem und sind nicht mit dem Microsoft-Betriebssystem verzahnt. Bei Fremdkomponenten baut Rohde & Schwarz Cybersecurity mit seinem Browser in the Box ausschließlich auf Open Source. So kann der vertrauenswürdige und unabhängige Hersteller aus Deutschland auch auf Code-Level Analysen durchführen und die eingebauten Komponenten und Module laufenden Kontrollen und Prüfungen unterziehen.

Mikrovirtualisierung bietet nur Mikroschutz

Browser-Lösungen auf Basis von Mikrovirtualisierung bieten nur ein reduziertes Sicherheitsniveau, weil sie abhängig vom Host-Betriebssystem – in der Regel Windows – mit einer bestimmten Kernel-Version sind. Der Schutz der Malware erfolgt direkt am Endpunkt durch hardware-isolierte Mikro-VMs (virtual machines). Oft werden vom Anbieter der Virtualisierungssoftware nur ganz bestimmte Kernel-Versionen zur Nutzung angeboten, die vom Nutzer nicht frei wählbar sind. Hier liegt ein zentrales Problem der Mikrovirtualisierung: Sie setzt nicht auf einem eigenen Betriebssystem auf. Stattdessen ist sie stark mit dem vorhandenen Betriebssystem verzahnt – alle Aktivitäten erfolgen also im gleichen Kernel. Auch die gleichen Windows-Programme kommen dabei zum Einsatz. Das heißt: Mindestens ein Kernel und optional viele weitere Komponenten werden mit dem Host-System geteilt. Damit ist die Mikrovirtualisierung zwar preiswerter als eine Vollvirtualisierung und beansprucht weniger Speicherplatz auf dem Rechner. Sie lässt aber Sicherheitslücken offen. Wird nämlich der Kernel mit Malware infiziert, gilt das auch für alle Mikro-VMs.

Dagegen bieten vollvirtualisierte Browser, wie der Browser in the Box, eine umfassende, mehrstufige Arbeitsplatzsicherheit. Weltweit ist die Browser in the Box-Produktfamilie bereits auf mehr als 250.000 Nutzersystemen installiert. Rohde & Schwarz Cybersecurity gewährleistet auch zukünftig die erforderlichen Sicherheitsanpassungen der Lösung. ■

Kontakt

Rohde & Schwarz Cybersecurity GmbH
München
Tel.: +49 30 65 884 223
cybersecurity@rohde-schwarz.com
cybersecurity.rohde-schwarz.com/de

KRITIS

Kritische Infrastrukturen gefordert

Definitionen, Pflichten und Möglichkeiten zur Sicherung von Kritischen Infrastrukturen – Teil 1

Besonders Kritische Infrastrukturen müssen mit ihren komplexen Versorgungssystemen vor unbefugten Zugriffen wirkungsvoll geschützt werden

Im Mai ist eine wichtige Übergangsfrist für Betreiber Kritischer Infrastrukturen abgelaufen. Sie betrifft die IT-Sicherheit und fordert die Umsetzung definierter Mindeststandards für den Schutz gegen Cyber-Attacken. Doch wer genau muss dieser Pflicht nachkommen? Wann Infrastrukturen kritisch sind und welche Schutzmaßnahmen deren Betreiber noch umsetzen müssen, erläutert der zweiteilige Beitrag von Arne Wriedt, Business Development Manager Versorger bei Assa Abloy. Im einführenden ersten Teil geht es um die Definition Kritischer Infrastrukturen und deren Herausforderungen für den Sicherheitsverantwortlichen sowie um aktuelle normative Fragestellungen.

Zu Kritischen Infrastrukturen zählen auch Energieversorgungsunternehmen, sie brauchen somit besonderen Schutz. Die Stadtwerke Kiel setzen auf die mechanische Schließlösung Verso Cliq der Marke Ikon von Assa Abloy

> Tangiert eine Betriebsstörung mehr als 500.000 Menschen, zählt das Unternehmen zur Kritischen Infrastruktur."

Infrastrukturen bestimmen unseren Alltag, ohne sie wäre eine funktionierende Volkswirtschaft nicht möglich. Sie werden untergliedert in materielle Infrastrukturen wie Verkehrsnetze, öffentliche Gebäude, Datenleitungen und Kanalisation und immaterielle Infrastrukturen, wie die Bildung der Bürger. Die Rechtsordnung eines Staates wiederum ist Teil der institutionellen Infrastruktur. Der Ausfall solcher Versorgungsnetze kann weitreichende Folgen haben, dementsprechend sind sie vor Störungen zu schützen.

Besondere Aufmerksamkeit gilt den sogenannten Kritischen Infrastrukturen – kurz KRITIS. Die EU-Richtlinie 2008/114/EG aus dem Jahr 2008 definiert eine Kritische Infrastruktur als eine „(...) Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung (...)" ist. Gefährdungen für solche KRITIS können natürliche Ereignisse, menschliches und technisches Versagen, Terrorismus und kriminelle Handlungen sowie Kriege sein.

KRITIS: Neun Sektoren – 29 Branchen

Die deutsche Bundesregierung setzt sich bereits seit Ende der 1990er-Jahre branchenübergreifend mit dem Schutz Kritischer Infrastrukturen auseinander. 2009 brachte das Bundesministerium des Inneren, BMI, die Nationale Strategie zum Schutz Kritischer Infrastrukturen, kurz KRITIS-Strategie, heraus. Darin sind KRITIS als Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen definiert. Deren Ausfall oder Beeinträchtigung hätte nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Konsequenzen zur Folge. Die Infrastrukturen gliedert das BMI in neun Sektoren: Energie, Gesundheit, Staat und Verwaltung, Ernährung, Transport und Verkehr, Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Medien und Kultur sowie Wasser. Die Sektoren werden nochmals in 29 Branchen unterteilt.

KRITIS ja oder nein? Es gibt Prüfmöglichkeiten

Doch nicht alle Anlagen aus diesen Sektoren und Branchen zählen automatisch zu Kritischen Infrastrukturen. Die Zugehörigkeit ist im Einzelfall zu prüfen. Dazu stehen den Betreibern der jeweiligen Versorgungsnetzwerke verschiedene Hilfsmittel zur Verfügung – von der kommunalen bis zur EU-Ebene. Mit der EU-Richtlinie 2008/114/EG sind Kriterien für europäische KRITIS in den Bereichen Transport und Energie festgelegt. In Deutschland bietet seit 2016 die BSI-KRITIS Verordnung einen Rechtsrahmen zur Bestimmung Kritischer Infrastrukturen. Das Bundesamt für Sicherheit in der Informationstechnik, BSI, legt darin fest, welche Branchen und Unternehmen etwa unter das IT-Sicherheitsgesetz fallen. Dieses gilt bereits seit 2015.

Im Hauptteil der BSI-KRITIS-Verordnung werden die Auswahlkriterien für die Sektoren Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr präzisiert. Der Anhang wiederum gibt Schwellenwerte und deren Berechnungsformel vor. Ein Anhaltspunkt ist der Betroffenheitsgrad: Tangiert eine Betriebsstörung mehr als 500.000 Menschen, zählt das Unternehmen zur Kritischen Infrastruktur.

Schutz vor Cyber-Attacken ist Pflicht

Mit der KRITIS-Strategie rief die Bundesregierung bereits 2009 alle Akteure – vor allem Bund, Länder, Kommunen und die Privatwirtschaft – dazu auf, das Schutzniveau für Kritische Infrastrukturen in Deutschland zu erhöhen. Prävention, Reaktion und Nachhaltigkeit seien dabei wichtige Aspekte. Doch was genau können beziehungsweise müssen Betreiber Kritischer Infrastrukturen dafür tun? Das IT-Sicherheitsgesetz verpflichtet die Betreiber dazu ihre EDV stets auf dem Stand der Technik zu halten. Der Nachweis darüber ist alle zwei Jahre in Form von Sicherheitsaudits, Prüfungen oder Zertifizierungen zu erbringen (§ 8a Abs. 3, BSIG).

Die Sektoren Finanzen und Versicherungen, Transport und Verkehr sowie Gesundheit haben bis Juni 2019 Zeit, die hohen IT-Sicherheitsanforderungen umzusetzen und zu belegen. Für die Branchen Energie, IT und Telekommunikation, Wasser sowie Ernährung endete die Frist für die Nachweispflicht bereits im Mai 2018. Darüber hinaus müssen KRITIS-Betreiber eine Kontaktstelle für die von ihnen betriebenen Kritischen Infrastrukturen benennen, bei der jederzeit jemand erreichbar ist (§ 8b Abs. 3, BSIG). Zudem müssen sie erhebliche IT-Sicherheitsvorfälle unverzüglich an das BSI melden (§ 8b Abs. 4, BSIG).

Bitte umblättern ▶

Versorgungsunternehmen nutzen weltweit Sicherheitssysteme und Schließlösungen von Assa Abloy

Für den physischen Schutz gibt es bislang nur Empfehlungen

Während das IT-Sicherheitsgesetz den Schutz vor Cyberattacken abdeckt und verpflichtend ist, konzentriert sich das Basisschutzkonzept auf die Abwehr physischer Gefährdungen. Es ist als Leitfaden zu verstehen und somit nur Kür für die Betreiber von KRITIS. Neben Erläuterungen zu Gefährdungsarten und Empfehlungen für bauliche, organisatorische, personenbezogene und technische Schutzmaßnahmen, bietet das Basisschutzkonzept einen Fragenkatalog und ein Muster für eine Checkliste, mit denen die Betreiber von Infrastruktureinrichtungen arbeiten können.

Die Liste benennt Schutzmaßnahmen für die Bereiche Objektschutz, Personal, Organisation, Risikomanagement sowie Notfall- und Ausfallplanung. Zum Objektschutz beispielsweise zählen die Lage des Objektes, dessen bauliche Gestaltung, die Vorfeld- sowie Gebäudesicherung und der Brandschutz. Fragen, die zu diesen Punkten gestellt werden, beinhalten unter anderem den Abstand zu den Nachbargebäuden, die verkehrstechnische Erschließung des Gebäudes, aber auch das Schließsystem des Unternehmens.

Sicherheitstechnik für Gebäudeschutz

Bei der Umsetzung der baulichen Schutzmaßnahmen arbeiten Kritische Infrastrukturen mit Partnern zusammen, wie dem Sicherheitstechnik-Hersteller Assa Abloy. Mit seinen Marken Effeff und Ikon bietet er KRITIS-konforme Lösungen an. Dazu zählen Produkte aus den Bereichen Rettungswegtechnik, Zutrittskontrolle, Schließanlage sowie Schlüsselmanagement, die hinsichtlich aller gesetzlichen Anforderungen zertifiziert und geprüft sind. Die Hersteller beraten Architekten und Planer sowohl bei Neubauten, als auch bei der Umrüstung eines bestehenden Objekts. Hauseigene Experten besichtigen vor Ort den Ist-Zustand und erstellen individuelle Konzepte je nach Einsatzbereich.

Der Vorteil: Die Hersteller kennen sowohl die Anforderungen an KRITIS, als auch den neusten Stand der Sicherheitstechnik. Zudem können Probleme, die nach der Umsetzung auftauchen durch ein dichtes Partnernetz schnell behoben werden.

Risiko- und Krisenmanagement

Neben dem Basisschutzkonzept stellen das Bundesamt für Sicherheit in der Informationstechnik, BSI, und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK, noch weitere Leitfäden zur Verfügung. Darunter auch „Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement". Er liefert Unternehmen das Handwerkszeug, um ein Risiko- und Krisenmanagement in Einrichtungen aufzubauen oder bestehende Systeme zu ergänzen. Das Dokument „Notstromversorgung in Unternehmen und Behörden" wiederum gibt Anleitung für die Planung, Einrichtung und den Betrieb einer Versorgung in Unternehmen und Behörden mit Notstrom. Und hinsichtlich des Bevölkerungsschutzes bietet der Leitfaden „Schutzkonzepte Kritischer Infrastrukturen im Bevölkerungsschutz" Orientierung. ■

Was hinsichtlich der Sicherheitstechnik bei KRITIS-Unternehmen im Einzelnen zu beachten ist, vertiefen wir im zweiten Teil des Beitrags in Ausgabe 9 der GIT Sicherheit sowie im Special GIT Cyber Security (erscheint ebenfalls im September als eigene Ausgabe).

Autor
Arne Wriedt,
Business Development Manager Versorger, Assa Abloy

Kontakt

Assa Abloy Sicherheitstechnik GmbH
Berlin
Tel.: +49 30 81060
berlin@assaabloy.com
www.assaabloy.de

OPERATIONAL SERVICES
YOUR ICT PARTNER

TOP SERVICE DEUTSCHLAND 2018 operational services Your ICT Partner TOP 10 B2B Handelsblatt ServiceRating

brand eins Thema B 2018 BESTE BERATER Heft 9

INNOVATIONSPREIS-IT BEST OF 2018 initiative mittelstand IT-SECURITY

WISSEN, WAS PASSIERT

Security Information & Event Management (SIEM)

Absolute IT-Sicherheit gibt es nicht: Jede aufgerufene Website, jede geöffnete E-Mail und jedes verpasste Update stellt eine potenzielle Gefahr für die Daten und Infrastrukturen eines Unternehmens dar. Eingeschleuste Schadsoftware wird durchschnittlich erst nach zwei bis neun Monaten erkannt.

Ein professionelles Security Information & Event Management hilft, bevor ein Schaden entsteht. Es erkennt Anomalien und potenzielle Angriffe automatisch und ermöglicht einen umfassenden Schutz. So wissen Sie stets, was passiert – und können rechtzeitig reagieren.

www.it-sicherheitsfachtagung.de

Mehr über SIEM:
8. IT-Sicherheitsfachtagung
7. Juni 2018, Wolfsburg

INDUSTRIAL SECURITY

Safety meets Security

Gemeinsame Strategie erforderlich

Der in Maschinen und Anlagen verbauten Sicherheitstechnik kommt über den gesamten Lebenszyklus der Applikation eine stetig steigende Bedeutung zu. Aufgrund der zunehmenden Vernetzung der Automatisierungssysteme mit der IT-Welt können jedoch Szenarien auftreten, die insbesondere von Safety-Anwendungen eine neue Herangehensweise erfordern.

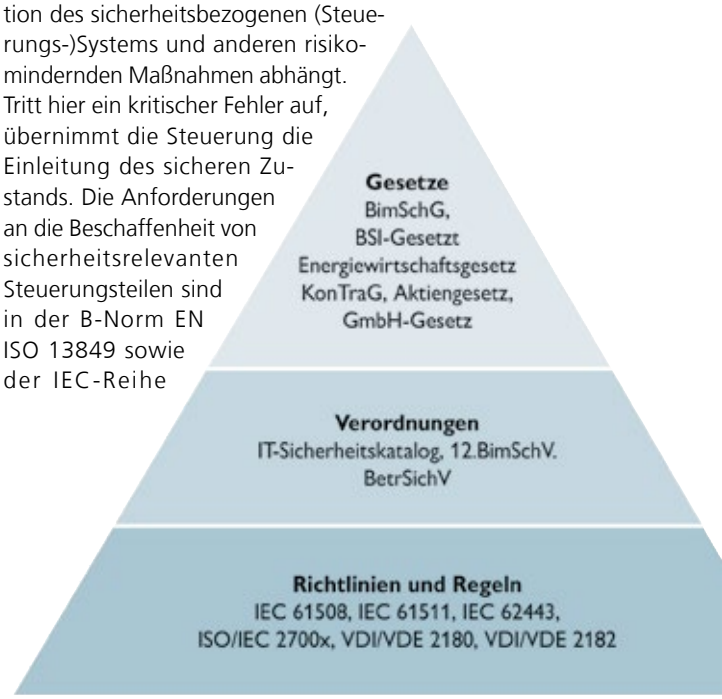
Da sich Fertigung und IT im Rahmen des Zukunftsprojekts Industrie 4.0 immer mehr im Internet der Dinge verbinden, wachsen auch die Herausforderungen in puncto Security. Ein wichtiges Einfallstor für Hacker stellen die Netzwerkübergänge zwischen der Office-IT und dem Produktionsnetz dar. Zu den Bedrohungen, denen industrielle Steuerungssysteme derzeit ausgesetzt sind, zählen beispielsweise:

- die Infektion mit Schadsoftware über das Internet und Intranet
- das Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- das Social Engineering, also die Beeinflussung von Personen mit dem Ziel, bei ihnen bestimmte Verhaltensweisen hervorzurufen
- menschliches Fehlverhalten und Sabotage
- ein Einbruch in das System über Fernwartungslösungen
- mit dem Internet über das IP-Protokoll gekoppelte Steuerungskomponenten
- technisches Fehlverhalten und höhere Gewalt
- die Kompromittierung von Smartphones im Fertigungsumfeld sowie von Extranet und Cloud-Komponenten.

Eine Studie des Softwareunternehmens Kaspersky aus dem Jahr 2017 zeigt, dass sich etwa jede dritte Cyberattacke auf Rechner für industrielle Kontrollsysteme gegen produzierende Unternehmen richtet. Für das Jahr 2018 befürchten die Experten das vermehrte Aufkommen von Malware, die sich auf Industriesysteme fokussiert. Werden Automatisierungslösungen zur Realisierung der funktionalen Sicherheit zum Ziel von Hackerangriffen, treffen die Welten von „Safety" und „Security" aufeinander. Zukünftig muss daher eine gemeinsame Strategie entwickelt werden. Dass dieses Szenario real ist, belegt der aktuelle Fall der Malware „Triton" in Verbindung mit einem Cyberangriff gegen ein sogenanntes „Safety Instrumented System (SIS)".

Indirekter Effekt auf das Endprodukt

Der Aspekt der funktionalen Sicherheit bezeichnet den Teil der Sicherheit eines Systems, der von der korrekten Funktion des sicherheitsbezogenen (Steuerungs-)Systems und anderen risikomindernden Maßnahmen abhängt. Tritt hier ein kritischer Fehler auf, übernimmt die Steuerung die Einleitung des sicheren Zustands. Die Anforderungen an die Beschaffenheit von sicherheitsrelevanten Steuerungsteilen sind in der B-Norm EN ISO 13849 sowie der IEC-Reihe



Überblick über die relevanten Gesetze, Verordnungen, Richtlinien und Regeln

61508/61511/62061 beschrieben. Je nach Risikohöhe werden die entsprechenden risikoreduzierenden Maßnahmen in unterschiedliche Sicherheitsniveaus – Performance Level (PL) oder Safety Integrity Level (SIL) – eingestuft.

Im Gegensatz zur funktionalen Sicherheit schützt die Security Güter vor einer nachteiligen Beeinträchtigung durch beabsichtigte oder versehentliche Attacken auf die Verfügbarkeit, Integrität und Vertraulichkeit ihrer Daten. Dazu werden vorbeugende oder reaktive technische und/oder organisatorische Maßnahmen verwendet. Die Vernachlässigung von Security-Aspekten im Safety-Umfeld kann neben den direkten Auswirkungen auf die Fertigungseinrichtungen ebenfalls einen indirekten Effekt auf den Produktionsprozess und damit das Endprodukt haben. Bei pharmazeutischen Artikeln oder sicherheitsrelevanten Bauteilen für die Automobilindustrie lassen sich die erheblichen Auswirkungen auf den Konsumenten leicht nachvollziehen. Die IEC 61511-1 fordert deshalb für Sicherheitseinrichtungen der Prozessindustrie eine IT-Risikobeurteilung. Hat der Betreiber einer PLT-Sicherheitseinrichtung (Prozessleittechnik) die IT-Risikobeurteilung nach dem vorliegenden NA-Verfahren der NAMUR durchgeführt und die identifizierten Maßnahmen umgesetzt, sollte er seine PLT-Sicherheitseinrichtung nach dem aktuellen Stand der Technik beurteilt haben und somit seiner Sorgfaltspflicht nachgekommen sein.

Aktive Suche nach Schwachstellen

In der funktionalen wie auch der Zugriffssicherheit muss das potenzielle Risiko zunächst auf Basis einer Risikobeurteilung respektive IT-Bedrohungsanalyse bewertet werden. Hier zeigt sich bereits ein wesentlicher Unterschied bei der Herangehensweise: Während sich die Konstrukteure im Rahmen der Risikobeurteilung gemäß Maschinenrichtlinie auf eher statische Risiken – beispielsweise mechanische oder elektrische Gefährdungen – einstellen müssen, findet sich der IT-Sicherheitsexperte in einem sich ständig verändernden Umfeld wieder. Dort suchen Angreifer mit immer neuen Methoden aktiv nach entsprechenden Schwachstellen, die im Bereich der funktionalen Sicherheit als systematische Fehler betrachtet werden.

Einen weiteren wichtigen Einfluss hat der „Faktor Mensch“: Auf dem Gebiet der Maschinensicherheit wird von „vorhersehbarem Missbrauch“ gesprochen, wenn zum Beispiel Schutzeinrichtungen – wie Türschalter – vom Bedienpersonal manipuliert werden. Bei groß angelegten Cyberangriffen auf Industrieanlagen muss hingegen von einem hohen Maß an krimineller Energie ausgegangen werden.

Erster Ansatz in einem NAMUR-Arbeitsblatt

Um den Produktlebenszyklus sicherheitsgerichteter Systeme oder Komponenten abzusichern, sind Hersteller, Systemintegratoren und Betreiber aufgefordert, innerhalb eines „Functional Safety Managements“ ein bedarfsgerechtes Qualitätsmanagement gemäß IEC 61508 anzuwenden. In der Security-Welt gibt es mit dem „Information Security Management“ nach ISO 27000 dazu eine vergleichbare Lösung. Bei so vielen Gemeinsamkeiten müsste es nun doch möglich sein, die beiden Handlungsfelder Safety und Security in der Praxis zu verzahnen.

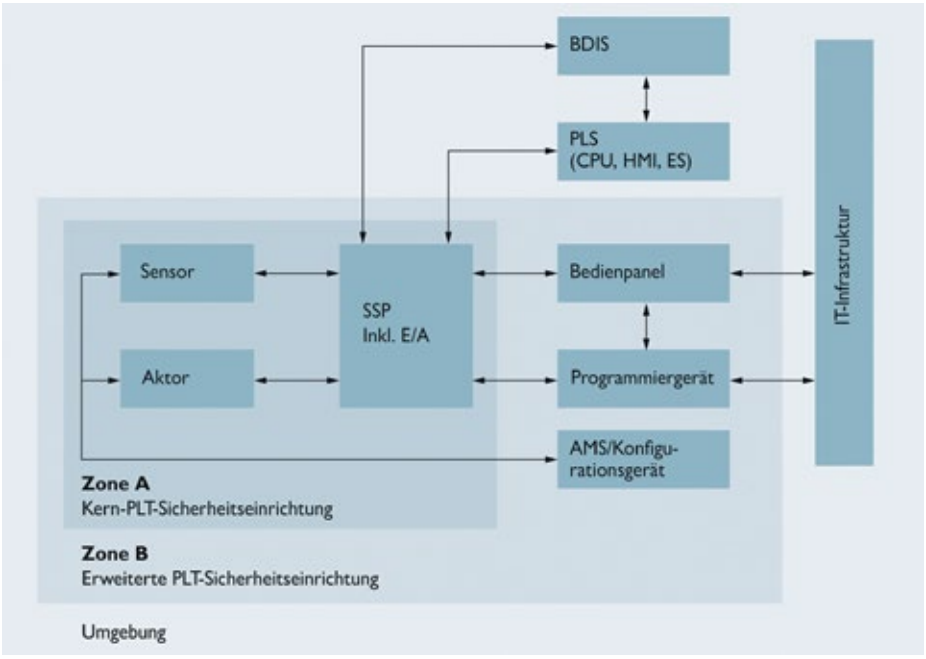
Einen ersten pragmatischen Ansatz in diese Richtung bietet das von der NAMUR veröffentlichte Arbeitsblatt „IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen“. Das darin beschriebene Verfahren zur IT-Risikobeurteilung in Anlehnung an die Security-Norm IEC 62443 bildet dabei die Grundlage für die Erhöhung der Widerstandsfähigkeit der PLT-Sicherheitseinrichtung gegen IT-Bedrohungen. Zu diesem Zweck wurden die drei Schritte der Phase 1 einmalig exemplarisch für ein System

Cloud-basierte Bereitstellung wichtiger Sicherheitssystemdaten

Die Proficloud von Phoenix Contact stellt Unternehmen wichtige Informationen zur Optimierung von Abläufen in der Fertigung zur Verfügung. Für die Anlagenbauer und Maschinenbetreiber bleibt zudem die Maschinensicherheit ein kritisches Thema. In erster Linie schützen Safety-Applikationen die Nutzer der Maschine, können aber auch ungeplante Betriebsunterbrechungen verursachen. Deshalb birgt die Möglichkeit, über das Internet der Dinge in Echtzeit auf die Sicherheitssystemdaten zugreifen und diese in aussagekräftige Informationen umwandeln zu können, ein großes Potenzial.

Mit einer Profinet-basierten Steuerungslösung lassen sich Statusinformationen von Standard- und Safety-Funktionen kontinuierlich in die Proficloud übertragen. Durch die ganzheitliche Betrachtung von Ressourcen und Maschinen ergeben sich so neue Möglichkeiten für Betreiber und Konstrukteure, um die Betriebsleistung zu erhöhen.

Verschiedene Schritte des Risikobeurteilungsverfahrens gemäß der NAMUR-Empfehlung NA 163



Einteilung PLT-Sicherheitseinrichtung in verschiedene Bereiche

durchgeführt, wie es typischerweise in den NAMUR-Mitgliedsunternehmen vorzufinden ist. Damit kann der Anwender die Nutzbarkeit des Verfahrens für die zu beurteilende PLT-Sicherheitseinrichtung überprüfen. Der vierte Schritt – die Kontrolle der Umsetzung der Maßnahmen sowie die Dokumentation der IT-Sicherheitsanforderungen und Randbedingungen – muss für jede zu evaluierende PLT-Sicherheitseinrichtung individuell durchlaufen werden und bildet die Phase II.

Keine Beeinträchtigung der funktionalen Integrität

Aus der Perspektive der Hard- und Software kann das untersuchte System demnach in drei Bereiche unterteilt werden:

- Die Kern-PLT-Sicherheitseinrichtung in Zone A umfasst die PLT-Sicherheitseinrichtung, wie sie in der IEC 61511-1 definiert ist. Dazu gehören das Logiksystem, die Ein- und Ausgabebaugruppen inklusive Remote-I/O sowie die Aktoren und Sensoren. Verbindungen und gegebenenfalls vorhandene Netzwerkkomponenten – beispielsweise Kabel oder Switches –, die der Ankopplung der in Zone A angesiedelten Geräte dienen, sind ebenfalls dieser Zone zugeordnet.
- Der erweiterten PLT-Sicherheitseinrichtung in Zone B werden Komponenten zugerechnet, die für die Ausführung der Sicherheitsfunktion nicht notwendig sind, das Verhalten der Kern-PLT-Sicherheitseinrichtung jedoch beeinflussen können. Als Beispiele seien hier Bedien-Eingabe-Panels, Visualisierungsstationen, das Programmiergerät für die PLT-Sicherheitseinrichtung sowie Vorrichtungen zur Sensor-/Aktor-Konfiguration genannt.
- Im als Umgebung bezeichneten Bereich befinden sich Komponenten und Systeme, die weder direkt noch indirekt bei der PLT-Sicherheitseinrichtung einzusortieren sind, aber in Verbindung mit der Sicherheitsfunktion stehen können. Dabei kann es sich um Reset-Anforderungen oder die Visualisierung des Zustands der Sicherheitsfunktion handeln.

Das gemeinsame Ziel der Bereiche ist, die funktionale Integrität der Sicherheitseinrichtung nicht durch Rückwirkungen aus der Umgebung zu beeinträchtigen.

Umfassende Schulung der beteiligten Personen

Um die Auswirkungen durch eine kompromittierte PLT-Sicherheitseinrichtung zu verringern oder Bedrohungen entgegenzuwirken, müssen Maßnahmen ergriffen werden. Dem „Faktor Mensch" kommt eine besondere Rolle in diesem Prozess zu. Denn über 50 Prozent der Cybersecurity-Vorfälle lassen sich auf das Verschulden der Mitarbeiter zurückführen. Es ist deshalb wichtig, dass es einen IT-Sicherheitsverantwortlichen für die Sicherheitseinrichtung gibt. In diesem Zusammenhang sollten alle für die Spezifikation und den Entwurf der Sicherheitseinrichtung relevanten Personen für das Thema Automation Security sensibilisiert und entsprechend geschult werden. Darüber hinaus ist es ratsam, dass der Endanwender mit seinen Vertragspartnern – also Herstellern, Lieferanten und externen Betreibern – Vertraulichkeitsvereinbarungen in Bezug auf Informationen und Kenntnisse hinsichtlich des Sicherheitssystems trifft.

Komponenten, Software-Tools und Lösungen von Phoenix Contact unterstützen den Anwender bei der flexiblen und wirtschaftlichen Kombination von Safety- und Security-Technik, damit er international noch wettbewerbsfähiger wird. Ergänzt um ein umfassendes Dienstleistungsangebot erhalten die Anlagenerrichter und –betreiber somit über den gesamten Sicherheitslebenszyklus ein optimal auf ihre Anforderungen abgestimmtes Leistungsspektrum. ■

Autor
Dipl.-Ing. (FH)
Carsten Gregorius,
Senior Specialist Safety im Geschäftsbereich I/O and Networks, Phoenix Contact Electronics

Kontakt

Phoenix Contact Deutschland GmbH
Blomberg
Tel.: +49 5235 3 1 20 00
info@phoenixcontact.de
www.phoenixcontact.de/safetyindercloud
www.phoenixcontact.de/security

BSI veröffentlicht Cyber-Sicherheitsempfehlung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Cyber-Sicherheitsempfehlung zum Thema „Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte" veröffentlicht. Die praxisnahen und umsetzungsorientierten Empfehlungen richten sich insbesondere an Hersteller von Medizintechnik und unterstützen diese dabei, den Stand der Technik sowie vorhandene normative Vorgaben in ihren Produkten praktisch umzusetzen. Zudem dient das Papier auch dazu, die Hersteller für die bei der Vernetzung und Digitalisierung von Medizinprodukten entstehenden neuen Gefährdungen zu sensibilisieren. Die Cyber-Sicherheitsempfehlung des BSI ist gemeinsam mit dem Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI) sowie mit Unterstützung des Bundesinstituts für Arzneimittel und Medizinprodukte (BfArM) erstellt worden.

Hierzu erklärt BSI-Präsident Arne Schönbohm: „Cyber-Angriffe auf Einrichtungen des Gesundheitswesens sind ebenso wie Schwachstellen in vernetzten Medizinprodukten Teil der dynamischen Gefährdungslage, die uns in Zeiten der Digitalisierung täglich neu herausfordert. Unsere Empfehlungen unterstützen den Gesundheitssektor dabei, flankierend zu den regulatorischen Vorgaben ein angemessenes Cyber-Sicherheitsniveau nach dem Stand der Technik zu implementieren. Als nationale Cyber-Sicherheitsbehörde leisten wir so einen wichtigen Beitrag zu einem insgesamt höheren Schutzniveau gegen Cyber-Attacken auf Gesundheitseinrichtungen." Krankenhäuser, die gemäß BSI-Gesetz als Kritische Infrastruktur eingestuft wurden, sind verpflichtet, dem BSI bis spätestens Juni 2019 nachzuweisen, dass sie IT-Sicherheitsmaßnahmen nach dem Stand der Technik erfolgreich implementiert haben. Der zunehmende Einsatz netzwerkfähiger Medizinprodukte ist dabei ein zentraler Aspekt.

www.bsi.bund.de ■

Speaker auf der Command Control 2018

Facebook-Chef Zuckerberg ist das beste Beispiel: Cyber-Security geht vor allem die Geschäftsführung etwas an. Welchen Rahmen müssen Unternehmen schaffen, um Kundendaten (rechts-)sicher zu nutzen? Welche Haftungsfolgen hat die Datenschutz-Grundverordnung (EU-DSGVO), die seit Mai in Kraft ist? Die Command Control vom 20.–22. September in München gibt Entscheidern Antworten. Cyber-Security-Szenarien werden in Showcases anschaulich dargestellt. Zahlreiche interaktive Formate ermöglichen es, sich mit Entscheidern aus unterschiedlichen Branchen auszutauschen. Die Messeteilnehmer tauchen tief in den hochrelevanten gesellschaftlichen Diskurs ein – und können daraus Ableitungen für das eigene unternehmerische Handeln erarbeiten. Die ersten Sprecher stehen fest: Eugene Kaspersky ist Mitgründer und Chief Executive Officer des russischen Security-Unternehmens Kaspersky Lab. Prof. Dr. Marco Gercke ist Experte im Bereich Cybersecurity/Cybercrime und Gründer und Direktor des Cybercrime Research Institute in Köln. Laura Jones ist Senior Risk Managerin, Cyber Security & Assurance bei Kimberly-Clark Corp., USA. Larry Clinton ist Präsident und CEO der Internet Security Alliance (ISA), USA.

www.cmdctrl.com ■

INTERNET OF THINGS

Winds of Change

Safety und Security in Zeiten des Internets der Dinge

Der Kauf analoger Videokameras ist heute eine echte Herausforderung. Praktisch jede Kamera auf dem Markt ist digital, sei es von traditionellen Anbietern oder von Newcomern, die noch nie analog entwickelt haben. Und während Kameras klare Vorreiter des Trends zur Digitalisierung und standardbasierten Vernetzung in der Sicherheitsbranche waren, hat es nicht lange gedauert, bis auch Türsteuerungen, Brandmelderzentralen, Beschallungs- und Einbruchmeldeanlagen folgten. Vernetzte und zentral verwaltete Sicherheitslösungen sind einfach zu vielversprechend und ermöglichen ein höheres Maß an Sicherheit durch Ereigniskorrelation sowie eine schnellere und gezieltere Reaktion auf Vorfälle. Durch die Nutzung vorhandener IP-Netzwerke anstelle proprietärer Kommunikationsverbindungen können Investitionsaufwand und Betriebskosten gesenkt werden, ebenso wie durch das zentrale Management der gesamten vernetzten Lösung.

▲ **Die meisten Sicherheitslösungen bestehen heute aus vernetzten Subsystemen, aber ein Großteil davon ist immer noch als geschlossene Lösung angelegt. Das Internet der Dinge (IoT) wird diese Situation dramatisch verändern, und es hat bereits damit begonnen**

Dr. Aleksandar Mitrovic, Senior Vice President Engineering bei Bosch Security Systems

Die Digitalisierung war der dramatischste Wandel in der Sicherheitsbranche seit mehr als einem Jahrhundert, dabei stehen wir noch ganz am Anfang. Die meisten Sicherheitslösungen bestehen heute aus vernetzten Subsystemen, aber ein Großteil davon ist immer noch als geschlossene Lösung angelegt, vielleicht mit ein paar externen Verbindungen für Fernüberwachung, Fernwartung und Alarmierung. Das Internet der Dinge (IoT) wird diese Situation dramatisch verändern, und es hat bereits damit begonnen. Wenn alles mit allem verbunden ist, werden neue Anwendungen entstehen – und es müssen neue Risiken berücksichtigt werden.

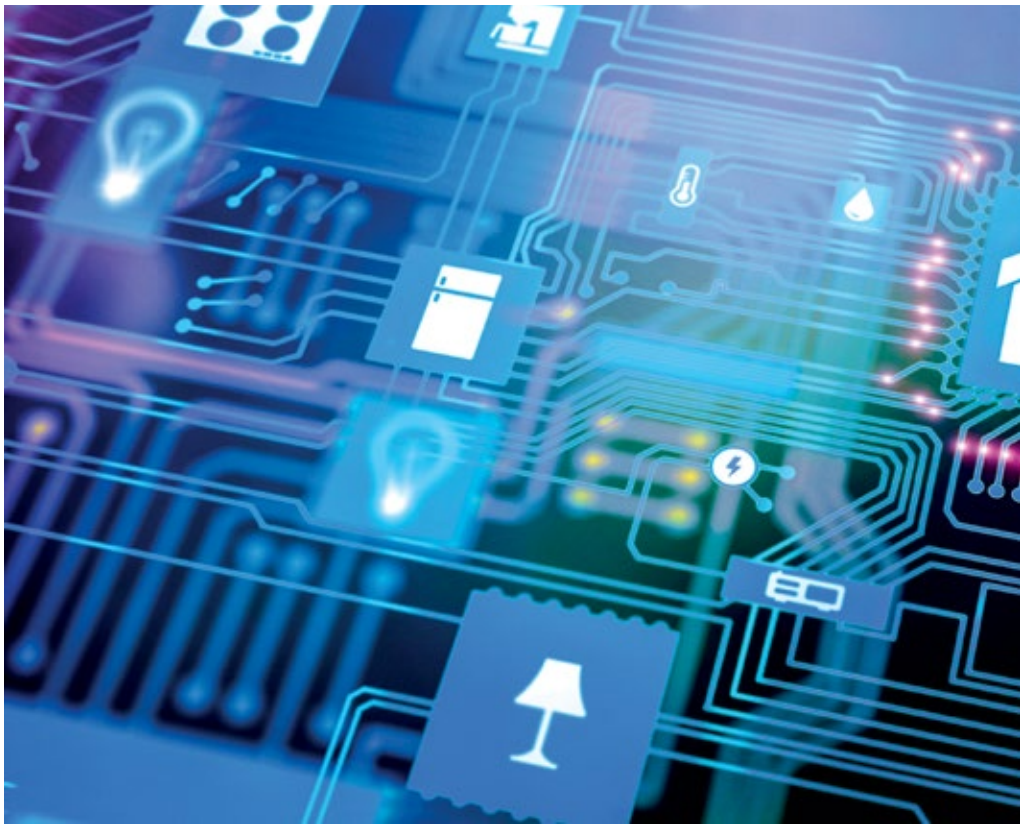
Bereits heute werden Cloud-Sicherheitsservices angeboten, die sowohl für kleine als auch für große Unternehmen sehr effizient sein können. Andererseits haben wir kürzlich gesehen, wie Malware wie Mirai und IoT Reaper internetfähige Kameras kapern und sie in ein Botnet einbinden kann, um massive Distributed Denial of Service (DDoS)-Angriffe gegen einzelne Organisationen oder ganze Netzwerke zu führen.

Veränderung des gesamten Geschäftsmodells

Wie in anderen Branchen auch, verändert das Internet der Dinge (IoT) die Art und Weise, wie Anbieter von Sicherheitssystemen ihre Geschäfte machen. Während heute die meisten Kunden die Konnektivität als Wegbereiter des IoT betrachten, sind Ethernet-Stecker und IP-Stacks letztlich nur eine Voraussetzung – das IoT ist viel mehr als nur vernetzte Systeme oder ein zentrales Managementsystem.

Nach Auffassung von Dr. Aleksandar Mitrovic, Senior Vice President Engineering bei Bosch Security Systems, wird das IoT letztlich das gesamte Geschäftsmodell der Branche verändern – mit Anbietern, die von Hardwarelieferanten zu Dienstleistern werden. „Während Qualität und Funktionen der Hardware heute die Hauptunterscheidungsmerkmale sind, werden wir erleben, wie softwarebasierte Funktionen und Analysen in einigen Jahren ebenso wichtig werden", so. Mitrovic. „Software wird völlig neue Anwendungen ermöglichen, und künstliche Intelligenz wird es unseren Kunden gestatten, ihre Geschäftsprozesse transparen-

ter zu machen und damit die Gelegenheit zu erhalten, sie zu verbessern. Wir stehen hier ganz am Anfang, aber Services wie die Fernüberwachung sind bereits kurz davor, sich überall durchzusetzen. Außerdem gibt es erste Anwendungen, die über die Sicherheit hinausgehen – wie die In-Store Analytics-Lösung von Bosch für den Einzelhandel."



Drei Schritte zum Internet der Dinge

Aus heutiger Sicht ist die Einführung des Internet der Dinge (IoT, Internet of Things) ein dreistufiges Unterfangen für traditionelle Anbieter von Sicherheitslösungen. Der erste Schritt ist es, Produkten Konnektivität zu verleihen. Hier sind die meisten Anbieter schon sehr weit. Konnektivität bedeutet jedoch nicht unbedingt, dass jedes einzelne Produkt mit einer Ethernet- oder WLAN-Schnittstelle und einem neuen Software-Stack ausgestattet werden muss. Während beispielsweise Kameras von dieser Konnektivität maßgeblich profitieren, können andere Sensoren wie Brand- und Einbruchmelder immer noch darauf verzichten, wenn sie auf geeignete Weise an IP-fähige Controller angeschlossen sind, z. B. über LSN (Local Security Network).

Während also der erste Schritt zum IoT – Konnektivität – hauptsächlich eine Aufgabe des Engineerings ist, die man gut im Griff hat, wird der zweite etwas schwieriger. Es geht darum, Geschäftsmöglichkeiten zu identifizieren, Anwendungen zu entwickeln und aussagekräftige Daten aus den Sicherheitssystemen in das Backend zu bringen, um diese zu realisieren und zu unterstützen. Ein gutes Beispiel hierfür ist eine Fernwartungsanwendung, die mit Echtzeitdaten gespeist wird, wie etwa dem Verschmutzungsgrad von Brandmeldern. Durch eine frühzeitige Meldung kann eine solche Anwendung einem Ausfall der Brandmelder vorbeugen. Wenn eine ähnliche Anwendung Zugriff auf alle Zustandsdaten einer Sicherheitslösung hat und auf entsprechenden Algorithmen basiert, kann sie optimierte Wartungsfenster berechnen und die Anzahl der Serviceanrufe und Vor-Ort-Einsätze reduzieren. Eine Reihe solcher, meist Cloud-basierter Services ist derzeit von verschiedenen Anbietern erhältlich, aber es ist noch ein weiter Weg, bis das volle Potenzial von Fernservices erschlossen sein wird.

Im dritten Schritt schließlich eröffnet das IoT eine völlig neue Welt für Anbieter von Sicherheitssystemen. Neben ihrer Rolle als Hardware-Anbieter und basierend auf Echtzeit- und/oder statistischen Daten im Cloud-Backend können und müssen sie sich sehr wahrscheinlich in Dienstleister verwandeln und eine breite Palette von Anwendungen entwickeln, die weit über die Sicherheit hinausgehen können – wobei die Datenanalyse der wichtigste Faktor ist. Anwendungen wie die Verfolgung einzelner Personen oder die Erkennung von Menschenansammlungen können immer noch für Schutz- und Sicherheitszwecke eingesetzt werden, aber wir beginnen, völlig neue Geschäftsanwendungen basierend auf Datenanalyse zu erkennen – bisher hauptsächlich im Einzelhandel, aber andere werden sicherlich folgen.

Die meisten Anbieter verkaufen heute einen Großteil ihrer Hardware ohne zu wissen, an welchen Endkunden ihre Produkte geliefert oder in welche Anwendung sie integriert werden. Aleksandar Mitrovic von Bosch prognostiziert: „In einer IoT-Welt werden wir nicht nur wissen, wo unsere Produkte installiert sind. Auch bei der Überwachung, Verwaltung und Aktualisierung von Produkten über den gesamten Lebenszyklus können sich unsere Kunden auf uns verlassen. Sie werden außerdem die Möglichkeit erhalten, von unseren Cloud-basierten Analysefunktionen als Wegbereiter für fortschrittliche Geschäftsanwendungen zu profitieren." Als Zusatznutzen wird diese Entwicklung auch die Kundenbindung erhöhen, sofern Datenschutz und Datensicherheit von jedem Anbieter angemessen berücksichtigt werden.

Neue Herausforderungen schaffen neue Gelegenheiten

Es wird also viele neue Geschäftsmöglichkeiten geben – eine offensichtlich gute Nachricht für die etablierten Anbieter. Aber jede Medaille hat zwei Seiten, und die Herausforderung wird es sein, eine Führungsposition zu verteidigen, während neue Anbieter auf den Markt kommen. In der Telekommunikationsbranche hat die Einführung von Voice over IP dramatisch gezeigt, wie schnell Newcomer in Zeiten des schnellen Wandels Fuß fassen können, während einige der ehemaligen Marktführer einfach verschwunden sind – auch solche mit Milliardenunternehmen. Da große Teile der Hardware in den nächsten Jahren standardbasiert und immer mehr zu einer Ware werden, werden agile neue Anbieter in der Lage sein, schnell intelligente Technologien zu nutzen und fortschrittliche Services anzubieten, ohne sich um die zugrunde liegende Hardware kümmern zu müssen. Die etablierten Anbieter müssen deshalb unbedingt verstehen, dass das IoT nicht nur eine neue Technologie ist, die sie ein Jahr früher oder später als ihre Wettbewerber einführen. Vielmehr kennzeichnet es einen kompletten Paradigmenwechsel, der den Markt völlig verändern wird.

Bei der Transformation von Hardwareanbietern zu Serviceanbietern werden zwei Dinge für jeden Anbieter in der Sicherheitsbranche entscheidend sein: Daten und Analysen. Daten sind offensichtlich die Grundlage für Services der nächsten Generation, wie man am Beispiel von Google, Facebook und ähnlichen Phänomenen leicht erkennen kann. Aber ohne fortschrittliche Analysen wird es schwierig, wenn

▲ Wenn alles mit allem verbunden ist, werden neue Anwendungen entstehen – und es müssen neue Risiken berücksichtigt werden

intersec
forum

CONFERENCE REVIEW

Artikel war Thema beim Intersec Forum 2018

nicht gar unmöglich sein, diese Daten zu nutzen und den Kunden einen echten Vorteil zu verschaffen. Dies ist der Hauptgrund, warum Bosch heute Videoanalysefunktionen als Standard in die meisten seiner Netzwerkkameras integriert, wie Dr. Mitrovic betont. „Man kann sich jedoch nicht darauf verlassen, dass die Sensoren allein diese Funktionen unterstützen", sagt der Bosch-Experte und verweist auf Brandmelder oder Einbruchmelder. „Hier müssen Sie Analysen im Backend implementieren, die in der Regel Cloud-basiert sind. Und selbst bei intelligenten Kameras werden neue Anwendungen von korrelierten Informationen aus mehreren Geräten abhängig sein, was wiederum zusätzliche Analysen in der Cloud erforderlich macht."

„Die Datenanalyse eröffnet eine Vielzahl neuer Anwendungen und damit Geschäftsmöglichkeiten für Anbieter von Schutz- und Sicherheitslösungen. Auch hier kommen einem sofort videobasierte Anwendungen wie Bewegungsanalyse oder Massenerkennung in den Sinn, aber denken Sie auch daran, was Sie mit realen Daten aus der Zutrittskontrolle oder Branderkennung machen können. Eine prädiktive Wartung, die auf einer kontinuierlichen Integritätsüberwachung basiert, kann Kunden bares Geld sparen und Ausfälle vermeiden", so Mitrovic weiter. Diese Daten können jedoch auch für Anwendungen verwendet werden, die weit über die Sicherheit hinausgehen. Nutzungsdaten von Zutrittskontrollsystemen und Temperaturinformationen von Brandmeldern können dazu beitragen, den HLK-Betrieb (Heizung, Lüftung, Klimatisierung) und den Energieverbrauch zu optimieren, während Videodaten perfekt geeignet sind, um Geschäfts- oder sogar Flughafenlayouts zu verbessern.

Nach der Einführung der Konnektivität von Sicherheitsprodukten werden nun die Geschäftsprozesse rund um diese Produkte digitalisiert. Der nächste Schritt wird die Schaffung hochwertiger Ökosysteme bei allen Herstellern sein. „Für Bosch geht IoT über die reine Konnektivität hinaus. Unsere umfangreiche Technologieerfahrung in zahlreichen Bereichen versetzt uns in eine einzigartige Position, um domänenübergreifende Ökosysteme zu fördern und anwendungsübergreifende Ökosysteme zu betreiben", sagt Mitrovic. „Wir arbeiten gemeinsam mit zahlreichen Industriepartnern an einem offenen, herstellerübergreifenden IoT-Ökosystem. Details zu dieser Plattform werden in einer unserer nächsten Veröffentlichungen beschrieben."

Datenschutz und Datensicherheit müssen berücksichtigt werden

Das Erfassen, Speichern und Verarbeiten von Kundendaten wird somit eine der tragenden Säulen des zukünftigen Geschäfts der Sicherheitsanbieter sein. Diese Entwicklung wird, wie wir gesehen haben, neue Möglichkeiten eröffnen, aber auch neue Herausforderungen mit sich bringen. Im Internet der Dinge sind Datenschutz und Datensicherheit von größter Wichtigkeit. Anbieter, die nicht garantieren können, dass die Daten ihrer Kunden sicher sind, können leicht vom Markt verschwinden. Konkret wird die Datenschutz-Grundverordnung der EU hier ab Mai 2018 neue und sehr strenge Maßstäbe setzen, mit hohen Strafen von bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes eines Unternehmens.

Dies bedeutet, dass alle Cloud-basierten Service-Angebote mit den besten Technologien gesichert werden müssen, und dass Datenschutz und Datensicherheit zu Designprinzipien für jedes vernetzte Produkt werden müssen. Das Kapern von Überwachungskameras, wie es in der jüngsten Vergangenheit bei Konsumgütern stattgefunden hat, darf bei ernsthaften Sicherheitsanwendungen einfach nicht passieren. „Unsere Aufgabe ist es, die Daten unserer Kunden allein zu ihrem Nutzen zu verwenden", so Aleksandar Mitrovic von Bosch Building Technologies. „Das ist unser oberstes IoT-Prinzip, und es ist eine Unternehmensrichtlinie, die alle Geschäftsbereiche von Bosch bindet – ob Automotive, Safety & Security, Hausgeräte oder Elektrowerkzeuge. In unserem Bestreben, IoT in unserer DNA zu verankern, werden Datenschutz und Sicherheit der Kundendaten immer an erster Stelle stehen." ■

Kontakt

Bosch-Sicherheitssysteme GmbH
Grasbrunn
Tel.: +49 800 7000444
info.service@de.bosch.com
www.bosch-Sicherheitssysteme.de

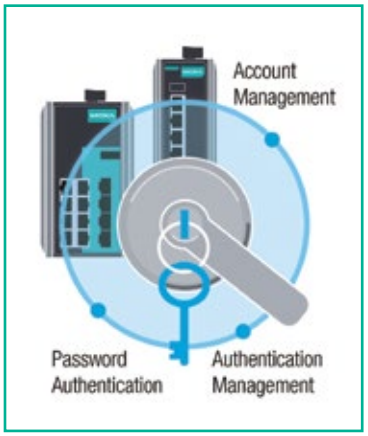
NETZWERKE

Draußen und sicher

Wie sich mit industriellen PoE-Switches zuverlässige Outdoor-IP-Überwachungsnetzwerke erstellen lassen.

IP -Überwachungsnetzwerke in Außenbereichen können von der Power-over-Ethernet-Technologie deutlich profitieren. Obwohl PoE-Lösungen durch die Übertragung von Strom und Daten über dasselbe Kabel bereits bei der Installation Aufwand und Kosten sparen, müssen Systemintegratoren auch den Stromverbrauch, die Netzwerkbandbreite, Wiederherstellungszeit und Sicherheitsanforderungen bedenken, um hohe Zuverlässigkeit und Verfügbarkeit zu erzielen.

Im Zuge des allgemeinen Trends hin zur Entwicklung smarter Städte ist auch die Nachfrage nach IP-Überwachungsanwendungen in den vergangenen Jahren stark gestiegen, da Regierungen und Immobilienbesitzer den Echtzeit-Status kritischer Infrastrukturen überwachen wollen, um die Betriebseffizienz zu verbessern sowie wichtige Wirtschaftsgüter zu schützen.

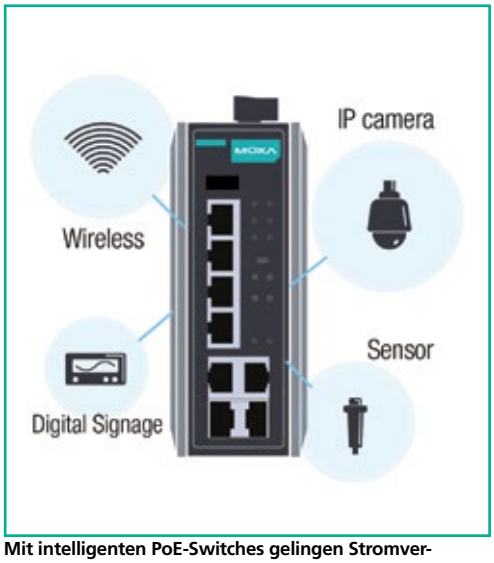


Clevere Sicherheitsfunktionen schützen betriebskritische Netzwerke

Um flexible, kosteneffiziente IP-Überwachungssysteme zu konstruieren, nutzen Sicherheitsmanager und Systemintegratoren oft die Vorteile der PoE-Technologie. PoE nutzt ein einziges Kabel, um Daten zu übertragen und Strom zu liefern. Dadurch lassen sich Verkabelungskosten sparen und die Installationszeit reduzieren. Zweifellos sind PoE-Switches mittlerweile beliebt, und ihr Einsatz für IP-Überwachungslösungen nimmt zu.

Insbesondere in IP-Überwachungssystemen für Außenbereiche wird PoE zur Kosten- und Aufwandsminderung eingesetzt. Es bietet überdies eine hohe Zuverlässigkeit für das System und alle verbundenen Geräte. Betriebskritische Anwendungen, die IP-Überwachung im Außenbereich einsetzen, sind typischerweise die Autobahnverkehrskontrolle und -überwachung oder die Überwachung von Öl-Pipelines, Stromerzeugung und -verteilung, die Überwachung von Wasser- und Abwasserstationen und viele weitere. In diesen Anwendungen fordern die Betreiber die höchste Zuverlässigkeit und Verfügbarkeit ihrer Überwachungssysteme, und sie benötigen konstantes Video-Streaming, da die Videoüberwachung die Personensicherheit sowie kritische Einrichtungen schützt und zusätzlich die Betriebseffizienz steigert. Darüber hinaus werden HD-PTZ-Kameras – die einen höheren Stromverbrauch und größere Bandbreiten erfordern – oft eingesetzt, um ein breites Spektrum abzudecken und unterbrechungsfreie HD-Videos zu liefern. Das ist für Sicherheitsverantwortliche wichtig, um die Standortbedingungen klar zu überwachen und bei auftretenden Ereignissen die nötigen Maßnahmen zu ergreifen. Die Herausforderung liegt jedoch darin, sicherzustellen, dass die PoE-Switches hohe Stromabgabe und ausreichende Netzwerkbandbreite bei gleichbleibend hoher Verfügbarkeit und Zuverlässigkeit liefern können, auch in rauen Umgebungen mit extremen Temperaturen, vielen Störfaktoren und potenziellen Cybersecurity-Risiken. Um diese Herausforderungen zu meistern, sollten Systemintegratoren vier Themen Beachtung schenken:

- PTZ-Kameras für den Außenbereich verbrauchen mehr Strom, als reguläre IP-Kameras, das muss in der Design-Phase berücksichtigt werden.
- Das PoE-Netzwerk muss ausreichend Bandbreite für die unterbrechungsfreie Übertragung von HD-Video vorhalten.



Mit intelligenten PoE-Switches gelingen Stromversorgung, Verwaltung und Diagnose mühelos.

■ Um ein hoch zuverlässiges und verfügbare Videosystem zu gestalten ist es wichtig, Wiederherstellungsmechanismen sowohl für die Netzwerkinfrastruktur, als auch die IP-Kameras einzusetzen.

■ Zu guter Letzt sollte im Netzwerk und in den Geräten Cybersecurity eingesetzt werden, um Cyber-Attacken zu vermeiden, welche die Personensicherheit oder kritische Einrichtungen gefährden können.

Moderne Überwachungsgeräte mit Hochleistung versorgen

Im Normalbetrieb verbraucht eine Überwachungskamera oft 10 bis 20 W, um grundlegende Überwachungsfunktionen durchzuführen. Wenn Kameras, die rund um die Uhr in Betrieb sind, bei wenig Licht IR-Strahler einsetzen müssen, kann das den Stromverbrauch auf bis zu 30 W erhöhen. Heutzutage gibt es eine Reihe von industriellen PoE-Switches, die angeschlossene Geräte mit bis zu 30 W versorgen und keine zusätzliche Stromversorgung benötigen. Manchmal reichen jedoch auch 30 W aufgrund zunehmend erforderlicher Funktionen in rauen Umgebungen nicht mehr aus. Eine nicht unproblematische Anwendung für PTZ-Überwachungskameras ist die Erfassung großflächiger Außenbereiche in Zeiten mit schwachem Licht. Zusätzliche Funktionen wie Heizungen oder Lüfter können in rauen Umgebungen mehr Strom als üblich benötigen. Für Installationen mit mehreren HD-PTZ-Kameras, die weitläufige Flächen mit viel Aktivität überwachen ist es wichtig, über einen PoE-Injektor oder einen Switch zu verfügen, der in der Lage ist, 60 W zu liefern sowie zusätzlich ein Strombudget und eine Spannungsversorgung für die ausreichende Versorgung aller weiteren verbundenen Geräte.

Um diesen Strombedarf zu decken, kaufen Systemintegratoren üblicherweise HD-PTZ-Kameras, die einen 60 W-PoE-Injektor beinhalten. Es gibt jedoch auch Grenzen für die Injektoren, da Überwachungsanwendungen im Außenbereich oft viele verschiedene technische Anforderungen stellen, so wie erweiterte Betriebstemperaturen und elektromagnetische Kompatibilität (EMV-Schutz). Integrierte Injektoren erfüllen diese Anforderungen meist nicht, sodass der Systemintegrator eine alternative Lösung finden muss. Eine bessere Option ist der Einsatz industrieller Managed PoE-Switches, da diese speziell für volle Leistung in rauen Umgebungen ausgelegt sind und direkt an die Kameras angeschlossen – so erübrigt sich ein individueller PoE-Injektor für jede Kamera. Eine weitere Herausforderung stellt die noch ausstehende Ratifizierung des 802.3bt High-Power PoE-Standards dar. Viele Kameras nutzen verschiedene, proprietäre vieradrige Verkabelungsdesigns, um 60 W PoE zu unterstützen. Dementsprechend ist es wichtig, einen industriellen PoE-Switch auszuwählen, der so programmiert werden kann, dass er verschiedene Arten des vieradrigen Designs unterstützt, sodass verbundene PTZ-Kameras mühelos angeschlossen und mit Energie versorgt werden können.

Ein Netzwerk mit ausreichend Bandbreite aufsetzen

Beim Design einer Netzwerktopologie mit mehreren Überwachungskameras in Industrieanwendungen ist es sehr wichtig, dass ausreichend Uplink-Bandbreite vorgehalten wird, um unter allen Umständen die unterbrechungsfreie Übertragung von Bilddatenpaketen mit hoher Qualität sicherzustellen.

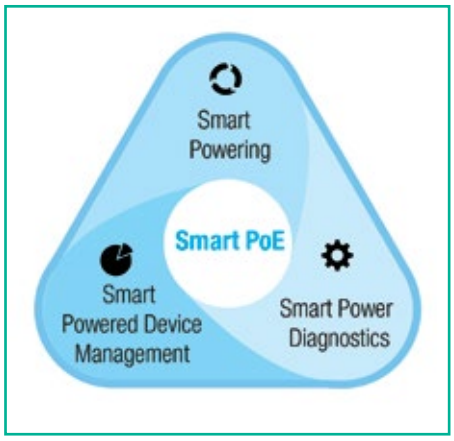
Das folgende Beispiel illustriert, wie sich ausreichend Bandbreite für ein Industrienetzwerk sicherstellen lässt. In modernen Überwachungsnetzwerken benötigen hochauflösende Kameras zwischen 10 und 20 Mbps, um 1080P bei 30 FPS mit H.264-Komprimierung zu unterstützen. Wird ein industrieller Ethernet-Switch eingesetzt, um 25 Kameras anzubinden, sollten 500 Mbps Bandbreite vorhanden sein, damit jede Kamera 20 Mbps für die zuverlässige Funktion erhält. Für derartige Installationen sollten rund 50 Prozent dieser Bandbreite reserviert werden, denn es gibt Phasen, in denen Extra-Bandbreite erforderlich ist. Beispielsweise dann, wenn PTZ-Kameras große Flächen überwachen oder im Überwachungsbereich mehrerer Kameras gleichzeitig viel Aktion stattfindet, gibt es Spitzen in der Bandbreitennutzung, die sonst zu Bildstottern oder Bildverlusten kommen kann.

Automatische Wiederherstellung in Überwachungsnetzwerke einbauen

In Videoüberwachungsanwendungen im Außenbereich werden immer mehr industrielle PoE-Switches eingesetzt, welche die automatische Wiederherstellung unterstützen und kein menschliches Eingreifen bei Netzwerkproblemen erfordern. Die drei größten Vorteile der eingebauten Wiederherstellung sind maximale Systemverfügbarkeit, Komfort und niedrigere Gesamtbetriebskosten.

Eine Situation, die in Netzwerken mit vielen IP-Kameras oft vorkommt, ist dass diese einfrieren, stottern oder Verzögerungen haben, was bis zu komplett unbrauchbaren Bildern führen kann. Für fast alle elektronischen Geräte, die Probleme haben, ist der erste Schritt zur Lösung der Neustart. IP-Kameras brauchen viel Bandbreite, da sie permanent Daten verarbeiten, was oftmals damit endet, dass die Kameras den gesamten temporären Speicherplatz aufbrauchen. Wenn ein im Netzwerk installierter industrieller PoE-Switch Geräte auf Störungen überprüft, und eine Kamera innerhalb einer bestimmten Zeitspanne nicht antwortet, kann der Switch die Stromversorgung der Kamera einstellen, wodurch sie abgeschaltet wird. Der Switch kann die Spannungsversorgung wieder aufnehmen, sodass die Kamera neu hochfährt und alle temporären Daten, die zu Problemen geführt haben, löscht. Meistens funktioniert diese einfache Vorgehensweise. Da Funktionsstörungen öfter vorkommen, kann ein solcher Switch hohe Kosten für Wartung und Fehlersuche/-behebung senken, während sich die Kameraverfügbarkeit erhöht.

Netzwerkredundanz ist auch eine wichtige Funktion, da sie Ausfälle verhindert und die Verfügbarkeit von Videostreams erhöht. Um reibungslose Videokommunikation in dynamischen Überwachungsbereichen sicherzustellen, sollte die Wiederherstellungszeit bei Ausfällen unter 500 ms über das gesamte Netzwerk liegen, da der Überwachungsbildschirm bei über 500 ms fragmentierte oder Standbilder zeigt. Zusätzlich zu den unangenehmen Netzwerkausfällen mit Verlust von Überwachungsmaterial ist ein weiteres Problem die teure Wiederherstellung durch Wartungspersonal vor Ort. Es gibt viele Gründe dafür, dass Unternehmenseigentümer die Besuche vor Ort möglichst verhindern möchten. Da die Standorte oft dezentral liegen, ist der Besuch zeit- und kostenintensiv. Zusätzlich dazu sind die Kameras oft an schwierig zu erreichenden Stellen installiert, wie an der Spitze von langen Masten. An diesen Stellen können die Kameras bessere Bilder aufnehmen und sind für Vandalen nicht erreichbar. Das macht aber auch die Wartung schwieriger. Obwohl industrielle PoE Switches mit Wiederherstellungsfunktion höhere Anschaffungskosten haben, können sie die Kosten und den Arbeitsaufwand über eine Projektdauer deutlich senken.



Industrielle Managed-PoE-Switches verfügen über zahlreiche nützliche Schnittstellen.

Netzwerke mit einer Kombination aus Geräteausfallprüfung und Netzwerkredundanz haben sehr viel weniger Ausfälle und entsprechend niedrigere Kosten für die Behebung.

Das Netzwerk durch Cybersecurity schützen

Ein ungesichertes oder gefährdetes IP-Überwachungssystem kann das Ziel von Cyberattacken werden, da IP-Überwachungssysteme oft für den Schutz der menschlichen Sicherheit und kritischer Einrichtungen eingesetzt werden, wie in der Strafverfolgung und Verbrechensverhinderung, der Transportsicherheit und Verkehrsüberwachung oder in der industriellen Prozessüberwachung. Lange Jahre war Cybersecurity für Systembetreiber kein wichtiges Anliegen, denn sie hielten ihre Überwachungsnetzwerke aufgrund der Isolierung von anderen Netzwerken für sicher. Mittlerweile müssen die Betreiber ihre Sicherheitspraktiken ständig erneuern, um Menschen und kritische Einrichtungen zu schützen. Isolierte Bereiche und bestimmte Geräte sind üblicherweise sicher vor gezielten Übergriffen. Es reicht jedoch schon das Eindringen in ein Gerät aus, um ein gesamtes Netzwerk zu kompromittieren. Daher wird für PoE-Switches in betriebskritischen Überwachungsanwendungen sowohl die Sicherheit auf Geräteebene, als auch auf Systemebene empfohlen.

Um Cybersecurity-Risiken abzuschwächen ist es für industrielle Managed-PoE-Switches wichtig, über Funktionen für die Sicherheit auf Geräte- und Systemebene zu verfügen. Dazu gehören starke Passwörter, Account-Verwaltung, Sperreinstellungen für Passwortfalscheingabe, Sticky-MAC-Adressen sowie 802.1X- und MAC Bypass-Authentifizierung. So können Eindringlinge keinen einfachen dezentralen Zugriff auf Geräte erlangen und die Einstellungen so verändern, dass Risiken für Geräte oder Netzwerk entstehen. Bei der Einstellung von Zugriffskontrolllisten können industrielle Managed-PoE-Switches beispielsweise den Datenverkehr von nicht autorisierten IP-oder MAC-Adressen verweigern. So können nicht autorisierte Geräte nicht auf Switches, Kameras oder andere Systeme zugreifen. Sticky-MAC-Adressen können außerdem spezifische Switch-Ports and spezifische Kamera-MAC-Adressen verknüpfen, sodass sie nicht mehr verfügbar sind, wenn jemand ein Originalgerät durch ein anderes Gerät ersetzen und lokal auf das Netzwerk zugreifen will.

Eine solide Sicherheitsleitlinie ist jedoch nur der erste Schritt. Es ist genauso wichtig, die Sicherheitseinstellungen mit der Weiterentwicklung des Netzwerks konsequent zu überprüfen. Je mehr Veränderungen sich im Netzwerk abspielen, desto mehr Chancen auf Schwachstellen entstehen, die für jemanden mit bösen Absichten die Zugriffsmöglichkeiten erhöhen.

Der Einsatz von PoE-Lösungen in IP-Überwachungsanwendungen birgt unter den vielen Optionen eindeutige Vorteile. Sie gelten als die zuverlässigsten und effizientesten Lösungen, müssen aber auch sorgfältig hinsichtlich High-Power-PoE-Design, Bandbreitenverfügbarkeit, Wiederherstellungsfunktionen und Cybersecurity-Schutz für die Anwendung ausgewählt werden. Obwohl ihr Einstandspreis relativ hoch ist, zahlen sich PoE-Switches langfristig aus, indem sie die Gesamtbetriebskosten senken. ■

Autor
Jackey Hsueh
Product Manager, Moxa Europe

Kontakt

Moxa Europe GmbH
Unterschleißheim
Tel.: 089/37003990
www.moxa.com

GIT SAFETY

INNENTITEL

Diesen Monat Schwerpunkt:
Safety-to-Cloud-Lösung von Schmersal
Seite 116

SCHMERSAL
Safe solutions for your industry

Die sicheren Signale werden in der Sicherheitssteuerung PSC1 ausgewertet, das gewährleistet kurze Reaktionszeiten

MASCHINEN- UND ANLAGENSICHERHEIT

Sicherheit und Produktivität gehen Hand in Hand

Safety-to-Cloud-Lösung unterstützt Predictive Maintenance

Predictive Maintenance ist eine Kernkomponente von Industrie 4.0, deren wesentlicher Vorteil sich mit einem Wort zusammenfassen lässt: Wirtschaftlichkeit. Um die Maschinenleistung im Sinne einer vorausschauenden Instandhaltung zu optimieren, müssen bereits auf der untersten Maschinenebene umfassend Daten erfasst werden. Bei der Analyse und Nutzbarmachung der Daten helfen Cloudlösungen. Schmersal stellt nun erstmals eine Safety-to-Cloud-Lösung vor, bei der Maschinensicherheit und Produktivitätssteigerungen Hand in Hand gehen.

In der Industrie 4.0 ist es das Ziel, nicht mehr reaktiv auf den Ausfall von Komponenten zu reagieren, sondern proaktiv einen kostspieligen Ausfall der Maschine zu verhindern. Defekte Bauteile, die womöglich bald zum Stillstand der Anlage führen, soll unabhängig von den üblichen Wartungsintervallen identifiziert und ausgetauscht werden, bevor tatsächlich Schaden entsteht.

Grundlage dafür ist eine permanente Zustandsüberwachung von technischen Prozessen und Bauteilen direkt an der Maschine. Sensoren messen zum Beispiel Kennzahlen wie Vibration, Temperatur oder Feuchtigkeit. Diese Sensordaten werden erfasst und ausgewertet, sodass frühzeitig ein möglicher Ausfall von Komponenten erkannt wird.

Dabei ist die Cloud eine Schlüsseltechnologie: Sie ermöglicht u.a. umfassende Datenanalysen. Die Auswertung von Monitoring-Informationen in der Cloud wird heute bereits vielfach erfolgreich praktiziert. Die Einbeziehung der Sicherheitstechnologie in derartige Konzepte war jedoch bisher nicht üblich. Dabei liegen die Vorteile auf der Hand: Komponenten, die zu Einhaltung von Sicherheitsstandards eingesetzt werden, können gleichzeitig als „Datenlieferant" zu Produktivitätssteigerung.

Umfangreiche Diagnosemöglichkeiten

Die Schmersal Gruppe hat jetzt erstmals eine Safety-to-Cloud-Lösung vorgestellt: Alle Sicherheitszuhaltungen und Sicherheitssensoren sowie einige Sicherheitslichtgitter von Schmersal, die mit einem SD-Interface ausgestattet sind, können über die Sicherheitssteuerung PSC1 oder ein SD-Gateway sowie über ein separates Edge-Gateway zyklischen Daten in eine beliebige Cloud übertragen. Eine Verknüpfung dieser zyklischen SD- Daten innerhalb der Cloud bietet dem Anwender umfangreiche Diagnosemöglichkeiten, dazu zählen z.B. Schaltzyklen, die Zustandssituation der Sicherheit, Grenzbereichswarnungen, Abstandswarnungen und vieles mehr. Diese neue Lösung von Schmersal ist hersteller- und systemunabhängig. Sie lässt dem Anwender

die freie Wahl bei der Entscheidung, welche Cloud er nutzen möchte.

Für die Übertragung von Monitoring- u. Zustandsdaten an die Cloud zur kundenindividuellen Auswertung bieten sich systemunabhängige Formate wie OPC UA, MQTT oder AMQP an. Bei der Smart Safety Lösung leitet das Edge-Gateway derzeit die Daten im MQTT-Format weiter. Es handelt sich dabei um ein offenes Kommunikationsprotokoll, das sich inzwischen zu einem der populärsten IoT-Standards entwickelt hat. Es ist zudem eine schlanke, kosteneffiziente Lösung, die sehr einfach zu implementieren ist. Prinzipiell sind jedoch auch Safety-to-Cloud-Lösungen möglich, bei denen OPC UA genutzt wird. OPC UA gilt als zukunftsweisender Standard für M2M-Kommunikationsprotokolle, da es Informationen über Maschinen oder Sensoren nicht nur transportiert, sondern auch eine semantische Beschreibung der Informationen ermöglicht.

Die neue Safety-to-Cloud-Lösung von Schmersal ist hersteller- und systemunabhängig

Visuelle Darstellung von Diagnoseinformation

In der derzeitigen Version der Smart Safety Solution können die zyklischen Daten beispielsweise auf Microsoft Azure gespeichert werden, einer gängigen Cloud-Plattform. Doch kann der Anwender der Smart Safety Solution jede beliebige Cloud-Plattform nutzen. Die Diagnoseinformationen können auf Bildschirmen visualisiert werden. Dashboards bieten eine Vielzahl von nützlichen Funktionalitäten für die Darstellung der Daten, z.B. in Form von Tabellen, Diagrammen oder Grafiken. Per Drag & Drop kann der Anwender ganz einfach diejenigen Daten auswählen, die er für die Analyse seiner individuellen Prozesse benötigt. Er kann sich beispielsweise die Anzahl der Betriebsstunden anzeigen lassen und wie häufig eine Maschine angelaufen ist. So kann der User den voraussichtlichen Verschleiß von Komponenten errechnen, sodass ein frühzeitiger Austausch möglich ist. An den Daten über die Betriebsspannung lässt sich z. B. erkennen, ob ein Netzteil ausgefallen ist. Selbst Informationen über die Häufigkeit des Öffnens und Schließens einer Schutztür lassen Rückschlüsse zu auf mögliche Probleme an einer Maschine. Durch eine solche permanente Datenanalyse bekommen die Nutzer zusätzlich ein sehr viel genaueres Bild ihrer Anlagen geliefert: Bedienfehler oder falsche Einstellungen sind damit schnell identifizierbar und können abgestellt werden.

Die Diagnoseinformationen können auch über mobile Endgeräte wie Tablets oder Handys abgerufen werden. Damit wird eine standortunabhängige Kontrolle von Fertigungsprozessen ermöglicht und darüber hinaus der proaktive Einsatz von Servicekräften, beispielsweise durch Push-Mitteilungen über das Handy, wenn etwa bei einem Versatz von Schutztüren vordefinierte Limits erreicht werden.

Sicherheitslösung für komplexe Anlagen

Ein weitere Vorteil der Smart Safety Solution ist, dass die Diagnoseinformation parallel zu den Sicherheitsfunktion an die Cloud weitergeleitet werden. Die sicheren Signale werden in der Sicherheitssteuerung PSC1 ausgewertet, sodass damit auch die erforderlichen schnellen Reaktionszeiten gewährleistet sind und die Sicherheitsfunktionen bei Fehlern in der Maschine zuverlässig ausgeführt werden. Die nicht-sicheren Diagnoseinformationen werden dagegen nicht über die Steuerung, sondern über das SD-Gateway sowie das Edge-Gateway direkt an die Cloud übermittelt. Das bedeutet, das ein zusätzlicher Entwicklungsaufwand für die Steuerung nicht erforderlich ist.

Bei dem SD-Gateway von Schmersal handelt es sich um eine bewährte proprietäre Lösung, mit der umfangreiche Status- und Diagnosedaten von Sicherheitsschaltgeräten mit SD-Interface übertragen werden können. Ein Vorteil der SD-Lösung ist, dass bis zu 31 Sicherheitssensoren und Sicherheitszuhaltungen in Reihe geschaltet werden können. Auf diese Weise können auch komplexe Anlagen mit einem erheblich reduzierten Verdrahtungsaufwand abgesichert werden. Auch Alt- und Bestandsmaschinen (Braunfield), die mit einer SD-Lösung abgesichert sind, können nachgerüstet und bestehende Anlagen nachträglich mit der Safety-to-Cloud-Lösung von Schmersal ausgestattet werden

> „Auch Alt- und Bestandsmaschinen (Braunfield) können nachträglich mit der Safety-to-Cloud-Lösung ausgestattet werden."

Um das zu verarbeitende Datenvolumen und den Daten-Traffic zu begrenzen, müssen dabei nicht alle Daten zur übergeordneten Ebene in der Automatisierungspyramide weitergeleitet werden. Bei komplexen Maschinen wählen die Konstrukteure oft eine dezentrale Steuerungsarchitektur. Die Sicherheitssteuerung Protect PSC1 von Schmersal lässt sich daran optimal anpassen, indem die Kompaktsteuerung PSC1-C-100 im Schaltschrank installiert wird und mehrere dezentrale Erweiterungsmodule in den Unterverteilungen angebracht werden können. Die sichere Remote-IO-Kommunikation gewährleistet in diesem Fall einen sicheren Signalaustausch zu den dezentralen Erweiterungsmodulen. Außerdem kommuniziert die Sicherheitssteuerung über das universelle Kommunikations-Interface mit der betriebsmäßigen Steuerung der Anlage. Der Betreiber der Anlage entscheidet, welche Daten in die Betriebssteuerung und welche in das ERP-System zu weiteren Verarbeitung weitergeleitet werden. ■

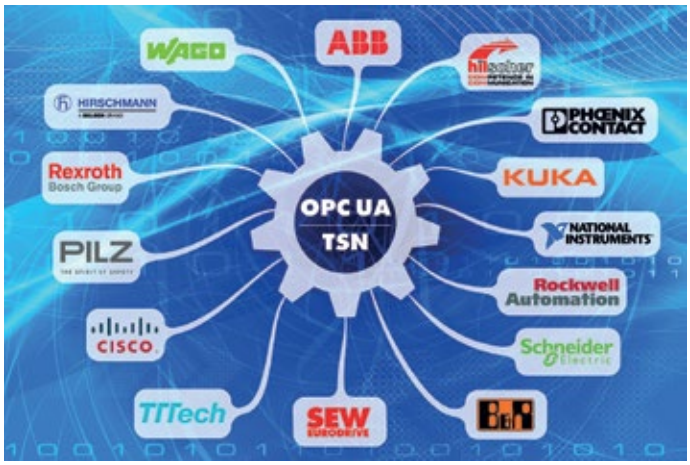
Automatica: Halle B6, Stand 328

Autor

Siegfried Rüttger,
Projektleiter Industrie 4.0,
Schmersal Gruppe

Kontakt

K.A. Schmersal GmbH & Co. KG
Wuppertal
Tel.: +49 202 6474 0
info@schmersal.com
www.schmersal.com



Automatisierungsunternehmen arbeiten zusammen

Rockwell Automation schließt sich den Branchenführern ABB, Belden, Bosch Rexroth, B&R, Cisco, Hilscher, KUKA, National Instruments, Phoenix Contact, Pilz, Schneider Electric, TTTech und WAGO (zusammen als „Shapers" bekannt) an, um eine Kommunikationslösung für Echtzeit- und Sensor-to-Cloud-Anwendungen im industriellen Umfeld zu entwickeln. Die auf OPC UA basierende Lösung, ermöglicht eine einfache und sichere Nutzung von Informationen über verschiedene Herstellersysteme hinweg. Zudem wird die Latenz und Robustheit in konvergierten industriellen Netzwerken durch TSN (Time-Sensitive-Networking) verbessert.

www.br-automation.com ■

Module für Service-Robotik im industriellen Umfeld

Das Automatisierungsunternehmen Pilz erweitert sein Portfolio um den neuen Produktbereich Service-Robotik: Die Module umfassen zu Beginn den Manipulator, das Steuerungsmodul und das Bedienmodul. Wesentliche Merkmale sind Offenheit, z. B. dank des Software-Frameworks ROS, anwenderfreundliche Bedienung und schnelle Inbetriebnahme nach dem Plug-and-Play-Prinzip. So können sich Anwender ihre individuelle Service-Roboter-Applikation zusammenstellen. Manipulator, Steuerungsmodul und Bedienmodul bilden zusammen ein von der DGUV (Deutsche Gesetzliche Unfallversicherung) zertifiziertes Paket nach EN ISO 10218-1 „Industrieroboter – Sicherheitsanforderungen" und bringen damit alle Voraussetzungen für die Umsetzung sicherer Roboterapplikationen mit. Das erleichtert den Weg zur obligatorischen CE-Kennzeichnung. Zu den Einsatzgebieten gehören z. B. Pick&Place-Anwendungen sowie modulare teilautomatisierte „Klein-Roboterzellen" in der Industrie. Auf der Automatica 2018 stellt Pilz erstmals seine Service-Robotik-Module vor (Halle B4, Stand 500).

www.pilz.com ■

Kommunikation auf Industrie 4.0-Niveau

Man sieht es ihm nicht an, aber der bislang kleinste Sicherheitsschalter von Euchner hat es in sich. Die eigentliche Innovation steckt nämlich im Inneren. Neben der bereits bekannten und vielfach genutzten Möglichkeit der Reihenschaltung von Sensoren bietet der Sicherheitsschalter CES-C07 eine weitaus umfassendere Diagnose. Mehr noch: Die Geräte liefern prozessrelevante Parameter in Echtzeit. Informationen zur präventiven Wartung sind damit garantiert. Die Sensoren messen relevante Umgebungsparameter und signalisieren rechtzeitig, bevor ein Ausfall der Maschine droht. Sogar Manipulationsversuche sind mit diesem System zu erkennen. In Kombination mit dem Sicherheitsmodul ESM-CB werden diese Informationen automatisch von jedem Schalter in der Kette abgefragt und via IO-Link der Steuerung zur Verfügung gestellt. Dass der Schalter über Funktionen wie Schwachbereichsanzeige des Transponderfelds und gut sichtbare Anzeige-LEDs verfügt, ist dabei selbstverständlich, ebenso wie die Sicherheitseinstufung in Kategorie 4/PLe.

www.euchner.de ■

KUKA und KEB mit sicherer Kommunikation

In der Industrie 4.0 verzahnt sich die Produktion mit modernster Informations- und Automatisierungstechnik. Basis dafür sind intelligente, digital vernetzte Systeme, die Maschinen und Anlagen verbinden. Beide Unternehmen zeigen nun, wie das praktisch aussieht. In diesem Themenfeld stellt KEB Automation eine neue Lösung bereit, um eine Konnektivität zu Robotern von KUKA Automation mit verschiedenen Anwendungen realisieren zu können. Mit dem C6 HMI LC bietet KEB nun die Möglichkeit, sowohl Daten auszutauschen als auch KUKA-Roboter zu steuern und zu programmieren. Das System von KEB kombiniert die Visualisierung mittels HMI und die Steuerung – eine PLC – in einem Gerät. Das vereinfacht die Komplexität des Systems und reduziert die Kosten. EtherCAT, als leistungsstarker Feldbus, erleichtert außerdem die Verbindung zum Roboter.

www.keb.de ■

Sicherheitsschalter mit Magnet- und RFID-Technologie

Die neue NS-Serie vereint all das Know-how, das Pizzato Elettrica in mehr als 33 Jahren Erfahrung in der industriellen Arbeitssicherheit gesammelt hat. Die Sicherheitsschalter der Serie NS mit E-Magnet- und RFID-Technologie verfügen über ein selbstverlöschendes schlagzähes Technopolymer-Gehäuse und eignen sich für leichte bis mittelschwere Anwendungen. Wichtige Merkmale sind u. a. die berührungslose Aktivierung durch RFID-Technologie sowie maximale Sicherheit mit nur einem Gerät: Die eigensicheren Schalter der Serie NS ermöglichen es, Absicherungen mit dem höchsten Sicherheitsniveau PLe und SIL3 zu realisieren, wobei bereits ein Schalter ausreichen kann. Zudem ist der Schalter ist mit einer großen Öffnung zur Zentrierung des Betätiger-Bolzens ausgerüstet. Diese Lösung macht es während der Montage- oder Justagephase einfacher, den Betätiger auf die Öffnung des Schalters auszurichten – z. B. bei dejustierten Türen.

www.pizzato.com ■

Kompetenz in Safety at Work

Leuze electronic stellte auf der Hannover Messe seine Kompetenz in Safety at Work und Industrie 4.0 in den Mittelpunkt. Auf Basis seiner Sicherheits-Lichtvorhänge MLC entwickelte der Optosensorikhersteller mit Smart-Process-Gating eine Alternative zum Mutingverfahren, das keine signalgebenden Sensoren benötigt. Ein weiteres Safety-Highlight ist der Sicherheits-Laserscanner RSL 400. Dessen neue Profinet/ProfiSafe-Varianten lassen sich einfach in industrielle Netzwerke integrieren. Ebenso neu ist die Kombination der RSL-Sicherheitstechnik mit einer hochwertigen Messwertausgabe für die Navigation von Automated-Guided-Vehicles (AGVs). Die Messwerte sind hierbei speziell auf die Anforderungen der AGV-Navigationssoftware ausgelegt. Smarte Industrie 4.0-Lösungen stellten einen weiteren Schwerpunkt des Messeauftritts dar. Anhand von praktischen Beispielen wurde gezeigt, wie Condition-Monitoring und Predicitive-Maintenance funktionieren. Hierfür stellte der Sensorhersteller u. a. erstmals eine intelligente Sensorleitung mit „SmartCore-Technologie" vor. Damit ist es möglich, einen drohenden Aderbruch präventiv und noch bevor die Sensorleitung ganz ausfällt zu erkennen.

www.leuze.com ■

Flexible Produktion

Auf der Hannover Messe konnten Besucher am Omron-Stand erleben, wie durch flexible Roboterzellen, Datenerfassung und -verarbeitung sowie künstliche Intelligenz Produktionsumgebungen möglich werden, in denen nahtlos zwischen benutzerdefinierter Produktion und Massenproduktion gewechselt wird. Durch die Zusammenarbeit von Roboter und Maschinen können Produktionslinien kurzfristig und effizient an Änderungen angepasst werden, z. B. wenn sich Produktionsvolumina ändern oder Spezialanfertigungen produziert werden müssen. Mobile und fixe Roboter arbeiten zusammen und erledigen Aufträge, die in der MMS vor Ort oder über eine sichere OPC-UA-Datenübertragung in einem Tablet-Computer eingegeben werden. Mit dieser integrierten Lösung zeigt Omron, wie Maschinenintelligenz, von der einzelnen Verarbeitungsebene bis zur Gesamtsystemebene, flexible und konfigurierbare Fertigungsprozesse ermöglicht.

www.industrial.omron.de ■

Funktionale Sicherheit ist Chefsache

Verschiedene Gesetze regeln, dass nur sichere Maschinen und Anlagen gehandelt und betrieben werden dürfen. Bei vorsätzlichen oder grob fahrlässigen Verletzungen dieser Pflichten greift neben dem Zivilrecht auch das Strafrecht und Gefängnisstrafen sind möglich. Dieses Risiko ist vielen Unternehmern nicht bewusst. Die Verantwortung einfach zu delegieren, ist nur begrenzt möglich. Wirksam ist dies nur, wenn derjenige, an den die Verantwortung delegiert wird, nicht nur die Konsequenzen übertragen bekommt, sondern auch die nötige Befähigung und die erforderlichen Befugnisse hat. Ist dies nicht der Fall, ist das Delegieren juristisch nicht wirksam und die Verantwortung fällt auf den Arbeitgeber zurück. Damit Unternehmer und Geschäftsführer rechtssicher agieren können, bietet Wieland Electric ein umfangreiches Schulungsprogramm rund um die Maschinensicherheit an. Der Kurs „Maschinenrichtlinie, CE Konformitätserklärungen und Haftungsfragen" behandelt die wichtigsten Fragen rund um die Sicherheit von Maschinen aus Sicht des Managements. Die Seminare finden in Bamberg oder auf Wunsch als Inhouse-Schulungen statt.

www.wieland-electric.com/de ■

Trends in Sachen Arbeitsschutz

Einmal im Jahr fasst die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) unter dem Titel „Arbeitswelt im Wandel" aktuelle Trends der Arbeitswelt zusammen. Mit vielen anschaulichen Grafiken informiert die kompakte Broschüre Praktiker des Arbeitsschutzes und die interessierte Öffentlichkeit gleichermaßen. Basierend auf dem Bericht „Sicherheit und Gesundheit bei der Arbeit 2016" (SuGA 2016) informiert die Broschüre über Zahlen, Daten und Fakten in Sachen Sicherheit und Gesundheit bei der Arbeit. Dabei bildet sie Themen wie Erwerbstätigkeit, Arbeitsbedingungen oder den demografischen Wandel einfach und verständlich ab. Daneben enthält „Arbeitswelt im Wandel 2018" aktuelle Zahlen zu Berufskrankheiten, Arbeitsbedingungen, Arbeitszeiten und Arbeitsunfähigkeit. Die Druckfassung gibt es gegen Versandkosten im Webshop der BAuA oder im PDF-Format unter

www.baua.de/publikationen ■

Kennzeichnung von Schutzkleidung

Die Ausrüstung muss auf die Gefahren des jeweiligen Arbeitsplatzes abgestimmt sein. Darauf wies Mewa anlässlich des 16. Welttages für Sicherheit und Gesundheit am Arbeitsplatz (28. April 2018) hin. Für die meisten Gefährdungen gibt es die entsprechende Schutzkleidung mit sichtbaren Zeichen zum Schutz der Gesundheit. Dieses Symbol ist Pflicht:

Jede Schutzkleidung auf dem europäischen Markt benötigt eine CE-Kennzeichnung. Mit dem CE-Kennzeichen erklärt der Hersteller, dass seine PSA den europäischen Gesetzen entspricht. Dieses Symbol befindet sich meist auf der Innenseite der Kleidung. Es gibt weitere Symbole für die häufigsten Schutzfunktionen: Schutzkleidung mit elektrostatischen Eigenschaften (EN 1149-5), gegen die thermischen Gefahren eines Lichtbogens (IEC 61482-2), bei Schweißarbeiten oder verwandten Verfahren (EN ISO 11611), gegen Hitze und Flammen (EN ISO 11612) und gegen flüssige Chemikalien (EN 13034, Typ 6).

www.mewa.de ■

Absicherung von Entry/Exit-Applikationen

Die Sicherheitslösung Safe-Portal-Solutions von Sick ist speziell auf die effiziente, flexible und normkonforme Absicherung von Materialübergabestationen zugeschnitten. Zwei vertikal ausgerichtete Sicherheits-Laserscanner mit intelligenter Überwachungsfallumschaltung sichern den Zugang ab. Objekte mit vordefinierten Konturen können sicher passieren. Dies ermöglicht einen flexiblen Produktionsprozess und optimiert die Produktivität. Safe-Portal-Solutions umfassen neben allen technischen Schutzeinrichtungen auch das zugehörige Engineering. Genau an dieser Stelle greift die Strategie von Sick, bei der Sicherheitstechnik konsequenter in „Lösungen" zu denken und die konkreten Herausforderungen einer ganzen Applikation zu betrachten. Auf diese Weise ist Sick nicht nur Produkt-, sondern Komplettanbieter für maßgeschneiderte „Sicherheitslösungen" – mit Sicherheitsdienstleistungen als integralem Bestandteil.

www.sick.com ■

Regionalforum auf der Arbeitsschutz Aktuell 2018

Digitale Technologien verändern die Arbeitswelt und damit auch die Anforderungen an einen effektiven Arbeits- und Gesundheitsschutz. Lang etablierte Methoden und Prozesse werden in kürzesten Zeiträumen modernisiert und revolutioniert. Entgrenzung von Arbeitszeit und Freizeit durch ständige Erreichbarkeit sowie Arbeitsverdichtung sind die Kehrseite von Flexibilität und Mobilität. Mit welchen Geschäftsmodellen und Lösungen meistern auch kleine und mittlere Unternehmen erfolgreich die Herausforderungen im Arbeits- und Gesundheitsschutz vor dem Hintergrund der Digitalisierung? Im Rahmen des Regionalforums, das vom 23.–25. Oktober als Teil der Arbeitsschutz Aktuell in Stuttgart stattfindet, erörtern Vertreter regionaler Unternehmen und Experten aus Wirtschaft und Forschung die wichtigen Fragen rund um einen zeitgemäßen Arbeits- und Gesundheitsschutz in der Arbeitswelt. Die Themen sind Arbeitsmedizin und Ergonomie, Betriebliches Gesundheitsmanagement (BGM) und Gefährdungsbeurteilung sowie Arbeit 4.0 und Digitalisierung.

www.Arbeitsschutz-Aktuell.de/Regionalforum ■

Asecos wird 25 Jahre

Als Experte für Gefahrstofflagerung hat asecos vor rund 25 Jahren als erstes Unternehmen weltweit Typ 90-Sicherheitsschränke entwickelt und 1994 im Markt eingeführt. Jetzt wurde mit einem großen Jubiläums-Gewinnspiel der Countdown zum Firmenjubiläum gestartet.

Bis März 2020 werden insgesamt 25 attraktive Preise verlost.

www.asecos.com ■

Sichere Signale, maximale Funktionalität

Digitale Signale unterschiedlichster Funktion über eine einzige Adresse mit dem Feldbus verbinden: Der FieldConnex Multi-Input Output (MIO) von Pepperl+Fuchs macht das jetzt möglich. Die kompakte Komponente bietet Eigensicherheit und steht für denkbar einfaches Handling. So ist höchste Flexibilität beim Anlagendesign sichergestellt. Über die FieldConnex MIO können binäre Signale mit vier unterschiedlichen Funktionen in die digitale Infrastruktur eingebunden werden. Sie erfasst z. B. bis zu zwölf diskrete Eingangssignale von NAMUR-Sensoren. Alternativ steuert sie bis zu vier Ventile inklusive Endlagenrückmeldung und Teilhubtest. Oder sie ermöglicht die Überlauf- und Leerstandüberwachung für Behälter und Rohrleitungen durch Vibrationsgrenzwertschalter. Erstmals ist die Komponente auch in der Lage, Signale von Impuls- und Frequenzgebern zu sammeln. Notwendig ist das u. a. bei der Stillstandsüberwachung von kritischen Motoren.

www.pepperl-fuchs.com ■

Bestseller-Katalog 2018

Aus einem Sortiment von über 10.000 Standard-Produkten die besten auszuwählen, ist nicht einfach. Die Erfahrungen der Anwender helfen hier weiter. Denios hat auf diesem Weg die Bestseller aus drei Einsatzbereichen praxisorientiert in einem Auszugskatalog zusammengestellt.

Gefahrstoffe regelkonform lagern

Auffangwannen aus Stahl, Edelstahl oder Polyethylen für verschiedenste Anwendungen bilden mit anderen Produkten das Kernsortiment der Denios-Gruppe. Auch die neuen Kleingebindewannen mit Leckage-Sensor gehören bereits jetzt zu den Best-Sellern. Aus dem umfangreichen Sortiment an Umwelt- und Sicherheitsschränken finden Kunden im Katalog schnell eine passende Lösung, um Gefahrstoffe direkt am Arbeitsplatz lagern zu können.

Handling und Transport

Ergonomie und Sicherheit sind die wichtigsten Merkmale von Produkten zur Handhabung von Gefahrstoffen. Die von Denios entwickelten Fasslifter und Fasskarren aus der Secu-Produktlinie fokussieren besonders auf diese Features. Der Transport und das Handling von Fässern gehen hiermit nicht nur leicht und mit minimalem Personaleinsatz von der Hand: Die Produkte garantieren zugleich maximale Sicherheit und sind je nach Typ auch in einer Version für den Ex-Bereich verfügbar. Auch das umfangreiche Falcon-Sortiment ist im Katalog zu finden: Annetz- und Sprühkannen, Tränk- und Tauchbehälter sowie die neuen Sicherheitskannen Lubriflex schützen Anwender beim Transport von Kleinmengen entzündlicher oder wassergefährdender Substanzen im Betrieb.

Sicherheits-Ausstattung für den Betrieb

Eine Vielzahl täglicher Handgriffe kann mit dem richtigen Produkt um ein Vielfaches sicherer für den Anwender gestaltet werden. Die persönliche Schutzausrüstung (PSA) wird direkt am Körper getragen, und hier kann bereits mit unscheinbaren Artikeln viel erreicht werden. Für effektiven Gehörschutz, Augen- oder Atemschutz genügt oftmals schon ein einzelnes Produkt.

www.denios.de ■

Latexhandschuhe nur ungepudert erlaubt

Die Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege (BGW) weist darauf hin, dass gepuderte Latexhandschuhe ein hohes Allergierisiko bergen. Sie dürfen deshalb nach den Technischen Regeln zum Arbeitsschutz in Deutschland nicht bei der Arbeit verwendet werden (TRGS 401). Die BGW hatte bei Betriebsbesuchen festgestellt, dass in tierärztlichen Praxen zum Teil noch gepuderte Latexhandschuhe im Einsatz sind. Die in Naturlatex enthaltenen Proteine können Allergien auslösen. Gepuderte Latexhandschuhe sind besonders gefährlich, da sich die Proteine am Puder anlagern. Beim An- und Ausziehen der Handschuhe werden die Allergieauslöser aufgewirbelt. So gelangen sie auch in die Umgebung und in die Atemwege. Eine Latexallergie kann je nach Situation zu verschiedenen und unterschiedlich intensiven allergischen Kontaktreaktionen führen.

www.bgw-online.de ■

Sensibilisieren und aufklären

Aus Anlass des „Welttages für Sicherheit und Gesundheit am Arbeitsplatz" halten asecos-Mitarbeiter – national sowie international – Experimental-Vorträge auf Messen und Events, aber auch Fachschulungen direkt in den Unternehmen, um auf die Gefahren durch Routine im Umgang mit gefährlichen Stoffen aufmerksam zu machen. Die Vorträge verdeutlichen das Gefahrenpotential und die möglichen Auswirkungen, die bereits bei Kleinmengen von Chemikalien immens sein können. Sowohl Neulinge als auch routinierte Profis werden praxisnah, aber im geschützten Rahmen mit den Risiken im Umgang mit Gefahrstoffen konfrontiert. Neben diesen Schulungen der asecos academy bietet das Unternehmen umfassendes Informationsmaterial in Form von Broschüren und Video-Clips.

www.asecos.com ■

Vollsichtbrille mit Anti-Fog-Beschichtung

Die 3M-Vollsichtbrille 2891 ist jetzt erstmals auch mit der Premium-3M-Scotchgard-Anti-Fog-Beschichtung erhältlich. Damit sorgt sie für Durchblick und sicheres Arbeiten unter den verschiedensten Arbeitsbedingungen. Dank der hochwertigen Beschichtung ist die Vollsichtbrille selbst für extreme Umgebungsbedingungen geeignet. Sie übertrifft die Anforderungen der EN166: K/N deutlich und gibt dem Träger höchste Sicherheit.

Die bekannten Vorteile der Vollsichtbrillen-Serie 2890 bleiben dabei unverändert bestehen: Das breite Kopfband mit verstellbarem Gelenk ermöglicht einen optimalen Sitz und eine leichte Anpassung. Optionale Belüftungsschlitze tragen zu einer besseren Luftzirkulation bei. Die 2890-Serie passt zudem hervorragend über Korrektionsbrillen und lässt sich sehr gut mit 3M-Halbmasken kombinieren.

www.3Marbeitsschutz.de ■

Gefahrstoffe am Arbeitsplatz

Rauch, Staub, Gase – längst nicht alle Gefahrstoffe tragen eine Kennzeichnung oder werden von den Beschäftigten als solche wahrgenommen. Dazu gehören z. B. so alltägliche Dinge wie Quarzstaub, Asbest in Baumaterialien, Holzstaub oder auch Wasser bei Feuchtarbeit. Ein Blick in die Statistik zeigt, dass gerade solche Stoffe die meisten Berufskrankheiten verursachen. Die Ausgabe 1/18 der amtlichen Mitteilungen der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) gibt einen Überblick über die Aktivitäten, Angebote und die aktuelle Forschungsarbeit zum Schutz der Beschäftigten vor Gefahrstoffen. .

www.baua.de/publikationen ■

Sicherheits-Laserscanner-Familie erweitert

Zwei neue netzwerkfähige Sicherheits-Laserscanner ergänzen den bereits erfolgreich am Markt eingesetzten microScan3 Core I/O von Sick. Die Varianten bieten die gleiche optische Leistungsfähigkeit und unterscheiden sich hinsichtlich Integrationsmöglichkeiten, Anschlusskonzept und Gerätegröße. Der microScan3 Core-EtherNet/IP ist laut Unternehmensangaben der erste Sicherheits-Laserscanner auf dem Markt mit CIP-Safety über EtherNet/IP und ist mit allen gängigen EtherNet/IP-CIP-Safety-Steuerungen kompatibel. Der microScan3 Core-Profinet ermöglicht durch das ProfiSafe-Protokoll eine sichere und zuverlässige Buskommunikation. Mithilfe der Profinet-IO-Busanbindung werden alle Signale von der übergeordneten Steuerung (FSPS) verarbeitet. Beide Netzwerkvarianten können mehrere Gefahrbereiche gleichzeitig absichern und bieten bis zu vier simultane Schutzfelder, wodurch die Aufgabe von mehreren konventionellen I/O-Scannern erfüllt werden kann.

www.sick.com ■

Vereinfachte applikationsspezifische Konfiguration

Pfannenberg hat die kompakten Rückkühlanlagen der CC-Serie weiterentwickelt und die CCE-Serie als Nachfolger auf den Markt gebracht. Der Spezialist für Produktionssicherheit bietet damit miteinander kombinierbare Vorkonfigurationen, abgestimmt auf verschiedene Anwendungsszenarien der Geräte. Dies vereinfacht die Auswahl für den Anwender und ermöglicht kurze Lieferzeiten. Die CCE-Rückkühlanlagen sind in sechs Leistungsklassen und zwei Baugrößen verfügbar und decken damit Leistungen von 1,1 bis 6,5 kW ab, sodass eine große Bandbreite an industriellen Anwendungen bedient wird. Eine noch einfachere Bedienung und Wartung standen bei der Weiterentwicklung im Vordergrund. Die vordefinierten Konfigurationspakete sollen vor allem die Verfügbarkeit verbessern und den weltweiten Service erleichtern.

www.pfannenberg.de ■

Leistungsstark unter allen Betriebsbedingungen

Datalogic, weltweit tätig im Bereich der automatischen Datenerfassung und Prozessautomatisierung, stellt mit dem DS5100 einen neuen flexiblen, leistungsstarken und kompakten Laserscanner vor. Die DS5100-Familie ist in mehreren Modellen erhältlich und bietet eine überlegene Leseleistung und integrierte industrielle Konnektivität in erstklassiger Industriequalität. Die wichtigsten und anspruchsvollsten Bedürfnisse aller Fertigungsbereiche wurden in einem einzigen Produkt vereint: eine kosteneffektive Lösung für alle Identifikationsanforderungen und viele Anwendungen, von der Automobilindustrie über die Lebensmittelindustrie bis hin zur Pharmaindustrie. Dank der Modelle mit Medium Range, Long Range, Schwingspiegel und für Tiefkühlanwendungen kann der Laserscanner DS5100 eine breite Palette von Anwendungen abdecken.

www.datalogic.com ■

Überspannungsschutz trotzt Wind und Wetter

DehnPatch CLE IP66 ist die neue Kompletteinheit aus Überspannungsschutz und Outdoor-Gehäuse. Mit Schutzart IP66, einer universellen Montagehalterung (horizontal/vertikal Mast, Wand) und der Übertragungsklasse E, ist der Überspannungsableiter DehnPatch ein optimales Schutzgerät für Ethernet-Anwendungen (auch PoE++) im Outdoor-Bereich. Gerade Systeme wie Überwachungskameras, WLAN-Access Points oder Punkt zu Punkt-Kommunikationsverbindungen (Wireless-Ethernet-Bridge) sind häufig an exponierten Stellen verbaut. Der notwendige Überspannungsschutz muss dann gegen witterungsbedingte Einflüsse geschützt werden. Das kostete Zeit, brauchte ein zusätzliches wetterfestes Gehäuse und weiteres Montagematerial und machte dazu die Wartung oft sehr aufwendig. DehnPatch CLE IP66 besteht aus einem mit Nickel beschichteten Alu-Druckguss Gehäuse, besitzt Deckelschrauben, die gegen Herausfallen gesichert sind, eine innenliegende Deckeldichtung und ist somit ein sehr funktionales Gehäuse in IP 66-Ausführung. Damit ist das Anbringen des Schutzgerätes im Außenbereich und auch in großen Höhen problemlos möglich.

www.dehn.de ■

Schutz für sensible Technik

Fachleute von Dehn informierten auf der Light+Building über Produkte, Schutzlösungen und Seminare sowie über die Prüfdienstleistungen des modernen DAkkS-akkreditierten Test- und Prüfzentrums. Der Support unterstützte direkt auf der Messe beim Umgang mit Normen und bei der Findung passender Schutzlösungen. Durch das Überspannungsschutz-Set für Wohngebäude oder Geräte mit neuer ACI-Technologie macht Dehn Anwendungen sicher, leicht und komfortabel. Die Technologie bietet Dimensionierungssicherheit und spart zudem Platz, Zeit und Kosten. Die Auswahl der passenden Ableitervorsicherung oder des notwendigen Leiterquerschnittes sind durch diese Technologie bereits technisch gelöst und eine Ableitervorsicherung nicht mehr notwendig. Der Blitzplaner – das Original- und Standardwerk in Sachen Blitz- und Überspannungsschutz erscheint in seiner 4. Auflage und bietet kompakte Hilfestellung für Planer und Ausführende. Neu sind Schutzgeräte wie DehnPatch Outdoor oder DehnGate FF5 TV.

www.dehn.de ■

Funktionale Handwerkskleidung für Frauen

Tischlerinnen, Installateurinnen, Elektrikerinnen – die Handwerkskammern registrieren einen deutlichen Zuwachs an weiblichen Arbeitskräften in den Handwerksberufen, die bislang eine Männerdomäne waren. Da sie die gleichen Arbeiten ausüben wie ihre männlichen Kollegen, brauchen Frauen im Handwerk eine Berufskleidung mit den gleichen Funktionen. Doch damit die Kleidung auch richtig sitzt, sind andere Schnitte gefragt – abgestimmt auf die weibliche Anatomie. Der Anbieter für Mietkleidung Mewa reagiert auf diesen Bedarf. Der Textildienstleister hat seine Kollektion Mewa Dynamic um Bundjacken und Bundhosen für Frauen erweitert. Weitere Artikel sind in Planung.

Das Outfit zeichnet sich durch eine besonders große Bewegungsfreiheit aus, verfügt über viele funktionale Details, zahlreiche Taschen und Stauraum für Kleinteile. Optisch erinnert das Design an Outdoor-Kleidung. „Wir haben eine erfolgreiche Kollektion erweitert, denn so kann ein Betrieb nun alle Mitarbeiterinnen und Mitarbeiter im gleichen Look ausstatten und der einheitliche Firmenauftritt bleibt gewahrt", sagt Silvia Mertens, Leitung Produktmanagement. Die Kleidung für Damen bietet Mewa im Full-Service an: Bringen, holen, waschen, instand halten der Kleidung gehören dazu.

www.mewa.de ■

MASCHINEN- UND ANLAGENSICHERHEIT

Cobots Claus, Clara & Co: kollaborative Robotik mit Sick Safety

Flexibilität, Kollaboration und Sicherheit der Mitarbeiter – schlanke MRK-Lösung bei Continental

Continental gehört zu den weltweit führenden Automobilzulieferern. Die zunehmende Modell- und Variantenvielfalt an Fahrzeugmodellen und Derivaten bei kürzeren Produktlebenszyklen in der Automobilindustrie erhöht auch die Dynamik bei den Zulieferern. In starr verkettete Fertigungslinien wirken sich Veränderungen und Störungen an einzelnen Stationen auf die Ausbringung der gesamten Linie gravierend aus. Je größer die Störungen ausfallen, desto schwieriger wird eine Kompensation.

Im Werk Babenhausen gehen rund um die Uhr alle 15 Sekunden High-Tech-Komponenten für Auto-Cockpits vom Band. Da ist wenig Luft nach oben, um Stillstandszeiten aufzuholen. Deshalb ersetzt Continental derzeit starre Prüf- und Bestückungslinien durch flexible redundante kollaborative Prüflinien: Die Cobots Claus und Clara bestücken die Prüfautomaten, und zwar dort, wo sie benötigt werden. Beschäftigte gehen ihnen, wenn nötig, sozusagen zur Hand. Für die Sicherheit im kollaborativen Miteinander sorgt eine Safety-Lösung von Sick bestehend aus Sicherheits-Laserscannern S300, Sicherheitsschaltern TR4 und Software-programmierbaren Sicherheitssteuerungen Flexi Soft.

In der komplett neu aufgebauten Prüflinie gibt es drei Prüfstände, die mit Robotern (Cobots) bestückt werden. Der Cobot nimmt sich ein Teil von einem Band, legt das in den Prüfautomaten ein, nimmt sich das geprüfte Gerät wieder mit und legt das auf ein nächstes Band auf.

Die Continental Automotive GmbH lässt die Cobots in ihrer Ausbildungsabteilung zusammenbauen

Sicherheit macht Mensch-Roboter-Kollaboration effizient

„Claus (Clever automatisiertes universelles Roboter-System) und Clara (Clever automatisierte Roboter Applikation) sind halbmobile Leichtbauroboter, die stationär arbeiten, aber mobil einsetzbar sind", beschreibt Heiko Liebisch, Industrial Engineering, Robotics, Continental Automotive GmbH, die Cobots und ihre Vorteile. „Mit diesem Konzept ist es möglich, den Roboter auszuheben und für eine andere Schicht an einen anderen Platz zu fahren. Somit hat man die Möglichkeit, an zwei Anlagen mit denselben Robotern zu arbeiten. In der Frühschicht an der einen und in der Spät- oder Nachtschicht an der anderen Anlage."

Mittels mechanischer Indexierung kann der Cobot jederzeit wieder optimal zum Prüfplatz positioniert werden, hier verifiziert ein Transponder-Sicherheitsschalter TR4 Direct Unique-Code Sensor, den TR4 Direct Unique-Code-Betätiger an Claus oder Clara

„Alles, was zum Thema Sicherheit in dem ganzen System steckt, wird über die Softwareprogrammierbare Sicherheitssteuerung Flexi Soft gesteuert. D.h., die Flexi Soft schaut nach, ob der codierte Sicherheitsschalter da ist. Wenn nicht, dann passiert gar nichts. Dann löst sie eine Fehlermeldung aus. Wenn der Schalter verifiziert wird, laden die Sicherheits-Laserscanner (S300 Advanced) die Feldsätze, die passend zu dem Arbeitsplatz hinterlegt sind und geben dem Cobot überhaupt erstmal die Freigabe, sein Programm zu laden und starten zu können", beschreibt Heiko Liebisch die Initialisierung. „Wir haben die Möglichkeit mehrere codierte Schalter vorne dran zu schrauben. So können wir den Cobot für mehrere Arbeitsplätze einrichten."

Die neue Linie bietet die Möglichkeit, ausgeschleuste Prüfteile wieder als Rückläufer in die laufende Anlage zu bringen. Hierfür geht ein Bediener im laufenden Betrieb zur Prüfanlage bzw. zum Cobot, legt das Prüfteil irgendwohin, wo gerade Platz ist, läuft wieder raus und der Cobot weiß selbstständig, da liegt was, das muss ich noch prüfen und macht ganz normal weiter.

Die Sicherheits-Laserscanner, die diagonal angebracht für die Rundum-Überwachung sorgen, zeigen frontseitig per Leuchtmelder in Ampelfarben die Schutzfeldzonen bzw. deren Verletzung an. Damit Bediener dies quasi bereits im Augenwinkel wahrnehmen können, leuchtet der ganze Korpus unter dem Cobotarm entsprechend der Signalampel-Automatik. Im kollaborativen Modus läuft Claus gelb an und reduziert die Geschwindigkeit. Im roten Modus bleibt er komplett stehen. Verlässt der Bediener das rote Schutzfeld, läuft das System und somit Claus automatisch wieder an. Der Bediener muss nicht quittieren.

Am Anfang steht immer die Risikobeurteilung – auch bei Cobots

Auch wenn Claus und Clara sich relativ langsam bewegen, generell kann ein Roboterarm einem Bediener lebensbedrohlich nah kommen. „Man muss immer das Gesamtkonzept beurteilen; deswegen haben wir die Greifer, die wir vorne einsetzen, lasergesintert – ohne spitze Kanten, alles verrundet."

Keine Mensch-Roboter-Kollaboration gleicht der anderen – daher ist eine individuelle Risikobeurteilung der MRK-Applikation selbst dann erforderlich, wenn der eingesetzte Roboter speziell für die Interaktion mit dem Menschen entwickelt wurde – ein solcher Cobot also schon von der grundsätzlichen Auslegung her eine Vielzahl von Merkmalen einer inhärent sicheren Konstruktion aufweist.

Bitte umblättern ▶

Alles, was zum Thema Sicherheit in dem System steckt, wird über die Software-programmierbare Sicherheitssteuerung Flexi Soft gesteuert

Gleichzeitig muss auch der Kollaborationsraum grundlegende Anforderungen erfüllen, z. B. hinsichtlich von Mindestabständen zu angrenzenden begehbaren Bereichen mit Quetsch- oder Einklemmgefahren. Normative Grundlage für die funktionale Sicherheit von MRK-Anwendungen sind zum einen generelle Normen wie die IEC 61508, die IEC 62061 und die ISO 13849-1/-2. Darüber hinaus sind die ISO 10218-1/-2 zur Sicherheit von Industrierobotern und speziell die ISO TS 15066 über Roboter für den Kollaborationsbetrieb zu berücksichtigen.

Das Team um Heiko Liebisch hat sich bzgl. der Auslegung, Richtlinien, gesetzlichen Vorgaben und Normen für Kollaborative Robotik von Sick beraten und schulen lassen. „Wir sind ganz glücklich mit dem System, wie es draußen läuft", kommentiert Heiko Liebisch das Ergebnis. „In der Praxis zeigen sich hier und da noch Optimierungsmöglichkeiten, die wir mit Sick als Partner für die Gesamtlösung weiter entwickeln werden."

Funktionale Sicherheit bei der Mensch-Roboter-Kollaboration (MRK)

Hoher Automatisierungsgrad versus flexible Fertigungsabläufe: Wenn Mensch und Maschine jetzt noch enger und dennoch sicher zusammenarbeiten, ist die funktionale Sicherheit in modernen Fertigungssystemen ein Schritt auf dem Weg zu mehr Flexibilität. Hierzu sind nicht nur ein umfassendes Verständnis der Roboteranwendungen, sondern auch Fachwissen bei der Risikobewertung und das entsprechende Portfolio an Sicherheitslösungen notwendig.

Bei bestimmten Anwendungen müssen der Mensch und der bewegte Roboter eng miteinander interagieren. In diesen sogenannten kollaborativen Szenarien stellen Kraft, Geschwindigkeit, Bewegungsbahnen des Roboters und das Werkstück inklusive Werkstückträger Gefahren für den Werker dar. Diese Gefahren müssen entweder durch die Nutzung inhärenter Schutzmaßnahmen oder/und durch die Anwendung zusätzlicher Maßnahmen zur Risikominderung beschränkt werden. Die Auswahl und die Auslegung der technischen Schutzeinrichtungen können sich sehr komplex gestalten.

Ein Beispiel für eine Anwendung, wie die Vernetzbarkeit mehrerer Sicherheits-Laserscanner die Lösung der Applikation erleichtert, ist die lückenlose 360°-Rundum-Absicherung von Robotern oder AGVs und AGCs mit S300 Mini, S300, S3000 oder dem neuen microScan3 Core im Verbund mit der Sicherheitssteuerung Flexi Soft von Sick. Durch diese Lösung ist die Sicherheit in alle Bewegungsrichtungen gewährleistet. Es handelt sich hierbei um eine integrationsfreundliche, hoch verfügbare und wirtschaftliche Komplettlösung aus einer Hand, d. h. ohne applikationstechnische Schnittstellenrisiken. Die Sick-spezifische EFI-Schnittstelle (Enhanced Function Interface) erlaubt eine direkte sicherheitsgerichtete Kommunikation der Geräte untereinander. Die Nutzung dieser Schnittstelle minimiert den sonst erforderlichen, hohen Verkabelungsaufwand für den Anwender – und damit gleichzeitig auch das Risiko von Verdrahtungsfehlern insbesondere in der Inbetriebnahmephase. Durch die zentrale Integration der Flexi Soft im Fahrzeug oder Roboterkorpus ist neben der einfachen Konfiguration auch eine verbesserte Diagnose des Laserscanner-Gesamtsystems von einer Stelle aus möglich. Dies spart nicht nur Zeit während der Inbetriebnahme, sondern optimiert die Wartung und Instandhaltung.

> „In diesen sogenannten kollaborativen Szenarien stellen Kraft, Geschwindigkeit, Bewegungsbahnen des Roboters und das Werkstück inklusive Werkstückträger Gefahren für den Werker dar."

Erfolgreiche Pilotlinie seit Anfang 2017

Heiko Liebisch und sein Kollege Dejan Pfaff haben die neue 4.0-Prüflinie der Continental Automotive GmbH in Babenhausen geplant und die Cobots konstruiert. Sie sind sozusagen die Väter von Claus und Clara, die bald Geschwister in Gestalt von Cora und Kurt bekommen werden. Die erfolgreiche Umstellung macht nämlich Schule bei Continental. Der Einsatz weiterer Cobots ist geplant. Apropos „Schule", gebaut werden die Cläuse und Claras von Auszubildenden der Continental Automotive GmbH. Mechaniker bauen das Grundgestell, Mechatroniker den Rest. Eine tolle Sache für die Auszubildenden. Wenn sie später mal in einer solchen Linie arbeiten, können sie mit Stolz sagen, das habe ich gebaut. ■

Autoren
Achim Sorg
Key Account Manager
Automotive Industry – Parts Supplier,
Sick Vertriebs-GmbH

Simon Ruenzi
Strategic Industry Manager
Sick AG

Niclas Steidl
Vertriebsaußendienst Sick
Vertriebs-GmbH

Kontakt

Sick AG
Waldkirch
Tel.: +49 7681 202 41 83
info@sick.de
www.sick.de

VERNETZTE SICHERHEIT

PSA intelligent

Sicherheit 4.0: Auch Persönliche Schutzausrüstung wird intelligenter und stärker vernetzt

Vielleicht ist Sicherheit nicht gerade der erste Anwendungsbereich, der einem in den Sinn kommt, wenn die Konzepte Industrie 4.0 und Smart Factory erwähnt werden. Dennoch wird selbst persönliche Schutzausrüstung (PSA) vom Typ „Low-Tech" immer intelligenter und stärker vernetzt. Im Folgenden erklärt Thomas Negre, Global Director für den Bereich Gasdetektion und vernetzte Mitarbeiter bei Honeywell Industrial Safety, warum vernetzte Sicherheit in den Smart Factories von heute eine zentrale Rolle spielt und den Schutz der Mitarbeiter sowie die Produktivität verbessert.

Industrie 4.0 verwandelt die verarbeitende Industrie. Die sogenannte vierte industrielle Revolution wird von einem beispiellosen Anstieg der Datenverfügbarkeit, Rechenleistung und Konnektivität sowie von neuen Formen von Mensch-Maschine-Interaktionen getragen, der den Verantwortlichen der Industriekonzernen helfen soll, bessere Entscheidungen schneller zu treffen, Betriebskosten zu sparen und die Effizienz und Produktivität zu steigern. Mit anderen Worten: Es geht darum, Fabriken intelligenter zu machen. Aber Industrie 4.0 setzt sich dank der neuesten Fortschritte in der vernetzten Sicherheitstechnik auch im Bereich der industriellen Sicherheit durch. Wenn die Unternehmen ihre Mitarbeiter wirksamer schützen können, verhilft ihnen dies zu einem Wettbewerbsvorteil, da viele Kosten im Zusammenhang mit dem Sicherheitsmanagement reduziert werden.

Traditionell papierbasiert

Die Europäische Rahmenrichtlinie über Sicherheit und Gesundheitsschutz bei der Arbeit (Richtlinie 89/391 EWG) verpflichtet Arbeitgeber, geeignete Präventivmaßnahmen zu ergreifen, um die Arbeit sicherer und gesünder zu gestalten, wobei die Bedeutung neuer Formen des Sicherheits- und Gesundheitsmanagements im Rahmen der allgemeinen Managementprozesse betont wird.[1] Vor diesem Hintergrund – und angesichts des wachsenden Bewusstseins für die hohen Geldbußen und Reputationsschäden, die sich aus Verstößen gegen die Sicherheitsvorschriften oder einfach aus der Nichtbeachtung der aufsichtsrechtlichen Bestimmungen ergeben können – haben viele Unternehmen im Laufe der Jahre Datenbanken angelegt, über welche die Expositionswerte ihrer Mitarbeiter erfasst werden und die zur besseren Verwaltung und Wartung der von ihnen verwendeten Sicherheitsausrüstung beitragen. Dennoch war und ist dies traditionell ein papierbasierter Prozess, der die manuelle Eingabe von Daten zu Arbeitsschutz und zur Gesundheit erfordert – trotz der Verfügbarkeit von Softwareanwendungen zur Vereinfachung der Aufgabe.

Dieser unsystematische Ansatz kann die Mitarbeiter letztendlich in Gefahr bringen, insbesondere in großen Fabriken, in denen die manuelle Eingabe von Daten äußerst schwierig zu bewältigen ist. Die Sicherstellung, ob PSA und andere Schutzvorrichtung ordnungsgemäß gewartet werden, ist dadurch erschwert. Auch lässt sich schwer feststellen, ob die Schutzausrichtung für den vorgesehen Zweck geeignet und auf dem neusten Stand ist sowie den Vorschriften entspricht. Darüber hinaus muss sichergestellt werden, dass die Mitarbeiter sie korrekt verwenden. Angesichts dessen, dass häufig mit weniger Mitteln mehr getan werden muss und dass die Sicherheitsfachkräfte heute für immer

Bitte umblättern ▶

> Der Arbeitsschutz entfernt sich eindeutig immer weiter von seiner „analogen“ Vergangenheit und passt sich dem digitalen Zeitalter an. Er spielt eine bedeutende Rolle beim Wandel in den Fabriken zu Zeiten von Industrie 4.0.“

größere Aufgabenbereiche zuständig sind, kann es sein, dass sich PSA-Inspektionen auf regelmäßige Werksprüfungen oder Stichprobenkontrollen beschränken. Außerdem sind sie zeitaufwendig und kostspielig und können die Produktivität beeinträchtigen. Zudem können sie Unternehmen potenziell in die Lage bringen, Bußgelder zahlen zu müssen. Zum Beispiel können kleine und mittlere Unternehmen (KMU) damit rechnen, bis zu 45.000 EUR pro Jahr für die Einhaltung der Gesundheits- und Sicherheitsvorschriften auszugeben, am Ende aber eine Geldstrafe von durchschnittlich rund 130.000 EUR zahlen zu müssen, wenn sie eines Verstoßes für schuldig befunden werden.[2]

Sicherheitsausrüstung intelligenter machen

Hier bietet sich die Gelegenheit, die Einhaltung der Vorschriften mit einer verstärkten Automatisierung zu verbinden. Der Schlüssel liegt darin, die Sicherheitsausrüstung intelligenter zu machen. Werden in die persönliche Schutzausrüstung Sensoren oder RFID-Technologie (RFID: Radiofrequenz-Identifizierung) integriert, werden sie zu Spitzengeräten im Internet der Dinge, die Daten sammeln und übertragen können – was die Datenerfassung beschleunigt und die Genauigkeit sowie die Effizienz steigert. In diesem Datensammlungssystem dient der mobile, vernetzte Mitarbeiter als der Mittelpunkt des Konzepts.

Mit Hilfe einer Bluetooth-Verbindung können Mitarbeiter nun zum Beispiel automatisch einen tragbaren Gasdetektor oder ein anderes Gerät mit ihrem Smartphone verbinden. Dank der Kombination aus drahtloser Konnektivität, der neuesten Software und Cloud-Technologie können Sicherheitsfachkräfte mittels Laptop oder Smartphone sofort sehen, welcher Mitarbeiter das Gerät benutzt und ob dieses alle wichtigen Eigenschaften erfüllt: ob das Gerät in Bezug auf die Einhaltung der Vorschriften auf dem neuesten Stand ist und wann es zuletzt gewartet wurde und auch ob der Mitarbeiter für den Umgang mit seiner Sicherheitsausrüstung angemessen geschult wurde. Sicherheitsfachkräfte können innerhalb von Sekunden auf diese Informationen zugreifen und erhalten darüber hinaus eine Fülle anderer Daten, wie z. B. Gaskonzentrationswerte, die Anzahl der Sicherheitsvorfälle in einem bestimmten Zeitraum und aktuelle Daten zu Zustand und Funktionsfähigkeit von Gerätesensoren.

Vernetzt und datengestützt

Die Automatisierung von Abläufen zur Einhaltung der Sicherheitsvorschriften ist nicht die einzige Möglichkeit, Techniken der vernetzten Sicherheit einzusetzen, um die Herausforderungen in den Smart Factories zu bewältigen. Von der Automobilindustrie bis hin zur Luft- und Raumfahrtindustrie ist die Umstellung auf vernetzte Sicherheit in vielen Umgebungen mit hohem Risikopotential bereits Realität, wie etwa in zugangsbeschränkten Bereichen. Dies hat gezeigt, wie ein datengestützter Ansatz Leben retten kann.

Von Gasflaschenschränken in Halbleiterwerken bis zu den Flügeln einer Boeing 747 sind zugangsbeschränkte Bereiche in der Fertigung weit verbreitet und gehören zu den gefährlichsten Umgebungen für die Mitarbeiter. Diejenigen, die sich in solchen Bereichen aufhalten, können Risiken wie

Sauerstoffmangel (oder manchmal auch Sauerstoffanreicherung), Exposition gegenüber toxischen oder entflammbaren Gasen, hohen Lärmpegeln und Stürzen ausgesetzt sein. Die Einsicht in die biomedizinischen Werte dieser Mitarbeiter (Herzfrequenz, Körpertemperatur, Atemfrequenz) sowie ihrer Expositionswerte in Echtzeit ist von größter Bedeutung, um die Mitarbeiter in einer potenziell gefährlichen Situation warnen und, wenn nötig, Notfallrettungseinsätze leiten zu können. Es ist entscheidend, die Gaskonzentration und die Position eines Mitarbeiters zu kennen, der das Bewusstsein verloren hat, bevor die Retter in Aktion treten. Nur so können sie mit der richtigen Ausrüstung zum Schutz gegen die Gefahren ausgestattet werden, mit denen sie es zu tun haben.

Vernetzung wird Teil des Smart Factory-Ökosystems

Da die Konnektivität nun zugänglicher und erschwinglicher wird, weitet sich die vernetzte Sicherheitsinfrastruktur auf Bereiche außerhalb der Umgebungen mit hohem Risikopotential aus und wird nach und nach Teil des Smart Factory-Ökosystems. Insbesondere das Smartphone hat sich zu einem vielseitigen Knotenpunkt für die Datenerfassung und -übertragung entwickelt. Dadurch erschließen sich ganz neue Möglichkeiten in Bezug auf die Sicherheit sowohl in Umgebungen mit hohem als auch in solchen mit geringem Risikopotential.

Es gibt mittlerweile mehrere Anbieter von Industrie-Smartphones, die ebenso benutzerfreundlich sind wie ihre Pendants für den privaten Gebrauch und gleichzeitig die robusten Anforderungen für industrielle Umgebungen erfüllen. Beispielsweise können Personen, die in explosionsgefährdeten Bereichen arbeiten, über ein mobiles Netzwerk für Gefahrenbereiche zertifizierte oder eigensichere Smartphones verwenden.

Wie bereits erwähnt, können Smartphones nun Verbindungen zu anderen Geräten wie etwa Gasdetektoren herstellen. Dadurch können auch Mitarbeiter, die keinen tragbaren Gasdetektor tragen, gewarnt werden, wenn durch ein stationäres Gaswarngerät in einem anderen Teil des Werks ein Gasleck erkannt wird. Sicherheitsfachkräfte können von jedem beliebigen Ort aus über ein Smartphone die Arbeitsschutz- und Gesundheitsdaten eines bestimmten Mitarbeiters einsehen und wenn nötig eingreifen. Dies kann z. B. dann der Fall sein, wenn der Mitarbeiter keinen Gehörschutz trägt, wo dieser erforderlich ist, oder wenn er diesen nicht richtig trägt. Die neuesten industriellen Smartphone-Apps bieten außerdem Funktionen wie On-Demand-Schulungen mit klaren visuellen Anweisungen und informieren sowohl den Mitarbeiter als auch die Sicherheitsfachkräfte darüber, welche Gasdetektoren und welche persönliche Schutzausrüstung (PSA) für die konkrete Aufgabe benötigt werden.

Die Daten werden außerdem gespeichert, so dass Sicherheitsfachkräfte Berichte über Mitarbeiter ausführen und ihre Exposition gegenüber gefährlichen Stoffen über einen längeren Zeitraum einsehen können. Dies ist entscheidend, um gegen gesundheitliche Probleme vorgehen zu können, bevor es zu spät ist. Diese Daten können dann auch als Grundlage für Entscheidungen zur Arbeitseinteilung herangezogen werden, so dass zum Beispiel die Exposition eines Mitarbeiters für den Verlauf einer bestimmten Schicht reduziert wird.

Produktivität steigern, Kosten senken

Diese Möglichkeiten der vernetzten Arbeitssicherheit, wie die Übermittlung der Daten eines Gasdetektors direkt an den Kontrollraum, können die Einhaltung der Sicherheitsvorschriften und das Monitoring der Arbeitssicherheit automatisieren und zudem die Produktivität steigern. Dies liegt vor allem daran, dass Mitarbeiter ihre Arbeit nicht alle paar Minuten unterbrechen müssen, um Informationen wie z. B. Gasmesswerte manuell zurückzusenden. Zudem können sich Mitarbeiter darauf verlassen, dass die von ihnen verwendete Ausrüstung für den jeweiligen Zweck geeignet ist und dass ihre Expositionswerte genau eingesehen werden können. So ist eine bessere Konzentration auf die Arbeit möglich, was die Gesamtproduktivität und -effizienz verbessert. Entsprechende Untersuchungen der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) haben ergeben, dass die Sicherheit des Arbeitsplatzes, neben einem festen Einkommen, zu den wichtigsten Aspekten „guter Arbeit" gehört. [3]

Wichtiger noch: Da die Techniken der vernetzten Sicherheit ein sofortiges Eingreifen und die Vermeidung gefährlicher Situationen sowie dauerhafter Erkrankungen ermöglicht, kann sie dabei helfen, die enormen Kosten möglicher Produktionsausfälle zu senken. Im vergangenen Jahr kam es in Deutschland zu 877.071 arbeitsbedingten Verletzungen, die für mehr als drei Fehltage sorgten.[4] Pro Jahr kann dies zu einem Produktionsverlust von bis zu 46 Mrd EUR führen.[5] Der vernetzte Mitarbeiter ist ein gesünderer, besser geschützter und produktiverer Mitarbeiter.

Anpassung an das digitale Zeitalter

Mit Blick auf die Zukunft ist zu sagen, dass die Vorteile der Automatisierung von Sicherheitsmanagementprozessen offensichtlich sind, aber eine Herausforderung für die Sicherheitsexperten für Smart Factories darin besteht, festzustellen, wie sich das wachsende Datenvolumen effektiv verwalten lässt. Früher waren die Sicherheitsfachkräfte für den gesamten Verwaltungsprozess im Zusammenhang mit der Sicherheitsausrüstung verantwortlich – von der Beschaffung bis zur Schulung und Inspektion. Ganz allgemein wird die Zusammenarbeit zwischen den verschiedenen Beteiligten – von PSA-Herstellern bis hin zu Software- und Telekommunikationsanbietern – für die Entwicklung einer vollständig vernetzten Lösung entscheidend sein, mit der die Smart Factories der Zukunft sicherer gestaltet werden können.

Der Arbeitsschutz entfernt sich eindeutig immer weiter von seiner „analogen" Vergangenheit und passt sich dem digitalen Zeitalter an. Er spielt eine bedeutende Rolle beim Wandel in den Fabriken zu Zeiten von Industrie 4.0. Die Möglichkeit, Daten zu Arbeitsschutz und -gesundheit effizienter zu sammeln und zu analysieren, wird nicht nur dafür sorgen, dass die Mitarbeiter in Smart Factories besser geschützt sind, sondern erhöht auch die Effizienz und die Produktivität. Letztlich erwarten die Mitarbeiter ihrerseits, dass die Technik, die ihnen bei der Arbeit an die Hand gegeben wird, ebenso benutzerfreundlich ist wie jene, die sie zu Hause verwenden. Die vernetzte Sicherheit kann ihnen dabei helfen, genau das zu erreichen.

Referenzmaterial

[1] https://osha.europa.eu/en/legislation/directives/the-osh-framework-directive/the-osh-framework-directive-introduction
[2] http://www.arinite.co.uk/the-cost-of-health-and-safety-compliance-vs-a-prosecution-fine/
[3] https://www.baua.de/DE/Angebote/Publikationen/Praxis/A81.pdf?__blob=publicationFile
[4] http://www.dguv.de/de/zahlen-fakten/au-wu-geschehen/index.jsp
[5] https://www.baua.de/DE/Themen/Arbeitswelt-und-Arbeitsschutz-im-Wandel/Arbeitsweltberichterstattung/Kosten-der-AU/Kosten-der-Arbeitsunfaehigkeit_node.html

Autor
Thomas Negre,
Global Director für den Bereich Gasdetektion und vernetzte Mitarbeiter bei Honeywell Industrial Safety

Kontakt

Honeywell Industrial Safety
gasdetection@honeywell.com
http://www.honeywellanalytics.com/de-de

In jeder Ausgabe erklären Sicherheitsexperten Begriffe aus der Maschinen- und Anlagensicherheit.

WAS IST EIGENTLICH...

... DNV-GL?

CARSTEN HIPPLER VON PFANNENBERG

IN DIESER AUSGABE

UNTERSTÜTZT VON PFANNENBERG

Carsten Hippler, Sales Product Manager Signaling von Pfannenberg erklärt, was die DNV-GL-Zertifizierung von Signalgebern bedeutet.

Signalgeräte mit DNV-GL-Zertifizierung eignen sich besonders für raue Industrieanwendungen, bei denen sie starken Erschütterungen, andauernden Vibrationen oder harten Stößen ausgesetzt werden. Zu den Anwendungsbereichen zählen die Schwer- und Automobil-Industrie, Hafenanlagen und Werften, die Lager- und Transportbereiche der Logistik bis hin zur prozesstechnischen Anlagen der Baustoff-, Holz-, Glas- und Pharmaindustrie. Eine hohe Schlagfestigkeit des Gehäuses ist auch dann wichtig, wenn Signalgeber unbeaufsichtigt im Freien eingesetzt werden, da diese dort gegen Hagelschlag und Vandalismus geschützt sein müssen.

Qualitätssiegel aus der maritimen Industrie

Die Zertifizierung durch die Det Norske Veritas (DNV) und den Germanischen Lloyd (GL) ist vor allem aus dem maritimen Bereich bekannt, wo die zusammengeschlossene Klassifikationsgesellschaft DNV-GL weltweit führend ist. Gegründet im Jahr 1864 in Norwegen sollte die DNV zu einer zuverlässigen und einheitlichen Klassifikation und Besteuerung norwegischer Schiffe beitragen. Ähnlich steht es um die gemeinnützige Organisation GL, die als unabhängige Klassifizierungsgesellschaft seit der Gründung 1867 in Hamburg die Qualität eines Schiffes bewertet. Seit Beginn des Bestehens kooperieren DNV und GL, in 2013 kam es dann zum Zusammenschluss beider Unternehmen.

In der maritimen Industrie sind die Zertifikate der DNV-GL nicht nur die Grundvoraussetzung dafür, dass elektrotechnische Komponenten wie Signalgeräte auf Schiffen eingesetzt werden dürfen, sondern gelten auch als Qualitätssiegel für Robustheit und Zuverlässigkeit. Zurückzuführen ist dies vor allem auf die strengen Bewertungskriterien und anspruchsvollen Testverfahren. So werden Signalgeber bei den Vibrationstests je nach Testverfahren einer Belastung von bis zu 2,4 g ausgesetzt.

Was in schwerer See besteht, erfüllt auch die Anforderungen der Schwerindustrie

Gemäß DNV-GL zertifizierte Signalgeräte erfüllen höchste Qualitätsstandards und zeigen sich besonders unempfindlich gegenüber mechanischen Belastungen. Um vibrationsbedingte Schäden zu verhindern, verfügen entsprechend zertifizierte Signalgeräte beispielsweise über besonders gesicherte Bauteile auf der Leiterplatte. Befestigungswinkel aus Metall absorbieren bzw. dämpfen die Schwingungen und Vibrationen zuverlässig. Auch ohne Einsatz eines Schutzkorbes widerstehen sie hohen mechanischen Beanspruchungen und gewährleisten jederzeit eine zuverlässige Funktion.

Verwindungssteife Kunststoffgehäuse mit Schlagfestigkeit IK08 und hohe Schutzarten wie IP66 oder IP67 gewährleisten zudem nicht nur höchste Robustheit, Schlag- und Stoßfestigkeit, sie besitzen auch eine sehr hohe Staubdichtigkeit, und sie widerstehen starkem Strahlwasser und zeitweiser Überflutung. Entsprechende Geräte eignen sich somit auch für Anwendungen, bei denen Rohstoffe zerkleinert werden, in der Verarbeitung Staub, Dunst und Dämpfe entstehen sowie für Arbeits- und Produktionsbereiche, die regelmäßig mit hohem Wasserdruck gereinigt werden.

Zuverlässigkeit im Industrieeinsatz

Die DNV-GL-Zertifizierung bestätigt die Unempfindlichkeit der Signalgeräte gegenüber Vibrationen, Erschütterungen und Stößen. Damit kann sie über den maritimen Bereich hinaus als Gütesiegel für Produkte im industriellen Einsatz angesehen werden. Entsprechend geprüfte und zertifizierte Signalgeräte sichern dem Maschinen- oder Anlagen-Betreiber höchste Zuverlässigkeit und Qualität auch unter starker Beanspruchung zu. Damit eignen sie sich für anspruchsvolle Anwendungen wie Abfüll- und Sortieranlagen, Kräne, Gießereien, Walzwerke, Kraftwerke, Transport- und Produktionsbänder, Siloanlagen, Pipelines, Tore, Schienenverkehr oder fahrbare Schwerlastverschieberegale.

Kontakt

Pfannenberg Europe GmbH, Hamburg
Tel.: +49 40 734 12 0
info@pfannenberg.com
www.pfannenberg.de

Jüngere Beschäftigte haben hohes Unfallrisiko

Von den durchschnittlich rund 915.000 Arbeitsunfällen pro Jahr (Zahlen der DGUV von 2005 bis 2015) entfielen 170.000 – und damit knapp ein Fünftel – auf die Gruppe der unter 26-Jährigen. Davon waren rund 40.000 Azubis. Die Berufsgenossenschaft Rohstoffe und chemische Industrie (BG RCI) hat daher einen Leitfaden für Unternehmer und Unternehmerinnen sowie Führungskräfte zum Umgang mit Betriebsneulingen herausgegeben. Dieser enthält zahlreiche Checklisten zur Vorbereitung des Eintritts, zum ersten Arbeitstag und zur Durchführung der Erstunterweisung. Am Beispiel des Patenmodells wird ein erfolgreiches betriebliches Einarbeitungsmodell vorgestellt. Weitere Beispiele für bewährte Einarbeitungskonzepte aus den Mitgliedsbetrieben der BG RCI gibt es unter dem Stichwort A 024 – ebenso eine stetig wachsende Sammlung von Best-Practice-Beispielen: **http://downloadcenter.bgrci.de** ■

Praktische Aspekte von Regeln und Qualitätssicherung

Ohne Messungen am Arbeitsplatz lassen sich die Belastungen bei Tätigkeiten mit Gefahrstoffen oftmals nicht beurteilen. Im Mittelpunkt des 5. Symposiums „Gefahrstoffe am Arbeitsplatz" (010/18) stehen praktische Aspekte zur Umsetzung der Regelungen, die für die Messung von Gefahrstoffen relevant sind, sowie über deren Messbarkeit. Das Gefahrstoffsymposium findet am 18. und 19. September 2018 in der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) in Dortmund statt.

Zum Symposium „Gefahrstoffe am Arbeitsplatz" laden die Arbeitsgruppe Analytik der Deutschen Gesetzlichen Unfallversicherung (DGUV) unter Federführung der Berufsgenossenschaft Rohstoffe und chemische Industrie (BG RCI), der Arbeitskreis „Luftanalysen" der Ständigen Senatskommission zur Prüfung gesundheitsschädlicher Arbeitsstoffe der Deutschen Forschungsgemeinschaft (DFG) und die BAuA ein. Angesprochen sind Vertreter von Messstellen und analytischen Laboratorien, Sicherheitsingenieure und Fachkräfte für Arbeitssicherheit, Behördenvertreter sowie Aufsichtspersonen der Länder und Träger der gesetzlichen Unfallversicherung.

Das Symposium greift praktische Aspekte der für die Messung von Gefahrstoffen relevanten Regelungen und der Qualitätssicherung auf. Zudem werden konkrete Beispiele und Probleme der Gefahrstoffmessung vorgestellt und diskutiert. Dabei gehen Referenten beispielsweise auf Entwicklungen im Technischen Regelwerk für Gefahrstoffe, Grenzwerte oder die Arbeit mit direkt anzeigenden Messgeräten ein. Zudem werden Ergebnisse aktueller Forschungsprojekte vorgestellt. Programm und Anmeldung: **http://analytik.bgrci.de** ■ **(Seiten-ID #70Q6). www.baua.de**

Die GIT SICHERHEIT ist wichtig für mich, weil sie zuverlässig und kompetent über aktuelle Entwicklungen, neue Trends und Lösungen für den Maschinen- und Anlagenbau informiert.

Birgit Sellmaier, VDMA

MASCHINEN- UND ANLAGENSICHERHEIT

Vorschriftsgemäß gesichert

Maschinensicherheitsnormen in der Praxis. Teil 5 – Risikoeinschätzung mit EN 23125

Für die Sicherheit von Maschinen gibt es drei Gruppen von Normen, nämlich die Gruppen A, B und C. In einer mehrteiligen Artikelserie für GIT SICHERHEIT befasst sich Jens Rothenburg von Euchner vor allem mit den übergeordneten A- und B-Normen – und der Frage, wie sie im praktischen Umgang gut zu nutzen sind. Jens Rothenburg ist im Produktmanagement von Euchner tätig. Er betreut außerdem Normengremien, Berufsgenossenschaftenund Verbände. Im folgenden fünften Teil geht es um spezielle Regelungen zur Risikobeurteilung von Drehmaschinen.

In den beiden vorhergehenden Beiträgen wurden Möglichkeiten zur Risikobeurteilung nach übergeordneten Normen, sogenannten B-Normen, vorgestellt. Für Drehmaschinen steht aber auch eine C-Norm, die EN ISO 23125, zur Verfügung. In dieser sind einige Regelungen zur Risikobeurteilung speziell bei Drehmaschinen aufgeführt.

Kapitel 4 der Norm enthält eine Liste mit möglichen signifikanten Gefährdungen. Sie dient dem Konstrukteur als Hilfestellung, welche Gefährdungen zu beurteilen sind. Wie bei C-Normen üblich, sind dies die Gefahrenstellen

in der Maschine, wie z. B. der Arbeitsbereich oder der Bereich des Späneförderers, aber auch die Gefahren selbst, wie z. B. Herausschleudern von Teilen oder auch Erfassen und Einziehen von Teilen. Selbst Gefährdungen, die von Feuer oder Explosion ausgehen, werden von der C-Norm mit behandelt.

Folgende Gefährdungen sind zu betrachten:
- Mechanische Gefährdungen
- Elektrische Gefährdungen
- Thermische Gefährdungen
- Lärm-Gefährdungen
- Strahlungs-Gefährdungen
- Material-/Substanzgefährdungen
- Ergonomische Gefährdungen
- Gefährdungen im Zusammenhang mit der Einsatzumgebung der Maschine

Diese Gefährdungen wiederum werden unterteilt in gefährliche Situationen und gefährliche Ereignisse. Bei mechanischen Gefährdungen könnten das zum Beispiel folgende sein:
- Beschleunigung/Abbremsung (kinematische Energie)
- spitze Teile
- Annäherung eines sich bewegenden Teils an ein feststehendes Teil

Die Gefährdungen werden sehr spezifisch behandelt und in einer Tabelle zusammengetragen. Für jede Gefährdung wird auf den Abschnitt in der Norm verwiesen, was bezüglich jedes einzelnen Punktes zu beachten ist.

Kapitel 5.11 der Norm mit dem Titel „Besondere Anforderungen infolge von Gefahren durch Ausfall der Steuerung" enthält eine Tabelle für den geforderten PL. Die Betrachtung in der Norm ist hier umgekehrt – die Risikominderung wird durch steuerungstechnische Maßnahmen erreicht. Dazu muss die jeweilige Maßnahme einen PL erfüllen. Dieser PL muss aber zumindest dem PL_r der Gefahrenstelle entsprechen.

Auch hierzu wieder ein Beispiel aus der Norm: Die Risikominderung durch eine Schutztür im Arbeitsbereich durch den Bediener muss mindestens Kategorie 3 und PL d erfüllen. Normativ wird das ein wenig umständlicher formuliert – es heißt hierzu in der Tabelle:

In dieser Tabelle wird neben dem PL für die Schaltung auch die Kategorie vorgegeben. Nach EN ISO 13849-1 könnte der PL d auch mit einer Kategorie 2 Schaltung erreicht werden, was entsprechend der Tabelle für die Drehmaschine aber nicht geeignet ist. Es muss die Kategorie 3 erfüllt werden.

Die Risikobeurteilung nach ISO 13849-1 Anhang A ergibt einen benötigten Performance Level (PL_r = Performancel Level required). Die Beurteilung nach EN 62061 dagegen einen SIL (Safety Integrity Level). Die EN ISO 12100 lässt völlig frei, wie das Ergebnis der Risikobeurteilung auszusehen hat. Die EN ISO 23125 enthält im Abschnitt 5.11 eine Tabelle zur Risikobeurteilung, die einen PL_r für spezifische Gefährdungen an Drehmaschinen ergibt. Die technische Risikominderung wird ebenfalls nach EN ISO 13849-1 beurteilt. Somit ist der Vergleich des PL_r mit dem PL der steuerungstechnischen Maßnahmen sehr einfach. Deshalb ist die Angabe eines PLr in der EN ISO 23125 sehr hilfreich. ■

Autor
Jens Rothenburg,
Produktmanagement Euchner

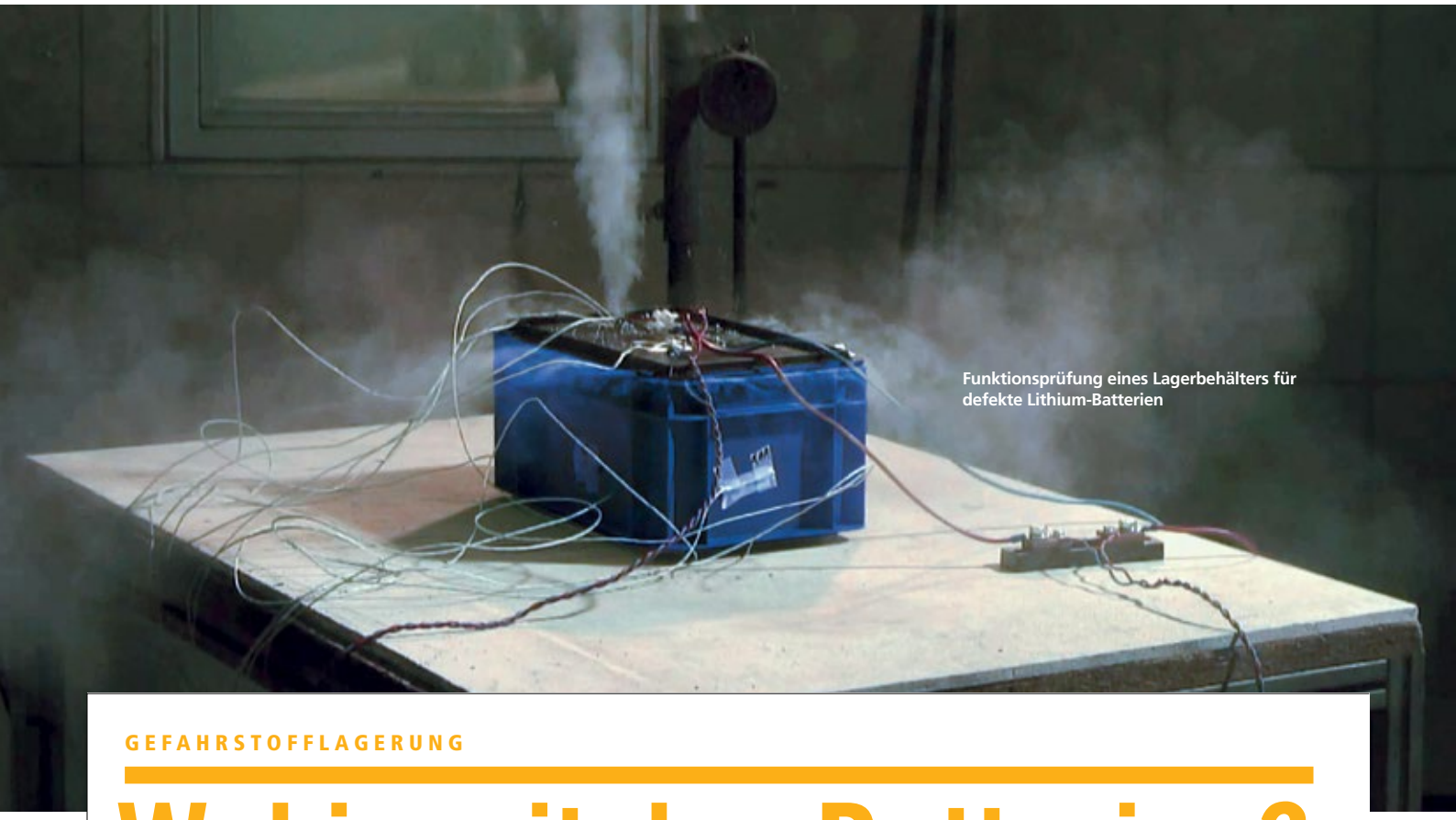
Kontakt

Euchner GmbH+ Co. KG
Leinfelden-Echterdingen
Tel.: +49 711 7597 0
info@euchner.de
www.euchner.de

Nr[a]	Gefahren, gefährliche Situationen und gefährliche Ereignisse	Situationen an Drehmaschinen	ISO12100:2010	Relevante Typ B-Norm [b]	Relevanter Abschnitt in dieser Internationalen Norm
B.1	**1 Mechanische Gefährdungen**				
—	Beschleunigung/ Abbremsung (kinematische Energie)		6.2.2.1 6.2.2.2 6.2.3 a) 6.2.3 b) 6.2.6 6.2.10 6.3.1 6.3.2 6.3.3 6.3.5.2 6.3.5.4 6.3.5.5 6.3.5.6 6.4.1 6.4.3 6.4.4 6.4.5	ISO 6385 ISO 13851 ISO 13854 ISO 13855 ISO 13856-2 ISO 13856-3 ISO 13857 ISO 14118 ISO 14119 ISO 14120 ISO 14122-1 ISO 14122-2 ISO 14122-3 ISO 14122-4 ISO 16156 IEC 60204-1	5.2.1.1 g) 5.2.3 a) 4) ii)
—	spitze Teile				5.1.2 5.2
—	Annäherung eines sich bewegenden Teils an ein feststehendes Teil				5.1.2 5.2
—	schneidende Teile, scharfe Kanten: Quetschen und Scheren				5.1.2 5.2
—	elastische Elemente Hochdruck: ein- oder ausspritzende Flüssigkeiten, Vakuum, Schwerkraft (gespeicherte Energie), Hochdruck, Höhe gegenüber dem Boden	Ableitung von innerhalb der Maschine gespeicherter Energie			5.2.4.5 b) 1) iii) 5.2.2.4 a) 1) 5.2.2.4 c) 6) 5.2.4.4 b) 5.2.4.3 a) 3) 5.2.4.4.1 c) 5.2.4.5 a) 3) 5.8 e) 1) iv) 5.8 h) 4) 5.10 d)

Auszug aus der Tabelle 3 – Übersicht der Gefährdungen und Verweisungen auf Typ B-Normen aus der EN ISO 23125

Verriegelung in Verbindung mit einer beweglichen trennenden Schutzeinrichtung für die folgenden Bereiche, … bezogen auf:	Geforderter Performance Level PL_r nach ISO 13849-1:2006	Geforderte Kategorie nach EN 954-1:1996
i) Arbeitsbereich durch den Bediener	d Kategorie 3	3



Funktionsprüfung eines Lagerbehälters für defekte Lithium-Batterien

GEFAHRSTOFFLAGERUNG

Wohin mit den Batterien?

Lagern wie Gefahrstoffe: Lithium-Batterien in Arbeitsräumen

Lithiumbatterien sind im Normalbetrieb als relativ sicher einzustufen. Probleme entstehen jedoch bei Beschädigung durch elektrische, mechanische oder thermische Einwirkung. Daher ist der Transport bereits seit Jahren im ADR detailliert geregelt. Für die innerbetriebliche Lagerung und Bereitstellung findet man bis dato keine gesetzlichen Vorschriften. Veranlasst durch eine Vielzahl von Schadensfällen, haben die deutschen Versicherer (GDV) Brandversuche gemacht, um mit den gewonnenen Erkenntnissen ein Merkblatt für Produzenten, Spediteure und Nutzer zu erstellen (VdS 3103:2016). In der zweiten Auflage liefert das Merkblatt die wichtigsten Hinweise zur Erarbeitung eines eigenen Brandschutzkonzepts. Ein Beitrag von Jens Erbstößer.

Nach Ansicht des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) sind Lithium-Batterien innerbetrieblich grundsätzlich wie ein Gefahrstoff zu behandeln. Dadurch bieten sich die Technischen Regeln für Gefahrstoffe „Lagerung von Gefahrstoffen in ortsbeweglichen Behältern" Nr. 510: Ausgabe 2013/2015 die richtige Orientierungshilfe für die verpflichtende Erstellung der Gefährdungsbeurteilung nach §5 Arbeitsschutzgesetz an. Durch Anwendung der in ihr verankerten Brandschutzmaßnahmen wird das Schutzziel, Gefährdungen zu beseitigen oder auf ein Minimum zu reduzieren, mit eingebunden.

Welche Gefahren bestehen?

Am Anfang steht natürlich die Gefährdungsbeurteilung. Für diese sind gewisse Definitionen wichtig, die man der TRGS 510:2013 entnehmen kann. So ist beispielsweise nicht jedes Abstellen gleich als ein Lagern zu verstehen. Mögliche Gefahren sind Teil der Betrachtung, insbesondere weil sie häufig auf fehlerhafter Handhabung oder Bedienung zurückzuführen sind. Die Hauptursachen sind Mechanischer Stress, Thermischer Stress und Überladung.

Weitere Gefahrenquellen ergeben sich aus den Batteriesystemen selbst: Hoher elektrischer Strom oder möglicher Austritt giftiger oder entzündbarer Inhaltsstoffe im Brandfall, die ein explosionsfähiges Gemisch bilden können (z. B. Fluorwasserstoff (2HF), Fluorwasserstoffsäure (Flusssäure, 3HF) und die hohe Brandlast der verwendeten Materialien und Komponenten. Bei Erwärmung kann es zu

einem plötzlichen Bersten von Batterien und Batteriezellen, bei Versagen des Sicherheitsventils kommen.

Sicherheitsregeln

Daher sind die folgenden Sicherheitsregeln grundsätzlich für alle Lithiumbatterien zu beachten: Einhaltung aller Vorgaben der jeweiligen Hersteller, Verhinderung äußerer Kurzschlüsse, Schutz vor hohen Temperaturen und Wärmequellen. Dies gilt natürlich auch durch die Bereitstellung und Lagerung.

In nicht durch automatische Löschanlagen geschützten Bereichen ist eine bauliche Trennung, alternativ eine räumliche Trennung von mind. 2,5 m zu allen anderen brennbaren Materialien einzuhalten.

Beschädigte oder defekte Lithium-Batterien sind umgehend aus den Arbeitsräumen zu entfernen und bis zur Entsorgung in sicherem Abstand oder in einem Brandschutztechnisch abgetrennten Bereich zwischenzulagern.

Nicht mit anderen brennbaren Stoffen lagern

Eine ungeschützte Mischlagerung mit anderen brennbaren Stoffen ist unbedingt zu vermeiden. Da auch die unterschiedlichen Leistungskapazitäten bei der Lagerung eine wichtige Rolle spielen, sind Lithiumbatterien, in drei Leistungskategorien eingeteilt worden:

- Geringe Leistung: <2g Li /Batterie (UN 3090) oder <100 Wh/Batterie (UN 3480)
- Mittlerer Leistung: >2g Li und ≤ 12 kg brutto/Batterie (UN 3090) oder >100 Wh und ≤12 kg/Batterie (UN 3480)
- Hohe Leistung: >2 g Li und ≥12 kg brutto/Batterie (UN 3090) oder >100 Wh und/oder >12 kg brutto/Batterie (UN 3480)

Spezifische Sicherheitsregeln treffen Lithium-Batterien mit geringer Leistung erst ab Lagerung größerer, zusammenhängende Mengen von mehr als 7 m3 oder mehr als sechs Europaletten. Dann gelten für sie die gleichen Regeln wie für Lithium-Batterie mittlerer Leistung. Diese sind von anderen räumlich (mindestens fünf Meter) oder baulich feuerbeständig (also Feuerwiderstandsfähigkeit mindestens F90-Separatlagerung) abzutrennen, je nach Ergebnis der Gefährdungsbeurteilung.

Zur Mischlagerung mit anderen Produkten, die einen Brand beschleunigen können, fallen beispielsweise Paletten, Papier, etc.: „Brandlast-Frei" ist hier die Devise. Der Lagerbereich mittlerer Lithium-Batterien muss durch eine geeignete Brandmeldeanlage mit Aufschaltung auf eine ständig besetzte Stelle überwacht werden.

Lässt sich eine Getrenntlagerung mit mindestens fünf Metern Sicherheitsabstand im Lager noch darstellen, stößt man in Arbeitsräumen (Produktion, Werkstatt, Service, Entwicklung, etc.) schnell an die Grenzen des Machbaren. Daher werden zur Separatlagerung häufig Gefahrstoffschränke nach EN DIN 14470-1 als sicheres Zwischenlager für die Mengen über den Tagesbedarf hinaus oder reparatur-und diagnosebedürftige Lithium-Batterie eingesetzt. Die Vorteile: Definierte Fluchtzeit für die im Raum Beschäftigten und Dritter bei einem Brand in der Werkstatt, selbstschließende Türen, Druckentlastungsöffnungen, geprüfte Brandschutzdurchführungen zum Einbringen von Elektrokabeln, etc.

Doch Vorsicht, bei der Separatlagerung gibt es einige Details zu beachten:

- Es dürfen keine anderen entzündbaren Stoffe oder gar Gefahrstoffe gelagert werden (z. B. Spraydosen, Lösemittel, etc.)
- Aufgrund der kritischen Temperatur der Lithium-Batterie von ca. 125 °C bis 130 °C, die man der Zündtemperatur eines Gefahrstoffes gleichsetzen kann, dürfen Lithiumbatterien nach TRGS 510:2013 nur in Sicherheitsschränken mit einer Feuerwiderstandsfähigkeit von 90 Minuten (Typ 90) gelagert werden.
- Der kritische Temperaturbereich ab 125 °C/130 °C wird bei einer Brandeinwirkung von außen früher erreicht als die zulässige Innentemperatur in einer Prüfung nach EN DIN 14470-1 (zulässige Innentemperatur: Umgebungstemperatur + ΔT=180 °C). Das bedeutet, dass Gefahrstoffschränke die angegebene, geprüfte Feuerwiderstandsfähigkeit (≈ Fluchtzeit) ggf. nicht erreichen (können). Diese ist jedoch eminent wichtig für die Planung der Fluchtwege und des Löschangriffs
- Gefahrstoffschränke halten ihre Feuerwiderstandsfähigkeit bei einer Brandeinwirkung von außen nach innen. Einen Brand von innen nach außen kann der Gefahrstoffschrank aber nur schwer eindämmen

Ein zwar geprüfter, jedoch unveränderter Gefahrstoffschrank nach EN DIN 14470-1 muss ertüchtigt werden, um diesen innerhalb seiner technischen Spezifikation nutzen zu können. In der Praxis bewährt haben sich unterschiedliche, technische Maßnahmen:

- Schrankinterne Separierung von Lithiumbatterien in einzelnen, Lager- oder Transport-Boxen, gefüllt mit geprüftem Löschmittel. Im Fall des thermischen Durchgehens einer Lithium-Batterie (thermal runaway) begrenzen die Boxen das Schadensszenario auf ihr Inneres.
- Branderkennung durch im Schrank angebrachte Sensortechnik, kombiniert mit einer Brandbekämpfung durch ein Spezial-Aerosol (VdS-zugelassen). Der Schrank ist ein geschlossenes System – dadurch kann das Aerosol über eine lange Stützzeit hinweg gebunden werden

Die Kombination mit Gefahrstoffschrank und den Löschverfahren bietet dem Anwender die Sicherheit bei der Lagerung im Arbeitsraum in beiden Richtungen. Außerdem entfallen durch die Verknüpfung von Schrank und Löschmittel die geforderten Sicherheitsabstände bei einer Getrenntlagerung. Fundamental für alle Maßnahmen ist jedoch die Erarbeitung eines wirksamen Schutzkonzepts mit Dokumentation für ihren Einzelfall. ■

◄ **Sicherheitsschrank mit VDS-Zugelassener Löschanlage**

Kontakt

Erbstößer GmbH
Maktheidenfeld
Tel.: +49 9391 4052
info@erbs.de
www.erbs.de

© Foto: Kübler

Die neue Warnschutzkleidung von Assistance Partner steigert Wiedererkennungswert und Wohlgefühl

PSA

Weit mehr als ein Hingucker

Exklusive Warnschutzkleidung für Assistance Partner

Rot ist die Farbe von Assistance Partner. Das rote A prangt gut sichtbar auf den einheitlich in Silber gehaltenen Einsatzfahrzeugen und auch die im Netzwerk von assistance partner tätigen Pannenhelfer sind für Kunden und Öffentlichkeit aufgrund ihrer roten Warnschutzbekleidung sofort zuordenbar. Am Rot ändert auch der kürzlich eingeleitete Kollektionswechsel nichts – ansonsten aber hat die neue Bekleidung, die der Berufsbekleidungsspezialist Kübler gemeinsam mit dem Fachhändler Drivetex, Eggolsheim, in enger Zusammmenarbeit mit Pannenhelfern entwickelt hat, mit der bisherigen fast nichts mehr gemein.

Die Messlatte für die neue Warnschutzkleidung hätte kaum höher liegen können. „Wir wollten eine für die Tätigkeiten des Pannenhelfers perfekte Lösung finden“, erklärt Erwin Schanda, dessen Unternehmen Drivetex die neue Kollektion bundesweit exklusiv vertreibt, auf Wunsch auch als Mietkleidung mit allen damit verbundenen Serviceleistungen. Hinzu kamen harte Preisvorgaben aus der Münchner Zentrale von assistance partner, die hochwertige Qualität aus europäischer Fertigung voraussetzte.

Um diese Ziele zu erreichen, wurden Anwender aus ausgewählten Betrieben in den gesamten Entwicklungsprozess eingebunden. In Gesprächen und durch die Beobachtung von Arbeitseinsätzen kristallisierte sich heraus, dass eine Überarbeitung der bis dato eingesetzten Warnschutzbekleidung von Nöten war. Bei inzwischen in die Jahre gekommenen Kleidung war die Passform nicht mehr zeitgemäß. Auch der angebotene Größenspiegel ließ zu wünschen übrig, was zu Lasten des Wohlbefindens, aber auch der Sicherheit ging. „Wir sahen hie und da hochgekrempelte Hosenbeine“, berichtet Schanda. Im ungünstigsten Fall seien die Vorgaben der Warnschutzklasse 3 für die Flächen an Hintergrund- und Reflexmaterial dann nicht mehr erfüllt, wodurch der Versicherungsschutz der Berufsgenossenschaft nach der aktuellen Norm EN ISO 20471 entfalle, warnt Schanda.

Mitarbeiter profitieren in vielerlei Hinsicht

Die neue Bekleidung besticht durch ihr modernes, schlankes Design. Sie sitzt wie eine zweite Haut und macht dennoch jede Bewegung mit. Dafür sorgen die von Kübler speziell eingearbeiteten Komfortzonen im Bund-, Rücken-, Nacken-, Arm- und Kniebereich, die unter anderem mit ergonomisch positionierten Nähten, Stretcheinsätzen und Strickbündchen ausgestattet sind. Bei der Hose trägt der elastische Bundeinsatz wesentlich zur hervorragenden Passform bei. Die prägnante Optik der Bekleidung in Warnrot mit anthrazitfarbenen Kontrasteinsätzen und segmentierten Reflexstreifen garantiert den Mitarbeitern von assistance partner zudem einen imageträchtigen Auftritt und einen hohen Wiedererkennungswert. Die Anordnung der

Reflexstreifen verschafft den Pannenhelfern zudem beste Rundumsichtbarkeit. „In den Genuss des hohen Tragekomforts und der verbesserten Schutzfunktion kommt jeder Pannenhelfer und jede Pannenhelferin“, unterstreicht Klaus Stemig, Geschäftsführer von assistance partner. Denn die neue, nach EN ISO 20471 zertifizierte Warnschutzkleidung umfasst auch Damenmodelle und deckt das komplette Konfektionsgrößenraster ab. Sondergrößen, wie 7 XL, sind ebenfalls erhältlich. Sie werden von Kübler individuell angefertigt.

Individueller Tragekomfort

Mit der neuen Warnschutzkollektion erhalten die Mitarbeiter und Mitarbeiterinnen von assistance partner die Möglichkeit, zwischen verschiedenen Bekleidungsteilen zu wählen. Für die Sommermonate stehen eine leichte Arbeitsjacke und eine Weste bereit. Alternativ zur Herrenbundhose gibt es eine Latzhose. Für die Übergangs- und Wintermonate haben die Designer bei Kübler eigens ein Zwiebelschalensystem entwickelt, bestehend aus Thermounterwäsche, Hose und Softshelljacke oder Weste sowie einer wasserdichten Warnschutzjacke mit atmungsaktiver Sympatex-Klimamenbran. Diese erfüllt in Kombination mit Bund- oder Latzhose die Klasse 3 der Warnschutznorm und die Klasse 3 der Wetterschutznorm EN 343. „So wird einerseits dem individuellen Kälteempfinden Rechnung getragen und andererseits verhindert, dass die Helfer ins Schwitzen geraten, wenn sie im Einsatzfahrzeug unterwegs sind“, berichtet Schanda und verweist auf die Kommentare der Träger, die die neue Bekleidung vorab getestet haben.

Auch die Taschenlösungen sind das Ergebnis der intensiven Auseinandersetzung mit den typischen Arbeitsabläufen bei assistance partner. Für das obligatorisch mitgeführte Tablet wurden Arbeits-, Softshell- und Wetterjacke sowie die Weste auf der rechten Brustseite mit einer Innentasche samt Reißverschluss ausgestattet. Ebenso clever konstruiert ist die in die linke Brusttasche integrierte Smartphonetasche mit seitlichem Eingriff. Die frei hängende Tasche am rechten Hosenbein nimmt Gabelschlüssel oder sonstiges Werkzeug auf. Weiteren Stauraum für Werkzeug bietet die linke Schenkeltasche mit Reißverschluss. Links- und Rechtshänder werden sich über die weit ausgeschnittenen Seitentaschen mit Übergrifffunktion freuen. Als ebenso bedienungsfreundlich erweisen sich die von oben schnell befüllbaren wasserabweisenden Knietaschen, die in Kombination mit dem passenden Kniepolster von Kübler nach EN 14404 zertifiziert sind. Cordura-Verstärkungen an Taschen, Knie und Ellenbogen sorgen dafür, dass die Bekleidung den Einsätzen beim Unfall- und Pannenservice lange Stand hält.

Bei der Hausmesse von assistance partner im Februar in München wurde die Warnschutzkleidung den Mitgliedsbetrieben erstmals vorgestellt. Schanda erinnert sich noch gut: „Die Resonanz war super.“ Der permanente Austausch mit Anwendern während der gesamten Entwicklungsphase habe sich gelohnt und zum gewünschten Ergebnis geführt.

Vom modernen Design und hohen Tragekomfort der für die Assistance-Pannenhelfer konzipierten Warnschutzkleidung können auch deren Kollegen in den KFZ-Werkstätten profitieren. Ihnen steht die Workwear-Kollektion Pulsschlag von Kübler zur Verfügung, die bei der neuen Warnschutzkleidung Pate stand. Damit haben die Partnerunternehmen von assistance die Möglichkeit, ihre Mitarbeiter durchgängig hochwertig einzukleiden. ■

Kontakt

Paul H. Kübler Bekleidungswerk GmbH & Co. KG
Plüderhausen
Tel.: +49 7181 8003 0
info@kuebler.eu
www.kuebler.eu

Bis zu zwei IBC-Container finden in dem Lager genügend Platz

GEFAHRSTOFFLAGERUNG

Wohin bloß damit?

Wirtschaftliche Gefahrstofflagerung bei maximaler Sicherheit

Es gilt für produzierende, verarbeitende und instandsetzende Betriebe gleichermaßen – viele haben es tagtäglich mit Gefahrstoffen zu tun. Sie fungieren als Additive und Prozessmittel, werden gezielt hergestellt oder fallen als Abfall am Ende der Produktionskette an. Vorhaltung und Lagerung sind in jedem Fall eine tägliche Herausforderung für Betriebe. Da nicht jedes Unternehmen eine kostspielige Großlösung benötigt, entwickeln Unternehmen wie Denios wirtschaftliche Kleinlösungen, die trotzdem alle Anforderungen an die Sicherheit erfüllen.

Aufstellung und Einsatz eines Gefahrstoffdepots können je nach Unternehmen ausgesprochen unterschiedlich ausfallen. Mittels einer breiten Palette an Zubehör – beispielsweise technischen Lüftungen, Heizungen oder PE-Inlinern – kann ein sehr großer Anwendungsbereich abgedeckt werden.

Eine solche Speziallösung ist kürzlich für einen deutschen Hersteller von Asphaltmischanlagen entstanden. Denios entwickelte ein speziell auf dessen Bedürfnisse abgestimmtes Gefahrstofflager aus der neuen Produktreihe Solid Maxx. Dieses sollte als Pumpenstation zur Anmischung von Betonzusätzen dienen. Hierfür musste eine frostfreie Lagerung gewährleistet werden, weswegen man auf die isolierte Variante des neuen Gefahrstofflagers zurückgriff. Bis zu zwei IBC-Container finden in dem Lager genügend Platz und auch die Arbeit am Gebinde ist aufgrund der komfortablen Maße möglich.

Das Lager diente quasi als Prototyp, weil der Kunde dauerhaft den gleichen Typ an Mischanlagen einsetzt und somit dauerhaft Bedarf an entsprechenden Lagerlösungen hatte. Zur Sicherstellung der frostfreien Lagerung ist ein Heizelement im Innerer des Lagers montiert. Abgestimmt auf das zu lagernde Medium und der daraus resultierenden Beständigkeit ist ein PE-Inliner in die eigentliche Auffangwanne eingelegt. Da die Auffangwanne aus Stahl ist, ermöglicht dieser Inliner die sichere Lagerung von Säuren und Laugen. Der Einsatz von Füllstandsensoren in der Auffangwanne und die Möglichkeit zur uneingeschränkten Einsicht in die Wanne wurden durch eigens angefertigte Aussparungen in der Aufstellfläche der Gebinde realisiert.

Gesetzliche Vorgaben

Da ein Gefahrstofflager wie das Solid Maxx unter die Bauprodukte-Richtlinie fällt, ist zur Aufstellung in Deutschland eine Zulassung des deutschen Instituts für Bautechnik, kurz DIBt-Zulassung, obligatorisch. Voraussetzung für die Zulassung ist unter anderem eine geprüfte Statik. Dem Kunden wird ermöglicht, verschiedenste Gebinde einzulagern, die ihrerseits unterschiedliche Dichten und damit Gewichte besitzen. Zum Vergleich: herkömmliche Lagermedien wie z.B. Mineralöle besitzen eine Dichte von 1,0kg/ dm³. Durch die stabile Ausführung der Auffangwanne des SolidMaxx, inkl. Gitterrosten, ist aber auch für Sonderfälle wie der Lagerung von Schwefelsäure mit einer Dichte von1,8kg/ dm³ und damit 1800 kg pro Stellplatz bzw. dem 1,8-fachen Gewicht ausreichend Sicherheit gewährleistet.

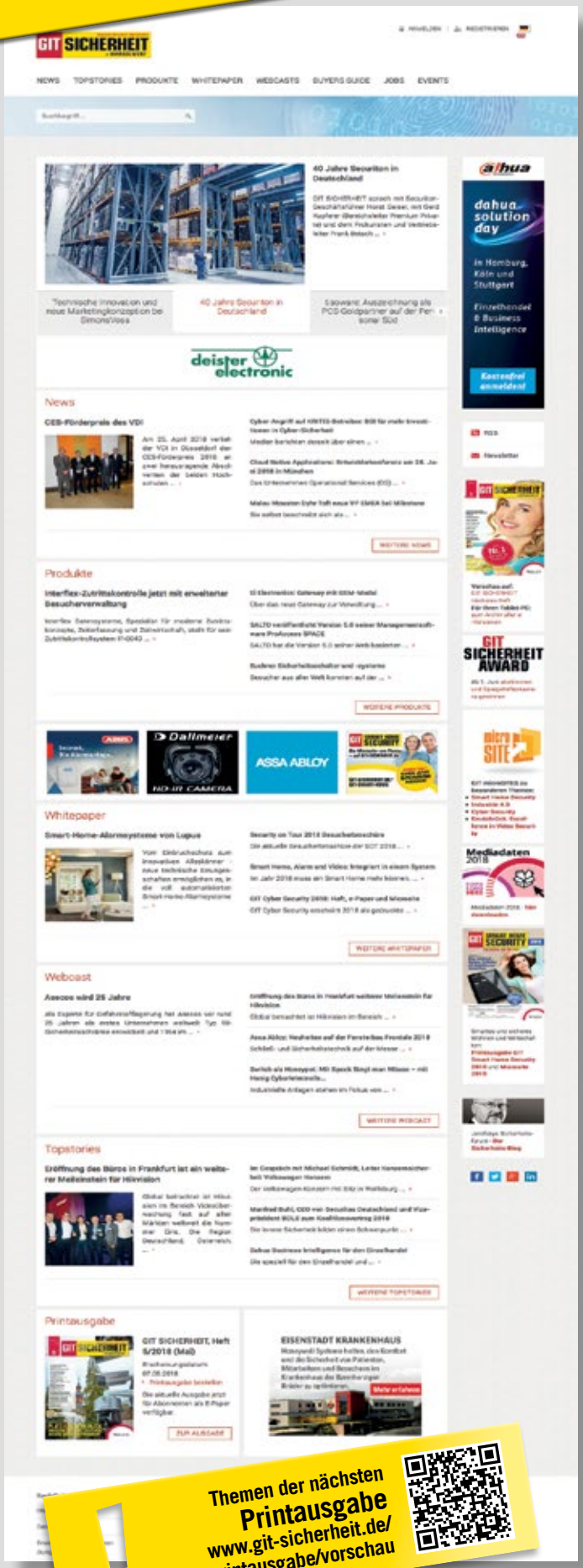
Ein anderer Aspekt ist der Aufstellort und damit z.B. auch die auf das Lager einwirkenden Schneelasten. Deutschland ist in die Schneelastzonen 1-3 unterteilt, wobei die Zone 1 die mit der geringsten Belastung und Zone 3 die mit der höchsten Belastung darstellt. Typische Werte für die auf den Boden wirkenden Schneelasten (sk) liegen zwischen 0,65kN/ m² und ≥1,10kN/ m². Da dieser Wert abhängig von der Geländehöhe um einiges höher sein kann, müssen die Lagersysteme dementsprechend angepasst sein. Um eine Einschränkung des Aufstellortes zu verhindern ist das Gefahrstofflager statisch mit einer Schneelast sk=2,5kN/m² ausgelegt.

Fertigungsverfahren

Die Denios-Gefahrstofflager Solid Maxx bestehen hauptsächlich aus einer Stahlkonstruktion. Vor allem die automatische Laser-Kant-Technik hat in der Fertigung dieser Produkte Einzug gehalten. Die Erstellung der Einzelteile ist eng durch die Konstruktion geführt und technischen Änderungen können sofort direkt über die Maschinenprogramme eingepflegt werden. Nach Fertigung der Einzelteile wird über eine Pulverbeschichtung der notwendige Korrosionsschutz aufgetragen. Die Auffangwanne besteht ebenfalls aus einzelnen Laser-Kant-Teilen, die als Schweißbaugruppe zusammengefügt sind. ■

Kontakt

Denios GmbH
Bad Oeynhausen
Tel.: +49 5731 753 306
info@denios.de
www.denios.de



IMPRESSUM

Herausgeber
Wiley-VCH Verlag GmbH & Co. KGaA

Geschäftsführer
Sabine Steinbach, Dr. Guido F. Herrmann

Geschäftsleitung
Wiley Corporate Solutions
Roy Opie, Dr. Heiko Baumgartner,
Steffen Ebert, Dr. Katja Habermüller

Beirat
Erich Keil, Fraport AG, Frankfurt
Prof. Dr. Frithjof Klasen, Institut f. Automation u. Industrial IT, FH Köln
Volker Kraiß, Kraiss Consult, Bruchköbel
Prof. Dr. Norbert Pohlmann, Institut f. Internet – Sicherheit, FH Gelsenkirchen
Bernd Saßmannshausen, Merck, Darmstadt
Dr. Burkhard Winter, Dechema e.V., Frankfurt

Objektleitung
Dipl.-Betriebswirt Steffen Ebert
Regina Berg-Jauernig M. A.

Wissenschaftliche Schriftleitung
Dipl.-Verw. Heiner Jerofsky

Commercial Manager, Anzeigenleitung
Oliver Scheel
+49 6201 606 748

Redaktion
Dr. Heiko Baumgartner
+49 6201 606 703
Regina Berg-Jauernig M.A.
+49 6201 606 704
Dipl.-Betrw. Steffen Ebert
+49 6201 606 709
Matthias Erler ass. iur.
+49 611 16851965
Sophie Platzer
+49 6201 606 761
Lisa Schneiderheinze M.A.
+49 6201 606 738

Textchef
Matthias Erler ass. iur.
+49 611 1685 1965

Herstellung
Jörg Stenger
+49 6201 606 742
Claudia Vogel (Anzeigen)
+49 6201 606 758

Satz + Layout Ruth Herrmann
Lithografie Elli Palzer

Sonderdrucke
Sophie Platzer
+49 6201 606 761

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

Wiley-VCH Verlag GmbH & Co. KGaA
Boschstr. 12, 69469 Weinheim
Telefon +49 6201 606 0
E-Mail: git-gs@wiley.com
Internet: www.git-sicherheit.de

Verlagsvertretungen
Manfred Höring
+49 61 59 50 55
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

Zurzeit gilt Anzeigenpreisliste vom 1.10.2017. Die namentlich gekennzeichneten Beiträge stehen in der Verantwortung des Autors.

2018 erscheinen 10 Ausgaben
„GIT SICHERHEIT"
Druckauflage: 30.000 (Q1 18)
inkl. GIT Sonderausgabe PRO-4-PRO

Abonnement 2018: 10 Ausgaben (inkl. Sonderausgaben) 118,00 €, zzgl. MwSt. Einzelheft 16,30 € zzgl. Porto + Mwst. Schüler und Studenten erhalten unter Vorlage einer gültigen Bescheinigung einen Rabatt von 50 %. Abonnement-Bestellungen gelten bis auf Widerruf; Kündigungen 6 Wochen vor Jahresende. Abonnementbestellungen können innerhalb einer Woche schriftlich widerrufen werden, Versandreklamationen sind nur innerhalb von 4 Wochen nach Erscheinen möglich.

Alle Mitglieder der Verbände BHE, BID, BDSW, BDGW, PMeV, Safety Network International, vfdb und VfS sind im Rahmen ihrer Mitgliedschaft Abonnenten der GIT SICHERHEIT + MANAGEMENT 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.

Druck
pva, Druck und Medien, 76829 Landau
Printed in Germany, ISSN 0948-9487

WILEY

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.

BusinessPartner im Buyers Guide auf GIT-SICHERHEIT.de

SICHERHEITS MANAGEMENT

Sicherheitsmanagement

BOSCH

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5 · 85630 Grasbrunn
Tel. 0800/7000444 · Fax 0800/7000888
Info.service@de.bosch.com
www.bosch-Sicherheitssysteme.de
Produkte und Systemlösungen für Videoüberwachungs-, Einbruchmelde-, Brandmelde-, Sprachalarm- und Managementsysteme sowie Zutrittskontrolle, professionelle Audio- und Konferenzsysteme. In ausgewählten Ländern bietet Bosch Lösungen und Dienstleistungen für Gebäudesicherheit, Energieeffizienz und Gebäudeautomation an.

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

EVVA
access to security

EVVA Sicherheitstechnik GmbH
Höffgeshofweg 30 | 47807 Krefeld | Germany
T +49 2151 37 36-0 | F +49 2151 37 36-5635
office-krefeld@evva.com | www.evva.de

Föpplstraße 15 | 04347 Leipzig | Germany
T +49 341 234 090-5 | F +49 341 234 090-5760
office-leipzig@evva.com | www.evva.de

Mechanik, mechatronische & elektronische Schließsysteme, Zutrittskontrolle, Zusatzsicherungen und Türbeschläge

Sicherheitsmanagement

funkwerk
video systeme

Funkwerk video systeme GmbH
Thomas-Mann-Str. 50 · D-90471 Nürnberg
Tel. +49(0)911/75884-0 · Fax +49(0)911/75884-100
info@funkwerk-vs.com · www.funkwerk.com
CCTV, Systemlösung, Systemintegration, Videoüberwachung, Security, Gebäudemanagement

Sicherheitsmanagement

ASSA ABLOY
The global leader in door opening solutions

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

Sicherheitsmanagement

Honeywell

Honeywell Security Group
Novar GmbH
Johannes-Mauthe-Straße 14 · 72458 Albstadt
Tel.: +49(0)74 31/8 01-0 · Fax: +49(0)74 31/8 01-12 20
www.honeywell.com/security/de
E-Mail: info.security.de@honeywell.com
Biometrie, Einbruchmelde-, Management-, Rettungsweg-, Video-, Zeiterfassungs- und Zutrittskontrollsysteme

Sicherheitsmanagement

AVS Alarmsysteme

AVS Alarmsysteme
BKH Sicherheitstechnik GmbH & Co. KG
Seebachring 74 · 67125 Dannstadt
Tel: +49 621 95 04 08 0
www.avs-alarmsysteme.de · info@avs-alarmsysteme.de
Alarmsysteme (Funk, Hybrid, Kabel konventionell & BUS), Einbruch- und Brandmeldetechnik, Bewegungsmelder (Innen und Außen), Magnetkontakte, Wählgeräte (LAN, WLAN, DUAL-GSM), Smartphone-App, Nebelanlagen, Lichtschranken, Perimeterschutz

Sicherheitsmanagement

nedap

Nedap GmbH
Postfach 2461 · D-40647 Meerbusch
Otto-Hahn-Straße 3 · D-40670 Meerbusch
Tel. +49 (0)2159 8145-400 · Fax +49 (0)2159 8145-410
info-de@nedap.com
www.nedapsecurity.com
Nedap Sicherheits-Systeme werden von Millionen von Menschen benutzt; in Banken, Flughäfen, Krankenhäusern, Regierungsgebäuden und im industriellen Service in allen Ländern der Welt.

Sicherheitsmanagement

NSC
Sicherheitstechnik GmbH

NSC Sicherheitstechnik GmbH
Lange Wand 3 · 33719 Bielefeld
Tel.: +49 (0) 521/13629-0
Fax: +49 (0) 521/13629-29
info@nsc-sicherheit.de · www.nsc-sicherheit.de
Brandmeldetechnik, Videotechnik, Sprach-Alarm-Anlagen

Sicherheitsmanagement

SCHILLE

Schille Informationssysteme GmbH
Goseriede 4, D-30159 Hannover
Tel. +49(0)511/542244-0 · Tel. +49(0)511/542244-22
info@schille.com · www.schille.com
Gebäudeleit- und Sicherheitstechnik, Störungs- und Gefahrenmanagementsysteme, OPC-Entwicklung, Videoübertragungssysteme

Sicherheitsmanagement

United Technologies
Climate | Controls | Security

UTC Fire & Security Deutschland GmbH
Im Taubental 16 · 41468 Neuss
Tel. +49 (0) 2131 3663 0 · Fax. +49 (0) 2131 3663 500
germany@fs.utc.com · www.utcfssecurityproducts.de
Produkte und Systemlösungen der Einbruch- und Brandmeldetechnik, Videoüberwachung, Zutrittskontrolle sowie integriertes Sicherheitsmanagement.

ALARM MANAGEMENT

Alarmmanagement

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.

Alarmmanagement

DAITEM

ATRAL-SECAL GmbH
Service Daitem
Eisleber Str. 4 · D-69469 Weinheim
Tel. +49(0)6201/6005-0 · Fax +49(0)6201/6005-15
info@daitem.de · www.daitem.de
Funk-Einbruchmeldesysteme, Funk-Brandmelder, Vertrieb über Sicherheits-Fachhandel

Alarmmanagement

DIGISOUND®

Digisound Electronic GmbH
Oststraße 54 · 22844 Norderstedt
Tel. 040/526869-0 · Fax 040/526869-13
contact@digisound.de · www.digisound.de
Akustische Signalgeber, Piezoelektrische Sirenen, Elektronische Blitzlampen, Lautsprecher- und Transducer

GEBÄUDE SICHERHEIT

Gebäudesicherheit

GEZE

GEZE GmbH
Reinhold-Vöster-Str. 21-29 · D-71229 Leonberg
Tel. 07152/203-0 · Fax 07152/203-310
info.de@geze.com · www.geze.com
Flucht- und Rettungswegsysteme, Zutrittskontrollsysteme, RWA, Feststellanlagen

Alarmmanagement

eps®
Weil jede Sekunde zählt.

EPS Vertriebs GmbH
Lütke Feld 9 · 48329 Havixbeck
Tel.: 02507/98750-0 · Fax: 02507/98750-29
info@eps-vertrieb.de · www.eps-vertrieb.de
Brandschutz und sicherheitstechnische Produkte. Systemlieferant für Alarm, Brand und Video.

Gebäudesicherheit

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

Gebäudesicherheit

Simons Voss technologies

SimonsVoss Technologies GmbH
Feringastr. 4 · D-85774 Unterföhring
Tel. +49(0)89/99228-180 · Fax +49(0)89/99228-222
marketing@simons-voss.de · www.simons-voss.de
Digitale Schließ- und Organisationssysteme mit optionalen Funktionen zu Zeiterfassung und Zutrittskontrolle

Gebäudesicherheit

DICTATOR

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

U&Z Uhlmann & Zacher

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

Alarmmanagement

i-Alarmsysteme
Großhandel für ALARM - ViDEO - ZUTRiTT

An der Horst 10a · 40885 Ratingen
Tel.: 02102 564 900-0
Kleinmachnower Weg 5 · 14165 Berlin
Tel.: 030 700 142 77-0
vertrieb@i-alarmsysteme.com
www.i-alarmsysteme.com
Alarmsysteme Funk und verdrahtet, Gefahrenmelder, Videoüberwachungs- und Zutrittssysteme.

Gebäudesicherheit

DOM

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-group.eu
Mechanische und digitale Schließsysteme

Gebäudesicherheit

wurster
Ideen in Blech

Walter Wurster GmbH
Heckenrosenstraße 38-40
70771 Leinfelden-Echterdingen
Tel.: 0711/949 62-0 · kontakt@wurster-online.de
www.wurster-online.de · www.ideeninblech.de
Geldübergabeschalter feuerbeständig bis F90 und beschusshemmend bis FB7, Durchreichen für Geld, Wertsachen und Dokumente, Hochsicherheits-Durchreichen, Bankschalter, Nachtschalter, Tankstellenschalter, Apothekenschalter, Ticketschalter für Sport- und Kulturstätten

Alarmmanagement

SCHNEIDER INTERCOM
Kommunikations- und Sicherheitssysteme

SCHNEIDER INTERCOM GmbH
Heinrich-Hertz-Str. 40 · D-40699 Erkrath
Tel.: 0211/88 28 53 33 · Fax: 0211/88 28 52 32
info@schneider-intercom.de
www.schneider-intercom.de
Schul-Notruf-Sprechstellen, Sprech- und Gegensprechanlagen, JVA-Kommunikation, Parkhaus-Kommunikation, Tunnel-Kommunikation, Intercom-Technik, Industrie-Sprechstellen

Gebäudesicherheit

EFAFLEX
schnelle und sichere Tore

EFAFLEX Tor- und Sicherheitssysteme GmbH & Co. KG
Fliederstraße 14 · 84079 Bruckberg
Tel. 08765 82-0 · Fax 08765 82-200
info@efaflex.com · www.efaflex.com
Schnelllauftore, Rolltore, Falttore, Industrietore, Hallentore.

PERIMETER SCHUTZ

Alarmmanagement

TAS
SICHERHEITS- UND KOMMUNIKATIONSTECHNIK

TAS
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
Fertigung und Entwicklung von Alarmübertragungstechnik, Alarmierungs- und Konferenzsystemen.

Gebäudesicherheit

euromicron
Deutschland GmbH

euromicron Deutschland GmbH
Siemensstraße 6 · 63263 Neu-Isenburg
Tel.: +49 6102 8222-0
info@euromicron-deutschland.de
www.euromicron-deutschland.de
Brandschutz, Gebäudemanagement, Kommunikation, Netzwerktechnik, IT-Sicherheit, Videoüberwachung

Perimeterschutz

LASE
PeCo Systemtechnik GmbH

LASE PeCo Systemtechnik GmbH
Rudolf-Diesel-Str. 111 · 46485 Wesel
Tel. +49(0)281/95990-0 · Fax +49(0)281/95990-111
sicherheit@lase.de · www.lase-systemtechnik.de
Freiflächen-, Objekt- und Dachüberwachung mittels Laserscanner und Dome-Kamera, Laserüberwachung, Videoüberwachung, Laser Tracking System LTS 400, 5-Echo-Technology

Perimeterschutz

... ein echter LEGI

LEGI GmbH
Im Meerfeld 83–89 · 47445 Moers
Tel. 02841/789-0 · Fax 02841/789-10
post@legi.de · www.legi.de
TÜV-geprüfte Zaunsysteme, kompatibel mit allen Überwachungssystemen, Sicherheitstore, Modulare Schiebtortechnik, Absturzsicherung Schrankensysteme, Drehkreuzanlagen, Projektplanung und -unterstützung

Videoüberwachung

CBC GROUP

CBC (Europe) GmbH
Hansaallee 191 · D-40549 Düsseldorf
Tel. +49(0)211/530670 · Fax +49(0)211/53067180
info@cbc-europe.com · www.cbc-europe.com
Videoüberwachungskomponenten; u.a. Kameras, Objektive, Monitore, Übertragungstechnologien, DVR, NVR.

Videoüberwachung

EIZO

EIZO Europe GmbH
Helmut-Grashoff-Str. 18
41179 Mönchengladbach
Tel.: +49 2161 8210 0
info@eizo.de · www.eizo.de
Professionelle Monitore für den 24/7-Einsatz in der Videoüberwachung, IP-Decoder-Monitore für den computerlosen Anschluss an IP-Kameras.

Perimeterschutz

SENSTAR

Senstar GmbH
An der Bleicherei 15 · D-88214 Ravensburg
Tel +49 751 76 96 24-0
info@senstar.de · www.senstar.de
Freigeländeüberwachung, Zaunmeldesysteme, Bodendetektionssysteme, Alarmmanagement-systeme, Planungsunterstützung, Beratung, Inbetriebnahme, Service

Videoüberwachung

alhua TECHNOLOGY

Dahua Technology GmbH
Monschauer Straße 1 · 40549 Düsseldorf
Tel: +49 1514 0418815
sales.de@global.dahuatech.com
www.dahuasecurity.com/de
IP-Produkte, HDCVI Produkte, Intelligente Gebäude, Machine Vision, Übertragungen & Display

Videoüberwachung

eps
Weil jede Sekunde zählt.

EPS Vertriebs GmbH
Lütke Feld 9 · 48329 Havixbeck
Tel.: 02507/98750-0 · Fax: 02507/98750-29
info@eps-vertrieb.de · www.eps-vertrieb.de
Brandschutz und sicherheitstechnische Produkte. Systemlieferant für Alarm, Brand und Video.

VIDEO ÜBERWACHUNG

Videoüberwachung

Dallmeier

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

Videoüberwachung

eyevis

eyevis GmbH
Hundsschleestr. 23 · D-72766 Reutlingen
Tel. +49(0)7121/43303-0 · Fax +49(0)7121/43303-22
info@eyevis.de · www.eyevis.de
Großbildlösungen aus einer Hand. Hersteller von DLP® Cubes, LCD Monitoren, Split-Controllern und Management-Software für Videowände in Kontrollräumen und Leitwarten.

Videoüberwachung

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 Privat-anwendern spezialisiert.

Videoüberwachung

DEKOM
VIDEO SECURITY & NETWORK GMBH

Ihr zuverlässiger Partner für professionelle Videoüberwachung

DEKOM Video Security & Network GmbH
Hoheluftchaussee 108 • 20253 Hamburg
Tel. +49 (0) 40 47 11 213-0 • info@dekom-security.de
Member of Dallmeier
www.dekom-security.de • www.dekom-security.at

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 Video-managementsoftware (VMS).

Videoüberwachung

AXIS COMMUNICATIONS

Axis Communications GmbH
Adalperostraße 86 · 85737 Ismaning
Tel. +49 (0)89/35 88 17 0 · Fax +49 (0)89/35 88 17 269
info-de@axis.com · www.axis.com
Netzwerk-Sicherheitslösungen: Axis ist Marktführer im Bereich Netzwerk-Video und bietet intelligente Sicherheitslösungen.

Videoüberwachung

digivod

digivod gmbh
Breite Straße 10, 40670 Meerbusch
Tel. +49 21 59/52 00–0 · Fax. +49 21 59/52 00–52
info@digivod.de · www.digivod.de
Videomanagement Software der Königsklasse. Flexibel für jeden Bedarf. Komplettsysteme und attraktive Bundle-Angebote. Lokaler Support!

Videoüberwachung

xtralis Honeywell
Xtralis is now a part of Honeywell

HeiTel Digital Video GmbH
Xtralis Headquarter D-A-CH
Hamburger Chaussee 339–345 · D-24113 Kiel
Tel.: + 49 431 23284-1 · Fax. + 49 431 23284-400
info@heitel.com · www.heitel.com
Videobasierte Sicherheitssysteme, Videoalarmüber-tragung, Leitstellenlösungen, Brandfrüherkennung

Videoüberwachung

BALTER
STAY AHEAD

Balter GmbH
Elisabeth-Selbert-Str. 19 · D-40764 Langenfeld
Tel.: +49(0)211-22975915 · Fax: +49(0)211-22975927
info@balter.de · www.balter.de
Hersteller und Distributor von hochwertigen IP- und Analog HD-Videoüberwachungssystemen, Video-Türsprechanlagen, Alarmanlagen und Smart Home Systemen.

Videoüberwachung

EFB ELEKTRONIK

EFB-Elektronik GmbH
Striegauer Str. 1 · 33719 Bielefeld
Tel. +49(0)521/40418-0 · Fax +49(0)521/40418-50
info@efb-security.de · www.efb-security.de
Spezialist für innovative und professionelle IP-Videoüberwachung und Einbruchmeldetechnik für Anforderungen von kleinen bis hin zu hohen Risikobereichen. Ebenso Hersteller und System-anbieter für die strukturierte Gebäudeinfrastruktur.

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

Videoüberwachung

Kucera

H. & H. Kucera GbR
Altziegelhaus 1 · D-74731 Walldürn
Tel.: +49 (0) 6282/92140 · Fax: +49 (0) 6282/921425
info@Kucera.de · www.Kucera.de
Distributor für Videotec, Watec, Dahua, Bpt / Came und weitere Marken.

Videoüberwachung

VICON

Vicon Deutschland GmbH
Gutenbergstraße 1 · 23611 Bad Schwartau
Tel. 0451/81189027 · Fax 0451/1602029
desales@vicon-security.com · www.vicon-security.de
Vicon zählt zu den weltweit führenden, unabhängigen Herstellern und Komplettanbietern im Bereich IP basierter Videosicherheitslösungen.

Zeit + Zutritt

Gantner technologies

GANTNER Electronic GmbH
Montafonerstraße 8 · A-6780 Schruns
Tel. +43 5556 73784-542
Fax +43 5556 73784-8000
info@gantner.com · www.gantner.com
Systemlösungen in Zutrittskontrolle/Biometrie, Zeiterfassung, Betriebsdatenerfassung, Schließsysteme, Zugriffsschutz, Schrankschließsysteme

Videoüberwachung

lunaHD
High Definition Video
www.luna-hd.de

ZEIT ZUTRITT

Zeit + Zutritt

intrakey

IntraKey technologies AG
Wiener Str. 114-116 · 01219 Dresden
Tel. 0351/31558-0 · Fax 0351/31558-129
info@intrakey.de · www.intrakey.de
Zutrittskontrolle online und offline, Schrankschlosssysteme, Raumvergabe, Zeiterfassung, Dienstplanung, Fuhrparkmanagement

Videoüberwachung

Security-Vision-Systems
MOBOTIX

MOBOTIX AG
Security-Vision-Systems
Kaiserstraße · D-67722 Langmeil
Tel. +49 (0) 6302/9816-0 · Fax +49 (0) 6302/9816-190
info@mobotix.com · www.mobotix.com
HiRes-Video-Komplettlösungen – hochauflösend, digital & kosteneffizient aufzeichnen

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

ISGUS

ISGUS GmbH
Oberdorfstr. 18–22
78054 Villingen-Schwenningen
Tel. 07720/393-0 · 07720/393-184
info@isgus.de · www.isgus.de
Betriebsdatenerfassung, Personaleinsatzplanung, Zeiterfassung, Zutrittskontrolle

Videoüberwachung

MONACOR INTERNATIONAL

MONACOR INTERNATIONAL
Zum Falsch 36 · 28307 Bremen
Tel. 0421/4865-0 · Fax 0421/488415
info@monacor.de · www.monacor.com
Videoüberwachungskomponenten und -systeme

Zeit + Zutritt

cryptins
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

pcs

PCS Systemtechnik GmbH
Pfälzer-Wald-Straße 36 · 81539 München
Tel. 089/68004-550 · Fax 089/68004-555
intus@pcs.com · www.pcs.com
Zeiterfassung, Zutrittskontrolle, BDE/MDE, Biometrie, Video, SAP, Handvenenerkennung

Videoüberwachung

BURG WÄCHTER
SANTEC

SANTEC BW AG
An der Strusbek 31 ▪ 22926 Ahrensburg ▪ Germany
Tel. +49 4102 4798 0 ▪ Fax +49 4102 4798 10
santec_info@burg.biz ▪ www.santec-video.com
Videoüberwachung ▪ Netzwerktechnik
IR-Freilandsensorik ▪ Dienstleistungen

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

phg
Die richtige Verbindung

phg Peter Hengstler GmbH + Co. KG
Dauchinger Str. 12 · D-78652 Deißlingen
Tel. +49(0)7420/89-0 · Fax +49(0)7420/89-59
datentechnik@phg.de · www.phg.de
RFID-Komponenten für Zutrittskontrolle, Zeiterfassung, BDE, Kantinendaten, Freizeitapplikationen, Aufputzgeräte, Einbaumodule, Biometrie, Identifikationsmedien und Zubehör

Videoüberwachung

SeeTec
An OnSSI Company

SeeTec GmbH
Werner-von-Siemens-Str. 2–6 · 76646 Bruchsal
Tel. +49 (0) 7251 9290-0 · Fax +49 (0) 7251/9290-815
info@seetec.de · www.seetec.de
Führender Anbieter von Video Management Software; Software-Lösungen für Sicherheitsanwendungen; zusätzliche branchenspezifische Lösungen in Bereichen Transport & Logistik, Handel, Finanzen sowie kritische Infrastruktur & Städte; basierend auf dem Systemkonzept der Multi Solution Platform, Erweiterungsmöglichkeiten und Schnittstellen zu Drittsystemen.

Zeit + Zutritt

FEIG ELECTRONIC

FEIG ELECTRONIC GMBH
Lange Straße 4 · 35781 Weilburg
Tel. 06471/3109-0 · Fax 06471/3109-99
obid@feig.de · www.feig.de
Elektronische Schließsysteme, Güteridentifizierung Zutritts-und Zufahrtskontrolle

Zeit + Zutritt

primion group
Digitek · GET · OPERTIS · primion

primion Technology AG
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

BRAND SCHUTZ

Zeit + Zutritt

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

Brandschutz

Prymos GmbH
Siemensstraße 18 · 63225 Langen
Tel. 06103/4409430 · Fax 06103/4409439
info@prymos.com · www.prymos.com
Prymos Kombi-Brandschutz: Die neuartige Kombination von einfach bedienbaren, komfortablen sowie wirtschaftlichen Feuerlöschsystemen; mehr Sicherheit für Ihre Mitarbeiter und Ihr Unternehmen.

Zeit + Zutritt

SECURITY DATA GmbH
Ihr Unternehmen für Daten-Sicherheitskommunikation.
Mercedesstr. 18 · 71384 Weinstadt
Tel. +49(0)7151/994050 · Fax +49(0)7151/994052
info@security-data.de · www.security-data.de
Ausweissysteme, 3-dimensionale Zutrittskontrolle, Zufahrtskontrolle, Zeiterfassung, Fluchtwegsteuerung, CCTV Systeme, Schlüsselmanagement, Integrale Sicherheitstechnik

Brandschutz

Ei Electronics GmbH
Franz-Rennefeld-Weg 5 · 40472 Düsseldorf
Tel. +49 (0)211 984 365 00 · Fax +49 (0)211 984 365 28
vertrieb@eielectronics.de · www.eielectronics.de
Rauchwarnmelder, Hitzewarnmelder, Kohlenmonoxidwarnmelder, funkvernetzte Warnmeldersysteme, Koppelmodule, Hörgeschädigtenmodule, Fernbedienungen, AudioLINK

Brandschutz

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

Brandschutz

EPS Vertriebs GmbH
Lütke Feld 9 · 48329 Havixbeck
Tel.: 02507/98750-0 · Fax: 02507/98750-29
info@eps-vertrieb.de · www.eps-vertrieb.de
Brandschutz und sicherheitstechnische Produkte. Systemlieferant für Alarm, Brand und Video.

Brandschutz

WAGNER Group GmbH
Schleswigstraße 1-5 · 30853 Langenhagen
Tel. 0511/97383-0 · Fax 0511/97383-140
info@wagnergroup.com · www.wagnergroup.com
Planung, Projektierung, Anlagenbau, Instandhaltung für: Brandmelde- und Löschtechnik, Brandfrüherkennung, Brandvermeidung, Brandschutz für Serverschränke, Gefahrenmanagement

NOTRUF SERVICE LEITSTELLE

Brandschutz

Novar GmbH a Honeywell Company

Dieselstraße 2 · D-41469 Neuss
Tel.: +49(0)2131/40615-600
FAX: +49(0)2131/40615-606
info@esser-systems.com · www.esser-systems.com
Brandmeldesysteme, Sprachalarmierung, Notbeleuchtung, Sicherheitsmanagement

GASMESS TECHNIK

Notruf- und Service-Leitstelle

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

Brandschutz

Hekatron Vertriebs GmbH
Brühlmatten 9 · 79295 Sulzburg
Tel. 07634/500-0 · Fax 07634/6419
info@hekatron.de · www.hekatron.de
Brandmeldesysteme, Rauchschaltanlagen, Rauchwarnmelder, Sicherheitsleitsysteme

Gasmesstechnik

GfG Gesellschaft für Gerätebau mbH
Klönnestraße 99 · D-44143 Dortmund
Tel. +49 (0)231/ 564000 · Fax +49 (0)231/ 516313
info@gfg-mbh.com · www.gasmessung.de
Gaswarntechnik, Sensoren, tragbare und stationäre Gasmesstechnik

Notruf- und Service-Leitstelle

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

Brandschutz

Kidde Deutschland GmbH
Halskestraße 38 · 40880 Ratingen
Tel. +49/(0)2102/5790-0 · Fax +49/(0)2102/5790-109
info@kidde.de · www.kidde.de
Brandmelde- und Löschtechnik, Brandvermeidung, Brandfrüherkennung, Feuerschutz für System- und Datenschränke

ARBEITS SICHERHEIT

Maschinen + Anlagen

PEPPERL+FUCHS

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

Gefahrstoffmanagement

SÄBU
BAUEN MIT SYSTEM

SÄBU Morsbach GmbH
Zum Systembau 1 · 51597 Morsbach
Tel. +49 (0)2294 694-23 · Fax +49(0)2294 694 6623
safe@saebu.de · www.saebu.de
Gefahrstofflagerung, Arbeits- + Umweltschutz, Auffangwannen, Fassregale, Regalcontainer, Brandschutz- Schränke + Container, Gasflaschenlagerung

Arbeitssicherheit

Ansell

Ansell GmbH
Stadtquartier Riem Arcaden
Lehrer-Wirth-Str. 4 · D-81829 München
Tel. +49 89 45118 0 · Fax +49 89 45118 140
info@anselleurope.com · www.ansell.eu
Ansell ist weltweit führender Anbieter von Schutzhandschuhen für alle Industriezweige, einschließlich Automobil-, Metall-, Pharma- und Lebensmittelindustrie

Maschinen + Anlagen

SSP
Safety System Products

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.

UNTER BRECHUNGSFREIE STROMVERSORGUNG

MASCHINEN ANLAGEN SICHERHEIT

Maschinen + Anlagen

.steute

steute Schaltgeräte GmbH & Co. KG
Brückenstr. 91 · 32584 Löhne
Tel. 05731/745-0 · Fax 05731/745-200
info@steute.de · www.steute.de
Hersteller von Sicherheits-, Sicherheits-Scharnier-, Seilzug-Notschaltern, Schaltgeräten mit Funktechnologie, Fuß-, Positions-, Bandschieflauf/Schlaffseil- & Türgriffschaltern, Magnetsendoren, Ex-Schaltgeräten & Stelleinrichtungen für die Medizintechnik

Unterbrechungsfreie Stromversorgung

SLAT
for safer buildings

SLAT GmbH
Leitzstraße 45 · 70469 Stuttgart
Tel.: 0711 89989 008 · Fax: 0711 89989 090
www.slat.com · info@slat-gmbh.de
DC-USVs nach DIN EN 54-4/A2 + DIN EN 12 101-10 (BMT, SAA, ELA), nach DIN EN 50131-6/3 + VdS 2115 (ZKT, EMT)
DC-Mikro-USVs m. integr. Li-Backup: Video, Zutritt, Übertragungs- u. Netzwerktechnik, Gebäudeleittechnik, Smart Metering, Medizin. Systeme, In- u. Outdoorbereich.

Maschinen + Anlagen

EUCHNER
More than safety.

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

GEFAHRSTOFF MANAGEMENT

Maschinen + Anlagen

SCHMERSAL
Safe solutions for your industry

K.A. Schmersal GmbH & Co. KG
Möddinghofe 30 · 42279 Wuppertal
Tel. 0202/6474-0 · Fax: 0202/6474-100
info@schmersal.com · www.schmersal.com
Sicherheitsschalter mit Personenschutzfunktion, Berührungslos wirkende Sicherheitsschalter, Sicherheitszuhaltungen, Sicherheits-Compact-Steuerung PROTECT SRB, Positionsschalter

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- und Arbeitsschutz, Sicherheitsschränke, Chemikalien- und Umluftschränke, Druckgasflaschenschränke, Gefahrstoffarbeitsplätze, Absauganlagen, Raumluftreiniger uvm.

Maschinen + Anlagen

Leuze electronic
the sensor people

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.de · www.leuze.com
Optoelektronische Sensoren, Identifikations- und Datenübertragungssysteme, Distanzmessung, Sicherheits-Sensoren, Sicherheits-Systeme, Sicherheits-Dienstleistungen

Gefahrstoffmanagement

BAUER SÜDLOHN

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

DIE VIP COUCH

Prof. Dr. Udo Weis

Vorstand Ressort Finanzen VDSI – Verband für Sicherheit, Gesundheit und Umweltschutz bei der Arbeit e.V.

- Udo Weis (Jahrgang. 1962), verheiratet, zwei Kinder, wohnt in Plankstadt bei Heidelberg.
- Dr. rer. nat., Dipl.-Chemiker, MBA und Professor für Wirtschafts-ingenieurwesen;
- Leiter Steinbeis Institut für International Business and Risk Management, Vorstand Inspire Forschung Netzwerk, Geschäftsführer IFNEK, verschiedene Lehraufträge an Hochschulen;
- Experte für Sicherheit, Gesundheit und Umweltschutz, Risikomanagement und Resilienz von Organisationen.

Menschen machen Märkte
in jeder Ausgabe Ihrer GIT SICHERHEIT bitten wir wichtige Personen, Entscheider, Menschen aus der Sicherheitsbranche auf unserer VIP-Couch Platz zu nehmen.

Ihr Berufswunsch mit 20 war:
Mir war klar – irgendetwas mit Naturwissenschaft. Mit Mathematik kann man kein Geld verdienen, Biologie war mir zu unspezifisch, Physiker kannte ich nicht, aber von der Chemischen Industrie hatte ich schon gehört – also entschied ich mich für Chemie.

Was hat Sie dazu bewogen, eine Aufgabe im Bereich Sicherheit zu übernehmen?
Mein Start ins Berufsleben. Ich arbeitete in einer mittelständischen Firma, die Arbeits- und Umweltschutz einführen musste – meine erste Aufgabe. Das war sehr kaltes Wasser, und ich lernte sehr gut schwimmen.

Welche sicherheitspolitische Entscheidung oder welches Projekt sollte Ihrer Meinung nach schon längst umgesetzt sein?
Die tatsächliche Erfassung aller Arbeitnehmer und Arbeitgeber, um einen Zugang zu Beratung für Sicherheit, Gesundheit und Umweltschutz zu erhalten.

Ein Erfolg, den Sie kürzlich errungen haben, war:
Alles natürlich im Team, aber nach mehr als zehn Jahren die Etablierung der Norm für Risikomanagement (ISO 31000) im deutschen Normungssystem. Für mich als Obmann (Vorsitzender) des DIN-Normungsausschusses eine Belohnung für viel Arbeit.

Welche Reform bewundern Sie am meisten?
Die deutsche Sozialgesetzgebung, oft unterschätzt, aber was vor über 130 Jahren begonnen wurde halte ich für die Basis der Stabilität in der Bundesrepublik. Leider wird das oft vergessen.

Wer hat Ihrer Meinung nach eine Auszeichnung verdient?
Für eine chinesische Delegation habe ich einmal das Katastrophen/Notfallmanagement in Deutschland erklärt – mir wurde bewusst, dass nahezu alles auf ehrenamtlichen Engagement basiert. Das sind daher meine Helden: Die Menschen im Ehrenamt.

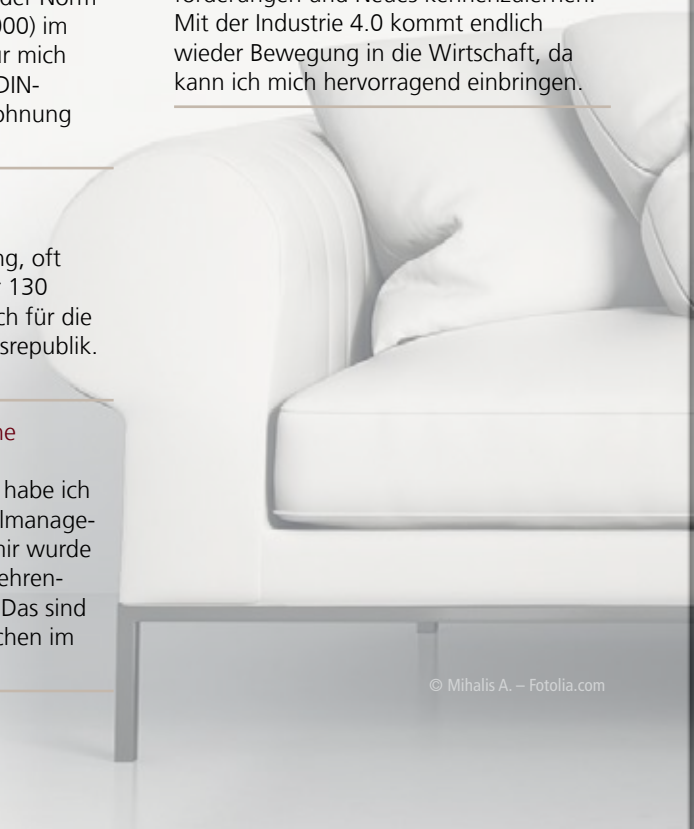
Wie würde ein guter Freund Sie charakterisieren?
An vielem (allem) interessiert, verlässlich, empathisch. So hoffe ich, dass man mich sieht.

Was motiviert Sie?
Neues zu schaffen und Dinge zu bewegen. Konstruktives Feedback.

Worüber machen Sie sich Sorgen?
Unpolitisches und unkritisches Verhalten. Mich machen Entwicklungen sehr betroffen, denn ich sehe die Gefahr, dass unpolitisches, unkritisches Verhalten zu negativen Entwicklungen führen kann.

Die beste Erfindung im Bereich Sicherheit ist Ihrer Meinung nach:
Es wäre die Sicherheitseinrichtung, die nicht manipulierbar wäre und den Menschen nicht behindern würde. Ich befasse mich allerdings mehr mit Analysemethoden für Risiken, die sind eigentlich die besten Erfindungen, da sie Ursachen oder Konsequenzen erkennen können.

Ihre gegenwärtige Geistesverfassung ist:
Freue mich auf die kommenden Herausforderungen und Neues kennenzulernen. Mit der Industrie 4.0 kommt endlich wieder Bewegung in die Wirtschaft, da kann ich mich hervorragend einbringen.



WILEY

GIT SMART HOME SECURITY

WIEDER NEU für 2018

Heft, e-Paper, Microsite und NEU als Smart Magazine

Clevere Lösungen, smarte Neuheiten in einem Cross-Media-Konzept.

GIT Smart Home Security: auch 2018 wieder als gedruckte Ausgabe, als e-Paper, als speziell auf dieses Thema zugeschnittene digitale Microsite und ganz neu als Smart Magazine – im responsiven Design. Mit den wichtigsten Informationen, Lösungen und Produkten für Eigenheime, Gewerbe, Wohnwirtschaft und KMUs.

Wenn Sie Hersteller oder Anbieter von Smart Home Security sind, dann kontaktieren Sie uns jetzt. **Werden Sie Partner und Sponsor.**

Kontakt: sophie.platzer@wiley.com

Event-Partner: light+building

Gefördert von: HEKATRON | LUPUS ELECTRONICS | SimonsVoss technologies | TELENOT

ASSA ABLOY | AXIS | CM security | DAITEM | DOM | eps | GEZE | HIKVISION | SECURITON | United Technologies

http://publikationen.git-sicherheit.de

Wir geben dem Thema Smart Home Security ein Zuhause!

GIT SICHERHEIT + MANAGEMENT
MAGAZIN FÜR SAFETY UND SECURITY

www.GIT-SICHERHEIT.de

DECKT ALLES ESSENZIELLE AB

WISENET L-Serie

Die Wisenet L-Serie Kameras mit integrierten IR-LEDs haben essenzielle Funktionen um Bilder höchster Qualität bei allen Lichtverhältnissen zu erfassen.

Erweiterte Wide-Dynamic-Range-Funktion (WDR) – erzeugt Bilder in Szenen mit hoher Helligkeit und gleichzeitig sehr dunklen Bereichen.

Die Hallway-View-Funktion ermöglicht die Überwachung enger vertikaler Bereiche wie Korridore oder Tunnel.

Die Wisenet L-Serie ist ideal für Multi-Kamera-Projekte – sie ist kostengünstig und einfach zu bedienen.

hanwha-security.eu/de

Hanwha Techwin