05-06 | 2026
technische-sicherheit.de
VDI Fachmedien



# Technische Sicherheit

Extra:
**Brandschutz**

BRANDSCHUTZ

Lithium-Ionen-Batterien sicher lagern

EXPLOSIONSSCHUTZ

Parfüms perfekt dosiert – aber sicher

INTERVIEW

Safety trifft Security: VDI Wiki vernetzt Disziplinen

VDI Fachmedien

# Jetzt Technische Sicherheit upgraden: Mit dem E-Paper-Abonnement


**Für nur 51 EUR inkl. MwSt.**

Sie wollen jederzeit und überall Zugriff auf Technische Sicherheit, die einzige unabhängige und themenübergreifende Fachzeitschrift für Sicherheits-, Prüf- und Regeltechnik, die sich betriebsübergreifend auch mit Fragen des Arbeitsschutzes und betrieblichen Umweltschutzes beschäftigt? Dann sichern Sie sich jetzt zusätzlich zu den 6 Technische Sicherheit-Printausgaben pro Jahr auch Ihr Abo-Upgrade E-Paper: 51 EUR inkl. MwSt..

**Ihre Vorteile: Downloadfunktion, Volltext-Suche, Lesezeichen, mobiloptimiertes Design, Zugriff auf das Archiv.**

**Technikwissen für Ingenieur*innen – jetzt bestellen:**

**ingenieur.de/abo-technischesicherheit**

# Wenn der Elektro-Rollstuhl im Altenheim brennt

Eine Schlagzeile in Niedersachsen vom 10. März 2026: „Elektro-Krankenfahrstuhl löst Brand im Altenheim aus“ und ein Pressebild dazu zeigt einen durch Brand zerstörten Krankenfahrstuhl. Am 26. März war im Presseportal der Feuerwehr München zu lesen: „In der Nacht auf Freitag ist es im Stadtteil Nymphenburg zum Brand eines elektrischen Rollstuhls gekommen“. Beide Brände ereigneten sich nachts und die Rollstühle befanden sich im Flur, beziehungsweise im Treppenraum. Die Auswirkungen unter anderem mit Personengefährdungen durch Brandrauch waren erheblich. Zu beiden Fällen gab es keine konkreten Informationen zur Ursache der Brandentstehung.

Unabhängig davon, ob möglicherweise die Batterien der Rollstühle ursächlich verantwortlich waren, ist die grundsätzliche Problematik des Abstellens von Krankenfahr- oder Elektro-Rollstühlen in Gebäuden, besonders in Fluren und Treppenräumen, vorhanden: Geht von den Umständen eine besondere Brandgefährdung aus und wenn ja, wie sieht dabei die Güterabwägung hinsichtlich der berechtigten Bedürfnisse von Menschen mit Behinderungen gegenüber einem erhöhten Risiko aus.

Die Brandentstehungsgefahr durch elektrische Rollstühle ist differenziert zu betrachten. Es gibt Beispiele für Brandstiftungen, Kurzschlüsse, Überhitzungen von Beleuchtungen, defekte Ladeeinrichtungen und den Brand der Batterie selbst. Bei Letzterem kann die Art der Batterien nach Alter und Fahrgerätetyp vom traditionellen Bleiakku, über die NiMH-Akkus bis zu den modernen Lithium-Ionen-Akkus mit unterschiedlichen Brandrisiken variieren.

Die Brandproblematik der Lithium-Ionen-Akkus mit hoher Ladungsdichte ist dabei ein zukünftig immer wichtigeres Thema. Denn es gibt einen verstärkten Trend zu kostengünstigen, elektrischen Rollstühlen beziehungsweise der Unterstützung von Rollstühlen mit Lithium-Ionen-Antrieben. Damit ist zu erwarten, dass deren Verwendung steigen wird. Die Akkus entsprechen denen von E-Bikes, deren Problematik durch Brände inzwischen deutlich geworden ist.

> „Das Abstellen im Nahbereich der behinderten Person kann entscheidend für diese Teilhabe sein, widerspricht aber in Teilen dem Brandschutz“

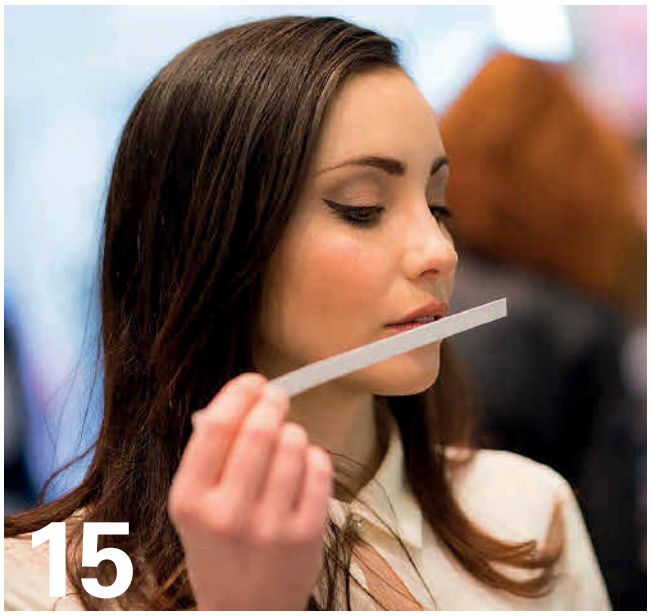
Nicht selten werden solche Fahrzeuge in Betreuungs- und Pflegeeinrichtungen, aber auch im allgemeinen Wohnungsbau, aus Platzgründen in Fluren oder auf Gemeinschaftsflächen abgestellt und auch geladen. Schaut man in diesem Zusammenhang zum Beispiel in die Information 208-047 der Deutschen gesetzlichen Unfallversicherer oder in das VFDB Merkblatt TWB 02-2005, so kommt schnell der Gedanke, solche Abstellung als erhöhte Brandgefahr zu verbieten. Auch die Landesbauordnungen einiger Bundesländer sind hier strikt.

Dies ist im Sinne der Betroffenen jedoch problematisch. Gerade Menschen mit Behinderungen und Einschränkungen sind dankbare Nutzer von Elektrounterstützung in vielfältiger Form. Restriktive Regelungen für das Abstellen und Laden von E-Bikes oder Scootern sind keinesfalls unmittelbar auf Behindertenfahrgeräte zu übertragen. So gelten zum Beispiel beim ÖPNV die Verbote der Mitnahme von Scootern nicht für Behindertenfahrgeräte. Denn die Gleichstellung von Menschen mit Behinderungen ist in Deutschland durch Artikel 3 Absatz 3 Satz 2 des Grundgesetzes (GG) verfassungsrechtlich verankert, unter anderem mit dem Ziel einer gleichberechtigten Teilnahme am öffentlichen Leben. Das Abstellen im Nahbereich der behinderten Person kann entscheidend für diese Teilhabe sein.

Brandschutzdienststellen, Feuerwehren und Betreiber von Einrichtungen stehen somit vor einem echten Dilemma. In Kenntnis der Auswirkungen von Bränden und den eingangs beschriebenen Einsatzerfahrungen ist eine Risikoerhöhung oft begründbar. Demgegenüber ist jedoch eine hohe Sensibilität gegenüber den Nutzern und anderen Bewohnern einer Wohn- oder Pflegeeinrichtung erforderlich. Pauschale, rein rechtlich basierte Lösungen treffen häufig auf Ablehnung und Unverständnis. Deshalb sind individuelle Lösungen, welche die Art des Elektro-Rollstuhls und die Umstände der Aufstellung berücksichtigen, wie zum Beispiel eine vorhandene Brandmeldeanlage oder die Situation der Flucht- und Rettungswege, erforderlich. Dies kostet Zeit, Aufwand und Verständnis. Entscheidend ist, dass Nutzer, Betreiber und Brandschützer individuelle Lösungen suchen, die das Risiko auf ein vertretbares Maß reduzieren und rechtlich zulässig sind.

**Prof. Ernst-Peter Döbbeling**
Hochschule Furtwangen
*Foto: Autor*


**Großbrandversuche mit Lithium-Ionen-Batterien.** *Foto: Fogtec*




**Die Mischung macht den Duft –** und Fricke-Dosieranlagen schaffen die Voraussetzung für das exakte Dosieren von Parfüms und Aromen im Fertigungsprozess. *Foto: Fricke*



**Diese Ausgabe enthält eine Beilage der Bundesanstalt für Arbeitsschutz**

19

**Großraumflugzeug rollt zum Start.** *Foto: smarterpix/Jaromir Chalabala*

## Rubriken




**Titelseite**

Beim Lagern von Lithium-Ionen-Batterien entstehen Gefahren, auch bei parkenden Autos an Ladesäulen. Welche Grundsätze beim Brandschutz zu beachten sind, finden sie im Heft. *Foto: smarterpix/SusPons*

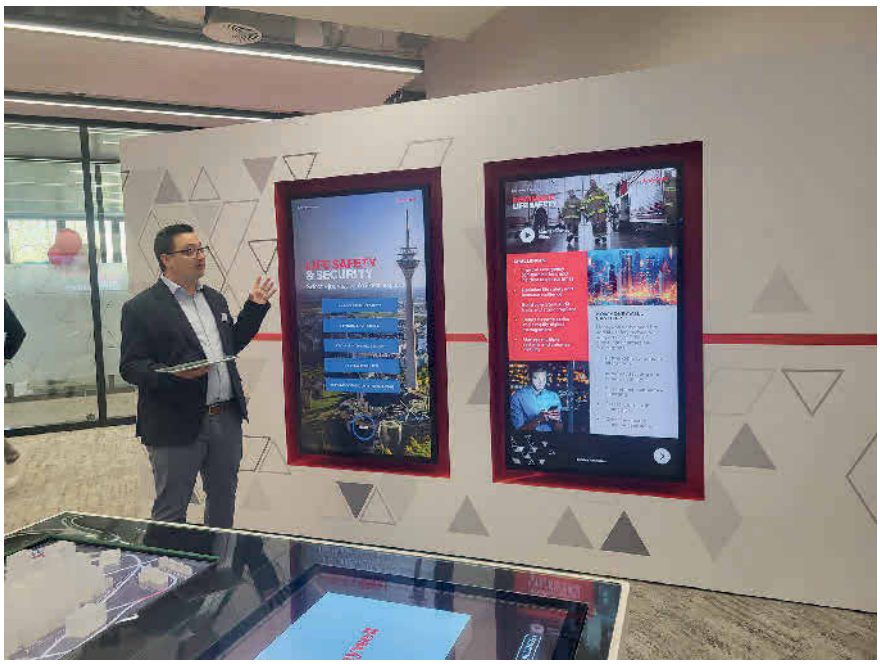
## KURZ NOTIERT

**Auf der Messe Feuertrutz gibt die Gesellschaft für innovative Bautechnologie mbH (GiB) Einblicke** in verschiedene Bereiche ihrer Arbeit – von der brandschutztechnischen Fachplanung über die Ausführungsplanung bis hin zur Fachbauleitung Brandschutz und zur Qualitätssicherung im Projektverlauf. Vorgestellt wird, wie Anforderungen aus dem Baurecht frühzeitig in die Planung eingebunden werden können und wie sich mögliche Schwachstellen schon in frühen Projektphasen erkennen lassen.

**Ein Vierteljahrhundert im Zeichen von Sichtbarkeit, Teilhabe und journalistischer Exzellenz:** Zum 25. Mal wurde am 22. April in Berlin der German Paralympic Media Award (GPMA) verliehen. Mit dem Preis würdigt die Deutsche Gesetzliche Unfallversicherung (DGUV) seit 25 Jahren herausragende Berichterstattung über den Breiten-, Rehabilitations- und Leistungssport von Menschen mit Behinderung. Zu den Gästen der feierlichen Verleihung zählten unter anderem die Bundesministerin für Arbeit und Soziales, Bärbel Bas, sowie Hans-Jörg Michels, Präsident des Deutschen Behindertensportverbands und Nationalen Paralympischen Komitees. Darüber hinaus nahmen zahlreiche Abgeordnete des Deutschen Bundestages sowie hochrangige Vertreterinnen und Vertreter aus Sport, Wirtschaft, Medien und Verbänden teil.

**Mit dem BORDO™ 6200K/120 erweitert der Sicherheitsexperte** ABUS seine hochsichere Faltschlossfamilie um eine neue, besonders lange Variante. Die neue Version des vielfach bewährten BORDO 6200K bietet mit einer Länge von 120 cm einen effektiven Schließumfang von circa 125 cm – ideal für Nutzer, die ihr Fahrrad noch vielseitiger sichern oder mehrere Räder miteinander verbinden möchten.

# Honeywell eröffnet neues Costumer Experience Center




**Alan Lang**, Senior Marketing Leader bei Honeywell, leitete die Tour durch das neue Customer Experience Centre in Ratingen. *Foto: A. Hilse*

Honeywell hat in Ratingen ein neues Customer Experience Center für vernetzte Gebäudetechnologien eröffnet. Dort zeigt das Unternehmen, wie Automatisierung und Physical AI die Leistungsfähigkeit und Effizienz des Gebäudebestands in Deutschland verbessern können. Das Zentrum dient als europäische Plattform für Innovation und Zusammenarbeit rund um Gebäudetechnologien in unterschiedlichen Branchen. Besucher erhalten Einblicke, wie digitale Lösungen und automatisierte Prozesse den Betrieb von Gebäudeportfolios optimieren können – etwa durch vorausschauende Wartung oder intelligentes Energiemanagement.

Mit dem neuen Customer Experience Center adressiert Honeywell zentrale Herausforderungen im Gebäudebetrieb: von heterogenen Infrastrukturen, wechselnden Nutzungs- und Sicherheitsanforderungen bis hin zu zunehmend strengeren Vorgaben im ökologischen und Umweltbereich. Vorgestellt werden Technologien, die Unternehmen dabei helfen, regulatorische Vorgaben einzuordnen und neue operative Effizienzpotenziale in Gebäuden verschiedenster Branchen zu erschließen.

„Der starke Fokus auf Energieeffizienz und die Modernisierung des Gebäudebestands macht Deutschland zu einem zentralen Markt für unsere europäischen Aktivitäten. Mit dieser Investition bekräftigen wir unser Engagement, Kunden in Deutschland und ganz Europa vernetzte Technologien bereitzustellen, die ihre Betriebsabläufe im Einklang mit diesen Prioritäten transformieren können“, so Achim Keifert, Chief Commercial Officer Europe bei Honeywell Building Automation. „Im neuen Customer Experience Center erleben Kunden unmittelbar, wie diese Systeme dabei helfen, die komplexen und individuellen Herausforderungen zu adressieren, vor denen sie stehen – mit dem Ziel, Leistung, Energieeffizienz und Sicherheit ihrer Gebäude weiter zu steigern.“

Honeywells Geschichte in Deutschland reicht bis ins Jahr 1848 zurück – unter anderem durch die Integration etablierter Marken wie Elster GmbH, Saia Burgess Controls und ESSER. Das Unternehmen versteht sich als strategischer Partner auf dem Weg zur industriellen Automatisierung in Deutschland und bietet umfassende Technologien und Services, um Kunden in unterschiedlichen Branchen – einschließlich kritischer Gebäudeinfrastrukturen – bei der Transformation hin zu KI-gestützten, autonomen Systemen zu unterstützen.

*www.honeywell.com*

# TÜV veröffentlicht Leitfaden für sicheren Umgang mit verunfallten Hochvoltbatterien

*Foto: TÜV-Verband/iStock*

Mit der steigenden Zahl von Elektrofahrzeugen wächst die Bedeutung eines sicheren Umgangs mit Hochvoltbatterien, die bei einem Unfall beschädigt worden sind. Der TÜV-Verband hat hierzu einen Leitfaden veröffentlicht, der Sachverständigen und Gutachtern eine praxisnahe Orientierung für die Bewertung solcher Batterien bietet. Ein zentraler Bestandteil des Whitepapers ist die sicherheitstechnische Bewertung von Unfallbatterien. Neben offensichtlichen Schäden müssen auch versteckte Risiken identifiziert werden – etwa interne Kurzschlüsse oder thermische Instabilitäten, die erst zeitverzögert zu gefährlichen Situationen führen können. Bei der Untersuchung kommen spezialisierte Prüfverfahren zum Einsatz, etwa die Messung des Isolationswiderstands, thermografische Analysen oder die Auswertung von Fahrzeugdaten. Diese ermöglichen es, kritische Zustände wie Überhitzung, Zellschäden oder elektrische Fehler zu identifizieren und geeignete Maßnahmen abzuleiten. Darüber hinaus sind Transportvorschriften und Lagerbedingungen für Unfallfahrzeuge zu beachten, um Risiken für Einsatzkräfte, Werkstattpersonal und Umwelt zu minimieren. Ob sich eine Instandsetzung lohnt, hängt neben der Art der Reparatur unter anderem vom Gesundheitszustand der Batterie, dem sogenannten „State of Health", und dem Fahrzeugwert zum Zeitpunkt der Untersuchung ab. Das Whitepaper „Bewertung verunfallter Hochvoltbatterien in Elektrofahrzeugen" ist beim TÜV-Verband abrufbar. *www.tuev-verband.de*

# Zertifizierung und Prüfung unter einem Dach

Die VdS Schadenverhütung GmbH, eine nach ISO 17065 akkreditierte Zertifizierungsstelle, und das Baltic Fire Laboratory (BFL), eine nach ISO/IEC 17025 akkreditierte Prüfstelle für Brandschutzsysteme mit Sitz in Tuchom, Polen, haben eine strategische Kooperation geschlossen. Künftig profitieren Hersteller von einem nahtlos integrierten End-to-End-Prozess von brandtechnischen Prüfungen bis hin zur Produktzertifizierung. Die Kooperation vernetzt zwei sich ideal ergänzende Kompetenzbereiche – die umfassenden Brandversuchskapazitäten des BFL sowie VdS als international anerkannte Zertifizierungsstelle. Daraus entsteht ein einzigartiges, leistungsstarkes Angebot für Hersteller von Wassernebel- und Feuerlöschanlagen, die eine Marktzulassung in Europa und weltweit anstreben. Im Rahmen seines ISO-17025-Akkreditierungsumfangs bietet das BFL mehr als 80 akkreditierte Prüfverfahren für Feuerlöschprodukte an und liefert präzise, reproduzierbare und international anerkannte Brandversuchsergebnisse. VdS nutzt im Rahmen seiner ISO-17065-Akkreditierung diese Ergebnisse, prüft zusätzliche Produkt- und Systemanforderungen und stellt Produktzertifizierungen aus. Diese wiederum ermöglichen den Zugang zu Märkten, Versicherern und zuständigen Behörden weltweit.
*www.vds.de*

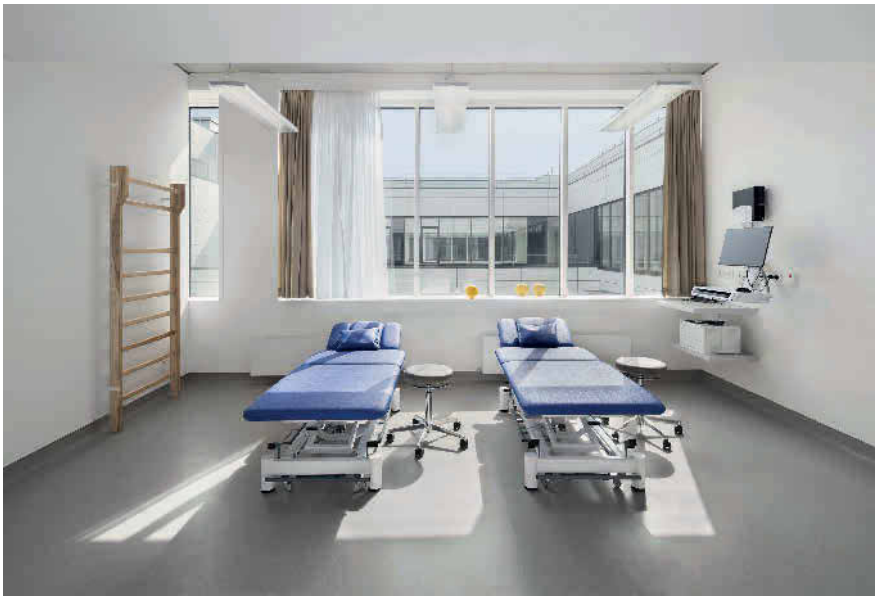
Peter Schramm, Geschäftsführer von VdS (l.), Bogdan Racięga, Direktor des Baltic Fire Laboratory (Mitte). *Foto: Vds*

# Kostenlose Hotline für kleine Holz- und Metallbetriebe

Welche arbeitsmedizinische Vorsorge muss ich meinen Beschäftigten anbieten? Wie viele Ersthelfer brauche ich in meinem Betrieb? Was muss ich beachten, wenn ich eine ältere Maschine sicher weiterbetreiben möchte? Auf solche und weitere allgemeine Fragen zu Arbeitsschutz und Arbeitsmedizin erhalten Arbeitsschutzverantwortliche aus Betrieben mit bis zu 50 Beschäftigten bei der Kompetenzzentren-Hotline (KPZ-Hotline) der Berufsgenossenschaft Holz und Metall (BGHM) Antworten. Die KPZ-Hotline ist unter der kostenfreien Telefonnummer 0800–9990080 montags bis freitags von 8 bis 18 Uhr erreichbar. Besetzt ist sie mit Arbeitsschutz-Fachleuten eines externen Dienstleisters, die in allgemeinen arbeitsmedizinischen oder sicherheitstechnischen Fragen beraten. Außerhalb der Service-Zeiten können Anruferinnen und Anrufer eine Nachricht auf dem Anrufbeantworter hinterlassen und um Rückruf bitten. „Die KPZ-Hotline ist ein Unterstützungsangebot der BGHM bei allgemeinen Arbeitsschutz-Fragen, die sich in kleineren Betrieben ergeben", sagt Boris Seipp, Fachreferent für Grundsatzfragen des Arbeitsschutzes bei der BGHM. Die BGHM weist darauf hin, dass die Fachleute am anderen Ende der Leitung keine unternehmensspezifischen Fragen beantworten können, da sie die Verhältnisse im Betrieb nicht kennen. Auch eine notwendige arbeitsmedizinische oder sicherheitstechnische Betreuung insbesondere vor Ort kann die Hotline nicht ersetzen. Für unternehmensspezifische Themen und Fragen ist die für den jeweiligen Betrieb zuständige Aufsichtsperson ansprechbar. Die BGHM stellt die KPZ-Hotline zunächst für einen Testzeitraum bis 31. Dezember 2026 zur Verfügung. Sie erhält keine Auskunft darüber, aus welchen Betrieben welche Fragen gestellt wurden. Anfang 2027 wird es eine Befragung geben, bei der die Anruferinnen und Anrufer Gelegenheit haben, ihre Erfahrungen mit der Hotline mitzuteilen.
*www.bghm.de*

# Brandschutzglas in Krankenhäusern

Medizinische Einrichtungen sind heute mehr als nur Zweckbauten: Ganzheitliche Konzepte tragen zur Förderung des Wohlbefindens der Patient:innen bei. Dabei spielt der Baustoff Glas eine wichtige Rolle, um eine heilungsfördernde Umgebung zu schaffen. In kritischen Bereichen wie Fluren von Intensivstationen, Notausgängen oder stark frequentierten Stationen reicht normales Glas nicht aus. Hier bietet eine Brandschutzverglasung den nötigen Schutz, indem sie Feuerbeständigkeit gewährleistet, ohne Hygiene oder Design zu beeinträchtigen. Die glatte Glasoberfläche erleichtert die Reinigung und sorgt für hohe Hygienestandards, vor allem im Hinblick auf die gefürchteten Krankenhauskeime MRSA, während der Blick ins Freie und das Tageslicht Stress reduzieren und die Genesung fördern. In Kombination mit speziellen Beschichtungen bietet Glas zudem wirksame Akustiklösungen und Privatsphäre und erfüllt so sowohl funktionale als auch komfortbezogene Anforderungen in Gesundheitseinrichtungen. Alarme, Sprinkleranlagen und Rauchmelder sind unverzichtbare Bestandteile der aktiven Brandbekämpfung. Wirklich wirksam werden sie jedoch nur, wenn sie von passiven Schutzsystemen wie feuerbeständigen Wänden, Trennwänden und Verglasungen unterstützt werden. Typische Anwendungsbereiche von Brandschutzglas sind Flure, Rettungswege, Türen und Trennwände (als Abschluss von Brandabschnitten), Operationssäle, Intensivstationen, Aufzugsschächte, Treppenhäuser und Krankenhausfoyers und vieles mehr. In Bereichen wie Fluren von Intensivstationen, Treppenhäusern, Aufzugslobbys oder Schutzbereichen bildet der passive Brandschutz die erste Verteidigungslinie. Feuerbeständige Verglasungen helfen, Rauch und Flammen einzudämmen, verschaffen Patient:innen, Personal und Besucher:innen mehr Zeit zur sicheren Evakuierung und verhindern, dass sich das Feuer auf andere Bereiche ausbreitet.



Die Atmosphäre in den Patientenzimmern des Interdisziplinären Tumorzentrums ITZ in Freiburg soll heilungsfördernd wirken. Für einen sicheren und geschützten Rahmen sorgt unter anderem die leistungsfähige Brandschutzverglasung CONTRAFLAM. *Foto: Werner Huthmacher*

Bestimmte Stationen im Krankenhaus bergen besonders hohe Risiken. Dazu gehören beispielsweise Intensivstationen, Operationssäle und Aufwachräume. Patient:innen in diesen Bereichen sind häufig nicht mobil und können nicht schnell evakuiert werden. Im Brandfall kann jede Verzögerung bei der Evakuierung lebensbedrohliche Folgen haben. Brandschutzglaslösungen unterstützen das Personal dabei, die Evakuierung kontrolliert und sicher durchführen zu können. Sie begrenzen die Ausbreitung von Rauch, welcher oft gefährlicher ist als die Flammen selbst – dies ist besonders entscheidend in Klinikbereichen mit Sauerstoffversorgung und medizinischen Gasen. Gleichzeitig befinden sich dort teure Geräte, die oft hitzeempfindlich oder leicht entflammbar sind. Und wenn ein Brand die Notstromsysteme des Krankenhauses beeinträchtigt, können noch gravierendere Konsequenzen folgen.
Eine Brandschutzverglasung hilft, diese Risiken zu beherrschen: Sie ermöglicht im Alltag klare Sicht und verwandelt sich im Brandfall in eine schützende Barriere. Das Brandschutzglas CONTRAFLAM wird unter großer Hitze opak, um die Ausbreitung von Flammen und Rauch zu verhindern. Dies ist ideal für eine wirksame Raumabschottung im Ernstfall und kann Panik minimieren.
Die von Vetrotech entwickelten Brandschutzverglasungen für Krankenhäuser können nahtlos mit geprüften Profilsystemen zuverlässiger Partner kombiniert werden. So ist sichergestellt, dass medizinische Einrichtungen leistungsstarke Glaslösungen mit passenden Brandschutztüren, Rahmen, Beschlägen und Zubehör der Systemanbieter erhalten. Vetrotechs Brandschutzgläser entsprechen den lokalen und internationalen Brandschutzvorgaben im Gesundheitswesen, sie halten Feuer 30, 60, 90 oder 120 Minuten (je nach Vorgabe der zu erfüllenden Normen) stand, schützen vor Hitze, Rauch und Flammen und unterstützen die Einhaltung von Hygienevorschriften, Nachhaltigkeit und langfristige Haltbarkeit.
*www.vetrotech.com*

# Start-ups setzen starke Impulse für den vorbeugenden Brandschutz


**Auf der FeuerTrutz 2026** stehen junge Unternehmen aus dem In- und Ausland im Fokus und präsentieren digitale Technologien, nachhaltige Ansätze und praxisnahe Lösungen. *Foto: NürnbergMesse/Heiko Stahl*

Start-ups stehen auf der diesjährigen FeuerTrutz im Fokus. Auf dem Gemeinschaftsstand startups@FeuerTrutz präsentieren zwölf junge Unternehmen aus dem In- und Ausland frische Ideen, neue Technologien und nachhaltige Ansätze. Die internationale Fachmesse für vorbeugenden Brandschutz findet am 24. und 25. Juni 2026 in Nürnberg statt und verzeichnet schon jetzt eine starke Nachfrage. Fachbesucherinnen und -besucher erwartet ein vielseitiges Angebot rund um den baulichen, anlagentechnischen und organisatorischen Brandschutz sowohl von etablierten Ausstellern als auch von jungen Unternehmen. Zum wiederholten Mal stellt die Feuertrutz als Fachmesse für vorbeugenden Brandschutz Start-ups ins Rampenlicht und schafft mit dem Gemeinschaftsstand startups@FeuerTrutz in Halle 4 einen zentralen Treffpunkt. Hier wird gezeigt, wie sich Digitalisierung, Nachhaltigkeit und Automatisierung praxisnah in den Brandschutz integrieren lassen. Die jungen Unternehmen befinden sich in direkter Nähe zu weiteren Sonderflächen auf der FeuerTrutz. So entwickelt sich beispielsweise mit dem Gemeinschaftsstand startups@FeuerTrutz und dem „Zukunftsraum“ eine Erlebnisfläche für Innovation, der Besucherinnen und Besuchern neue Technologien und frische Lösungsansätze gebündelt zugänglich macht. Phillip Blass, Leitung FeuerTrutz, sieht den Gemeinschaftsstand als große Chance: „Die jungen Unternehmen profitieren auf der FeuerTrutz von einer einzigartigen Sichtbarkeit und dem direkten Austausch mit Entscheiderinnen und Entscheidern der Branche. Im Gegenzug bringen wir als Veranstalter gemeinsam mit den Start-ups frische Ideen, digitale Impulse und neue Perspektiven in die Branche. Dieses Zusammenspiel schafft einen wichtigen Mehrwert für beide Seiten und stärkt die Zukunftsfähigkeit im vorbeugenden Brandschutz.“
Zu den teilnehmenden Unternehmen gehören unter anderem Pastor Deutschland, die nachhaltige und moderne Brandschutztechniken vorstellen sowie die MagiCAD Group GmbH, die mit BIP-fähiger Planung und Simulation präzise Entwürfe in der technischen Gebäudeausrüstung ermöglicht. Auch BSB Management präsentiert intelligente Tools für Standort- und Sicherheitsmanagement, während die 7systems GmbH zeigt, wie digitale Wartung und mobile Lösungen Arbeitsprozesse vereinfachen sowie viele weitere Start-ups die wegweisende Technologien vorstellen sind vertreten. Die Start-ups der FeuerTrutz zeigen: Smarte Technologien und nachhaltige Ansätze treiben die Zukunft des vorbeugenden Brandschutzes entscheidend voran.
*www.feuertrutz-messe.de, www.nuernbergmesse.de*

## Entrauchungsklappe für schmale Schächte

Die Priorit AG erweitert ihr Sortiment um die Entrauchungsklappe PRIOAIR SD-SLIM, die für deutlich kleinere Mindestabmessungen ausgelegt ist und somit auch in schmalen Schächten mit geringer Einbaubreite eingesetzt werden kann. Es ist eine einflügelige, feuerbeständige Entrauchungsklappe, die zum Verschluss von Abströmschächten als Teil von Rauchschutz-Druck-Anlagen (RDA) dient. Ihr Hauptzweck ist die Rauchfreihaltung von Sicherheitstreppenräumen. Im Brandfall öffnet die Klappe automatisch durch die Steuerung der RDA und ermöglicht eine große, ungehinderte Abströmfläche für Brandgase im Verhältnis zur Einbauöffnung. Die Entrauchungsklappe ist rauchdicht verschließbar und bietet eine Feuerwiderstandsfähigkeit von 90 Minuten (EI90) bei Montage in einer Abschnittsgrenze sowie 120 Minuten (EI120) bei Montage in oder an einer Leitung. Sie ist für den vertikalen, flächenbündigen Einbau in massiven Wänden zur Ableitung von Rauch konzipiert und kann mit Entrauchungsleitungen gemäß EN 12101-7 kombiniert werden. Die Prüfung erfolgte nach EN 1366-8 oder EN 1366-9. Die Entrauchungsklappe ist für den Einbau in Wänden und Leitungen klassifiziert und erfüllt die notwendigen Anforderungen für Entrauchungsklappen ($v_{edw}$). Die Klappe erreicht mit nachgewiesener Druck-Sog-Stufe 2 (1 000 Pa) und automatischer motorischer Auslösung (AA). Die Entrauchungsklappe ist in Außenabmessungen von 440 mm x 870 mm bis 1 000 mm x 2 500 mm (B x H) lieferbar und bietet somit höchste Flexibilität für die Planung und Umsetzung. Zu den weiteren Ausstattungsmerkmalen gehören eine integrierte Modbus-Schnittstelle, eine automatische Umkehr der Bewegungsrichtung bei Hinderniserkennung sowie ein einfaches System zur Notentriegelung.
*www.Priorit.de*

# „Verkehrsunterricht rettet Leben“

Die Deutsche Verkehrswacht unterstützt Forderung von Lehrkräften nach mehr Angeboten in der Mobilitätsbildung. Laut einer Online-Umfrage der ADAC Stiftung kritisieren viele Lehrerinnen und Lehrer die mangelnden Fähigkeiten von Kindern, sich sicher im Straßenverkehr zu bewegen. Demnach sei jedes zweite Kind zu unaufmerksam und mehr als jedes Dritte reagiere in entscheidenden Momenten falsch. Die befragten Lehrkräfte wünschen sich darum deutlich mehr Unterrichtstunden für die Mobilitätsbildung und bestätigen damit zentrale Forderungen der Deutschen Verkehrswacht (DVW). Um dem wachsenden Bedarf entgegenzukommen, engagiert sich die DVW seit Jahren für einen Ausbau der schulischen Verkehrserziehung, wie Verkehrswacht-Präsidentin Kirsten Lühmann unterstreicht: „Immer mehr Kinder zeigen motorische Defizite, während die Anforderungen an die sichere Verkehrsteilnahme wachsen. Das können wir mit unseren außerschulischen Projekten und Aktionen nicht auffangen. Wir müssen nicht nur Eltern wie-

**Eltern und Lehrkräfte** sollen Kinder in der Mobilitätserziehung unterstützen.
*Foto: DVW/ Foto Gloger*

der stärker einbinden, sondern vor allem ein lückenloses Angebot in der schulischen Mobilitätserziehung schaffen. Verkehrsunterricht rettet Leben!“
Das Verkehrserziehungs-Programm der DVW setzt bereits in der Kita an und führt sich durch die Grundschule bis zur Radfahrausbildung in der 3. und 4. Klasse fort. Im Sekundarbereich passiert jedoch zu wenig, weshalb sich die DVW seit einigen Jahren für ein verpflichtendes Radfahrtraining in weiterführenden Schulen einsetzt. Damit reagierte der Verband auf die hohen Unfallzahlen in der Altersgruppe und entspricht laut Umfrage ebenfalls dem Wunsch von Lehrkräften. Viele Verkehrswachten engagieren sich vor Ort seit vielen Jahren erfolgreich in der Schulwegsicherheit und unterstützen Lehrkräfte und Eltern bei der Verkehrserziehung oder vermitteln Kindern Grundlagen selbstbestimmter Mobilität. Darum hat sich die DVW für 2026 „Sicher zur Schule“ verbandsweit als Jahresthema gegeben. Ziel ist es, die vielfältigen Projekte und Aktionen sichtbarer zu machen und die Mobilitätserziehung wieder in den Fokus zu rücken. Eingesetzt werden dabei auch die umfangreichen Materialien der Verkehrswacht und des Verkehrswacht-Verlags VMS.
*https://deutsche-verkehrswacht.de/presse*

## Das Löschen von Bränden verändert sich

Die Gloria GmbH stellt auf der diesjährigen Interschutz vom 1. bis 6. Juni 2026 in Halle 13, Stand G06 aus. Im Fokus stehen unter anderem die PFAS-freien Feuerlöscher „Made in Europe“ sowie der VR Fire Trainer, der das Feuerlöschtraining digitaler und flexibler gestaltet. Bereits seit der zweiten Jahreshälfte 2024 produziert Gloria ausschließlich PFAS-freie Feuerlöscher, um den Anforderungen der EU-Regulierung mit dem seit Oktober 2025 geltenden Verbot zu entsprechen. Am Stand der Experten können sich die Messebesucher darüber informieren, welche Feuerlöscher von dem Verbot betroffen sind, welche Pflichten sich für Betreiber aus den Restriktionen ergeben und wie der schrittweise Umstieg auf PFAS-freie Feuerlöschschäume gelingt. Ein weiteres Highlight am Messestand wird der VR Fire Trainer sein, ein modernes System für realitätsnahes, virtuelles Feuerlöschtraining. Mithilfe eines Virtual-Reality Headsets, eines Controllers und einer Feuerlöscher-Attrappe können Unternehmen ihre Mitarbeitenden zeit- und ortsunabhängig auf den Ernstfall vorbereiten. Die Teilnehmenden werden in unterschiedliche Brandszenarien versetzt, in denen sie eingeständig agieren müssen. Sie sehen Flammen, nehmen Rauch wahr und müssen innerhalb kürzester Zeit entscheiden, welches Löschmittel geeignet ist. „Das System gibt direkt Feedback und Fehler sind ausdrücklich erwünscht. Denn nur so werden Abläufe verinnerlicht, was im Ernstfall Menschenleben und Sachwerte retten kann“, erklärt Marion Heidrich, Operative Direktorin bei der Gloria GmbH. Als Erweiterung steht bald ein Augmented-Reality-Modus zur Verfügung. Dabei werden digitale Inhalte über die reale Umgebung gelegt, wodurch das Brandszenario noch realer und das Training noch einprägsamer wird.


Gloria stellt auf der Interschutz PFAS-freie Löscher und den VR Fire Trainer in den Fokus. *Foto:GLORIA GmbH*

„Wir freuen uns darauf, vielen Messebesucherinnen und -besuchern die Möglichkeit einer optimalen Informationsbeschaffung in Sachen Feuerlöscher der Zukunft zu geben und die Vorteile einer möglichst nachhaltigen und umweltschonenden Brandbekämpfung darzulegen. Außerdem laden wir herzlich dazu ein, unseren VR Fire Trainer einmal live zu testen. Das ist eine tolle Chance, das eigene Können in unterschiedlichsten Szenarien unter Beweis zu stellen – oder es eben aufzufrischen“, schließt Heidrich ab.
*www.Gloria.de*

# Akku-Brände vermeiden: Lithium-Ionen-Batterien sicher lagern

Europaweit hat die Zahl der Lagerhausbrände mit Lithium-Ionen-Batterien (LIB) stark zugenommen. Es ist naheliegend, dass ein Zusammenhang zwischen der zunehmenden Verwendung im Alltag, dem Umstieg auf Elektroautos und stationäre Energiespeicher und dem Bedarf an LIB besteht. So wurden im Januar 2026 erstmals mehr als zwei Millionen reine Elektrofahrzeuge zugelassen. Entsprechend nimmt auch die Anzahl der LIB-Fabriken und die damit verbundenen Brandgefahren in Produktions- und Lagerbereichen zu. Ein Konsortium führte dazu im Forschungsprojekt SUVEREN2use Ende 2025 Brandversuche in einem realistischen Szenario durch. Die Ergebnisse zeigten, welche Gefahren beim Lagern von Lithium-Ionen-Batterien vorhanden sind und welche Grundsätze beim Brandschutz zu beachten sind.

**TEXT:** *Manuel Heinelt, Alexandra Langstrof*

Lithium-Ionen-Batterien (LIB) sind heutzutage aus unserem Alltag nicht mehr wegzudenken. Ihre Verwendung findet sich in einer Vielzahl von Alltagsgegenständen wie Smartphones, Laptops, Zahnbürsten oder Staubsaugern, die mit kleinen oder wenigen Zellen ausgestattet sind. Gleichzeitig sind immer häufiger nicht fachgerecht entsorgte LIB die Brandursache in Recyclinghöfen und Abfallbehandlungsanlagen wie der Großbrand der Mülldeponie in Swisttal im Mai 2025 wieder zeigte. Aber nicht nur kleine, sondern auch größere LIB-Module werden in E-Bikes, E-Autos sowie in Heimspeicheranlagen oder in Batterie-Energiespeichersystemen (BESS) verbaut, wie sie zunehmend in der Industrie verbreitet sind. Hinzu kommen die politischen Ziele, die weltweit strengere Emissionsvorschriften fordern. Es wird erwartet, dass die Nachfrage weiter steigt

**Großbrandversuche mit Lithium-Ionen-Batterien.** *Foto: Fogtec*


**Bild 1** Batteriebrand im Realmaßstab. Foto: Fogtec

und damit verbunden auch der Bedarf an einer sicheren Lagerung, wie die Ereignisse der letzten Monate zeigten.

In Polen kam es Anfang 2025 zum Beispiel zu mehreren Lagerhallenbränden, darunter ein Feuer in einem 6 000 m² großen Verpackungswerk in Bydgoszcz und ein Brand in einem Lagerhaus mit Elektrofahrrädern in Gdansk. Der kürzliche Brand im Januar 2026 in einer Logistikanlage von DB Schenker in Tarnowo Podgórne bei Posen löste auch eine Debatte über die Sicherheit von Lithium-Ionen-Batterien in Lagerhallen aus, da diese Vorfälle neben einem hohen Sachschaden auch intensive Löscharbeiten nach sich ziehen. Lithium-Ionen-Batterien brennen zwar nicht häufiger als andere Elektrogeräte, weisen allerdings aufgrund ihrer spezifischen Eigenschaften ein abweichendes Brandverhalten im Vergleich zu den bekannten Brandklassen auf.

## Herausforderungen bei LIB-Bränden in Lagerhallen

Durch mechanische, thermische oder elektrische Belastung kann es zu einem Schaden einzelner Zellen kommen, die eine sich selbst verstärkende exotherme Reaktion auslösen, das sogenannte thermische Durchgehen (engl. Thermal Runaway, TR). Daraus folgt, dass sich der Brand einer einzelnen Zelle sehr schnell auf benachbarte Zellen ausweiten kann. Durch das Zersetzen des Elektrolyts bilden sich außerdem sogenannte Venting- oder OFF-Gase, die brennbar und giftig sein können. Brandversuche zeigten, dass es möglich ist, dass sich diese Venting-Gase aufgrund der hohen Temperaturen entzünden und zu einem intensiven und langanhaltenden Brand führen.

Dies zeigte auch ein Brandereignis in einer 3 000 m² großen Lagerhalle in Frankreich, nördlich von Toulouse. Hier befanden sich 900 t LIB sowie Akkus, die recycelt werden sollten und durch den Brand vollständig zerstört wurden, da die in der Halle montierten Sprinkler keine Wirkung zeigten. Die Brandbekämpfung wurde mit einem massiven Löschangriff durchgeführt, der circa 12 000 m³ kontaminiertes Löschwasser zur Folge hatte, das giftige und umweltgefährdende Stoffe enthielt. Auch bei der Brandbekämpfung einer mit 83 t LIB befüllten Lagerhalle in Illinois im Juni 2021 war nicht klar, wie mit kontaminiertem Löschwasser umgegangen werden sollte, woraufhin das Löschen mit Wasser vorübergehend eingestellt wurde. Diese und weitere Ereignisse verdeutlichen die Herausforderungen, die bei Bränden mit großen Mengen an LIB entstehen. Aus diesem Grund ist ein auf die Gefahrenlage abgestimmter Brandschutz von entscheidender Bedeutung.

## SUVEREN2use: Brandversuche im Realmaßstab

Im vom Bundesministerium für Wirtschaft und Energie (BMWE) geförderten Forschungsprojekt SUVEREN2use werden seit Ende 2022 Brandversuche im Realmaßstab durchgeführt. Sie stehen unter dem Motto „Löschsysteme und Havariekonzepte für den sicheren Umgang mit Batteriebränden über den gesamten Produktlebenszyklus“. Die ersten Versuche wurden in einem offenen Raum mit natürlichen Ventilationsbedingungen durchgeführt, bei denen echte LIB mit einer Speicherkapazität von bis zu 112 kWh zum Einsatz kamen. (**Bild 1**). Die Ergebnisse wurden vom IFAB nach der Norm EN 14972 zertifiziert und vom TÜV begutachtet. Den Höhepunkt dieses Projekts stellten die Brandversuche im Oktober und Dezember 2025 dar. Zur Realisierung des Projekts wurde ein Regallager für LIB nachgebaut und voll funktionstüchtige Batteriemodule auf Paletten eingelagert.

Das Konsortium bestand aus zwei wissenschaftlichen Einrichtungen, dem Lehrstuhl Chemische Sicherheit und Abwehrender Brandschutz der Bergischen Universität Wuppertal und dem Fraunhofer Heinrich-Hertz-Institut (HHI) und den Firmen FOGTEC Brandschutz und Lobbe. Ergänzt wurde das Team durch einen wissenschaftlichen Beirat, der aus erfahrenen Brandschutzexperten besteht und weiteren assoziierten Partnern, unter anderem Dräger, DB Systemtechnik und BDE e. V. Im Sinne des Forschungsmottos wurde die Sicherheit von LIB nicht nur während der Anwendungsphase, sondern von der Herstellung bis hin zum Recycling oder der Entsorgung beleuchtet.

## Vorschriften zur Absicherung von Lagern

Zwar gibt es verschiedene Vorschriften zur Absicherung von Lagern und Lagerhallen, welche Detektoren und Löschanlagen vorschreiben, allerdings existieren aktuell kaum öffentlich-rechtliche Vorschriften zur Lagerung von Lithium-Batterien, die die spezifischen Eigenschaften und Gefahren von LIB berücksichtigen. Daher war es wichtig, ein möglichst realistisches Szenario für die Durchführung nachzubilden und Richtlinien, Schutzmaßnahmen und Arten zur Lagerung von LIB zu analysieren.

Für die Versicherungen hat der VdS eine Publikation über LIB veröffentlicht, welche die Lagerung von funktionsfähigen Batterien behandelt. Das VdS Merkblatt 3856 regelt wiederum den Sprinklerschutz für die LIB-Lagerung. In beiden Publikationen wird das Risiko anhand der gespeicherten Energie klassifiziert. Es werden Begrenzungen für die maximale Energie der in einer Lagereinheit befindlichen LIBs gegeben, aber auch physische Barrieren aus Metall gefordert und ein Sprinklerschutz innerhalb der Regalebenen. Hier wird deutlich, dass ein generel-

ler Objektschutz bei der LIB-Lagerung nicht mehr ausreichend ist. Es wird auch darauf hingewiesen, dass diese Regelungen nicht einfach für LIB im Recyclingprozess übernommen werden können, sondern dass diese noch einmal gesondert beurteilt werden müssen.

Die Factory Mutual Insurance Company (FM) liefert zum Beispiel wichtige Informationen zum Verständnis von Risikominderungsstrategien und zur Vermeidung von Sachschäden und behandelt die Herstellung und Lagerung in einem ausführlichem Datenblatt. So wird geschrieben, dass Lagerbereiche mit Sprinkler beziehungsweise Wassernebelanlagen zur Absicherung und die OFF-Gas Detektion für eine frühzeitige Erkennung, sowie Barrieren verwendet werden sollen. Denn wird die Temperatur im betroffenen Bereich schnellstmöglich gesenkt, können die LIB-Zellen gekühlt und somit ein Voranschreiten des thermischen Durchgehens verhindert werden.

Auch die NFPA-Guideline 755 für Batterieenergiespeichersysteme behandelt in Kapitel 14 die Lagerung von LIB und gibt Hinweise auf die Möglichkeiten der Lagerung, erklärt aber auch, dass das Deflagrationsrisiko innerhalb geschlossener Bereiche analysiert werden muss. Denn hier sind eine Vielzahl an Batterien dicht beieinander gepackt und werden nicht beaufsichtigt, anders als bei der Nutzung von Geräten oder in Energiespeichersystemen, die durch ein Batteriemanagementsystem überwacht werden. Bei der Lagerung von genutzten Batterien ist nicht nur der Ladezustand unbekannt, sondern auch der Gesundheitszustand beziehungsweise State of Health (SOH) der LIB. Somit können bereits beschädigte LIB eingelagert werden, die ein erhöhtes Potenzial tragen, im weiteren Verlauf zu einem Brandereignis zu führen.

## Eine Tonne Batterien pro Palette verbrannt

Um ein realistisches Szenario zu imitieren, wurde im Rahmen der Marktanalysen der Fokus auf die Material- und Konstruktionsweise der Regale, die Zusammensetzung und Verpackung der Brandlast sowie die Anordnung gelegt und ein handelsübliches Lagerregal in Back-to-Back-Anordnung geplant. Das bedeutet, dass die Batterien – so, wie es in großflächigen Lagerstätten üblich ist – gemeinsam auf Paletten gelagert werden

**Bild 2** Verpackungsmaterialien können den Brandverlauf beeinflussen. *Foto: 123RF.com*

sollten. Die geplante Brandlast setzte sich aus bis zu einer Tonne intakter LIB-Module pro Palette (bis zu 190 kWh) zusammen. Für Variationen in der Zellchemie und -geometrie wurden NMC- und NCA-Zellen mit einem State-of-Charge (SOC) von 100 %, sowie prismatische als auch zylindrische Zellen vorgesehen. Da auch Verpackungsmaterialien den Brandverlauf beeinflussen können, mussten diese ebenfalls für einen realistischen Ansatz berücksichtigt werden. (**Bild 2**). Somit waren die Eckpunkte der Versuchsserie gesetzt.

Doch diese realistische Herangehensweise stellte eine Herausforderung dar, weil ein Ort gefunden werden musste, um den Brandversuch mit LIB in dieser Dimension, mit der enormen Brandlast und dem entsprechend großen Aufbau, durchzuführen. Da ein passendes Brandlabor nicht einfach zu finden war, verzögerte sich der geplante Start. Doch Ende 2025 war es so weit. In Spanien konnte mit der Versuchsserie gestartet und der geplante Aufbau realisiert werden. Das Lagerregal wurde mit Metallplatten als physische Barrieren in Brandabschnitte unterteilt und mit einer Hochdruckwassernebel-Brandbekämpfungsanlage (HDWN-BBA) ausgerüstet.

Das definierte Schutzziel der Versuche bestand zum einen in der Begrenzung des Brandes auf einen abgetrennten Bereich und zum anderen in der Verhinderung der Ausbreitung auf benachbarte Brandabschnitte. Aufgrund der Lagerung der Batterien auf einer Palette innerhalb eines Lagers war es naheliegend, dass im Brandfall die betroffene brennende Palette nicht vollständig gelöscht, sondern der Brand nur begrenzt werden kann. Die Auswirkung des Brandes und dessen Eindämmung wurde durch aufwändige Messtechnik analysiert, die Temperaturentwicklung beispielsweise mit Thermoelementen gemessen und Infrarotkameras eingesetzt. Durch die Kombination dieser Methoden war eine präzise Analyse des Brandverlaufs und der Temperaturentwicklung möglich. Diverse Gasmessgeräte ermittelten die Gasbestandteile, die bei einem Batteriebrand entstehen und sich in ihren Eigenschaften von denen gewöhnlicher Brandlasten unterscheiden. Zusätzlich wurden Untersuchungen der Luft und von Rückständen durch die BUW durchgeführt.

## Gefahr potenziell höher als bisher angenommen

Die Ergebnisse der durchgeführten Versuche zeigen sehr deutlich die Brandgefahren, die sich aus der dichten Lagerung großer Mengen an Batterien in engem Raum ergeben. Kommt es zu einem Thermal Runaway ist dieser nicht ohne Weiteres zu stoppen und kann sich schnell auf weitere Module innerhalb der brennenden Palette ausweiten. Es zeigte sich eine hohe Brandintensität, die nur durch intensives Kühlen eingedämmt und so das Durchgehen verhindert werden konnte. Wie bereits vorangegangene Versuche belegten, wurde erneut bewiesen, dass sich Wasser aufgrund seiner guten Kühlwirkung als effizientes Brandbekämpfungsmittel für LIB-Brände eignet.

Versuche aus dem Schwesterprojekt SUVEREN_Storage haben gezeigt, dass Aerosol- oder Inertgas-Löschanlagen das Feuer durch die Verdrängung von Sauerstoff zwar reduzieren und auch ablöschen, allerdings nicht den Thermal Runaway stoppen können. Zu beobachten war, dass weiterhin brennbare und giftige Gase aus den Zellen ausgestoßen werden und sich sammeln können. Treffen diese auf vorhandenen Sauerstoff und eine Zündquelle, kann es zu verheerenden Folgen kommen. Dies haben vor allem vorangegangene Untersuchungen und Brandereignisse im Bereich der Energiespeicher gezeigt.

**Bild 3** Heiße zylindrische LIB-Zelle, circa 30 m vom Versuchsaufbau entfernt. *Foto: Fogtec*

**Bild 4** HDWN-Brandbekämpfungsanlage wird zur Eindämmung des Brandes verwendet. *Foto: Fogtec*

Besonders die brennenden zylindrischen Batteriezellen, die häufig in E-Bikes oder medizinischen Geräten verbaut werden, flogen bis zu dreißig Meter weit. (**Bild 3**). Durch den offenen Versuchsaufbau konnten diese Auswirkungen erstmals im realen Maßstab festgestellt werden, die das bisher kaum beachtete Risiko zeigten, das für flüchtende Personen und Rettungskräfte durch die damit verbundene Brandausbreitung entstehen kann. Im schlimmsten Fall können brennende Zellen weitere LIB oder andere Brandlasten entzünden, die weiter entfernt sind und Personen verletzen, die sich in der Umgebung aufhalten. Wird keine Standard-Schutzausrüstung wie Brandschutzkleidung oder Atemschutz, Handschuhe und Schutzbrille getragen, können die brennenden Zellen zu schweren Brandverletzungen führen. Dies muss auch bei der Auslegung der Brandbekämpfungsanlage (BBA) bedacht werden.

## Ziel erreicht: Ausbreitung des Brandes verhindert

Betrachtet man das Ziel des Forschungsprojektes, die weitere Ausbreitung eines LIB-Brandes in Produktions- und Lagerbereichen auf das initiale Regalfach zu begrenzen, konnte die Wirksamkeit einer stationären Hochdruck-Wassernebel (HDWN)-Brandbekämpfungsanlage erneut nachgewiesen werden. Der Temperaturanstieg in den unbeschädigten Modulen konnte unterbunden werden, indem die bei den Reaktionen entstehende Wärme abgeführt und die Batterien, bei denen direkt an der Oberfläche des Batteriepacks bis zu 1 000 °C gemessen wurden, effektiv gekühlt wurden. Die Oberfläche der winzigen Tröpfchen mit einem mittleren Durchmesser von 20 bis 100 µm führte zu einer hohen Wärmeaufnahmefähigkeit (**Bild 4**).

Durch die mehr als 1 600-fache Volumenvergrößerung bei der Verdampfung des Wassers wurde der Luftsauerstoff direkt am Brandherd verdrängt. Gleichzeitig kam es durch dieses Verdampfen des mikrofeinen Wassernebels im direkten Umfeld des Brandes zu einer Inertisierung der Atmosphäre, das heißt, die Sauerstoffkonzentration wurde in der unmittelbaren Umgebung reduziert, sodass eine Verbrennung nicht mehr möglich war, beziehungsweise unterbrochen wurde, was den Brand aktiv auf die brennende Brandlast eindämmte. Die direkt benachbarte Brandlast wurde zwar beschädigt und einzelne Module brannten, aber ein vollständiger Übergang des Brandes auf eine zweite Brandlast konnte aktiv verhindert werden.

Die Hochdruck-Wassernebel-Technologie zeichnete sich zudem durch einen stark reduzierten Wasserverbrauch aus, wodurch weniger Wasser für die BBA vorgehalten werden muss. Zudem entstanden deutlich geringere Mengen an kontaminiertem Löschwasser als bei herkömmlichen Sprinklersystemen, was für die Umwelt von großer Bedeutung ist, wie bisherige LIB-Brandereignisse zeigten. Somit zeigte die Kombination von Abschottung in Brandabschnitte mit Metallplatten in Verbindung mit der HDWN-BBA eine effektive Methode zur Brandbekämpfung bei der Lagerung von LIB.

## Fazit

Das Forschungsprojekt SUVEREN2use zeigte, dass ein auf die Lagerung der LIB angepasstes Schutzkonzept unerlässlich ist. Der Aufbau des Lagers, die Anpassung der BBA und weitere Vorgaben für die Lagerung von LIB sind von enormer Bedeutung, um ein mögliches Brandereignis einzudämmen und einen Totalverlust sowie negative Auswirkungen für die Bevölkerung und Umwelt durch Brandgase und kontaminiertes Löschwasser zu vermeiden.

Die Ergebnisse der Brandversuche zeigen, dass

- die Lagerung von Lithium-Ionen-Batterien eine nicht zu unterschätzende Gefahr ist
- beim Brand Zellen mehrere Meter weit fliegen können und dadurch zur Brandausbreitung beitragen können
- eine Hochdruck-Wassernebel-Löschanlagen die Ausbreitung des Feuers mit minimaler Wassermenge effektiv bekämpfen kann

„Hochdruck-Wassernebel vereint zwei entscheidende Wirkmechanismen in einem System: die effektive Kühlung eines Batteriebrands und die Möglichkeit der gleichzeitigen Abführung der dabei entstehenden brennbaren Gase. Das macht diese Technologie zu einem zukunftsweisenden Konzept für den Brandschutz von Batterie-Energiespeichern“, erklärt Constantin Zborowska, Produktmanager BESS und Projektleiter des Forschungsprojektes SUVEREN2use bei FOGTEC. „Die feinstverteilten Wassertröpfchen erzielen durch die hohe Oberfläche eine effektive Kühlleistung, die eine Propagation des thermischen Durchgehens wirksam verlangsamen kann. Da im Vergleich zu konventionellen Sprinkleranlagen nur ein Bruchteil der Wassermenge benötigt wird, vereinfachen sich zudem die Anforderungen an Wasserbevorratung und Löschwasserrückhaltung erheblich.“ ■ TS1133

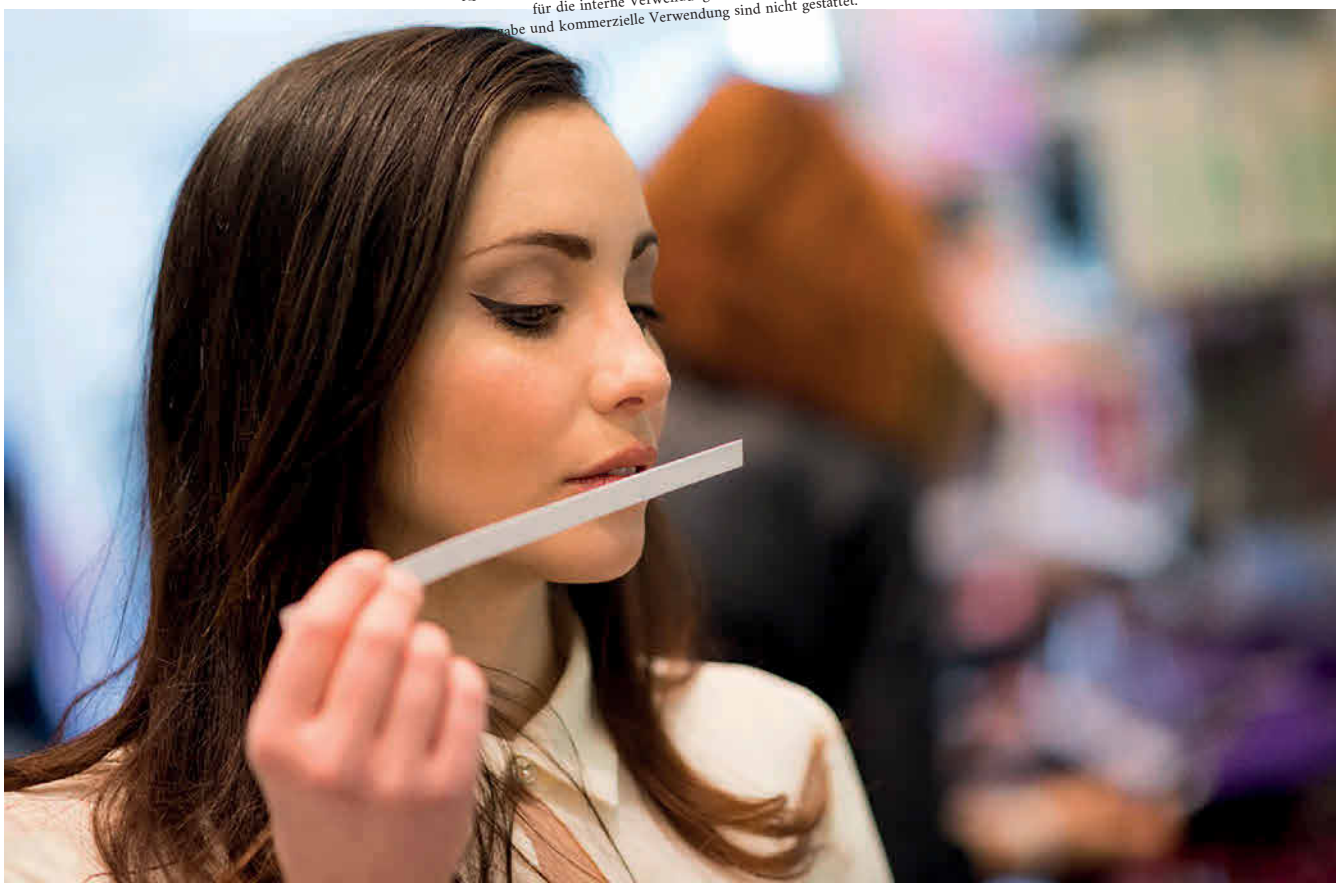
*www.fogtec-international.com*

**Manuel Heinelt**

Leiter Forschung & Entwicklung, Fogtec Brandschutz GmbH

**Alexandra Langstrof**

Freie Fach-Journalistin



**Die Mischung macht den Duft** – und Fricke-Dosieranlagen schaffen die Voraussetzung für das exakte Dosieren von Parfüms und Aromen im Fertigungsprozess. *Foto: Fricke*

**Maschinensicherheit und Ex-Schutz bei Fricke**

# Parfüms und Aromen perfekt dosiert – aber sicher

Dosierungen vom Feinsten versprechen die Anlagen der Fricke Abfülltechnik GmbH & Co. KG. Das gilt sowohl für die Präzision der Prozesse als auch für die Qualität der mehreren hundert Flüssigkeiten, die eine Anlage bevorraten kann. Denn mit den Dosieranlagen von Fricke werden die Rezepturen für Parfüms und Aromen hergestellt. Dabei leisten Ex-Sicherheitsschaltgeräte von steute einen wichtigen Beitrag für die Sicherheit des Personals im Umfeld und der Prozesssicherheit in der Anlage.

**TEXT:** *Rainer Lumme*

Wenn Kopf-, Herz- und Basisnote in der richtigen Balance sind – dann hat die Rezeptur eines Parfüms gute Chancen, zum Markterfolg zu werden. Und wenn die vom Parfümeur vorgegebenen Inhaltsstoffe mit einer Dosieranlage von Fricke hergestellt werden, wird das Parfüm – nach dem Motto „Die Mischung macht den Duft“ – in reproduzierbarer Qualität in der gewünschten Menge bereitgestellt (**Bild 1**).

Für dieses Aufgabenfeld ist das in Minden ansässige und in fünfter Generation geführte Familienunternehmen weltweit bekannt – nicht nur in der Welt der Par-


**Bild 1** So werden Parfüms und Aromen produziert: Die Concordia-Anlagen von Fricke erlauben exakte Dosierprozesse aus einem Spektrum von mehreren hunderten Flüssigkeiten. *Foto: Fricke*

fümproduktion, sondern auch bei den Herstellern von Aromen.

## Hochpräzises automatisiertes Dosieren von Parfüms und Aromen

Das Grundprinzip jeder Fricke-Dosieranlage ist einfach, die Technik selbst hoch komplex. Aus bis zu 1 000 Lagerbehältern werden Inhaltsstoffe mit höchster Präzision dosiert. Von wenigen Millilitern bis zu hohen Tonnagen sind dabei sehr unterschiedliche Dosiermengen möglich. Die entsprechenden Ventile entwickelt und fertigt Fricke ebenso selbst wie die extrem anspruchsvolle Steuerungstechnik, zu der die Dosierung und auch ein eigenes Manufacturing Execution System (MES) gehört.

Bei Fricke befinden sich immer mehrere Dosieranlagen im Aufbau, von kleinen Labordosieranlagen bis zu sehr großen Produktionsanlagen der Baureihe Concordia. In weiteren Hallen produziert das Unternehmen Abfüllanlagen für verschiedenste Flüssigprodukte wie Lebensmittel, Chemikalien, Bauhilfsstoffe, Farben und Lacke sowie Pflege- und Reinigungsmittel (**Kasten**).

Dass diese Anlagen den Herstellern von Parfüms und Aromen ein sehr hohes Maß an Produktionssicherheit und auch Produktivitätssteigerung bieten – schon allein durch die extreme Präzision der Dosiervorgänge und den hohen Automatisierungsgrad –, versteht sich von selbst. Außerdem gewährleisten sie zuverlässigen Schutz vor Kreuzkontamination bei jeder Dosierung. Auch hochviskose Rohstoffe und Medien mit niedrigem Flammpunkt sind dosierbar. Zudem können die Dosieranlagen, wenn gewünscht, unbeaufsichtigt im Nachtbetrieb arbeiten.

### MAßGESCHNEIDERTE ANLAGEN FÜR DAS ABFÜLLEN UND DOSIEREN

Die Fricke Abfülltechnik GmbH & Co. KG aus Minden ist ein Spezialist für Dosier- und Abfüllanlagen – maßgeschneidert nach Kundenwunsch „Made in Germany". Die über den gesamten Globus verteilten Kunden aus der Parfüm- und Aromenindustrie sowie der chemischen Industrie vertrauen auf das Engineering Know-how für effiziente Produktionsabläufe. Durch die breit gefächerte Expertise, mehr als 130 Mitarbeitende und 155 Jahre Erfahrung als Familienunternehmen im Spezialmaschinenbau bietet das Unternehmen eine einzigartige Gesamtleistung: hocheffizient, präzise und transparent in jedem Arbeitsschritt. Die Abfüllanlagen für niedrigviskose bis pastöse Flüssigkeiten werden kundenspezifisch und bedarfsgerecht an den Anwendungsfall angepasst. Mit den Dosieranlagen, die in diesem Beitrag vorgestellt werden, bietet Fricke hoch produktive und weitgehend automatisierte Produktionslösungen für die Parfüm- und Aromenindustrie. Aus bis zu 1 000 Einzelsubstanzen werden mit höchster Präzision und im Gewichtsspektrum von 1 mg bis 10 t die gewünschten Mischungen bereitgestellt. Die von Fricke selbst entwickelte Steuerungs- und MES-Software gewährleistet dabei eine optimale Systemleistung.

## Doppelte Sicherheit

Ein sicherer Betrieb der Dosieranlagen muss in gleich zweifacher Hinsicht gewährleistet sein. Die Mehrzahl der Anlagen ist nach den Anforderungen des Explosionsschutzes gefertigt – konkret: für Gas-Ex-Zone 1 (II 2 G T4) –, und selbstverständlich gelten die Anforderungen der Maschinensicherheit.

Auf der Vorderseite der Anlage, wo die mobilen Batch-Container mit der Parfüm- oder Aromen-Mischung zugeführt und abtransportiert werden – verhindern optoelektronische Schutzeinrichtungen ein Betreten des Gefahrenbereichs. Ansonsten sorgt eine trennende Schutzeinrichtung – sprich: ein Schutzzaun – für Sicherheit, wobei die Konstrukteure immer auch die Produktivität der Anlage im Blick haben.

Dirk Sandmann, Head of Electrical Engineering bei Fricke: „Wir können die Anlage segmentweise abschalten und den Zugang zu einzelnen Bereichen ermöglichen. Ein sicherheitsgerichtetes, geregeltes Herunterfahren ist ebenfalls möglich."

## Im Einsatz: Ex-Zuhaltung der neuesten Generation

An den Schutztüren in der Umzäunung sind Sicherheitszuhaltungen montiert – so ist es üblich bei hoch automatisierten Anlagen. Die Elektrokonstrukteure von Fricke gehörten zu den ersten Anwendern der Ex-Sicherheitszuhaltung Ex STM 515, die steute als Nachfolger der bisher eingesetzten Baureihe Ex AZM 415 (vorher STM 295) vorstellte (**Bilder 2** und **3**) – und sie sehen deutliche Vorteile in diesem Generationswechsel. Sandmann: „Das Gerät ist robust, die Zuhaltekraft höher. Der größere Anschlussraum kommt uns entgegen, weil wir oft mit großen Leitungsquerschnitten arbeiten." Außerdem kann die Zuhaltung aufgrund der Integration in die Maschinenfunktionen auch neue Funktionen übernehmen.

Die Anwender der Anlagen sind ebenso zufrieden, weil die robuste Konstruktion der Ex STM 515 Fehlauslösungen verhindert. Sie profitieren im Praxisbetrieb auch davon, dass Fricke sich für die Zusatzoption der (natürlich normenkonformen) Fluchtentriegelung entschieden hat (**Bild 4**). Im unwahrscheinlichen Fall, dass ein Bediener versehentlich im Gefahrenbereich eingeschlossen wurde, kann er diese Entriegelung betätigen und die Schutztür von innen öffnen. Auch hier gilt für Fricke das Konzept der Redundanz: Ein Logout/Tagout-System dient als zusätzliche Wartungssicherung.

**Bild 2** Für ungünstige Umgebungsbedingungen und für den Einsatz in Gas- und Staub-Ex-Zonen entwickelt: die Sicherheitszuhaltung Ex STM 515. *Foto: steute*

## Immer auf der sicheren Seite

Damit ist Fricke auch dann auf der sicheren Seite, wenn ein hohes Sicherheitsniveau (bis $PL_d$) erreicht werden soll. Dieses Niveau wird von Grund auf in die Anlage „hineinkonstruiert". Zum Beispiel ermitteln die Konstrukteure Durchgriffszeiten bei optoelektronischen Schutzein-

**Bild 3** Die Schutztüren der Concordia-Anlagen sind mit der Ex STM 515 abgesichert. *Foto: steute*

**Bild 4** Die Fluchtentriegelung ist eine Option für den unwahrscheinlichen Fall, dass Personal im Gefahrenbereich eingeschlossen wird. *Foto: steute*

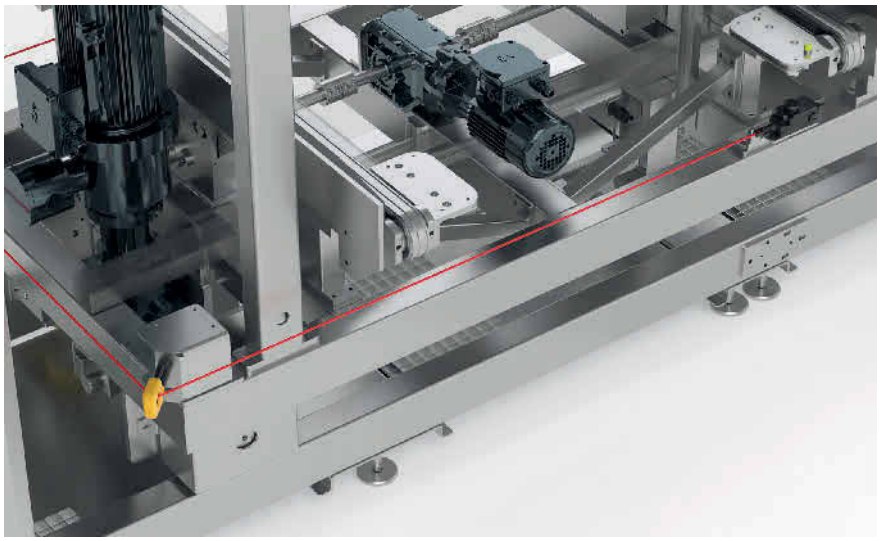


**Bild 5** Fricke verwendet auch diverse andere (Sicherheits-)Schaltgeräte aus dem Gas-Ex-Programm von steute, unter anderem Ex-Positionsschalter mit Sicherheitsfunktion und Ex-Seilzug-Notschalter (hier im Bild zu sehen). *Foto: Fricke*

**Bild 6** Dirk Sandmann, Head of Electrical Engineering bei Fricke (rechts) und Rainer Lumme, Business Development Manager Controltec bei steute. *Foto: steute*

richtungen und wählen die Sicherheitsabstände entsprechend. In manchen Anwendungen setzen sie auch auf Redundanz und verwenden zwei prinzipverschiedene Sicherheitsschaltgeräte, zum Beispiel Sicherheits-Positionsschalter vom Typ Ex 99 (**Bild 5**), als Ergänzung zur Sicherheitszuhaltung.

Auch in anderen Anwendungsbereichen – sowohl in der Dosier- als auch in der Abfülltechnik – bedienen sich die Fricke-Konstrukteure aus dem Ex-Schaltgeräte-Programm von steute für die Gas-Ex-Zone 1. Außer Grenztastern, Endschaltern, Sicherheitssensoren sind auch Seilzug-Notschalter dabei, die für einen besonderen (und mobilen) Anwendungsfall benötigt werden. Sandmann: „Diese verwenden wir, mehrfach umgelenkt, als Sicherheitselement für die mobilen Shuttles zum Transport der Fertigprodukte. Weil es keine Bumper für die Ex-Zone 1 gibt, haben wir diese Lösung, die gut funktioniert, selbst entwickelt."

## Eigeninitiative und gemeinsame Lösungsansätze

Dieses Beispiel zeigt nicht nur großes Engagement und hohe Kompetenz, sondern auch die Kreativität und Eigeninitiative der Fricke-Konstrukteure, wenn es um Maschinensicherheit unter Ex-Schutzbedingungen geht. Dabei wird immer eine möglichst hohe Produktivität mitgedacht, und steute ist hier seit Jahren ein Partner (**Bild 6**). Sandmann: „Wir haben weitere Ideen für Sicherheitsprodukte sowie -bauteile für den Ex-Bereich und freuen uns auf gemeinsame Lösungsansätze." ■ TS1138

*www.frickedosing.com, www.steute.com*

**Rainer Lumme,**

Business Development Manager Controltec, steute Technologies GmbH & Co. KG, Löhne.

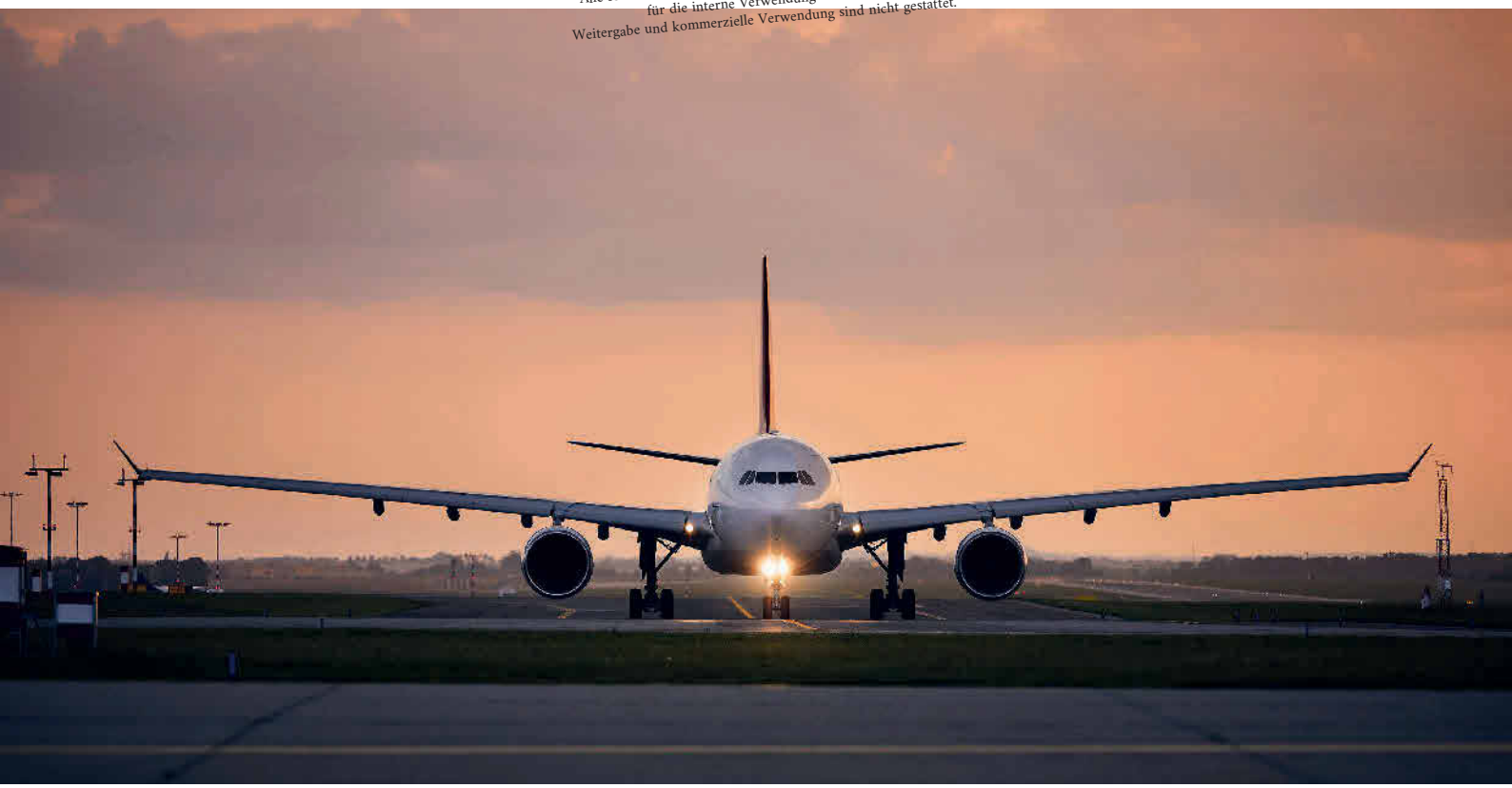
# DGWZ führt neues Verzeichnis der sachkundigen Personen für Brandschutzklappen ein

Die Deutsche Gesellschaft für wirtschaftliche Zusammenarbeit (DGWZ) führt ab sofort ein öffentliches Verzeichnis der sachkundigen Personen für Brandschutzklappen nach DIN EN 15650. In das Verzeichnis werden Personen aufgenommen, die eine entsprechende Schulung mit bestandener Abschlussprüfung nachweisen, die nicht älter als 5 Jahre ist. Voraussetzung für die Eintragung in das Verzeichnis ist die Einverständniserklärung zur Veröffentlichung und der Nachweis einer ordentlichen Geschäftstätigkeit.

Zur Aufnahme in das Verzeichnis muss ein schriftlicher Antrag gestellt werden. Die Aufnahme ist kostenfrei und erfolgt auf Basis der Bedingungen zur Aufnahme in das Verzeichnis der sachkundigen Personen. Die Antragsunterlagen können über die Website *www.dgwz.de/sachkundige-personen-brandschutzklappen* abgerufen werden.

Brandschutzklappen dürfen gemäß DIN EN 15650 und DIN 31051 nur von sachkundigen Personen gewartet, geprüft und instandgehalten werden. Die DIN EN 15650 regelt die Leistungsanforderungen an den Feuerwiderstand, die Rauchdichtigkeit sowie die mechanische Dauerhaftigkeit der Bauteile. Sie stellt sicher, dass die Klappen im Ernstfall zuverlässig auslösen und die Ausbreitung von Feuer und Rauch über die Lüftungsleitungen unterbinden.

*www.dgwz.de*



**Ein Großraumflugzeug** rollt zum Start (Symbolbild). *Foto: smarterpix/JAROMIR CHALABALA*

# Unternehmensphilosophie und Sicherheit

Anfang der 1960er Jahre begann das Zeitalter der Großraumflugzeuge. Gleichzeitig wurden Stimmen laut die befürchteten, dass diese Entwicklung mit zu hohen Risiken verbunden sein könnte. Ein Jahrzehnt später, zu Beginn der 1970er Jahre, ereigneten sich die ersten katastrophalen Abstürze. Die Betroffenheit war groß als sich herausstellte, dass diese Unfälle durch unternehmerische Inkompetenz, undurchdachte und fehlerhafte Konstruktionsdetails und auch durch staatliche Nachlässigkeit verursacht wurden.

**TEXT:** *Rainer Konersmann*

## Vorwort

Wenn ein Flugzeug abstürzt, ein Schiff untergeht oder ein Zug entgleist, werden üblicherweise umfangreiche Untersuchungen angestellt. Nachdem man sich sicher ist, welche Ursachen zum Unfall führten, werden in der Regel Abhilfemaßnahmen vorgeschlagen, die bewirken sollen, dass sich der Unfall nicht wiederholen kann. Die Umsetzung obliegt dann den dafür zuständigen Behörden. Untersuchungsberichte müssen oftmals auch zur Klärung der Schuldfrage herangezogen werden. Die juristische Nachbereitung einer Katastrophe eröffnet mitunter tiefere Einblicke in die Hintergründe, als dies ein Untersuchungsbericht, der meist nur die technischen Aspekte untersucht, leisten kann. In einigen Fällen zeigt sich dann, dass unternehmerische Zielvorgaben die sicherheitstechnischen Anforderungen in den Hintergrund treten ließen. Man geht schon lange davon aus, dass eine rigide wirtschaftliche Denkweise die Moral negativ beeinflusst. Der Konkurrenzdruck führt oftmals dazu, dass das wirtschaftliche Eigeninteresse allen anderen Überlegungen vorangestellt wird [1]. Man muss allerdings hinzufügen, dass dies größtenteils so gewollt ist. Es gehört quasi zu den Spielregeln, ohne die unser Wirtschaftssystem nicht funktionieren

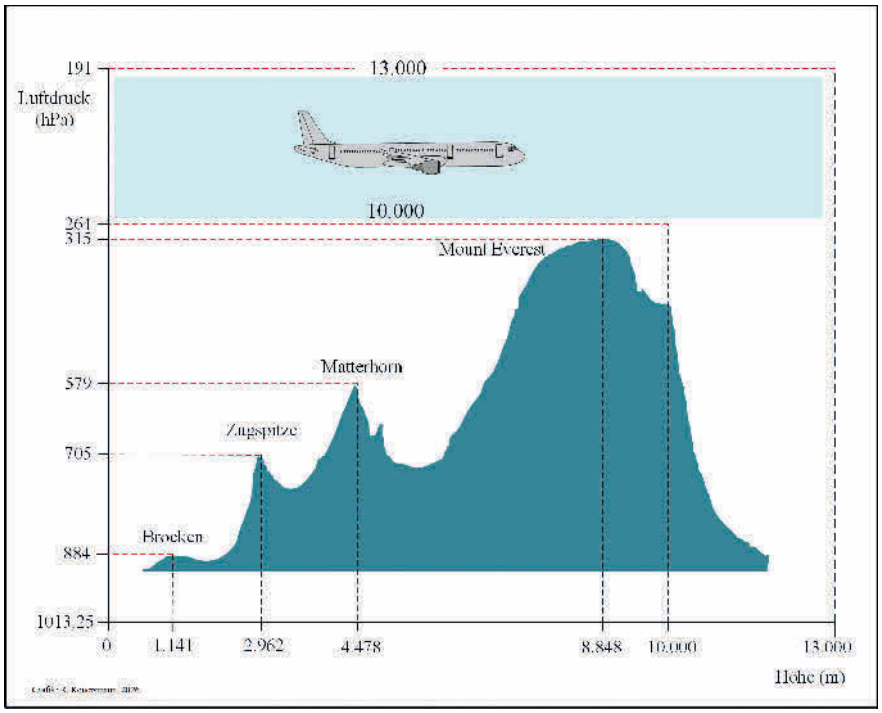



**Bild 1** Abnahme des Luftdrucks mit der Höhe. *Grafik: R. Konersmann*

würde. Die Moralität lässt sich damit offensichtlich nur schwer synchronisieren. Dies ist beziehungsweise wäre dann die Aufgabe von Institutionen, die, mit staatlicher Autorität ausgestattet, interessenneutral die Durchsetzung sicherheitstechnischer Erfordernisse durchsetzt. Meistens funktioniert es auch, aber in einigen Fällen auch nicht.

## Wie ein kleines Detail zum Problem werden kann

Wenn man die Wirtschaftsnachrichten in den Medien verfolgt, dann kann man den Eindruck gewinnen, dass viele Managementetagen nur mit Juristen, Betriebswirtschaftlern und Finanzfachleuten besetzt sind. Führungskräfte mit technischer Expertise scheinen in der Minderheit zu sein. Daraus erklärt sich dann, dass ein mittelständischer Betrieb oder sogar ein ganzer Konzern in eine Problemkette hineinschlittert, aus der er sich nur unter hohen Verlusten wieder befreien kann. Die eindrucksvollsten Beispiele dafür lassen sich bei den großen Flugzeugbauern finden. Dies liegt vor allen Dingen daran, weil Flugzeugkatastrophen sehr akribisch untersucht, dokumentiert und in der Regel auch der Öffentlichkeit zugänglich gemacht werden. Nicht zuletzt tragen dazu auch Rechtsanwaltskanzleien bei, die sich der Probleme sehr gern annehmen. In einigen Fällen können auch Recherchen unabhängiger Medien zur Klärung unangenehmer Sachverhalte beitragen. Bevor dies an einem konkreten Beispiel erklärt wird, müssen noch einige Details besprochen werden.

## Das Passagierflugzeug – ein fliegender Druckbehälter

In Reiseflughöhen zwischen zehn- bis dreizehntausend Metern Höhe kann kein normaler Mensch mehr genug Sauerstoff aufnehmen. Darum werden die heutigen Passagierjets ausnahmslos als zigarrenförmige Druckbehälter gebaut, in denen die Atemluft auf einen Innendruck von circa 750 bis 810 hPa gehalten werden kann. Dieser sogenannte Kabinendruck entspricht ungefähr dem Luftdruck in einer Höhe von 2 500 m. Dieser Druck ist für alle Menschen noch erträglich. Der Druck auf Meereshöhe, mit dem die meisten Menschen sozialisiert wurden, beträgt circa 1 013 hPa (**Bild 1**). Dies bedeutet, dass ein Flugzeug (ein hoch fliegender Druckbehälter) hermetisch abgeschlossen sein muss. Das heißt, dass alle Öffnungen, Türen, Fenster, Klappen, die diesen Druck-Überlebensraum gegenüber der Atmosphäre abschließen, absolut dicht schließen müssen und während der gesamten Lebensdauer des „Systems Flugzeug“ auch dicht bleiben müssen.

Bei den Fenstern, die sich sowieso nicht öffnen lassen, ist dies kein Problem. Die Passagier- und Frachttüren, die ständig geöffnet und geschlossen werden müssen, erfordern jedoch spezielle Lösungen.

## Eine unabdingbare Notwendigkeit – dichte Türen

Die ersten druckfesten Passagierkabinen wurden Anfang der 1930er Jahre gebaut und seitdem ständig weiterentwickelt. Während des 2. Weltkrieges wurden die hochfliegenden Kampfflugzeuge mit Druckkabinen ausgestattet, die ersten zivilen Passagierflugzeuge folgten in den 1950er Jahren.

Es mussten auch Rückschläge in Kauf genommen werden, zum Beispiel bei der de Havilland Comet, die die Konstrukteure zur Verzweiflung brachten, bis eine Lösung gefunden wurde (siehe TS 3/4-2021). Nach der Beseitigung der ersten „Kinderkrankheiten“ verfügen alle Flugzeugbauer über den notwendigen Erfahrungsschatz, um diese Technik alltagstauglich umzusetzen. Der notwendige Kabinenüberdruck wird mittels der sogenannten Zapfluft, die aus den Triebwerken „abgezapft“ wird, erzeugt. Damit wird die mit steigender Flughöhe immer dünner werdende Atemluft auf einem konstanten Niveau gehalten. Den Kabinenüberdruck macht man sich auch zunutze, um die druckdichte Verriegelung der Passagiertüren herbeizuführen. Dies funktioniert mit einem einfachen Trick: Die Türöffnung, also der Rahmen, ist kleiner als das Türblatt. Wenn das Türblatt durch den inneren Überdruck gegen den kleineren Rahmen gedrückt wird, dann wird die Tür automatisch abgedichtet. Mit steigender Druckdifferenz, also in größeren Höhen, wird es niemandem gelingen, eine solche Tür zu öffnen. Aber dies bedeutet, dass die Tür nach innen geöffnet werden müsste. Dies wäre jedoch für das Ein- und Aussteigen der Passagiere äußerst hinderlich, zumal an der Innenseite die aufblasbare Notrutsche befestigt ist. Darum öffnet die Flugzeugtür immer nach außen. Aber wie kann dies funktionieren? Die konstruktive Lösung ist ein Meisterstück der Mechanik. Nach Betätigung des Türhebels lösen sich innerhalb der Türverkleidung die Zuhaltehaken und die sogenannten Gates an der Ober- und Unterseite des Türblatts klappen etwas nach innen. Dadurch verringert sich die Höhe des Türblatts. Nun kann die Tür mit

Hilfe der zwei Scharniere und einer Kurvenscheibe, die das Türblatt in eine leichte Schräglage zwingt, zunächst nach innen geschwenkt, um dann, leicht geneigt, wieder nach außen, an die Außenhaut des Flugzeugs geklappt zu werden (**Bild 2**). In der Rahmenkonstruktion sind Dichtungen und Halterungen verbaut, die, mehrfach patentgeschützt, nur zu erahnen sind. Diese sogenannte Plug-Door lässt sich von den Flugbegleitern in der Regeln mühelos öffnen und schließen. Sie verlangen keine komplizierte Einweisung, folgen einem automatisch ablaufenden Funktionsablauf und sind daher quasi, es gibt leider keine treffendere Bezeichnung, idiotensicher. Dieses Prinzip des Herausschwenkens wurde und wird von vielen Flugzeugbauern in den USA verwendet. Daneben wurden noch andere Varianten erprobt, zum Beispiel nach oben in den Rumpf einfahrende Türblätter, ähnlich der Sicherheitstüren, die in den Raumschiffen in Science-Fiction-Filmen zu bestaunen sind. Diese eleganten Slide-Up-Doors waren sehr platzsparend, nahmen keine Schwenkradien und Türangeln in Anspruch und wurden trotzdem bald wieder verworfen. Die Vorteile der leichten Bedienbarkeit wurden wahrscheinlich durch die anspruchsvolle Antriebstechnik und das damit verbundene Mehrgewicht wieder aufgehoben. Der Hersteller Airbus verwendet ein eigenes Konzept. Auch hier kommt das Plug-Prinzip zur Anwendung, allerdings durch eine andere technische Lösung. Bei Airbus gibt es keine aufgesetzten Gates. Hier wird die druckdichte Verriegelung durch eine innenliegende Mechanik erzeugt. Die neuesten Entwicklungen kommen ohne Schwenkmechanismen aus. Neuerdings werden die Passagiertüren parallel zum Rumpf nach außen geschwenkt und die Abdichtung erfolgt durch eine spezielle Mechanik mit druckbeaufschlagten Dichtungssystemen. Diese „Translating-Doors“ zeigen immer ihre Außenseite, es erfolgt keine Schwenkbewegung mehr [2].

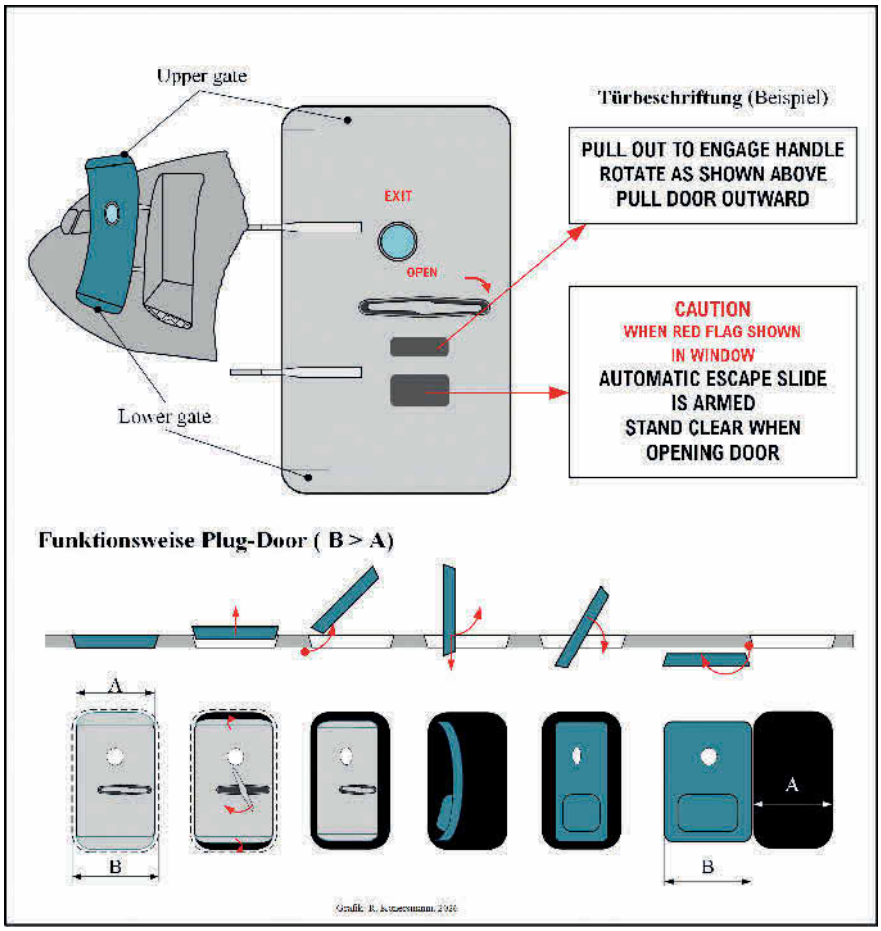



**Bild 2** Funktionsweise einer Plug-Door-Passagiertür. *Grafik: R. Konersmann*

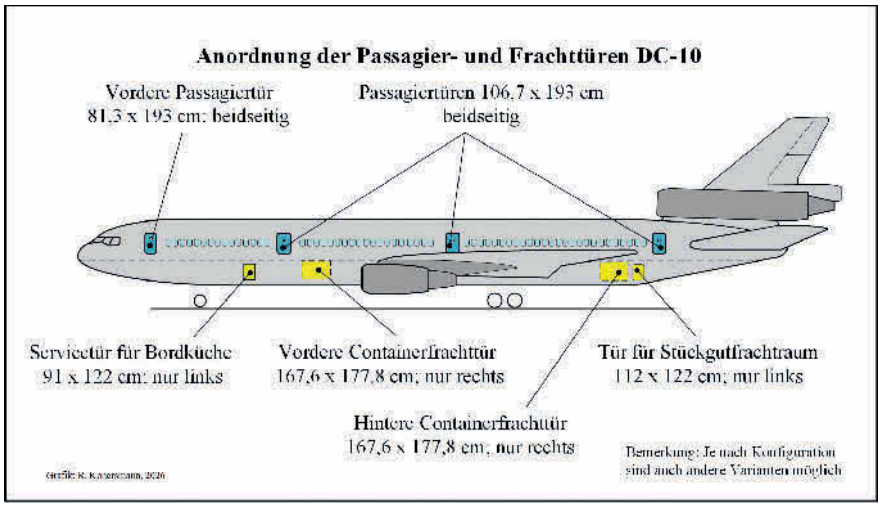



**Bild 3** Anordnung der Passagier- und Frachttüren in einer McDonnell Douglas DC-10. *Grafik: R. Konersmann*

## Notwendige Ergänzung

Bevor wir die Tür zuschlagen und es zu Missverständnissen kommt, muss an ein Ereignis vom 5. Januar 2024 erinnert werden. An diesem Tag startete eine Boeing 737Max9 zu einem Inlandflug von Portland (Oregon) nach Ontario (San Bernardino County, Kalifornien). Nach dem Start, in einer Flughöhe von 4 520 m, verlor die Boeing eine unsachgemäß eingebaute Notausgangstür. Der Kabinendruck fiel abrupt von 970 auf 620 hPa, sodass die Sauerstoffmasken aus der Kabinendecke fielen. Der Pilot leitete sofort einen Sinkflug ein. Die Maschine konnte sicher gelandet werden und bis auf leichte Verletzungen gab es keine Personenschäden [3]. Dieser Vorfall war in den Medien über einige Tage präsent und erzeugte einige Irritationen. Bei dieser Tür handelte es sich um keine Zugangstür, sondern um eine Notausgangstür, die ausschließlich im Katastro-

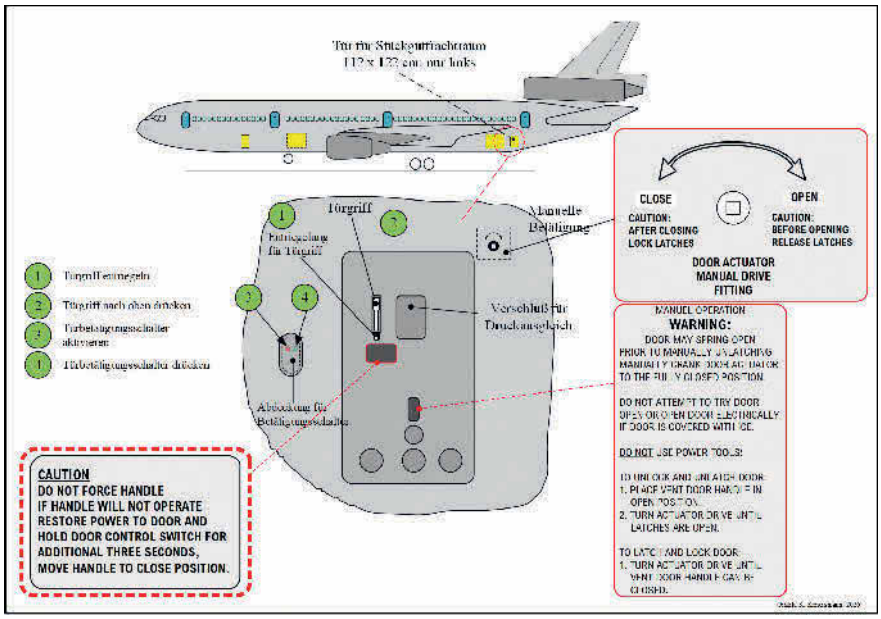



**Bild 4** Handlungsablauf zum Öffnen und Schließen einer Frachtraumtür am Beispiel der hinteren Frachtraumtür einer DC-10. *Grafik: R. Konersmann*

phenfall, bei einer schnellen Räumung des Flugzeugs, zum Beispiel einer Notlandung und bei Ausbruch eines Feuers, zum Einsatz kommt. Sie wird vom Kabinenpersonal nur geöffnet um sicher zu stellen, dass alle Passagiere innerhalb der von der Zulassungsbehörde geforderten Zeitspanne das Flugzeug verlassen können. Diese Tür versagte, weil man bei der Montage vergaß alle Arretierungselemente einzubauen, vier Stück fehlten. Der Druckunterschied in der Flughöhe von circa 4 500 m reichte offenbar aus, um die Tür aus der Verankerung zu reißen.

## Die Frachttüren

Unter den Passagierdecks der Verkehrsflugzeuge befinden sich die Frachträume für das Gepäck der Fluggäste, Vorratsräume für die Bordküchen und Stauraum für Post, Pakete und Kleinkram. Damit alles sicher gestaut werden kann, werden die Koffer mit Netzen gesichert und so verzurrt, dass sie während des Flugs nicht verrutschen können. In Großraumflugzeugen werden kleinere Handelswaren in speziellen Containern gestaut, die der Kontur des Flugzeugrumpfs angepasst sind. Auch die Frachträume sind Bestandteil des Druckkörpers, das heißt hermetisiert (**Bild 3**). Mitunter gibt es spezielle Compartments, die auch beheizt werden können, zum Beispiel zum Transport von Tieren.

Die Service- und Frachttüren sind konstruktionsbedingt die Schwachstellen des Flugzeugs. Zum einen dadurch, dass sie sich nur nach außen öffnen lassen. Dies ist die logische Konsequenz dessen, dass der innenliegende Stauraum optimal ausgenutzt werden muss. Die Abdichtung dieser Türen kann deshalb nicht nach dem Plug-Door-Prinzip (B > A) funktionieren, sondern muss durch pneumatisch oder elektrisch betätigte Verriegelungen erfolgen. Neben den Verriegelungsmechaniken müssen noch diverse Dichtungsprofile verbaut werden, die durch das Schließen der Tür für den dichten Verschluss sorgen. Das Schließen einer Frachtraumtür ist im Prinzip nicht komplizierter als das Schließen einer Autotür und läuft immer nach demselben Schema ab (**Bild 4**).

Zunächst wird der Türgriff mit einem Drucktaster entriegelt, der sich direkt unter dem Griff befindet. Der Türgriff klappt etwas nach oben aus und wird danach bis zum Anschlag hoch gedrückt. Nachdem die Abdeckung für die Betätigungsschalter geöffnet wurde, wird zunächst ein rot gekennzeichneter Schalter umgelegt, der die elektrische Türbetätigung freischaltet. Danach wird ein grüner Schalter betätigt, der die Türöffnung auslöst. Sollte kein Bordstrom anliegen, kann die Frachtraumtür auch manuell betätigt werden. Das Schließen erfolgt in umgekehrter Reihenfolge und das Zurückführen der Betätigungselemente in ihre Ausgangsposition.

## Großraumflugzeuge

Anfang der 1960er Jahre zeichnete sich immer deutlicher ab, dass es einen Markt für sogenannte Großraumflugzeuge gibt mit denen sich bis zu 600 Passagiere, manchmal auch mehr, befördern lassen. Man war sich aber auch darüber im Klaren, dass ein Absturz eines solchen Flugzeugs unberechenbare wirtschaftliche und gesellschaftliche Nachwirkungen verursachen könnte. Es durfte einfach nicht passieren, und wenn doch, dann nur äußerst selten. Aber was heißt das schon? Was ist „selten?“ Jedenfalls schien die Aufgabe lösbar zu sein. Im Jahr 1967 fusionierten die McDonnell Aircraft Corporation und die Douglas Aircraft Company zur McDonnell Douglas Corporation. Beide Hersteller kannten sich in der Flugzeugproduktion aus, sowohl im zivilen als auch im militärischen Bereich. Durch diesen Zusammenschluss sollte die Marktposition auf dem zivilen Sektor gestärkt werden, wenn nicht sogar die Pole-Position auf dem Markt für Großraumflugzeuge angestrebt werden. Aber die Konkurrenz schlief nicht. Der Boeing-Konzern hatte inzwischen seine 747 zur Serienreife entwickelt. Der Erstflug erfolgte im Februar 1969. Die McDonnell Douglas DC-10, ein dreistrahliges Großraumflugzeug, das je nach Version für den Mittel- oder Langstreckenbereich eingesetzt werden konnte, absolvierte ihren Erstflug am 29. August 1970. Der zweite große Flugzeughersteller, die Lockheed-Corporation, folgte im November 1070 mit der Lockheed-Tristar. Das erste europäische Großraumflugzeug, der Airbus A300, hatte seinen Erstflug im Oktober 1972. Dieser kurze Exkurs ist geboten um auf die Konkurrenzsituation der US-amerikanischen Hersteller hinzuweisen.

## Der 12. Juni 1972

Der 12. Juni 1972 war ein schicksalhafter Tag. Um 14:36 Uhr Ortszeit startete eine DC-10 der American Airlines, mit 56 Passagieren, 2 Piloten und 11 Flugbegleitern an Bord, zu einem Linienflug von Los Angeles über Detroit und Buffalo nach New York/La Guardia. Im hinteren Frachtraum, an der „Backbordseite“, befanden sich neben den Koffern der Passagiere auch ein Sarg, der nach Buffalo überführt werden sollte. Der Flugplan sah einen Zwischenstopp in Detroit (Michigan) und Buffalo (Staat New York) vor

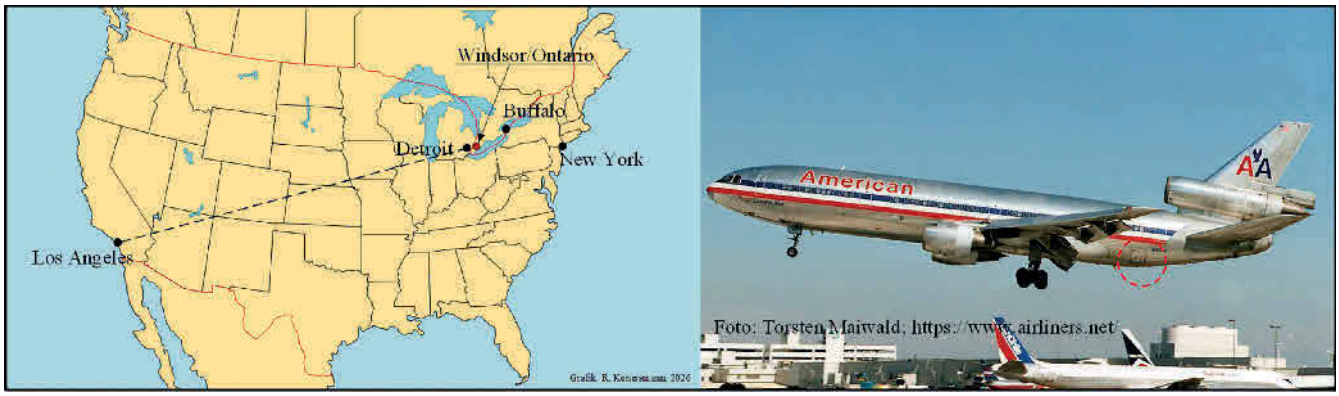



**Bild 5:** Flugplan American Airlines Flight 96 und Foto der DC-10 mit der Tür zum Stückgutfrachtraum. *Grafik links: R.Konersmann; Foto rechts: Torsten Maiwald*

(**Bild 5**). Die fast neue DC-10 hatte erst 2 142 Flugstunden auf dem Buckel, sie wurde am 28.7.1971 an American Airlines übergeben. Es war die fünfte von inzwischen 40 gebauten Serienmaschinen. Die erste Zwischenlandung in Detroit, um 18:36 Uhr Ortszeit, verlief problemlos.

Ungefähr fünf Minuten nach dem Start in Detroit schien eine Explosion das Flugzeug zu zerreißen. Der Verschluss einer Frachtraumtür im Heckteil der Maschine (**Bild 6**) hatte sich in 3 582 m Höhe geöffnet. Im Heck klaffte nun ein rechteckiges Loch, durch das dutzende Koffer und auch der Sarg über eine Strecke von mehreren Kilometern über der kanadischen Stadt Windsor verstreut wurden. Durch die Öffnung des Rumpfes, durch die plötzliche Dekompression[1)], wurde oberhalb des Frachtraums ein Teil des Kabinenbodens zerstört.

Der einstürzende Boden zerriss sämtliche Steuerungssysteme für die horizontalen und vertikalen Leitwerksflächen und für die Steuerung des Hecktriebwerks. Eine Flugbegleiterin wurde unter den Trümmern eingeklemmt. Glück im Unglück: Dadurch konnte der Luftsog sie nicht aus dem Flugzeug ziehen. Eine andere Stewardess konnte sich geistesgegenwärtig in die Bordtoilette retten und die Tür verriegeln [4].

Der gesamte Vorfall, vom Aufreißen der Tür bis zur Landung, hatte nicht mehr als 30 Minuten gedauert. Dieses Ereignis


**Bild 6** Ein Ingenieur der FAA untersucht die Reste der abgerissenen Frachtraumtür. *Foto: FAA*

hatte eine hohe Brisanz. Das Lösen einer Frachttür während des Reiseflugs, mit 67 Überlebenden, war ein Vorkommnis, das schnellstmöglich gelöst werden musste. Noch am gleichen Tag meldete die kanadische Polizei die Gepäck-Funde in einem Maisfeld bei Windsor. So bekamen die Unfallermittler zeitnah die Wrackteile der Frachttür in die Hände und machten eine schockierende Entdeckung. Die DC-10 war zwar mit geschlossener, aber nicht gesicherter Tür unterwegs. Als die Maschine an Höhe gewann und der Innendruck ein kritisches Niveau erreichte, war es nur eine Frage der Zeit, bis die Tür nachgab und herausflog. Anlässlich der Untersuchungen wurde noch ein weiterer Mangel entdeckt: Im Bereich des Kabinenbodens oberhalb des Frachtraums wurden keine Druckentlastungsöffnungen installiert [5].

## Erste Erkenntnisse

Die Untersuchungsbeamten des NTSB fanden durch intensive Befragungen heraus, dass der Gepäckverlader in Detroit Schwierigkeiten hatte, die Frachttür zu schließen. Er gab an, die Tür elektrisch geschlossen und dann so lange gewartet zu haben, bis er das Geräusch des Stellmotors nicht mehr hörte. Er ging davon aus, dass die Tür nun geschlossen sei. Beim Versuch den Türgriff nach unten zu drücken, spürte er einen deutlichen Widerstand. Erst durch das Gegendrücken mit dem Knie konnte er dann den Griff in die Ruhelage drücken. Sicherheitshalber winkte er noch einen Mechaniker heran und bat ihn nachzuprüfen, ob die Frachttür geschlossen und verriegelt war. Der bestätigte den korrekten Verschlusszustand.

## Wie konnte es dazu kommen?

Um diese Frage zu klären, müssen wir das Geschehen einige Jahre zurückspulen. Am Bau eines Flugzeugs sind viele Unternehmen beteiligt. Für den Rumpf der DC-10 wurde die Consolidated Vultee Aircraft Corporation (Convair) als Auftragnehmer verpflichtet. Eine Stärke der Convair-Corporation lag im Bereich der Rumpfstrukturen. Das Unternehmen genoss durch seine Erfahrungen bei der Entwicklung von Kampfflugzeugen und in der Weltraumtechnik einen exzellenten Ruf. Convair griff für den Verschlussmechanismus der Frachtraumtür auf altbewährte Systeme, die schon bei den Passagierflugzeugen DC-8 und DC-9 verwendet wurden, zurück [6]. Diese Verschlüsse wurden hydraulisch betätigt. Aber diese Hydraulik war einem Groß-

**Fußnote**

[1)] Eine Dekompression tritt auf, wenn der Kabinendruck aufgrund einer Leckage nicht mehr gehalten werden kann. Bei einer plötzlichen Dekompression, die in vielen Fällen von einem Knallgeräusch begleitet wird, entsteht ein Sog in Richtung des Lecks. Alle losen Gestände werden in Richtung des Lecks gesaugt.

kunden des McDonnell-Douglas-Konzerns, der Fluggesellschaft American Airlines, zu schwer. Um 12,7 kg Gewicht einzusparen, sollte nunmehr ein neues, elektrisches Betätigungssystem mit manueller Notbetätigung, eingebaut werden. Noch vor dem „Windsor-Ereignis", stellte sich heraus, dass das neue System unzuverlässig war. Für den Elektromotor, der die Hydraulikkomponenten ersetzte, waren zu geringe Kabelquerschnitte gewählt worden und der komplizierte Verriegelungsmechanismus war sehr fragil und konnte, obwohl die Teile des Mechanismus nicht richtig ineinandergriffen, auch mit Gewalt geschlossen werden. Und genau so hatte es der Verlader in Detroit am 12.6.1972 gemacht.

## Wie ging es nun weiter?

Die Leistung der Piloten, ein Flugzeug in fast ausweglosser Situation noch sicher zu landen und die makabre Landung eines Sargs in einem Maisfeld, wurde natürlich sofort von den Medien aufgegriffen. Davon unabhängig schaltete sich einen Tag später die US-amerikanische Federal Aviation Administration (FAA), die Bundesluftfahrtbehörde der USA, in die Untersuchungen ein. Der Hersteller, McDonnell Douglas, wurde zu den Frachtraumtüren befragt, zur Konstruktion, zu eventuellen Vorkommnissen in der Vergangenheit, eben so, wie es Untersuchungsbeamte zu tun pflegen. Die Kooperationsbereitschaft des Flugzeugherstellers wird in vielen Veröffentlichungen als eher lustlos beschrieben. Man gab schließlich zu, früher mal ein paar kleinere, unerhebliche Schwierigkeiten gehabt zu haben. Die Herausgabe aussagekräftiger Betriebsberichte, Untersuchungsprotokolle usw. kam nicht zustande [7, 8]. Aber dadurch wurde die Angelegenheit für die Untersuchungsbeamten noch interessanter. Die FAA-Ingenieure, oftmals selbst erfahrene Piloten, wussten sich zu helfen. Sie fanden heraus, dass etwa 100 Zwischenfälle aktenkundig waren und dass der Fehler in allen Fällen daran lag, dass die elektrisch betriebenen Fallhaken die an der Unterkante der Tür angebrachten Ankerrollen nicht voll umfasst hatten. Oftmals kam es vor, dass die Haken sich verklemmten und quasi den Verschluss nicht herstellen konnten. Zu diesem Zeitpunkt war die DC-10 seit etwa zehn Monaten im Einsatz und etwa 40 Exemplare waren bei den Fluggesellschaften aktiv. Dem steht eine Anzahl von circa 100 Versagensberichten über nicht geschlossene Frachtraumtüren gegenüber. Diese Relation verdeutlicht, dass dieses Risiko nicht mehr akzeptabel war. „Glücklicherweise" war der unvollständige Verschluss immer vor einem Start entdeckt worden. Bis zum „Windsor-Fall."

## Ein merkwürdiger und riskanter Deal

Unmittelbar nach den Ermittlungen des NTSB wurden der Federal Aviation Administration (FAA) mehrere Empfehlungen übermittelt, die als „Lufttüchtigkeitsanweisung" umzusetzen gewesen wären. Eine Lufttüchtigkeitsanweisung ist ein scharfes Schwert, quasi eine Maßnahme mit Gesetzeskraft. Der Hersteller, McDonnell Douglas, sowie alle Fluggesellschaften, die die DC-10 in Betrieb hatten, wären zu Konstruktionsänderungen an der Frachttür zwingend verpflichtet. Ohne Umrüstung kein Flugbetrieb. Doch dann geschah etwas Seltsames. Der Führungsetage bei McDonnell Douglas gelang es, mit führenden Mitarbeitern der FAA mehrere „klärende Gespräche" zu führen, die letztlich dazu führten, dass die FAA von einer Lufttüchtigkeitsanweisung absah [9]. McDonnell Douglas wurde zugestanden, sogenannte „Service Bulletins" herauszugeben. Dies ist quasi eine innerbetriebliche Änderungsmitteilung, die bestimmte Konstruktionsdetails betrifft, die im laufenden Fertigungsprozess umzusetzen sind, ohne dass die Fertigung unterbrochen werden muss. Ein Bulletin bewirkte keine grundlegenden Konstruktionsänderungen, sondern eine „Modifizierung" aller Türen der Flugzeuge, die gerade montiert wurden.

## Die technische Umsetzung

Die Anordnung einer Lufttüchtigkeitsanweisung hätte ein sofortiges Startverbot für alle DC-10 Maschinen bedeutet, mit immensen wirtschaftlichen Folgen. Nachdem dieser Schreck überwunden war, wurde krampfhaft nach einer Übergangslösung gesucht, eine konstruktive Lösung, die sich schnell umsetzen ließ, keine großen Änderungen verlangte, die den quengelnden FAA-Ingenieuren als Geniestreich verkauft werden konnte. Während dieser Übergangszeit würde dann noch genügend Zeit bleiben, um eine neue konstruktive Lösung zu finden, getreu dem Motto: Kommt Zeit, kommt Rat. Die Zeit verging, aber Rat kam nicht. So kurz nach dem „Windsor-Schreck" fiel keinem der Eingeweihten etwas Vernünftiges ein. Beim Hersteller, McDonnell Douglas und der Luftfahrtbehörde FAA, war man eigentlich ratlos.

Aber dann kam die rettende Idee: Damit sich die Mechanik nicht mehr durch ein gewaltsames Zudrücken verbiegen ließ, wurde die Installation einer sogenannten Stützplatte angeordnet. Und damit die Belader auf den Flughäfen der Welt überprüfen konnten, ob die Tür auch wirklich verriegelt war, wurde der Einbau eines Sichtfensters im unteren Türbereich als hilfreich erachtet. Dieses Sichtfenster, 2,5 cm im Durchmesser, sollte einen Blick auf die Verriegelungshaken erlauben, damit das Bodenpersonal erkennen konnte, ob die Haken auch alle ordnungsgemäß eingerastet waren. Es gibt Hinweise, dass die Praxistauglichkeit dieser Lösung von der FAA angezweifelt wurde [7, 8]. Die Türschwelle der DC-10 befindet sich 2,79 m über dem Boden. Bei einer Überprüfung müsste sich der Verlader auf seiner Arbeitsbühne, nach dem Herunterklappen der Tür, irgendwie mit dem Auge dem „Guckloch" nähern, um dann, auch in der Dunkelheit, zu prüfen, ob sich der Sperrbolzen in der vorschriftsmäßigen Stellung befindet. Vorher müsste er sich jedoch mit dem Hinweisschildern vertraut gemacht haben (**Bild 7**).

Die drei Änderungsvorschläge: Verstärkungsplatte, Guckloch, Beschriftung, waren in sicherheitstechnischer Hinsicht ein Skandal. Vor allen Dingen auch deshalb, weil diese nur bei sehr wenigen DC-10 Maschinen sofort ausgeführt wurden. Zum Zeitpunkt des Windsor-Unfalls waren 40 DC-10 Maschinen im Einsatz. 90 Tage nach Herausgabe der Änderungsmitteilungen, am 2. Juli 1972, waren erst fünf Maschinen umgerüstet worden und 18 Maschinen wurden im Verlauf des Jahres 1973 „nachbearbeitet." Die vielleicht effektivste Maßnahme, der Einbau einer Verstärkungsplatte zur Versteifung des Sperrmechanismus, wurde in einigen Fällen durch organisatorische Defizite, um es vornehm auszudrücken, vergessen. Dieser Umstand führte im Jahr 1974 zu einem der verheerendsten Unfälle in der zivilen Luftfahrt.

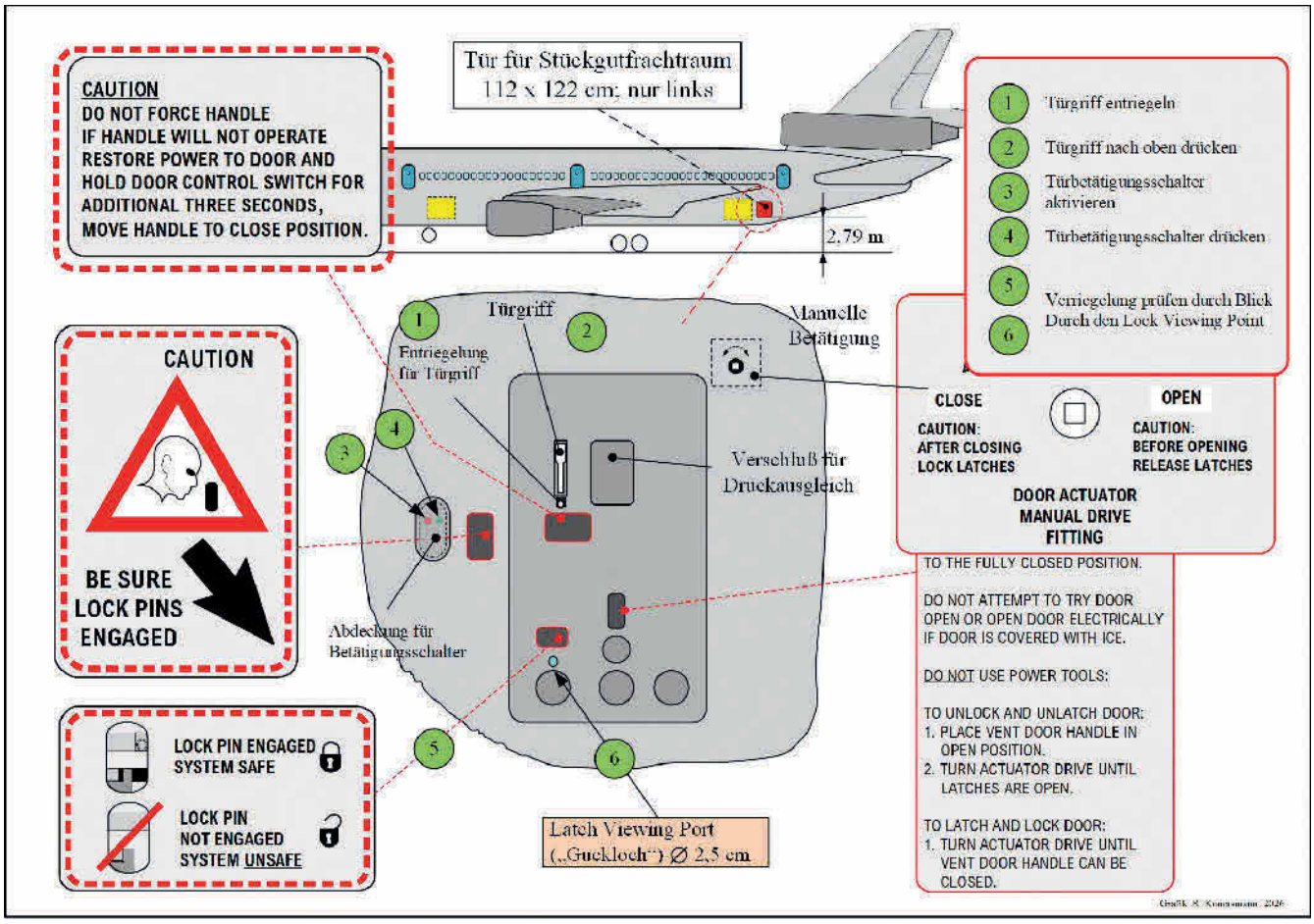



**Bild 7:** Die überarbeitete Bedienung der Frachtraumtür nach dem Windsor-Vorfall 1972. *Grafik: R. Konersmann*

## Das Gewissen eines Ingenieurs

Nach dem „Windsor-Vorfall", dem Schuss vor den Bug, den die Chefetage von McDonnell Douglas der FAA als belanglos verkaufen konnte, regte sich das Gewissen des Ingenieurs Frederick Daniel („Dan") Applegate (9.11.17–17.1.1999). Applegate war Leiter einer Entwicklungsabteilung bei Convair, die mit der Konstruktion des DC-10 Rumpfes beauftragt war, einschließlich der Frachttüren. Einige Wochen nach der Beinahekatastrophe des American-Airlines-Flugs 96 verfasste er einen offenen Brief an seine Vorgesetzten, in dem er darauf aufmerksam machte, dass die Schließmechanik der DC-10 Frachttür nicht zuverlässig sei.

Das „Applegate-Memo" kritisierte die von McDonnell Douglas und der FAA abgenickte Notlösung heftig und warnte eindrücklich davor, dass dieses Provisorium zu einer Katastrophe führen könnte. Es passt zu den Spielregeln des Geschäftslebens, dass das Management von Convair sich dazu nicht äußern wollte. Man fühlte sich nicht zuständig dieses Memo an McDonnell Douglas weiterzuleiten. Die bislang guten Geschäftsbeziehungen sollten unter keinen Umständen Schaden nehmen. Man ist geneigt, diesbezüglich an das Sprichwort mit den Rabenvögeln zu erinnern, die sich gegenseitig nichts Böses antun. Der Autor sieht davon ab, hält den Hinweis jedoch für notwendig. Jedenfalls sollten sich die Warnungen des „Applegate-Memorandums" bald bestätigten. Am 3. März 1974 ereignete sich einer der schwersten Unfälle der zivilen Luftfahrt, ausgelöst durch das Versagen einer Frachtraumtür.

## Turkish Airlines Flug 981

Am 3. März 1974 startete der Turkish Airlines Flug 981 um 12:30 Uhr Ortszeit vom Flughafen Paris-Orly nach London Heathrow. An Bord befanden sich 333 Passagiere, 2 Piloten und 11 Flugbegleiter. Die DC-10 flog zunächst Richtung Osten und drehte dann nach Norden ab um Paris zu umfliegen, wegen des Lärmschutzes. Gegen 11:38 Uhr wurde die Flugfläche 90 erreicht, also eine Höhe von circa 2 743 m über Meereshöhe. Einige Sekunden vor 11:40 Uhr registrierte die Cockpit-Sprachaufzeichnung das Geräusch einer Dekompression, kommentiert vom Co-Piloten mit der Bemerkung, dass wohl der Rumpf geplatzt sei. Gleichzeitig ertönten im Cockpit akustische Warnsignale, die einen Druckverlust und Bruchteile später eine Geschwindigkeitswarnung meldeten. Um 11:40:13 Uhr verschwand Flug TK 981 vom Sekundärradar des Fluglotsens. Zu erkennen war noch die Höhenangabe FL 130, also eine Höhe von circa 3 960 m. Die spätere Untersuchung ergab, dass sich während des Steigflugs die Frachtraumtür öffnete und dann abriss. Als die Tür kollabierte betrug die Flughöhe ungefähr 3 900 m. Die Druckdifferenz lag zwischen 330 und 360 hPa [10]. Die Tür war 1,12 m breit und 1,22 m hoch. Dies bedeutet, dass ungefähr 4,5 bis 5 t Luft von innen gegen eine nur teilweise verriegelte Tür drückten. Nach

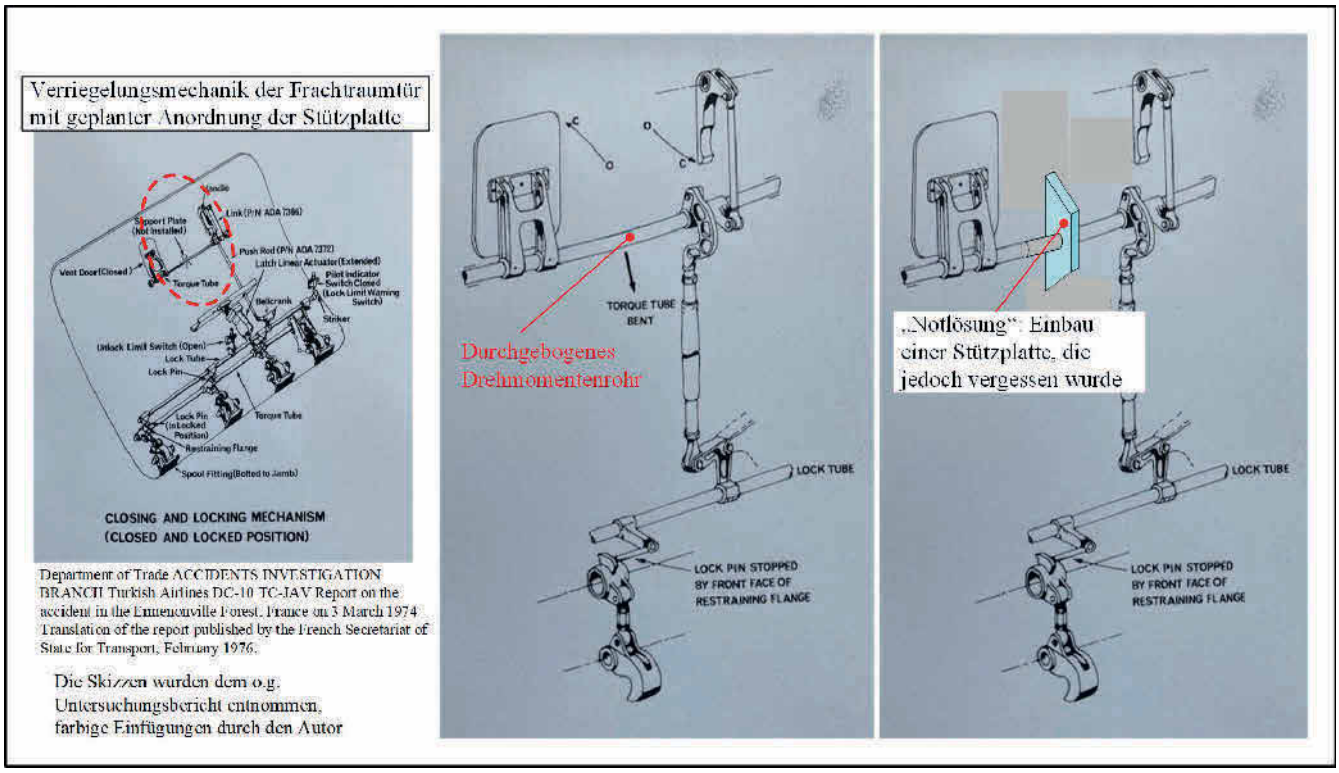



**Bild 8:** Der Verschlussmechanismus der hinteren Frachtraumtür. *Grafik: Autor*

dem rasanten Druckverlust im hinteren Frachtraum lastete der Innendruck nun auf dem Fußboden, auf dem die Sitzreihen befestigt sind. Infolge des Druckausgleichs brachen Teile des Bodens ein, sodass die hinteren zwei Sitzreihen mitsamt den sechs dort angeschnallten Passagieren aus der Maschine gesaugt wurden. Die DC-10 stürzte in einen Wald. Die Schneise war 700 m lang und 100 m breit. Die Zerstörung war so verheerend, dass einige der 346 Opfer nie identifiziert werden konnten. Die Umstände des Verlusts von Turkish-Airlines-Flug 981 waren nahezu identisch mit dem Vorfall mit American-Airlines-Flug 96 (Windsor).

Der Gepäckabfertiger, also der letzte Mann, der gegen 10:35 Uhr die Tür schloss, stammte aus Algerien. Er beherrschte zwei Sprachen fließend: Arabisch und Französisch. Mit dem Englischen tat er sich schwer. Die Hinweisbeschriftungen auf der Tür verstand er nicht. Er hatte zwar hin und wieder beobachtet, dass ein Bodeningenieur durch das Guckloch schaute, doch weshalb und warum, blieb ihm verborgen [11]. Ihm war nie erklärt worden, warum dies notwendig war.

Er wird später zu Protokoll geben, dass er beim Schließen der Tür keinen übermäßigen Widerstand verspürt hatte und daher davon ausgegangen war, dass die Tür sicher verriegelt war.

Die Unglücksmaschine wurde drei Monate nach der Veröffentlichung der Service-Bulletins, die nach dem Windsor-Unfall zwischen McDonnel Douglas und einigen FAA-Mitarbeitern ausgekungelt wurden, fertiggestellt. Weitere drei Monate später wurde sie an Turkish Airlines ausgeliefert. Aus den Arbeitsprotokollen der Baunummer 29 (der abgestürzten Maschine) ging hervor, dass alle Umbauarbeiten durchgeführt worden waren. Tatsächlich war die wichtigste Konstruktionsänderung, die das Verbiegen des Drehmomentrohrs verhindern sollte, nicht ausgeführt worden (**Bild 8**). Im Laufe der Zeit wurde das Drehmomentrohr zunehmend beansprucht und „ausgeleiert", was dem Gepäckabfertiger von Flug 981 vorgaukelte, dass die Tür verriegelt sei, obwohl dies nicht der Fall war.

## Das Geständnis

Drei Wochen nach der Katastrophe lud McDonnell Douglas zu einer Pressekonferenz ein. Der Präsident musste vor den versammelten Journalisten zugeben, dass die verunglückte Maschine der Turkish Airlines das Werk ohne die entscheidende Korrektur der hinteren Frachtraumtür verlassen hatte. Wie dies geschehen konnte, konnte er nicht erklären. In allen Produktionsprotokollen zu den einzelnen Fertigungsschritten war nachzulesen, dass alle Arbeiten ausgeführt wurden. Irgendjemand musste die Aktenlage, ohne Kenntnis der Vorgesetzten, der gewünschten Wirklichkeit angepasst haben. Der Präsident der McDonnell Douglas Corporation versicherte, dass diese Angelegenheit aufgeklärt wird, mit allem Nachdruck. Einer seiner Ausführungen dazu lautete: „Wir wissen, dass wir eine große Verantwortung haben, und wir nehmen diese Verantwortung sehr ernst. Es dürfte Ihnen wie uns bewußt sein, dass eine Douglas-Maschine immer eine Douglas-Maschine bleibt, gleichgültig, wem sie gehört, wie lange sie im Einsatz ist oder was mit ihr geschieht, noch lange nachdem wir keine Kontrolle mehr über sie haben. Unsere Flugzeuge sind ein Teil unseres Lebens, ein Teil unserer Identität – auch aus diesem Grund entwickeln und bauen wir sie mit soviel Sorgfalt." (Zitat entnommen [12]).

Die Vorhersage des Ingenieurs Dan Applegate hatte sich leider erfüllt, für ihn war die Katastrophe keine Überraschung. Die DC-10 war aufgrund von Problemen mit der Frachttür abgestürzt, so, wie er es vorhergesehen hatte. Seine Intervention

prallte an seinen Vorgesetzten ab. Durch die juristischen Auseinandersetzungen und die Schadenersatzklagen wurde sein Memorandum doch noch weltbekannt. Seitdem gilt es als ein Beispiel für verantwortungsbewusstes Handeln.

## Eine Bemerkung zum Schluss

Ein Passagierflugzeug hat für seine Größe ungewöhnlich viele Türen, dies ist eigentlich nicht weiter verwunderlich. Das Ein- und Aussteigen soll ja nicht ewig dauern, und für den Ernstfall gibt es sogar noch extra Ausgänge. Die Passagiertüren sind ausgeklügelte Konstruktionen, die sich sogar fast selbsterklärend bedienen lassen. Sie werden zudem von ausgebildetem Personal bedient, mehrmals täglich, jahrelang, ohne Probleme. Die Frachtzugänge im „Bauch" des Fliegers sind nicht minder wichtig, sie müssten in sicherheitstechnischer Hinsicht ebenso raffiniert durchkonstruiert sein wie die Passagiertüren. Sie sind im Grunde genommen genauso wichtig, eher noch wichtiger, denn sie werden auf den Flughäfen der Welt von den unterschiedlichsten Menschen bedient. Viele sind der englischen Sprache nicht mächtig, sind vielleicht Nachauftragnehmer, Seiteneinsteiger, Leiharbeiter, eben alles, was es heute an Beschäftigungsverhältnissen so gibt. Und diese Leute sollen hochwichtige Aufgaben übernehmen und Kontrollfunktionen ausüben, von denen das Leben hunderter von Menschen abhängt. Was also liegt näher, als ihnen diese Arbeit abzunehmen und den Schließmechanismus konstruktiv so zu gestalten, dass nichts schief gehen kann? Es musste sich erst eine Katastrophe ereignen, eine für die McDonnell Corporation ausweglose Situation entstehen, bis sich die vom Präsidenten John Brizendine (3.8.1925–2.7.2024) gepriesene Sorgfalt durchsetzte. ■ TS1132

**Literatur**

[1] https://aktuelles.uni-frankfurt.de/forschung/rationalitaet-und-moralitaet-schliessen-sich-nicht-aus
[2] Lagemann, M.: Dichtung und Wahrheit, Passagiertüren in Verkehrsflugzeugen, Flug Revue 8/2007.
[3] NTSB: Aviation Investigation Report AIR-25–04.
[4] https://www.smithsonianmag.com/air-space-magazine/book-excerpt-flight-981-disaster-180967121/
[5] NTSB: Aircraft Accident Report NTSB-AAR-73–2: American Airlines, Inc. McDonnell Douglas DC-10–10, N103AA, near Windsor, Ontario, Canada, June 12,1972.
[6] https://www.designnews.com/aerospace/designed-for-disaster-the-dc-10-airliner
[7] DER SPIEGEL 49/1976: Flug in den Tod.
[8] U.S. Government Printing Office: Report by the Special Subcommittee on Investigations of The Committee on Interstate and Foreign Commerce, House of Reprensentatives, Ninety-Third Congress, Second Session, Washington, December 1974.
[9] Time online: SCANDALS: The Great DC-10 Mystery, https://content.time.com/time/subscriber/article/0,33009,908559-2,00.html
[10] Department of Trade, Accindents Investigation Branch: Turkish Airlines DC-10 TC-JAV Report on the accident in the Ermenonville Forest, France on 3 March 1974. Translation of the report published by the French Secretariat of State for Transport, February 1976.
[11] Stewart, St.: Flugkatastrophen, die die Welt bewegten, Bernhard & Graefe 1989.
[12] DER SPIEGEL 50/1976: Flug in den Tod.

Dr.-Ing.
**Rainer Konersmann**

Ehemals Bundesanstalt für Materialforschung und -prüfung (BAM)

# Neue Sicherheitsbox für Drohnen-Ports von hensec

Für Drohnenbetreiber, die sich vor dem Start einer Drohne versichern wollen, dass keine Störsender oder andere Flugobjekte im näheren Umkreis sind, hat das Sicherheitsunternehmen hensec das System „Drone-MonSta Box" entwickelt. In der Nähe von Drohnen-Ports installiert, erkennt es automatisch Jamming und Spoofing der GPS-Signale sowie Flugobjekte aller Art. Im Falle einer GPS-Anomalie oder einer anderen Drohne in der unmittelbaren Umgebung wird ein Alarm ausgelöst, um den automatischen Start einer Drohne zu verhindern. Zielgruppe sind Behörden und Organisationen mit Sicherheitsaufgaben (BOS) wie Polizei, Feuerwehr, Rettungsdienste sowie Katastrophenschutz- und Zivilschutzorganisationen. Hinzu kommen Drohnenbetreiber mit BVLOS-Genehmigung (Beyond Visual Line of Sight), die für autonome Starts auf eine „saubere" Luftlage angewiesen sind. Diese Drohnen, die außerhalb der direkten Sichtweite des Piloten fliegen, werden beispielsweise für Lieferdienste, Inspektionen oder Überwachungsflüge eingesetzt. Darüber hinaus ist der Einsatz des Systems auch bei Drohnenshows angeraten.

Wie hensec betont, wird „Drone-MonSta" in Deutschland hergestellt. Alle Komponenten stammen ausnahmslos aus EU-Ländern (Entwicklung und Fertigung). Das gesamte System ist in einem kompakten, wetterfesten Außengehäuse untergebracht und lässt sich einfach am Startplatz oder auf dem Dach eines Kontroll- beziehungsweise Sicherheitsgebäudes installieren. Neben dem System für den stationären Betrieb („Drone-MonSta Box") ist auch eine portable Kofferversion („Drone-MonSta Case") erhältlich. Technisch kombiniert das System eine fortschrittliche Luftraumüberwachung mit einer kontinuierlichen Überprüfung der GNSS-Qualität. Drone-Monsta visualisiert den überwachten Luftraum lückenlos und bietet dadurch einen umfassenden Überblick über den gesamten Luftverkehr rund um den autonomen Startpunkt. Hierzu integriert hensec Daten aus allen relevanten Quellen einschließlich DroneID (Fernidentifikation von Drohnen), ADS-B (Automatic Dependent Surveillance–Broadcast, automatisches Aussenden von Positionsdaten durch Luftfahrzeuge), ADS-L (Automatic Dependent Surveillance–Local, lokale Positionsübertragung im begrenzten Luftraum), FLARM (Flight Alarm, Kollisionswarnsystem für Luftfahrzeuge) und bei Bedarf noch weiteren Sensoren. Alle relevanten Informationen sowie eventuelle andere Drohnen im Startbereich werden auf einer einheitlichen Benutzeroberfläche dargestellt.

*www.hensec.com; www.luftraumueberwachung.com/de; www.euromarcom.de*

**Die Zukunft von Rechenzentren**

# Sicherheitsmaßnahmen im Zeitalter der KI

KI und Cloud treiben den Ausbau von Rechenzentren voran und erhöhen die Anforderungen an Sicherheit, Resilienz und Effizienz. Betreiber müssen sich gegen Bedrohungen wappnen und gleichzeitig Verfügbarkeit und Energieeffizienz aufrechterhalten. Gefragt ist ein vernetztes, adaptives Sicherheitsökosystem, das Risiken vorhersieht und Reaktionen automatisiert.

**TEXT:** *Achim Keifert*

Mit dem rasanten Wachstum von KI- und Cloud-Anwendungen hat die Nachfrage nach Rechenzentren im Jahr 2025 neue Höchststände erreicht. Branchenprognosen deuten darauf hin, dass sich der europäische Markt für Rechenzentren bis 2030 fast verdoppeln und jährlich um knapp 13 % wachsen könnte. Das ist ein deutliches Signal für eine anhaltend hohe Nachfrage [1]. Mit den steigenden Investitionen in diese kritischen Infrastrukturen vergrößert sich zugleich die Angriffsfläche und damit das Risiko, Ziel von Sicherheitsvorfällen zu werden.

Der Schutz von Rechenzentren und anderer kritischer Infrastrukturen erfordert mehr als reaktive Maßnahmen. Gefragt ist ein integriertes, adaptives System, das Lagebilder verbessert, Bedrohungen frühzeitig erkennt und automatisierte Reaktionen ermöglicht.

Auch wenn die Wachstumsraten regional variieren, ist die Tendenz einheitlich: Mit dem beschleunigten Ausbau steigen auch die Anforderungen an Betrieb und Sicherheit. Dieser Druck ist auch in Europa, insbesondere in Deutschland, deutlich spürbar. Der steigende Bedarf an KI- und Cloud-Diensten setzt Rechenzentren unter Druck, Kapazitäten schnell und in großem Umfang bereitzustellen – oft unter infrastrukturellen Einschränkungen.

Allein in Berlin belaufen sich die ausstehenden Anträge auf Netzanschlüsse für Rechenzentren auf insgesamt rund 2,8 GW und übersteigen damit die verfügbare Kapazität der Stadt [2]. Bundesweit führen Engpässe im Stromnetz zu Verzögerungen von bis zu sieben Jahren beim Anschluss, wie die IEA berichtet. Diese Einschränkungen bremsen nicht nur den Ausbau, sondern erhöhen auch die betriebliche Komplexität und damit die potenzielle Angriffsfläche. Wenn Betreiber bestehende Infrastrukturen optimieren, Übergangslösungen integrieren oder Projekte beschleunigt umsetzen, wird es schwieriger, einheitliche Sicherheitsstandards zu gewährleisten. Das erhöht den Bedarf an integrierten und adaptiven Sicherheitsstrategien.

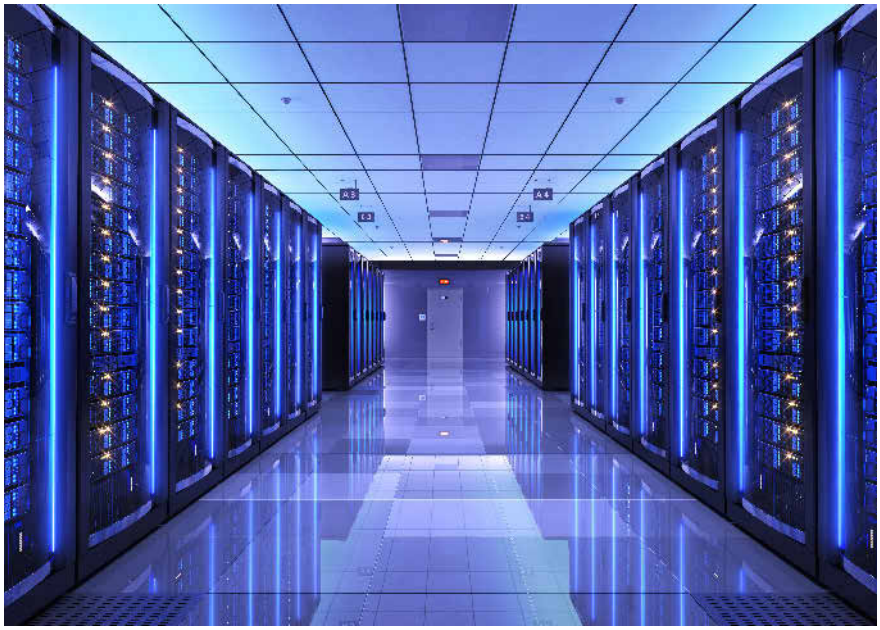


*Foto: Smarterpix/Sashkin7*

## Hybride Bedrohungen nehmen zu

Cyberangriffe entwickeln sich ebenso schnell weiter wie die Technologien, auf die sie abzielen. Für die kommenden zwölf Monaten zeichnet sich eine weitere Verschärfung ab: Sowohl Umfang als auch Intensität dürften weiter zunehmen. KI-gestützte Phishing-Angriffe und zunehmend ausgefeilte Ransomware erhöhen den Druck auf OT-Umgebungen in allen Branchen. Laut dem Honeywell Cyber Threat Report stieg die Zahl der Ransomware-Erpressungsfälle um 46 % [3]. Darüber hinaus verzeichnete der Jahresbericht des National Cyber Security Centre einen Anstieg um 50 % bei gravierenden Cybervorfällen und bezeichnete Ransomware als die „akuteste und am weitesten verbreitete“ Cyberbedrohung der Gegenwart [4].

Für Rechenzentren verschärft sich diese Lage durch die zunehmende Konvergenz von IT und OT. Gebäudemana-

gementsysteme, HLK-Anlagen und IoT-Sensoren können zu Einfallstoren für Cyberangriffe werden, wenn sie nicht überwacht oder gepatcht werden. Diese Konvergenz erhöht den Bedarf an Sicherheitskonzepten, die sowohl digitale als auch betriebliche Umgebungen abdecken.

Gleichzeitig verändert sich die physische Bedrohungslage. Fortschritte in der Drohnentechnologie ermöglichen beispielsweise neue Formen der Überwachung oder unbefugte Zugriffsversuche. Zudem entstehen durch den Ausbau von Rechenzentren in ländlichen Regionen neue Risikofaktoren: begrenzte Infrastruktur, eingeschränkte Notfallressourcen und Fachkräftemangel beeinflussen zunehmend Sicherheitskonzepte und Reaktionsstrategien.

Um diesen Entwicklungen zu begegnen, muss sich die Sicherheit von Rechenzentren von isolierten Einzellösungen hin zu einem durchgängig vernetzten Sicherheitsökosystem entwickeln.

## Von reaktiver Abwehr zu vernetzter, adaptiver Sicherheit

Die Zukunft liegt in der Integration: physische, digitale und operative Informationen werden in einem einheitlichen System zusammengeführt. Cloudbasierte Plattformen ermöglichen es nun, diese Ebenen miteinander zu verbinden.

Ein integrierter Ansatz bündelt verschiedene Sicherheitsanwendungen, um physischen Schutz und Cybersicherheit zu verbinden. So erhalten Rechenzentrumsbetreiber einen durchgängigen Überblick über ihre Risiken. Die Zusammenführung von Zutrittskontrolle, Videoüberwachung, Einbruchmeldetechnik und Cybersicherheit in einer Plattform ermöglicht es, Echtzeit-Transparenz gewinnen, blinde Flecken minimieren und ihre Reaktionsabläufe optimieren.

Dieser Trend zur Integration spiegelt einen umfassenderen Wandel im Gebäudebetrieb wider: den Übergang von traditionellen Steuerungsmechanismen hin zu intelligenzgesteuerten Abläufen. Betreiber aller Branchen benötigen Tools, die Silos aufbrechen, Routineaufgaben automatisieren und konkrete Einsichten liefern, die ihnen helfen, Anlagen effizienter zu betreiben – Fähigkeiten, die mittlerweile zu grundlegenden Erwartungen geworden sind.

## Schlüsseltechnologien für durchgängige Transparenz und Reaktionsfähigkeit

- KI-gestützte Videoanalyse kann Anomalien erkennen und klassifizieren, darunter unbefugte Zutritte, ungewöhnliche Bewegungen oder Unregelmäßigkeiten, die dann automatische Warnmeldungen oder Workflow-Aktionen auslösen können.
- Mobile Zugangsdaten und erweiterte Authentifizierung bieten eine sichere, nachverfolgbare Zugangskontrolle. Im Gegensatz zu physischen Schlüsselkarten, die verloren gehen oder leicht geklont werden können, schützen mobile Zugangsdaten in Verbindung mit biometrischer Verifizierung die Identität der Benutzer und reduzieren Reibungsverluste.

### COSTUMER EXPERIENCE CENTER

Honeywell hat in Ratingen ein neues Customer Experience Center für vernetzte Gebäudetechnologien eröffnet. Dort zeigt das Unternehmen, wie Automatisierung und Physical AI die Leistungsfähigkeit und Effizienz des Gebäudebestands in Deutschland verbessern können. Das Zentrum dient als europäische Plattform für Innovation und Zusammenarbeit rund um Gebäudetechnologien in unterschiedlichen Branchen. Besucher erhalten Einblicke, wie digitale Lösungen und automatisierte Prozesse den Betrieb von Gebäudeportfolios optimieren können – etwa durch vorausschauende Wartung oder intelligentes Energiemanagement. Mit dem neuen Customer Experience Center adressiert Honeywell zentrale Herausforderungen im Gebäudebetrieb: von heterogenen Infrastrukturen, wechselnden Nutzungs- und Sicherheitsanforderungen bis hin zu zunehmend strengeren Vorgaben im ökologischen und Umweltbereich. Vorgestellt werden Technologien, die Unternehmen dabei helfen, regulatorische Vorgaben einzuordnen und neue operative Effizienzpotenziale in Gebäuden verschiedenster Branchen zu erschließen.

- Integration von Cybersicherheit trägt dazu bei, dass jedes Gerät im vernetzten System – von HLK-Anlagen bis zu IoT-Geräten – geschützt, gewartet und kontinuierlich auf Einbruchsversuche überwacht wird.
- Cloudbasierte Zutrittskontrolle ermöglicht die Fernverwaltung und -überwachung von Sicherheitssystemen. So können Betreiber von jedem Standort aus Berechtigungen aktualisieren, Zugriffsprotokolle überwachen und umgehend auf Vorfälle reagieren.

Im Zusammenspiel ermöglichen diese Technologien eine verbesserte Lageübersicht, schnellere Erkennung und automatisierte Reaktionen – sei es durch das Melden eines kompromittierten Geräts, das automatische Sperren eines Bereichs oder das Auslösen von Videoüberwachung zur Aufzeichnung wichtiger Bilder.

## Interoperabilität: die Grundlage für integrierte Betriebsabläufe

Um einen intelligenten Betrieb in großem Maßstab zu erreichen, ist eine bessere Interoperabilität unerlässlich. Da Gebäude immer mehr Informationen generieren, benötigen Betreiber Systeme, die Daten anhand gemeinsamer Standards und Ontologien interpretieren können. Bis vor kurzem basierten die Anlagen auf herstellerspezifischer Software und geschlossenen Datenmodellen, was eine Integration extrem erschwerte. Diese Fragmentierung hat weitere Innovationen behindert.

Mit dem rasanten Anstieg von KI- und IoT-Geräten bauen vernetzte Frameworks diese Barrieren nun ab, ermöglichen einen freieren Informationsfluss über unterschiedliche Anlagen hinweg und sorgen dafür, dass die Automatisierung fundiertere Maßnahmen ergreifen kann. Dank einer stärker standardisierten Datenstruktur können Betreiber die Leistung mehrerer Systeme über eine einzige Schnittstelle bewerten und durchgängige Maßnahmen koordinieren, die zuvor erhebliche manuelle Eingriffe erforderten.

Mit der Weiterentwicklung dieser Frameworks wird die Interoperabilität wohl zu einem entscheidenden Faktor bei der Anbieterauswahl werden, wobei Branchenverbände intensiv daran arbeiten, Standards zu formalisieren, die eine nahtlosere Integration ermöglichen.

## Automatisierung und prädiktive Datenanalyse

Der Übergang zu KI-gestützten Gebäudemanagementsystemen trägt in mehreren Bereichen zu einer verbesserten Effizienz und Leistung bei. Durch die Zusammenführung von Gerätedaten, wie Temperatur und Energieverbrauch, können diese Plattformen die Leistung analysieren und im Laufe der Zeit Ausfälle vorhersagen, bevor sie den Betrieb stören. Vorausschauende Analysen ermöglichen es Wartungsteams, Störungen lange vor ihrem Auftreten zu erkennen, was frühzeitige Warnungen und eine rechtzeitige Planung von Wartungsarbeiten ermöglicht und gleichzeitig dazu beiträgt, die Lebensdauer kritischer Anlagen zu verlängern.

Beispiele hierfür sind der Einsatz von KI-gestütztem Gebäudemanagement durch Verizon, um kritische Gebäude- und Systemprobleme vorherzusagen, bevor sie schwerwiegend und kostspielig werden, sowie die Nutzung einer KI-Plattform durch die Vanderbilt University zur Steigerung der Effizienz von Gebäudesystemen und zur Senkung des Energieverbrauchs, insbesondere in älteren Gebäuden [5].

Der Echtzeit-Zugriff auf Daten verändert auch die Art und Weise, wie Betreiber Entscheidungen treffen. Anstatt sich auf historische Berichte zu verlassen, können sie in Echtzeit sehen, wie Systeme funktionieren, und Anpassungen vornehmen, um den Energieverbrauch zu optimieren – einer der höchsten Betriebskostenfaktoren in Einrichtungen.

## Planungsaspekte für widerstandsfähigere Rechenzentren

Der Bedarf an Datenspeicherung und -verarbeitung steigt, da Unternehmen sich bei ihrer Entscheidungsfindung auf Daten stützen und diese zur Verbesserung der betrieblichen Effizienz nutzen. Dieses Wachstum wirkt sich sowohl auf das Datenvolumen aus, das Rechenzentren verarbeiten müssen, als auch auf die Anzahl der benötigten Rechenzentren. Eine Herausforderung dieses Wachstums ist die Bewältigung der energetischen Auswirkungen: Schätzungen zufolge könnten Rechenzentren bis 2030 bis zu 10 % des weltweiten Wachstums des Strombedarfs ausmachen [6].

Moderne Kühltechnologien, energieeffiziente Kältemittel und alternative Kühlsysteme tragen zur Reduzierung von Energieverbrauch und Emissionen bei. Auch Energiespeicherlösungen (BESS), thermische Speicher (TESS) und erneuerbare Kraftstoffe gewinnen an Bedeutung, um Versorgungssicherheit und Nachhaltigkeit zu verbessern.

Systeme zur Energieüberwachung (EPMS) liefern zudem wichtige Daten zur Optimierung des Betriebs. Gleichzeitig sollten IT- und OT-Komponenten regelmäßig modernisiert werden, um Effizienzgewinne zu realisieren.

## Warum KI zu einem leistungssteigernden Faktor wird

Der Personalmangel stellt für Facility-Teams nach wie vor eine anhaltende Belastung dar, da viele Unternehmen Schwierigkeiten haben, erfahrene Fachkräfte einzustellen oder zu halten. Angesichts dieses anhaltenden Drucks entwickelt sich KI zu einem unverzichtbaren Assistenten an vorderster Front. KI als Kraftmultiplikator für Teams auf jedem Qualifikationsniveau hilft dabei, Zustände zu bewerten, Probleme aufzudecken, die Aufmerksamkeit erfordern, und geeignete nächste Schritte vorzuschlagen, insbesondere in Zeiten hoher Arbeitsbelastung oder personeller Engpässe. Zudem sollen bis Ende 2026 vorausschauende Wartung und automatisierte Energieanpassungen als Standardpraxis unauffällig im Hintergrund laufen, und damit das, was einst als Spitzentechnologie galt, in alltägliche Realität verwandeln.

## Sicherheit durch vernetzte Systeme neu denken

Ein vernetzter Sicherheitsansatz ist entscheidend, um Rechenzentren wirksam gegen zunehmend komplexe Bedrohungen zu schützen. Durch die Integration von physischer Sicherheit, Cybersicherheit und Betriebsdaten entsteht ein ganzheitliches Lagebild, das schnellere Reaktionen und fundierte Entscheidungen ermöglicht.

Angesichts wachsender Angriffsflächen und hybrider Bedrohungsszenarien kommt es darauf an, Risiken frühzeitig zu erkennen, Sicherheitsprozesse zu automatisieren und Systeme kontinuierlich zu überwachen. Moderne, vernetzte Lösungen tragen dazu bei, Sicherheitslücken zu reduzieren und den Schutz kritischer Infrastrukturen nachhaltig zu verbessern.

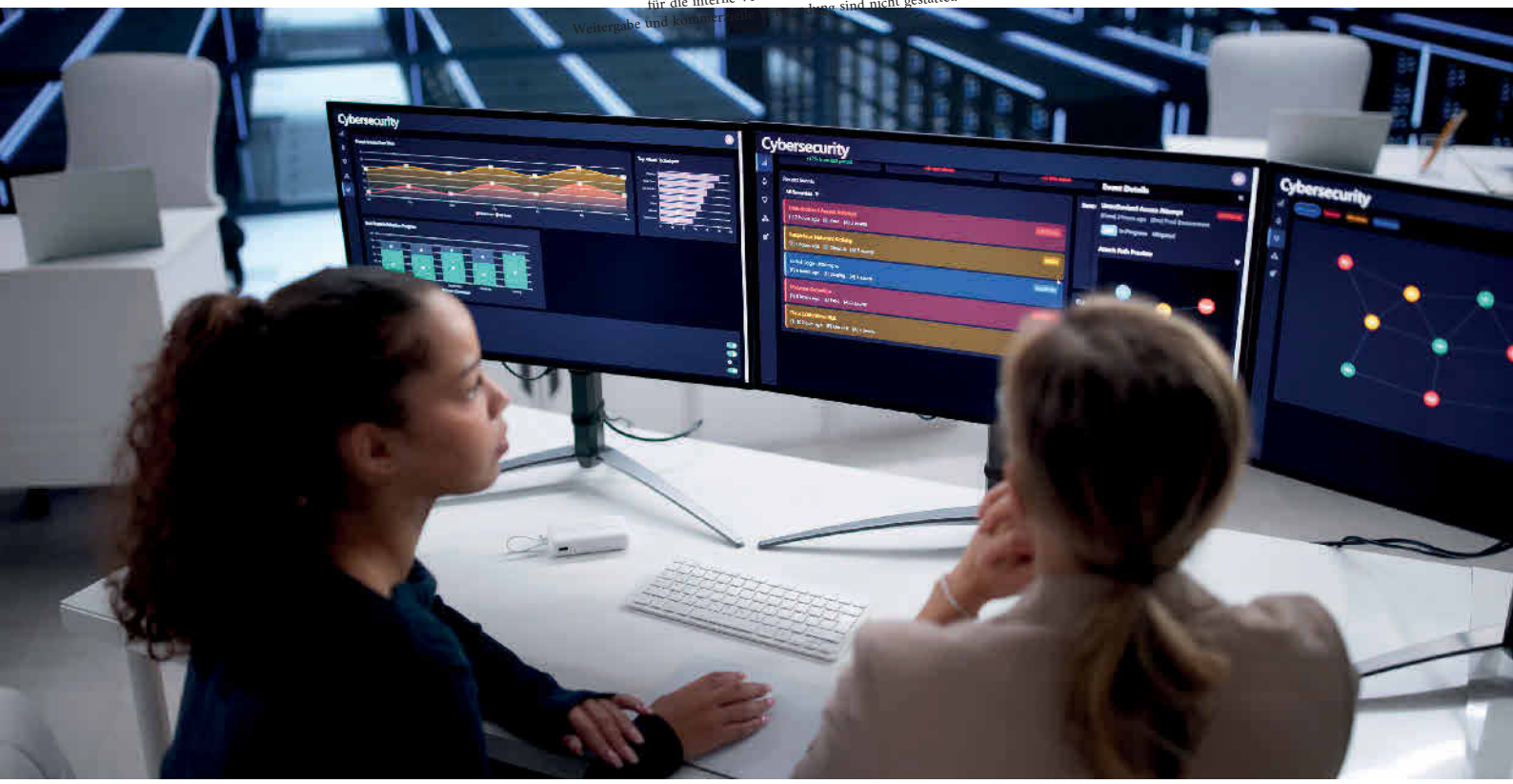
Rechenzentren sind ein zentraler Bestandteil der digitalen Infrastruktur. Umso wichtiger ist es, Sicherheitsstrategien konsequent weiterzuentwickeln und an neue technologische und regulatorische Anforderungen anzupassen. Angesichts der zunehmenden Verbreitung von Rechenzentren ist es entscheidend, dass Betreiber zudem Wege finden, den Energieverbrauch und die Resilienz besser zu steuern. Es bedarf also einer Reihe von Maßnahmen, nicht nur einer einzigen, um dies zu erreichen und für die Zukunft besser gerüstet zu sein. ■ TS1140

**Literatur**

[1] Research and Markets: Europe Data Center Market Landscape 2025-2030. Mai 2025, https://www.researchandmarkets.com/reports/5550000/europe-data-center-market-landscape-2025-2030?, zuletzt abgerufen am 23.4.2026.
[2] German Datacenter Association: Datacenter Outlook Germany 2025/26. German Datacenter Conference, https://www.germandatacenters.com/en/news-en/publications/datacenter-outlook-germany-2025/26, zuletzt abgerufen am 23.4.2026.
[3] National Cyber Security Centre: UK experiencing four 'nationally significant' cyber attacks every week. Pressemitteilung vom 14.10.2025, https://www.ncsc.gov.uk/news/uk-experiencing-four-nationally-significant-cyber-attacks-weekly, zuletzt abgerufen am 23.4.2026.
[4] Honeywell: Honeywell 2025 Cyber Threat Report. Juni 2025, https://www.honeywell.com/content/dam/honeywellbt/en/documents/gated/hon-corp-honeywell-2025-cyber-threat-report.pdf, zuletzt abgerufen am 23.4.2026.
[5] Honeywell: Honeywell Unveils AI-Powered Building Management Solution. Pressemitteilung vom 10.7.2025, https://www.honeywell.com/us/en/press/2025/06/honeywell-unveils-ai-powered-building-management-solution, zuletzt abgerufen am 23.4.2026.
[6] Bundesministerium für Wirtschaft und Energie: Wie Rechenzentren unseren Energiebedarf antreiben. Energiewende direkt 07/2025, https://energiewende.bundeswirtschaftsministerium.de/EWD/Redaktion/Newsletter/2025/07/Meldung/direkt-erfasst.html, zuletzt abgerufen am 23.4.2026.

**Achim Keifert**

Chief Commercial Officer – Europe, Building Automation bei Honeywell.




**Die Wirtschaft gerät immer stärker in das Fadenkreuz** professioneller Cyberkrimineller. (Symbolbild) *Quelle: smarterpix_AndreyPopov*

# Cybercrime – Tendenzen 2025/2026

Die Digitalisierung nahezu aller Wirtschafts- und Lebensbereiche führt dazu, dass Cybercrime ein beständig wachsendes Segment krimineller Bedrohungen einnimmt. Dabei ist eine Reihe von Trends zu beobachten, die in das Jahr 2026 hineinreichen.

**TEXT:** *Reinhard Rupprecht*

## Cybercrime im engeren und weiteren Sinne

Die Sicherheitsbehörden unterscheiden zwischen Computerkriminalität oder Cybercrime im engeren Sinn, Straftaten, die sich gegen das Internet und informationstechnische Systeme richten und in der Polizeilichen Kriminalstatistik (PKS) im einzelnen kategorisiert werden (so Computerbetrug, der circa 80 % von Cybercrime im engeren Sinn ausmacht, Fälschung beweiserheblicher Daten und rechtsrelevante Täuschungen bei der Datenverarbeitung, Datenveränderung, Computersabotage, Ausspähen von Daten und Datenhehlerei) und Cybercrime im weiteren Sinn. Darunter fallen alle Delikte, die unter Nutzung von Informationstechnik begangen werden, bei denen das Internet vorwiegend Tatmittel ist. Die Wirtschaft gerät immer stärker in das Fadenkreuz professioneller Cyberkrimineller. Die Zahl der Opfer auf Unternehmensseite hat sich seit 2020 verdreifacht und ist allein 2025 um über 90 % angestiegen [1]. Die PKS weist im Jahr 2013 circa 89 000, 2023 rund 134 000 Fälle auf. 2024 ist die Zahl zwar auf über 131 000 leicht gesunken. Die Sicherheitsbehörden gehen jedoch von einem fünfmal so hohen Dunkelfeld nicht angezeigter Fälle aus. Hinzu kommen 2024 weitere über 200 000 Cyber-Straftaten, die vom Ausland oder einem unbekannten Ort aus begangen wurden und daher in der PKS nicht registriert werden Nicht einmal jeder dritte Fall wurde 2024 aufgeklärt (31,9 %). Der Trend ist auch für 2026 ansteigend. Denn

die Professionalität der Täter nimmt beständig zu. Und auch die Sicherheitslücken und schlecht geschützten Schwachstellen haben zugenommen. Bei einer Befragung von Unternehmen in der Schweiz durch die Hochschule Luzern im Jahr 2025 gingen über 80 % der Befragten von einem weiteren Anstieg der Cyberkriminalität aus [2].

## Ransomware und Datenexfiltration

Ransomware bleibt die prägende Bedrohung im Cyberraum, auch wenn international koordinierte Ermittlungen der Sicherheitsbehörden 2024 gegen Ransomware-Banden zu einem Rückgang der Angriffe führten. Nach dem von der europäischen Behörde ENISA vorgelegten Bericht „Threat Landscape 2025“ steht Ransomware weiterhin im Zentrum der Angriffe, zumal die Cyber-Botnetze nach den Ermittlungserfolgen ihre Strukturen dezentralisiert und Taktiken geändert haben [3]. Zunehmend zielen die Angriffe nicht primär auf Lösegeldzahlungen ab. Die Erbeutung von Zugangsdaten, die sich im Darknet gut weiterverkaufen lassen, spielt eine immer größere Rolle. Die angezeigten Fälle von Verschlüsselungstrojanern sind 2024 im Vergleich zum Vorjahr von über 1 000 auf circa 950 zurückgegangen. Erwartet werden kann, dass auch in diesem Jahr die Zahl der Ransomware-Angriffe und der Lösegeldzahlungen wenigstens nicht wieder ansteigt.

## Datendiebstahl und DDoS-Angriffe

Hacking-Angriffe verfolgen ganz unterschiedliche Ziele. Zumeist sind sie auf den Diebstahl von Daten, Email-Adressen, Telefonadressen, Wahlanschriften, Kontonummern oder Reisepässen ausgerichtet. Am häufigsten sehen es die Datendiebe auf Microsoft-Programme ab [4]. Etwa ein Viertel der Phishing-Mails zielen bei Angriffen auf Unternehmen auf Daten von Vorständen oder Systemadministratoren. Im Darknet werden bereits „Phishing as a Service-Plattformen“ angeboten. Ein beliebtes Ziel von Hackerangriffen sind QR-Codes, weil sich in ihnen nicht lesbare Hyperlinks codieren lassen. Wird der Code von Zielpersonen eingescannt, landen sie auf einer vom Angreifer kontrollierten Webseite [5]. Auch im Zuge der gegenwärtigen geopolitischen Entwicklungen nehmen hacktivistische DDoS (Distributed Denial of Service)-Angriffe weiter zu [6]. Laut European Cyber Report von dem Computerunternehmen „Link11“ stieg die Zahl der dokumentierten DDoS-Attacken im Link11-Netzwerk im ersten Halbjahr 2025 gegenüber dem Vorjahreszeitraum um mehr als 200 % an. Das Angriffsvolumen habe 438 TB betragen. Während der Zugang zum Onlinebanking zumeist gut abgesichert wird, ist das Email-Postfach oft ein leichtes Ziel für Kriminelle. Nach einer repräsentativen Yougov-Umfrage bei über 2 000 Personen im Auftrag der Initiative „Sicher Handeln“ schützen nur 13 % ihr Email-Konto durch Multifaktor-Authentifizierung und setzen nur 8 % das Sicherungsverfahren Passkey ein. Auch 2026 wird daher die Zahl und die Ausbeute von Hackingangriffen nicht zurückgehen.

## Schadsoftware

Die Herstellung und Verbreitung von Schadsoftware ist ein zentrales Delikt der Cyber-Kriminellen. Besonders hervorzuheben sind Computerprogramme, die Schadsoftware freisetzen und sogar nachladen können. Der Einsatz von Schadsoftware erfolgt multifunktional. Systeme wie Qakbot oder Pikabot sammeln und exfiltrieren Daten, andere wie Truebot dienen als Fernzugriffs-Tool und können den Remote Access auf die befallenen Systeme etablieren [7].

## Betrügerische Angriffe

Trotz des leichten Rückgangs von Fällen des Computerbetrugs 2024 bleibt der Betrug das häufigste Ziel von Cyber-Kriminellen. In einer Umfrage des Bankenverbandes im Herbst 2025 gab ein Viertel der 1 000 Befragten an, sie seien binnen zwei Jahren Opfer eines gelungenen oder versuchten Onlinebetrugs geworden. Einem Bericht des Cyberunternehmens Surfshark zufolge haben Betrüger 2025 weltweit etwa 830 Millionen Euro mithilfe von Deepfakes erschwindelt. Dabei weist die Angriffsart ein breites Spektrum auf. Das zeigt eine Auswahl jüngst gemeldeter Fälle, über die in Medien berichtet wurde. Die häufigsten angegebenen Angriffsszenarien waren Online-Shopping (34 %), Phishing (30 %) und Identitätsbetrug (22 %). Der Einsatz von künstlicher Intelligenz macht es Firmen zunehmend schwer, Betrug klar zu erkennen [8]. Eine Analyse des „Threat Labs“ des IOT-Sicherheitsunternehmens Gen kommt zu dem Ergebnis, dass bereits jede vierte Anzeige auf den Meta-Plattformen Facebook und Instagram in Deutschland einen Betrugsversuch darstellt. In Deutschland haben die Forscher dazu 5,6 Millionen Anzeigen auf Meta-Plattformen analysiert. Am häufigsten ist die Weiterleitung zu gefälschten Shops, die Nutzern Waren verkaufen, die sie gar nicht besitzen. Das BSI warnt vor der neuen Betrugsmasche „Ghost Pairing“ [9]. Der Angriff beginnt meist mit einer Nachricht, die scheinbar von einem Freund stammt, dessen Konto aber bereits gekapert wurde. Die Nachricht enthält einen Link, der auf eine täuschend echt aussehende Webseite führt. Sie zeigt einen Code an, der angeblich der Sicherheit dienen soll. Wer den Code in die eigene WhatsApp eingibt, gestattet einem fremden Gerät vollen Zugriff auf sein Konto.

## Underground Economy

Das Darknet spielt im Bedrohungsspektrum eine zunehmend große Rolle [10]. Sie ist zum primären Umschlagplatz für illegale Waren, gestohlene Datenpakete und „Cybercrime as a Service“-Angebote geworden [11]. Kriminelle Plattformen im Darknet bieten auch technischen Support für Spionage-Software wie Keyloggers oder Remote Access-Trojaner an [12]. Nach einer Bedrohungsanalyse von Europol vom 22. Juli 2024 nutzen vor allem organisierte Banden das Darknet für ihre Geschäftsmodelle. Das Blockchain-Analyseunternehmen Chainalysis schätzt den Umsatz von den ausgewerteten Darknet-Marktplätzen schon im Jahr 2022 auf 1,5 Milliarden $. „Cybercrime as a Service“ wird inzwischen in industriellem Maßstab angeboten. Web.de meldete am 22. August 2025, dass Kriminelle im Darknet ein Datenpaket mit 16 Millionen Paypal-Zugangsdaten zum Schleuderpreis von 750 $ anboten, E-Mail-Adressen und Passwörter, die durch Malware gesammelt wurden. Tendenziell ist für 2026 keine Abnahme dieser Bedrohung zu erwarten.

## Schwachstellen als Eintrittsvektor

Sogenannte Schwachstellen und Sicherheitslücken in IT-Produkten bieten Cyber-Kriminellen hervorragende Angriffsmöglichkeiten. Wie das BSI im Lage-

bericht 2025 mitteilt, wurden im Berichtszeitraum (1. Juli 2024 – 30. Juni 2025) täglich durchschnittlich 119 neue Schwachstellen bekannt, ein Zuwachs von 24 % gegenüber den vorherigen 12 Monaten. Nach Angaben des BSI stecken allein in der aktuellen Google Crome-Version insgesamt 26 solcher Schwachstellen [13]. Auch der am 25. Februar 2026 vorgelegte Lagebericht „2026 X-Force Threat Intelligence Index" von IBM betont, das Kernproblem sei immer das gleiche: Die Systeme der angegriffenen Institutionen haben zu viele Schwachstellen. Nach dem ENISA-Bericht „Threat Landscape 2025" bildet die Ausnutzung von Schwachstellen mit über 21 % den zweithäufigsten Angriffsvektor (nach hacktivistischen Aktivitäten mit fast 80 %). Über 40 % der nach diesem Bericht erfassten Bedrohungen richteten sich gegen Smartphones, vielfach unter Nutzung von Schadsoftware [14]. Es ist zu hoffen, dass die ständigen Hinweise der Sicherheitsbehörden und IT-Sicherheitsunternehmen auf die Gefährlichkeit von Schwachstellen ernst genommen werden. Nutzer sollten den dringenden Empfehlungen folgen, die durch die zumeist von verantwortlichen Herstellern zur Verfügung gestellten Patches sofort aufzuspielen und damit diese Anfälligkeit tendenziell zu reduzieren.

## Einsatz von künstlicher Intelligenz

KI hat die Möglichkeiten, Cybersecurity zu verstärken, enorm erhöht. KI kann verdächtiges Verhalten, Kontexte und zeitliche Abfolgen analysieren und komplexe Angriffsszenarien erkennen, die mit herkömmlichen Methoden kaum sichtbar wären. Und sie kann – insbesondere als KI-Agent – schneller und autonom geeignete Reaktionen gegen Angriffe einleiten. Aber sie ist eben auch für den Missbrauch durch Cyberkriminelle hervorragend geeignet. So werden Phishing-Mails durch den Einsatz von KI sprachlich professioneller und persönlicher, sodass der Empfänger sie nicht als Phishing-Mail erkennt. Ein aktuell bekannt gewordenes Modell von Anthropic namens „Claude Mythos" könnte verheerende Auswirkungen haben, wenn Hacker es nutzen, um ohne großen Aufwand unzählige bisher unbekannte Sicherheitslücken in IT-Systemen aufzuspüren. Mit dem Modell hat Anthropic schon tausende schwerwiegende Schwachstellen gefunden. Und Anthropic warnt eindringlich davor, dass diese Technik bald auch Hackern zur Verfügung stehen könnte [15]. Silicon.de beschreibt am 30. März 2026 die „Ära autonomer Betrüger", wenn KI-Agenten Identitäten kapern. Solche autonomen „AI Fraud Agents" sind autonome Systeme, die Verifizierungsprozesse end to end durchführen. Sie generieren Identitäten oder Dokumente und korrigieren sich selbst, wenn ein Schritt fehlschlägt. In Deutschland steigen Angriffe mit Deepfakes und synthetischen Identitäten aktuell stark an. Nach einer Umfrage der Allianz Versicherung ist KI auf der Liste der für Unternehmen gefährlichen Bedrohungen inzwischen von Platz 10 auf Platz 2 vorgerückt. Die nächste Welle von Cyberangriffen wird zunehmend auch von KI-Agenten ausgeführt werden, die selbstständig Muster erkennen, Schwachstellen ausnutzen und Social Engineering-Attacken personalisieren können. Eine „Zero Trust"-Strategie im Umgang mit verdächtigen oder unbekannten Absendern wird deshalb immer wichtiger. Dieses Prinzip, das vor allem auf Netzwerksegmentierung, stärkere Überprüfung von Identitäten und höchstmögliche Einschränkung von Berechtigungen ausgerichtet ist, bedeutet einen Paradigmenwandel in der IT-Sicherheitsstrategie [16].

## Branchenspezifische Bedrohungen

Der Mittelstand steht besonders im Fokus von Cyberkriminellen, weil sie wissen, dass den KMU (kleine und mittlere Unternehmen) oft das Sicherheitsbewusstsein und noch öfter die Mittel fehlen, um ein wirksames Abwehrsystem aufzubauen. Nach dem IBM-Lagebericht „2026 X-Force Threat Intelligence Index" haben Hacker vor allem die europäische Finanz- und Versicherungsbranche in den Blick genommen und greifen dabei oft auf KI-Systeme zurück, um umfangreiche Datensätze zu kapern und zu analysieren. Und fast täglich warnt die Bafin vor neuen „Maschen", die gutgläubige Anleger um ihr Geld bringen sollen. Besonders perfide sind Angebote, die über soziale Medien verbreitet werden und die Identitäten echter Finanzdienstleister vorspielen. Allein zu Betrugsversuchen über WhatsApp-Gruppen sind der Finanzaufsicht inzwischen mehr als 100 Tatkomplexe bekannt, vor denen sie gewarnt hat. Ständig kommen neue Fake-Angebote auf den Markt. Das BSI warnte am 4. August 2025 vor Phishing-Mails mit denen Betrüger versuchen, an Bankkunden heranzukommen. Zu den Angriffsmethoden gehört die Aufforderung, das Kundenkonto zu schließen, wenn bestimmte Daten nicht bestätigt werden, oder die Aufforderung, Daten zu verifizieren, weil ein Sicherheitszertifikat auslaufe. Mehrfach wurden 2025 IT-Systeme von Flughäfen angegriffen, sodass es zu erheblichen Störungen im Flugverkehr kam. Laut einem im Juni 2025 veröffentlichten Bericht von Thales stieg die Zahl der Cyberangriffe auf den Luftverkehr 2025 gegenüber dem Vorjahr erheblich an.

## Hybride Bedrohungen

Über hybride Bedrohungen ganz unterschiedlicher Art wird in den Medien berichtet. Zum einen bedrohen Kriminelle Unternehmen – insbesondere kritische Infrastrukturen – in der Kombination von physischen Angriffen auf betriebliche Anlagen mit Cyberattacken. Zum anderen verknüpfen Staaten in Spannungssituationen Cyberangriffe mit Desinformationskampagnen. In der gegenwärtigen geopolitischen Lage steht seit dem Krieg Russlands gegen die Ukraine auch Deutschland im Fokus solcher Kampagnen. Die TH Ingolstadt hat gemeinsam mit dem Bundesverband VSW im Dezember 2025 ein Whitepaper zur „hybriden Kriegsführung als Herausforderung für die deutsche Wirtschaft" mit dem Fokus auf strategische Handlungsfelder für Unternehmen veröffentlicht.

## Fazit

Insgesamt bleibt die IT-Sicherheitslage in Deutschland auch im Jahr 2026 angespannt. Viele Organisationen machen es Angreifern nach wie vor zu leicht, mit vergleichsweise geringem Aufwand großen Schaden anzurichten. Aber es gibt zunehmende Ermittlungserfolge, vor allem bei der Abschaltung von Botnetzen und der Schließung von Darknet-Marktplätzen. Europol erfüllt hier eine wichtige Koordinierungsfunktion. Und die Sicherheitsbehörden – allen voran das BSI – erweitern Hilfsangebote, um die Resilienz von IT- und OT-Systemen der Unternehmen zu stärken. ■ TS1141

**Literatur**

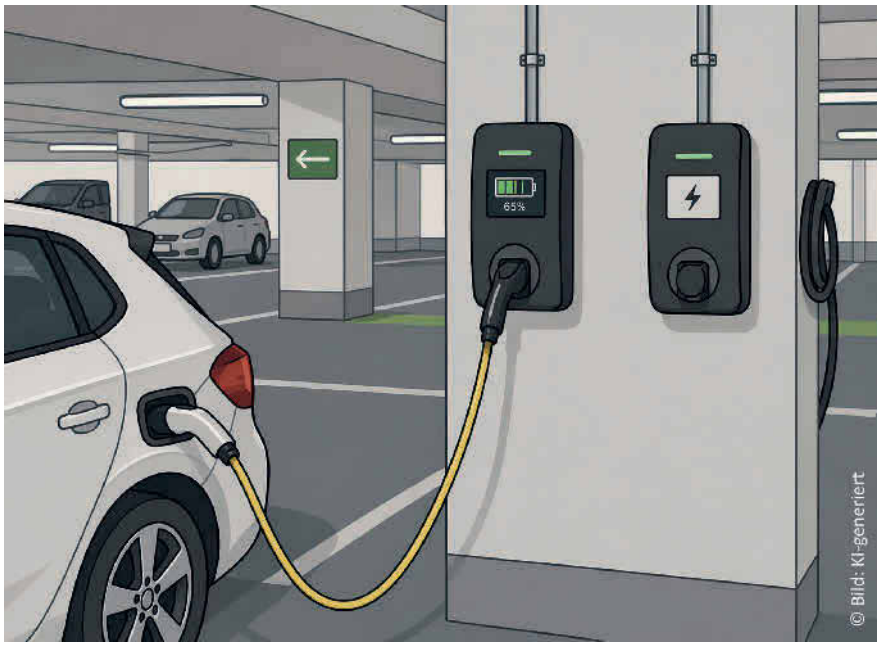
**[1]** Security Navigator 2026 von Orange Cyberdefence
**[2]** BKA, Bundeslagebild Cybercrime 2024, veröffentlicht am 1.10.2025
**[3]** ENISA, „Threat Landscape 2025
**[4]** Darktrace, „Cyber Threat Report 2026“
**[5]** heise.online am 20.8.2025
**[6]** BKA, Bundeslagebild Cybercrime 2024
**[7]** BKA, Bundeslagebild Cybercrime 2024
**[8]** Süddeutsche Zeitung am 20.1.2026
**[9]** giga.de am 30.1.2026
**[10]** Rupprecht R.. Darknet: Freiraum für sensible Kommunikation oder Underground Economy?, Technische Sicherheit, 1–2/2025, S. 32–34
**[11]** BKA, Bundeslagebild Cybercrime 2022, S.8
**[12]** Polster, Dr. Chr., Materna Radar Cyber Security, in Protector, 3/2024, S.24/25
**[13]** BSI, Pressemitteilung v. 27.3.2026
**[14]** Behördenspiegel, Novemberausgabe 2025
**[15]** FAZ vom 14.4.202,6
**[16]** Pyper St.; „Zero Trust – denn der Angriff hat begonnen“, in DSD 1/2026, S. 16/17

MinDir. a.D.

**Reinhard Rupprecht**

# VdS-Fachtagung zu Lithium-Batterien, Brandschutz und Arbeitssicherheit

Die aktuelle Ausgabe der VdS-Fachtagung „Lithium-Batterien: Herausforderung für den Brandschutz und die Arbeitssicherheit“ findet am 4. September 2026 im Kölner Hotel Pullman statt und kann auch im Livestream verfolgt werden.
Ob in der E-Mobilität, in elektronischen Geräten aller Art oder in stationären Energiespeichersystemen: Lithium-Batterien und die wieder aufladbaren Lithium-Ionen-Akkus sind aus unserem Alltag nicht mehr wegzudenken. Sie bieten enorme Vorteile, bergen aber auch Brandrisiken.
Aus diesem Grund beleuchtet die VdS-Fachtagung „Lithium-Batterien: Herausforderung für den Brandschutz und die Arbeitssicherheit“ wieder die aktuellen Herausforderungen im Umgang mit Lithium-Batterien aus Sicht des Brandschutzes, der Arbeitssicherheit und der Versicherungswirtschaft. Sie kann am 4. September 2026 wahlweise vor Ort in Köln oder online im Livestream besucht werden.
Die Referenten sind namhafte Experten, die ihr Wissen und ihre Erfahrungen weitergeben und Fragen beantworten. Sie zeigen auf, wie sich Lithium-Batterien sinnvoll nutzen und ihre Risiken bewerten und minimieren lassen. Themen wie Lithium-Batterien und Risiken – was die Versicherer bewegt, das Projekt „Sekur“ oder E-Fahrzeuge in Großgeragen stehen auf auf dem Programm. Die Fachtagung „Lithium-Batterien“ kann zum vergünstigten Kombipreis zusammen mit den Fachtagungen „Brandschutz im Betrieb“ (1. September 2026 in Köln und online) sowie „Bauen und Brandschutz im Bestand“ (11. September 2026 in Köln und online) gebucht werden.
*vds.de/ft-lion*




**Die VdS-Fachtagung** „Lithium-Batterien: Herausforderung für den Brand- und Arbeitsschutz“ klärt über Risiken und Sicherheitsmaßnahmen auf – unter anderem bei Elektrofahrzeugen (Bild KI-generiert). *Grafik: VdS*

**Interview mit Prof. Kai-Dietrich Wolf (Teil 1)**

# Tür auf oder Tür zu – Wie Safety und Security diesen Zielkonflikt entscheidet

Die fest verschlossene Tür macht es dem Einbrecher schwer, gleichzeitig behindert sie uns im Brandfall. Dieses Bild zeigt sehr vereinfacht und plakativ in welchen Spannungsfeld sich Safety und Security bewegen. In beiden Fällen geht es um Sicherheit, trotzdem stehen führt es oft zu unterschiedlichen Anforderungen, um den Schutz von Menschen und Anlagen zu gewährleisten, folgt aber unterschiedlichen Logiken. Zufällige Ereignisse treffen auf bewusste Angriffe, funktionale Sicherheit auf Cyberbedrohungen. Univ.-Prof. Dr.-Ing. Kai-Dietrich Wolf erklärt im Interview warum sich die Anforderungen durch Vernetzung und Digitalisierung zuspitzen, weshalb klassische Metriken an Grenzen stoßen und wie Unternehmen mit den Widersprüchen umgehen können.

***Herr Wolf, wie definieren Sie die Begriffe „Safety" und „Security" – und wo überschneiden sie sich?***
*Wolf*: Safety bezieht sich auf zufällige Ereignisse, die häufig von technischen Systemen ausgelöst werden und Leben, Gesundheit oder Wohlbefinden von Menschen beeinträchtigen können. Security hingegen adressiert gewollte Angriffe, die zu denselben Beeinträchtigungen führen können. Die Überschneidung liegt im Schutzziel, der Unterschied in der menschlichen Willensbildung – und daraus ergeben sich andere Anforderungen an die Risikomodellierung.

***Oft wird unter „Security" vor allem IT-Sicherheit verstanden. Sie kommen aus der physischen Sicherheit – wo liegt dort der Fokus?***
*Wolf*: Physische Sicherheit ist eigentlich älter als IT-Security. Es geht um Türen, Zäune, Videoüberwachung, Detektion, Verzögerung und Intervention. Also darum, Menschen und Sachwerte gegen klassische Angriffe zu schützen. IT-Security ist durch die zunehmende Vernetzung hinzugekommen. Heute werden auch sicherheitsrelevante Systeme, etwa in Fahrzeugen oder der Prozessindustrie, über IT angreifbar. Das heißt: Cybersecurity und funktionale Sicherheit sind enger gekoppelt als vielen lieb ist. Ein wesentlicher Unterschied ist das Prinzip „Defense in Depth", das in der physischen Sicherheit lange etabliert ist: Mehrere Verteidigungslinien von der äußeren Umzäunung bis zur Intervention erschweren Angreifern den Zugang. In der IT-Security ist dieses mehrschichtige Vorgehen bislang weniger konsequent umgesetzt.

**Univ.-Prof. Dr.-Ing. Kai-Dietrich Wolf** ist Universitätsprofessor für Mechatronik an der Bergischen Universität Wuppertal und beschäftigt sich mit Fragestellungen der Security kritischer Infrastrukturen sowie den Wechselwirkungen zwischen Safety und Security.
*Foto: Uni Wuppertal*

***Wie verändert die Digitalisierung die Anforderungen an Safety und Security?***
*Wolf*: Die Vernetzung macht technische Systeme vulnerabel für Cyberangriffe. Das betrifft inzwischen auch Systeme der funktionalen Sicherheit, etwa Airbags, Bremssysteme oder Schutzeinrichtungen in der Prozessindustrie. Die Anforderungen an Safety- und Security-Funktionen sind dabei oft widersprüchlich. Deshalb wird es immer wichtiger, beide Bereiche bei der Entwicklung technischer Systeme integriert zu betrachten, um diese Widersprüche überhaupt zu erkennen und, wenn möglich, aufzulösen. Durch die globale Vernetzung entstehen zudem neue Angriffswege, etwa über Lieferketten. Nicht nur die Betreiber kritischer Infrastrukturen, sondern auch deren Zulieferer müssen heute hohe Sicherheitsanforderungen erfüllen.

***Worin besteht dieser Zielkonflikt konkret?***
*Wolf*: Ein klassisches Beispiel ist das Gebäude mit verriegelten Außentüren. Verriegelung erhöht die Security, behindert aber im Brandfall die Flucht, also die Safety. Ähnlich bei funktionalen Sicherheits-

systemen: Ein Airbag muss im Ernstfall extrem schnell auslösen. Würde man vor jeder Auslösung eine zusätzliche Security-Prüfung einbauen, könnte das die Safety gefährlich beeinträchtigen, weil es zu Verzögerungen kommt.

***Wie lassen sich solche Widersprüche entschärfen?***
Wolf: Der Königsweg ist die Szenarioentkopplung. In Gebäuden sieht man das etwa am Panikschloss: Von außen kann die Tür verriegelt sein, von innen lässt sie sich im Notfall immer öffnen. Technisch ist das eine richtungsabhängige Szenariounterscheidung, das System „versteht", ob gerade ein Security-Szenario (Schutz vor unbefugtem Zutritt) oder ein Safety-Szenario (Evakuierung im Brandfall) im Vordergrund steht. Ähnliche Prinzipien brauchen wir in vielen anderen Bereichen.

***Sie betonen, dass sich Security-Risiken nicht so einfach berechnen lassen wie klassische Safety-Risiken. Warum ist das so schwierig?***
Wolf: In der Safety können wir vieles mit Wahrscheinlichkeiten und Verteilungen modellieren – technisches Versagen, Komponentenfehler, selbst bestimmte Formen menschlichen Fehlverhaltens. Im Security-Bereich haben wir es dagegen mit bewussten Angreifern zu tun. Deren Verhalten lässt sich nicht zuverlässig probabilistisch erfassen. Wir sprechen von epistemischer Unsicherheit. Unsicherheiten dieser Art können eine auf Risikomodellen basierende Entscheidungsfindung infrage stellen. Das muss man explizit berücksichtigen.

***Wie können Unternehmen mit dieser Unsicherheit umgehen?***
*Wolf*: An einigen Stellen kommt man um Managemententscheidungen nicht herum. Dort, wo ich Unsicherheiten nicht berechnen kann, muss ich bewusst festlegen: Wie viel Risiko will ich mir leisten? Welche Angriffsarten möchte ich auf jeden Fall ausschließen? Man wird oft gut beraten sein, bei Security eher „draufzusatteln", solange Maßnahmen nicht die Safety beeinträchtigen und wirtschaftlich vertretbar sind. Es ist immer ein Mix aus quantitativer Analyse und bewussten Entscheidungen.

***Welche Rolle spielt die Sicherheits- und Zuverlässigkeitskultur in den Organisationen?***
*Wolf*: Eine sehr große. Safety ist seit Langem hoch priorisiert. „Safety first" ist ein etablierter Slogan. Security muss eine ähnlich hohe Priorität bekommen. Dazu gehört, dass Führungskräfte Verantwortung übernehmen, dass es klare Zuständigkeiten für Safety und Security auf Vorstandsebene gibt und dass operatives Personal geschult wird. Nicht alle Schutzziele lassen sich mit Technik erreichen. Informierte Mitarbeitende, klare Abläufe im Fall von Sicherheitsvorkommnissen und Sicherheitsexperten auf allen Hierarchieebenen sind unverzichtbar.
Es gibt keine Patentlösung für den Zielkonflikt zwischen Safety und Security. Der Weg zu einer optimalen Balance erfordert immer eine kontextspezifische, lernbereite Herangehensweise und die Bereitschaft, Erfahrungswissen aus unterschiedlichen Disziplinen zusammenzuführen.

***Das Interview führte Gudrun Huneke***

---

**Interview mit Prof. Kai-Dietrich Wolf (Teil 2)**

# Safety trifft Security: Wie das VDI-Wiki Disziplinen vernetzt

Verschiedene Richtlinien und Branchenstandards prägen den Umgang mit Safety und Security. Hier treffen oft getrennte Welten aufeinander. Das VDI-Wiki bringt nun Methoden und Begriffe verschiedener Disziplinen zusammen. Denn die zunehmende Komplexität und Vernetzung technischer Systeme macht es nötig, Wissen aus verschiedenen Sicherheitsdisziplinen strukturiert und vergleichbar aufzubereiten, hiervon profitieren nicht nur Menschen, sondern auch lernende Systeme wie Künstliche Intelligenz. Prof. Kai-Dietrich Wolf erklärt, wie sich Risikomodelle unterscheiden, welche Rolle epistemische Unsicherheit spielt und warum kuratierte Wissensquellen für die Zukunft entscheiden

***Herr Wolf, warum hat der VDI ein Wiki zu Safety und Security initiiert – und was ist das Besondere daran?***

*Kai-Dietrich Wolf*: Viele Expertinnen und Experten arbeiten streng nach ihren Normen und Richtlinien und bewegen sich damit in einer weitgehend geschlossenen Welt. Es gibt zahlreiche Richtlinien zur funktionalen Sicherheit, die sich in Methoden und Inhalten stark ähneln, sich aber an wichtigen Stellen unterscheiden.

Genau dort wird es spannend: Warum geht die eine Disziplin so vor, die andere anders und welche Annahmen über Risiko, Unsicherheit und Verantwortung liegen dem zugrunde? Das Wiki ist nach Disziplinen aufgebaut und orientiert sich an Leitfragen. So lassen sich Ansätze vergleichen, ohne jede Richtlinie einzeln kaufen und durcharbeiten zu müssen.

***Welche Rolle spielen Normen, Standards und Regelwerke dabei?***
*Wolf*: Sie sind die Basis professioneller Sicherheitsarbeit, aber sie sind nicht frei zugänglich und oft sehr umfangreich. Das Wiki soll keinen Volltext ersetzen, sondern einen strukturierten Überblick geben: Welche Methoden werden in welcher Disziplin verwendet, welche Begriffe, welche Schutzziele? Durch eine einheitliche Struktur und konsistente Terminologie entsteht ein kuratierter Wissensspeicher, der nicht etwa alles nur sammelt, sondern das Wesentliche strukturiert, einordnet und vergleichbar macht. Davon profitieren sowohl Nutzer als auch KI-Systeme, die auf verlässliche, gut strukturierte Informationen angewiesen sind.

***VDI: Sie sagen, ein Wiki ist nie fertig. Wo sehen Sie aktuell Lücken?***
*Wolf*: Es gibt sicher noch einige Disziplinen, die wir aufnehmen können, von weiteren Industriezweigen bis hin zu Bereichen wie Lebensmittelsicherheit. Wir sind stark von internationalen Lieferketten abhängig, etwa bei Futtermitteln. Wenn hier etwas schiefläuft, merken wir das sehr schnell in der Versorgung. Solche Abhängigkeiten werden bislang oft noch nicht als Teil kritischer Infrastrukturen wahrgenommen. Wenn sich Expertinnen und Experten finden, die dazu beitragen, wird das Wiki weiterwachsen. Die Herausforderungen durch komplexe, internationale Lieferketten betreffen längst nicht mehr nur klassische Infrastrukturen wie Strom oder Verkehr, sondern auch andere Bereiche. Viele Risiken werden erst sichtbar, wenn Störungen auftreten – genau diese impliziten Abhängigkeiten wollen wir im Wiki systematisch sichtbar machen.

***Das Wiki differenziert zwischen Safety-Risikomodellen und Security-Modellen. Wo liegt der zentrale Unterschied?***
*Wolf*: In der Safety lassen sich Risiken meist probabilistisch beschreiben, etwa durch Ausfallwahrscheinlichkeiten und statistische Verteilungen. In der Security ist die große Herausforderung die Abbildung menschlicher Intentionalität. Angreifer verhalten sich nicht wie zufällige Störungen. Wir sprechen hier von epistemischer Unsicherheit. Wird diese nicht berücksichtigt, können Entscheidungen, die auf Risikomodellen basieren, in die Irre führen. Im Safety-Bereich kann man das gut handhaben, wenn man sorgfältig arbeitet. Im Security-Bereich ist das deutlich schwieriger.

Univ.-Prof. Dr.-Ing. Kai-Dietrich Wolf ist Universitätsprofessor für Mechatronik an der Bergischen Universität Wuppertal und Leiter des Instituts für Sicherungssysteme. Im Mittelpunkt seiner Arbeit stehen die Security kritischer Infrastrukturen sowie die Analyse von Wechselwirkungen zwischen Safety und Security. Er verfügt über langjährige Erfahrung in der Zusammenarbeit mit Industrie, Forschungseinrichtungen und Behörden und ist als Gutachter für nationale und internationale Fachzeitschriften sowie Forschungsprogramme tätig.

***Wie lässt sich vor diesem Hintergrund der Schutz von Safety-Funktionen durch Security-Maßnahmen bemessen?***
*Wolf*: Das ist eine der schwierigsten Fragen. Man möchte Security-Maßnahmen risikogerecht auslegen, also angemessen, aber nicht überzogen. Gleichzeitig haben wir keine belastbaren Wahrscheinlichkeiten für Angriffe. In vielen Fällen wird man gut beraten sein, bei Security eher etwas großzügiger zu dimensionieren, solange Maßnahmen die Safety nicht beeinträchtigen und die Kosten vertretbar bleiben. Der Schutz von Menschenleben hat dabei stets Vorrang.

***Welche Rolle spielen Künstliche Intelligenz, Machine Learning und autonome Systeme in dieser Entwicklung?***
*Wolf*: Diese Systeme bergen Chancen und Risiken. Systeme, die sich selbst verändern können, lassen sich nur schwer einem Konformitätsnachweis gegenüber bestehenden Standards unterwerfen. Andererseits könnten lernfähige Systeme in Zukunft besser zwischen Safety- und Security-Szenarien unterscheiden, etwa zwischen Brand und Einbruch. Die Entkopplung von Safety- und Security-Funktionen durch Szenarioerkennung ist aus meiner Sicht der Königsweg, um Widersprüche zwischen Anforderungen aufzulösen.

***Was bedeutet das für die Art, wie wir Wissen organisieren?***
*Wolf*: Wenn wir KI-Systemen Aufgaben wie die Einordnung komplexer technischer Fragestellungen im Spannungsfeld von Safety und Security übertragen wollen, brauchen sie kuratierte, abgesicherte Quellen – also fachlich geprüfte, nachvollziehbar hergeleitete Inhalte. Gerade bei Fragestellungen, die widersprüchliche Anforderungen in sich tragen, reicht es nicht aus, Informationen isoliert zu betrachten oder nur auf einzelne Normen zu verweisen. Genau hier sehe ich eine große Zukunft für Plattformen wie das VDI-Wiki: Es strukturiert Wissen, nutzt eine konsistente Terminologie und bezieht sich auf seriöse Quellen. Dadurch wird es möglich, auch Zielkonflikte zwischen Safety- und Security-Anforderungen nachvollziehbar einzuordnen. Ich gehe davon aus, dass künftig KI-Systeme häufig bei der fachlichen Bewertung entsprechender Zielkonflikte auf Basis solcher Wissensspeicher eingesetzt werden.

***Welche drei Empfehlungen geben Sie Organisationen, die damit beginnen, Safety und Security systematisch zusammenzuführen?***
*Wolf*: Erstens: Seien Sie offen für andere Sichtweisen! Es gibt mehr relevante Disziplinen, als man spontan denkt.
Zweitens: Sicherheit im Sinne von Safety und Security ist ein menschliches Grundbedürfnis. In vielen Abläufen und Technologien steckt enorm viel Erfahrungswissen, das man sichtbar und nutzbar machen sollte. Drittens: Verwenden Sie einen weiten Security-Begriff. Security ist nicht nur IT-Security, sondern auch physische Sicherheit, eine deutlich ältere Disziplin, aus der wir viele Lösungsansätze für Widersprüche zwischen Safety- und Security-Funktionen übernehmen können. Wichtig ist: Es gibt keine universelle Standardmethode. Der Umgang mit Zielkonflikten und Unsicherheiten erfordert Offenheit, kontinuierliches Lernen und die Bereitschaft, Erfahrungen aus unterschiedlichen Branchen und Disziplinen kontextsensitiv zu adaptieren.

***Das Interview führte Gudrun Huneke***

# Muting in der Praxis: Wenn Sicherheit zur Schwachstelle wird

Muting ermöglicht es, die Sicherheitsfunktion an Maschinen oder Anlagen vorübergehend zu überbrücken, damit Material durch Schutzeinrichtungen wie Lichtvorhänge oder Laserscanner ein- oder ausgeschleust werden kann – und das, ohne den Produktionsprozess zu unterbrechen. Die Sicherheit für Personen muss dabei jederzeit gewährleistet bleiben. In der Praxis stoßen Muting-Applikationen jedoch immer wieder an Grenzen: Fehlbedienung und Manipulation sind möglich. In solchen Fällen sind alternative Sicherheitskonzepte gefragt.

**TEXT:** *Dr. Albrecht von Pfeil*

## Unbewusste Risiken

In der industriellen Automatisierung kommen verschiedene Muting-Arten zum Einsatz: 2-Sensor-, 4-Sensor-, zeitgesteuerte oder sequenzgesteuerte Verfahren. Die internationale Norm DIN EN IEC 62046[1)] regelt die Anforderungen an Ein- und Ausschleusstationen mit Muting und schreibt insbesondere vor:

- Muting muss mindestens über zwei voneinander unabhängige Überbrückungssignale aktiviert werden
- Muting muss Schutz gegenüber vorhersehbarer Fehlbedienung oder Manipulation bieten

Die Norm definiert so klare Anforderungen für die Umsetzung von Muting-Anwendungen. In der Praxis werden diese jedoch nicht immer vollständig eingehalten – sei es, weil die spezifischen Applikationsanforderungen nicht in allen Details bekannt sind und dadurch von realen Situationen abweichen, oder weil zugunsten einer hohen Prozessstabilität bewusst riskante Kompromisse eingegangen werden. Das Ergebnis: Sicherheitsfunktionen verlieren ihre Wirksamkeit, Manipulationen oder Fehlbedienungen werden begünstigt. Für Betreiber bedeutet das ein unbewusst

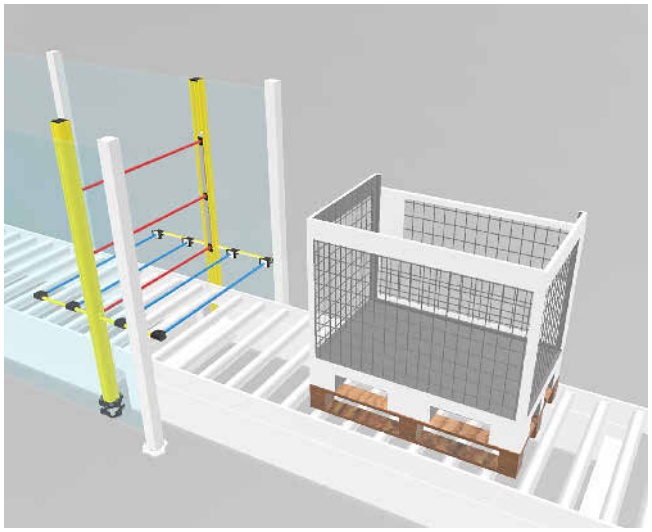


**Bild 1** Eine Gitterbox wird auf einer Palette eingeschleust. *Foto: Leuze*

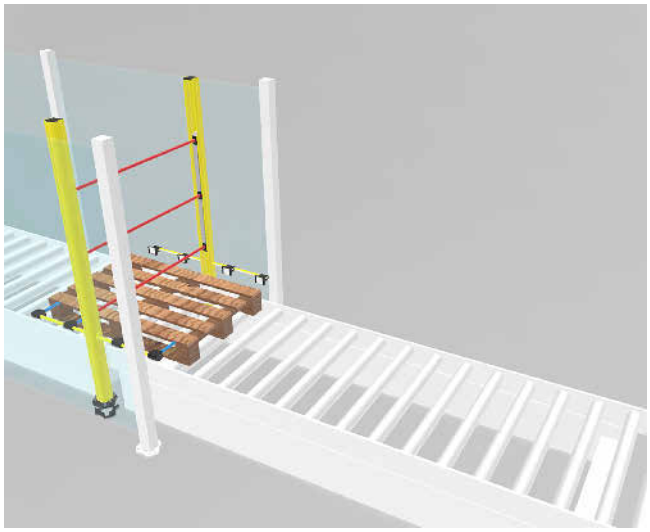


**Bild 2** Muting auf Palette. *Foto: Leuze*

erhöhtes Haftungsrisiko und potenziell gravierende Folgen für die Arbeitssicherheit der Mitarbeiter.

## Gefährdung 1: Sicherheitslücke durch "Palettenmuting"

In automatisierten Anlagen werden häufig Gitterboxen oder andere, für die Muting-Sensoren schwer detektierbare Objekte, auf Paletten ein- oder ausgeschleust (**Bild 1**). Die Gitterstruktur mit ihren Löchern verhindert ein stabiles Schaltsignal der Muting-Sensoren, wodurch ein Muting der Sicherheitsvorrichtung unmöglich wird. In der Praxis wird gelegentlich die Palette selbst als Auslöser für das Muting verwendet (**Bild 2**) – eine Vorgehensweise, die nicht zulässig ist: Eine Person könnte etwa eine Leerpalette in der Sicherheitsvorrichtung platzieren und die Schutzeinrichtung dadurch bewusst außer Kraft setzen. (**Bild 1** und **Bild 2** siehe linke Seite).

## Lösung: Smart Process Gating (SPG)

Diese Sicherheitslücke lässt sich mit dem Smart Process Gating-Verfahren (SPG) zuverlässig schließen. Die Überbrückungsfunktion wird dabei durch zwei unabhängige Steuersignale ohne externe Muting-Sensoren aktiviert. Zur Aktivierung des Gatings am Sicherheits-Lichtvorhang dienen

- ein CS-Schaltsignal (Control Signal) aus der Anlagensteuerung als erstes (Initiierungs-)Signal
- ein PFI-Schutzfeldunterbrechungssignal (Protective Field Interruption), ausgelöst durch das Transportgut im Lichtvorhangschutzfeld, als zweites (Verifizierungs-)Signal

Die Gating-Funktion wird durch die korrekte Abfolge von CS-Schaltsignal und Schutzfeldunterbrechung aktiviert und vom Lichtvorhang überwacht (**Bild 3**). Kurz vor der Einfahrt des Transportguts in das Schutzfeld sendet die Prozesssteuerung (SPS) das CS-Schaltsignal an den Sicherheits-Lichtvorhang. Der Zeitpunkt muss so eingestellt sein, dass der Abstand zwischen Transportgut und Schutzfeld weniger als 200 mm beträgt – so wird verhindert, dass kurz vor der Durchfahrt noch eine Person passieren kann. Wenn das Transportgut innerhalb von vier Sekunden in das Schutzfeld einfährt, nutzt der Lichtvorhang sein eigenes PFI-Signal und unterdrückt eine Sicherheitsabschaltung. Das Gating endet entweder automatisch unmittelbar nach Durchfahrt des Förderguts und dem Freiwerden des Schutzfeldes, oder durch Rücksetzen des CS-Schaltsignals durch die SPS. Dieses Verfahren ermöglicht ein besonders kompaktes und platzsparendes Anlagendesign, weil keine zusätzlichen, unmittelbar vor- und nachgelagerten Muting-Sensoren erforderlich sind.

**Bild 3** CS-Schaltsignal und PFI-Signal aktivieren die Überbrückung. *Foto: Leuze*

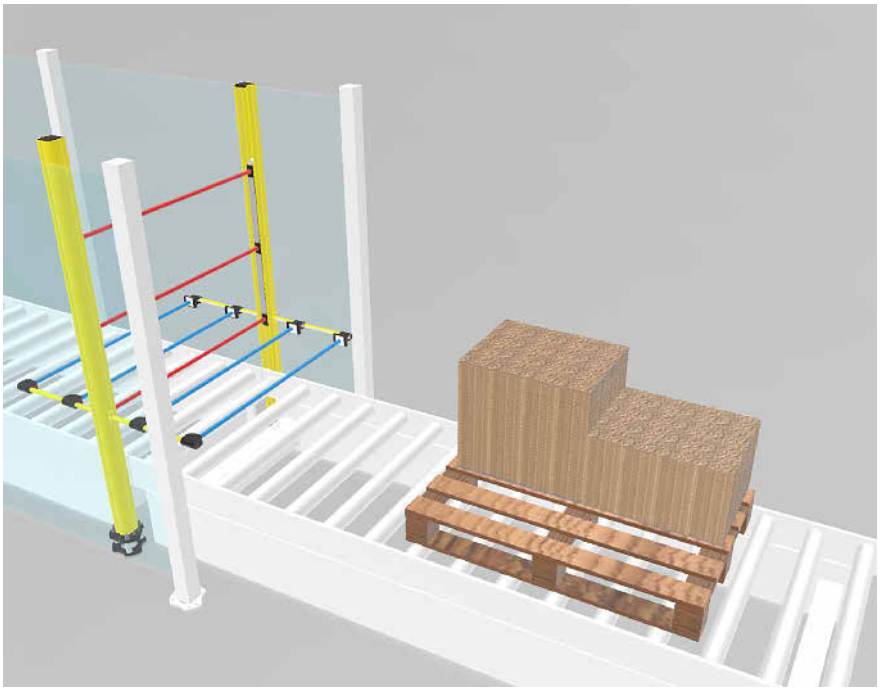


**Bild 4** Zu großer Abstand beim Muting: Eine Person kann hier neben dem Fördergut unbemerkt in den Gefahrenbereich gelangen. *Foto: Leuze*

## Gefährdung 2: Sicherheitslücke durch unvollständig beladene Paletten

Ist eine Palette nur teilweise beladen oder sind die Förderobjekte deutlich schmaler als die Fördertechnik, entsteht während des Mutings eine Lücke. Durch diese Lücke kann eine Person in den Gefahrenbereich gelangen, ohne dass die Sicherheitsfunktion ausgelöst wird. Um die Sicherheitslücke zu schließen, ist der ma-

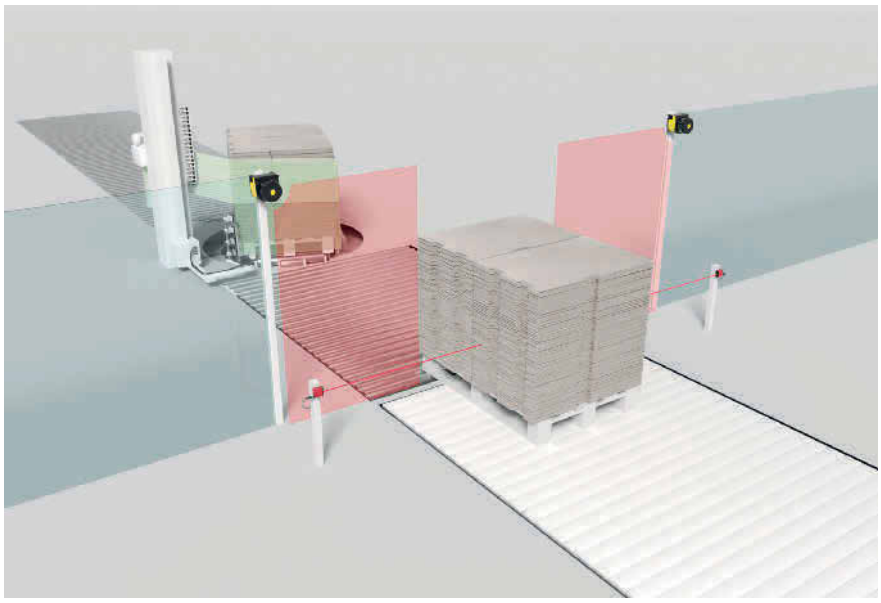


**Bild 5** Zugangssicherung mit dynamischer Formatanpassung. *Foto: Leuze*

ximal zulässige Freiraum neben dem Transportgut normativ auf 200 mm begrenzt. In realen Applikationen finden sich immer wieder Durchgangslücken, die deutlich größer sind und damit eine einfache Umgehung der Schutzeinrichtung ermöglichen (**Bild 4**).

## Lösung: Zugangssicherung mit dynamischer Formatanpassung

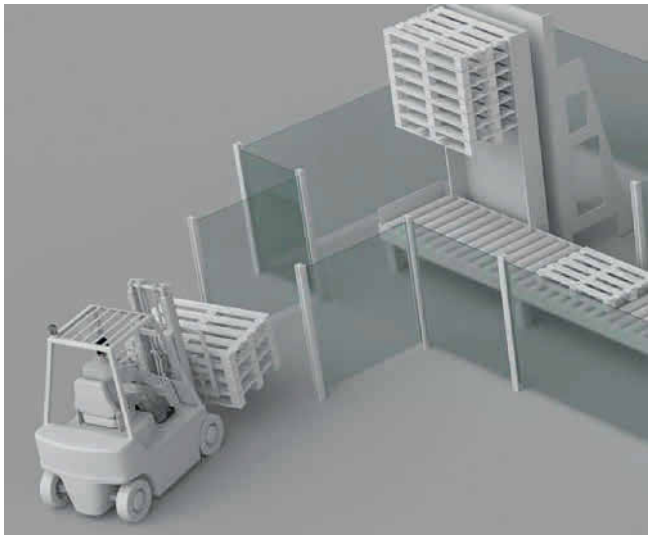
Diese Gefährdung lässt sich durch eine Zugangssicherung mit dynamischer Formatanpassung lösen. Hierbei erzeugen zwei Sicherheits-Laserscanner ein gemeinsames, geschlossenes, vertikales Schutzfeld. Zusätzlich auf beiden Seiten neben der Förderstrecke installierte Abstandssensoren erfassen die Position beziehungsweise Breite der Ware auf der Palette – alternativ lässt sich dies auch durch die integrierte Messfunktion der Scanner ermitteln. Mit diesen Informationen gibt das Sicherheitssystem im Schutzfeld einen entsprechenden Bereich frei, durch den sich das Transportgut unterbrechungsfrei fördern lässt. Seitlich neben der Ware bleibt der Zugang weiterhin normkonform abgesichert. Nach Durchfahrt des Transportguts wird das Schutzfeld automatisch wieder geschlossen. Sollte eine Person mitlaufen oder -fahren, wird dies auch sicher erkannt. Das innovative Sicherheitskonzept dieser Sicherheitslösung ermöglicht Performance Level d nach EN ISO 13849–1[2]), (**Bild 5**).

## Gefährdung 3: Sicherheitslücke durch Gabelstapler-Muting

In diesem Beispiel dienen zwei Induktionsschleifen oder Ultraschall-Sensoren als Auslöser für die Mutingfunktion. Sobald sich der Stapler im Sensorbereich befindet, wird Muting initiiert und so die Sicherheitsfunktion des Lichtgitters deaktiviert. Der Stapler kann in die Station einfahren. Diese Lösung ist gemäß dem neuen Entwurf der DIN EN 415–4[3]) so nicht mehr zulässig, denn die Gefahr bleibt bestehen: Eine Person kann den Gefahrbereich betreten – in der Annahme, dass sich die Maschine durch Auslösen des Lichtvorhangs im sicheren Zustand befindet, was während des Mutings nicht gegeben ist (**Bild 6** links/rechts 2 Bilder).

## Lösung: Sequenzieller Restart

Bei dieser Sicherheitslösung wird die gefahrbringende Bewegung immer gestoppt, wenn das Lichtvorhangschutzfeld unterbrochen wird. Verlässt der Stapler den Gefahrenbereich, erzeugen speziell angeordnete Induktionsschleifen eine definierte Sequenz, die einen automatischen Wiederanlauf der Anlage ermöglicht. Können die Induktionsschleifen nicht in den Boden eingebracht werden, dann lässt sich die Staplerbewegung auch per Radarsensorik überwachen. Beide Ansätze erfüllen



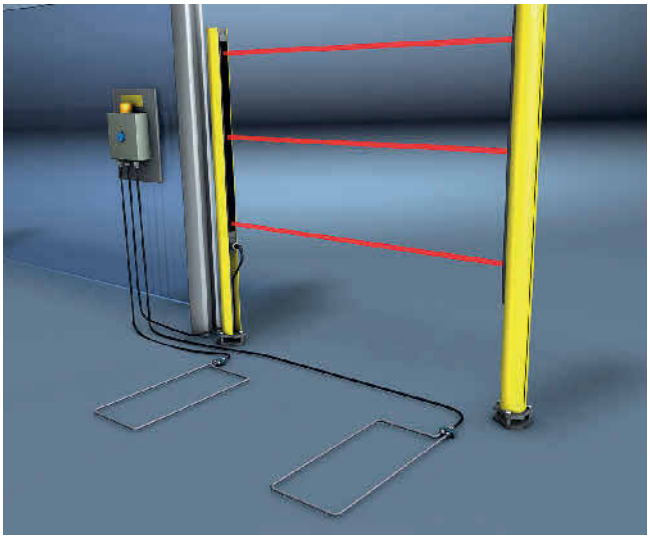


**Bild 6 (l.) und Bild 6** (r.) Stapler mutet das Lichtgitter über zwei Induktionsschleifen – die Gefahr bleibt bestehen. *Fotos: Leuze*

die Anforderungen an die funktionale Sicherheit und verhindern Manipulationen zuverlässig. Diese Sicherheitslösung entspricht ebenfalls Performance Level d nach EN ISO 13849–1.

## Grenzen des Mutings und Alternativen

Zusammengefasst ermöglicht Muting es, zwischen Förderobjekten und Personen zu unterscheiden und trägt zur Automatisierung und Effizienz bei. Allerdings muss das Verfahren immer gegen vorhersehbare Fehlbedienung und Manipulation abgesichert sein. Alternative Sicherheitslösungen sind insbesondere erforderlich, wenn Mutingsensoren die Förderobjekte nicht zuverlässig erkennen oder die Objektbreite stark variieren kann und so neben dem Transportgut zu große Lücken entstehen. Auch das Muting auf Gabelstapler ist sicherheitstechnisch nicht mehr Stand der Technik. In all diesen Fällen bleibt die Gefährdungsstelle potenziell zugänglich und gefährlich. Für diese Herausforderungen stehen sichere und normkonforme Lösungen zur Verfügung. Leuze unterstützt dabei mit einem klar strukturierten Entwicklungs- und Testprozess – von der Planung über die Programmierung bis zur umfassenden Validierung und Verifikation.

## Zur sicheren Lösung

Der Weg zur Sicherheitslösung von Leuze beginnt mit der individuellen Anforderung des Kunden: Ein automatisierter Betrieb soll zuverlässig und sicher laufen. Nach einer gründlichen Analyse mit Risiko- oder Gefährdungsbeurteilung entwickelt ein Safety-Designer ein maßgeschneidertes Konzept und erarbeitet spezifische Sicherheitsfunktionen für den jeweiligen Anwendungsfall. Im Engineering-Team wird die passende Hardware und Sensorik ausgewählt, integriert, programmiert und getestet. Ein konsequentes Vier-Augen-Prinzip sorgt für eine funktional sichere Umsetzung. Umfassende Funktionstests gewährleisten, dass alle Sicherheits- und Standardfunktionen zuverlässig arbeiten. Erst nach erfolgreicher Validierung unter realen Bedingungen erfolgt die Inbetriebnahme beim Kunden. Abschließend erhält dieser eine vollständige Dokumentation inklusive Validierungsplan und CE-Konformitätserklärung.

Damit verbinden sich drei zentrale Vorteile:

- Einfach – funktionale Sicherheit ist komplex; dank des Know-hows, Engineerings und der Dienstleistungen von Leuze wird sie für den Kunden einfach.
- Sicher – alle Lösungen sind strikt normenbasiert und lückenlos dokumentiert, sodass die Einhaltung jederzeit nachgewiesen werden kann.
- Produktiv – funktionale Sicherheit und effiziente Abläufe greifen ineinander und sorgen für einen zuverlässigen, wirtschaftlichen Betrieb.

■ TS 11347

**Fußnoten**

[1] DIN EN IEC 62046: Sicherheit von Maschinen – Anwendung von Schutzeinrichtungen zur Anwesenheitserkennung von Personen, https://www.dinmedia.de/de/norm/din-en-iec-62046/296735438

[2] DIN EN ISO 13849-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze, https://www.dinmedia.de/de/norm/din-en-iso-13849-1/367893072

[3] DIN EN 415–4: Sicherheit von Verpackungsmaschinen – Teil 4: Palettierer und Depalettierer und zugehörige Ausrüstungen, https://www.dinmedia.de/de/norm-entwurf/din-en-415-4/336338018

**Dr. Albrecht von Pfeil**

Director Safety Solutions, Leuze electronic GmbH+Co. KG

# Vorschau 7-8/2026

*Foto: smarterpix/akarelias*

## New Work und KI in der Bauprojektabwicklung

Die Bauprojektabwicklung befindet sich in einem strukturellen Spannungsfeld aus steigender Komplexität, hohem Zeit- und Kostendruck sowie einem ausgeprägten Fachkräftemangel. Forschungsergebnisse der Bergischen Universität Wuppertal zeigen, dass bei Baustellenführungspersonen eine deutliche Verbreitung sowohl physischer als auch psychischer Überlastung vorliegt. Gleichzeitig hat sich der Fachkräftemangel seit 2014 im Baugewerbe zum größten Geschäftsrisiko entwickelt. In diesem Kontext haben sich New-Work-Konzepte als strategischer Ansatz zur Steigerung der Arbeitgeberattraktivität und zur Verbesserung der Arbeitsbedingungen im Bauprojektmanagement etabliert.



In Deutschland arbeiten neuen Schätzungen zufolge rund 7,2 Millionen Beschäftigte im Freien und sind der Sonnenstrahlung ausgesetzt. *Foto: Peter Greven, Physioderm GmbH*

**UV-Schutz**

# Neue verschärfte Regelung erhöht den Druck auf Arbeitgeber und Beschäftigte

Die jüngst veröffentlichten Technischen Regeln für Arbeitsstätten A5.1 der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin legen fest, dass Schutzmaßnahmen ab einem UV-Index von 3 ergriffen werden müssen. Dazu gehört auch die Verwendung von Sonnenschutzmitteln für ungeschützte Körperstellen.

**TEXT:** *Anja Dick*

In Deutschland arbeiten rund 7,2 Millionen Menschen vorwiegend im Freien. Sie alle sind einem hohen Risiko ausgesetzt, an weißem Hautkrebs zu erkranken. Denn auf Dauer können die UV-Strahlen der Sonne das Erbgut der Hautzellen schädigen. In einem gewissen Maße kann der Körper diese Schäden zwar erkennen und reparieren. Wenn die Haut der Sonne jedoch zu intensiv und zu lange ausgesetzt ist, können Krebszellen entstehen. Nach Angaben der Deutschen Krebshilfe erhalten in Deutschland jährlich rund 373 850 Menschen die Diagnose Hautkrebs. Er ist damit eine der häufigsten Krebserkrankungen. Die meisten Betroffenen erkranken am weißen Hautkrebs, dessen Hauptarten wiederum das Basalzell- und das Plattenepithelkarzinom sind.

Seit 2015 können der weiße Hautkrebs – oder genauer: das Plattenepithelkarzinom – und seine Vorstufen (multiple aktinische Keratosen) als Berufskrankheit Nummer 5103 (BK 5103) anerkannt werden. Seither übernimmt die gesetzliche Unfallversiche-

rung die Kosten, wenn bei einem Arbeitnehmenden weißer Hautkrebs diagnostiziert und als beruflich bedingt eingestuft wird. In den zehn Jahren seit der Aufnahme in die Liste der Berufskrankheiten hat sich eine Menge getan. Dank der vielen Aufklärungskampagnen von Berufsgenossenschaften, Unfallversicherung, Medien oder Herstellern sind die Menschen sensibilisiert für den UV-Schutz. Das Thema ist so präsent in der Öffentlichkeit wie nie zuvor. Zurecht, denn viele Statistiken und die hohen Verdachtszahlen bei den Berufskrankheiten zeigen, wie groß die Gefährdung ist. So belegt der weiße Hautkrebs schon traditionell Spitzenpositionen bei den Verdachtsanzeigen auf eine Berufskrankheit.

## UV-Index als Orientierungswert

Durch den Klimawandel und seine Auswirkungen hat sich die Gefahr, an weißem Hautkrebs zu erkranken, aus vielerlei Gründen deutlich erhöht. Auch deswegen hat die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) reagiert und im August 2025 die Technischen Regeln für Arbeitsstätten (ASR) A5.1 vorgelegt (**Bild 1**). Aktuell gehen wir also in die erste Saison mit den neuen Regeln. Die verbindlichen Regeln konkretisieren den Arbeitsschutz im Freien und in offenen Arbeitsstätten mit Blick auf Witterungseinflüsse wie UV-Strahlung. Eine wesentliche Neuerung ist, dass erstmals der UV-Index verbindlich zur Gefährdungsbeurteilung herangezogen wird. Ab sofort müssen Arbeitgeber ab einem UV-Index von 3 dafür sorgen, dass ihre Beschäftigten Schutzmaßnahmen gegen die Sonnenstrahlung ergreifen. Der UV-Index ist ein Orientierungswert für die schädigende Wirkung natürlicher UV-Strahlung; er wird in ganzzahligen Werten zwischen 0 und 11+ angegeben. Dabei sind UV-Index-Werte bis 2 mit einer geringen, bis 5 mit einer mittleren, bis 7 mit einer hohen, bis 10 mit einer sehr hohen und ab 11 mit einer extremen Gefährdung durch natürliche UV-Strahlung verbunden. Um sich über den aktuellen UV-Index zu informieren verweist die BAuA beispielsweise auf die Internetseiten des Bundesamtes für Strahlenschutz (*https://www.bfs.de*) und des Deutschen Wetterdienstes (*https://kunden.dwd.de/uvi_de*), auf denen die Werte für viele Orte in Deutschland abgerufen werden können. Zudem wird darauf verwiesen, dass in unklaren Gefährdungssituationen ergänzende Messungen vor Ort zur Berechnung des lokalen UV-Index zweckmäßig sein können. Dafür werden grundsätzlich drei Optionen genannt: 1.) Messungen mit tragbaren oder auf der Haut aufbringbaren UV-Sensoren; 2.) Integralradiometer; und 3.) Spektralradiometer, die sehr präzise sind, aber mit dem Computer ausgewertet werden müssen, was im Alltag schwer umzusetzen sein dürfte.

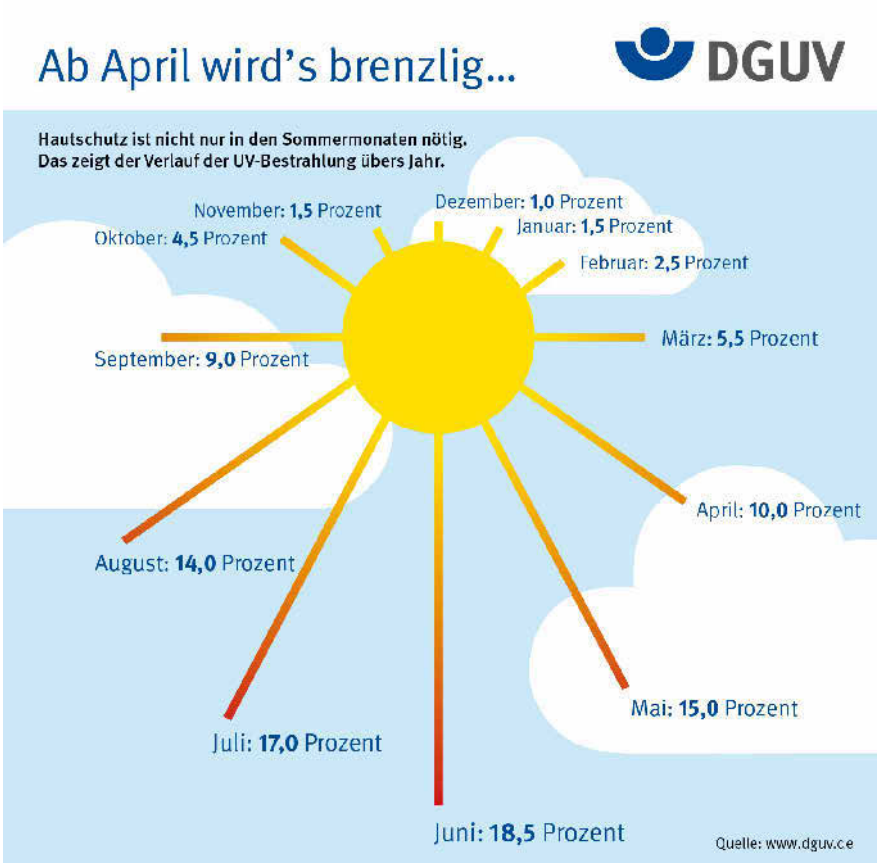



**Bild 1** Bereits im Frühjahr nimmt die Stärke ultravioletter Strahlung in unseren Breiten deutlich zu. *Grafik: Deutsche Gesetzliche Unfallversicherung*

Ab einem UV-Index von 3 müssen laut der Technischen Regeln für Arbeitsstätten A5.1 zwingend Schutzmaßnahmen ergriffen werden. Dabei müssen zunächst technische, dann organisatorische und schließlich persönliche Maßnahmen ergriffen werden. Eine technische Maßnahme ist beispielsweise das Verschatten von Arbeitsplätzen durch Sonnensegel. Zu den organisatorischen Maßnahmen gehört, die Arbeitszeiten in die Morgen- und Abendstunden zu verlagern, um so der sonnenintensivsten Zeit zwischen 11 und 14 Uhr zu entgehen. Sowohl technische als auch organisatorische Maßnahmen sind im Arbeitsalltag aber natürlich nicht immer umzusetzen. Letztendlich läuft es also in den allermeisten Fällen auf persönliche Schutzmaßnahmen hinaus. Viermal „H" lautet hier die Eselsbrücke: Hemd, Hose, Hut – und hoher Lichtschutzfaktor (**Bild 2**).

Für den richtigen Sonnenschutz ist zunächst einmal eine Kopfbedeckung gefragt. UV-Schutz-Hüte und -Mützen tun hier gute Dienste. Auch der Kleidung kommt eine wichtige Schutzfunktion zu. Hier gibt es beispielsweise den UV-Schutz nach Standard 801. Diese international anerkannte Messmethode dient dazu, den UV-Schutz-Wert von Textilien zu ermitteln. Sie bezieht dabei auch die besonderen Anforderungen mit ein, denen Textilien im Einsatz ausgesetzt sind und die den Sonnenschutz potenziell senken können – wie zum Beispiel die Dehnung des Gewebes beim Tragen, Feuchtigkeit durch Schweiß oder Wasser sowie die Abnutzung beim Gebrauch oder durch die Wäsche. Die Messung des UV-Schutzfaktors nach dem UV Standard 801 legt immer die ungünstigsten Trage- und Nutzungsbedingungen zugrunde. Deswegen gilt sie als besonders anspruchsvoll.


**Bild 2** Outdoor-Worker wie beispielsweise Dachdecker sollten unbedingt Lichtschutzfaktor 50 nutzen. *Foto: Peter Greven Physioderm*


**Bild 3** PGP bietet das umfangreichste UV-Schutzprogramm der Branche und für nahezu jeden Anwendungsbereich die passende Lösung. *Foto: Peter Greven Physioderm*

## Auf ausreichenden UV-A-Schutz achten

In jedem Fall und zwingend zählt das Verwenden von dermalen Sonnenschutzmitteln für Körperstellen, die nicht durch Kleidung oder Kopfbedeckung geschützt werden können, zu den persönlichen Schutzmaßnahmen. Diese besonders neuralgischen Stellen sind beispielsweise Nase, Ohren, Unterlippe, Nacken oder Hände. Neu ist, dass die ASR A5.1 ausdrücklich vorgibt, dass „wasserfeste Produkte mit einem hohen bis sehr hohen Lichtschutzfaktor (mindestens 30, besser 50+), einschließlich ausreichendem UV-A-Filter“ geeignet sind. Bei der Auswahl der Produkte sollte man deswegen darauf achten, dass die Mittel mit dem „UVA“ im Kreis ausgezeichnet sind.

Wie nun unterscheiden sich UV-A- und UV-B-Strahlen? UV-B-Strahlen sind kurzwelliger, energiereicher und dringen weniger tief in die Haut ein als UV-A-Strahlen. Die UV-A-Strahlen sind langwelliger und haben weniger Energie, sie dringen aber tiefer in die Haut ein. Nach wissenschaftlichen Erkenntnissen ist für lichtbedingte Hautschäden nicht nur die UV-B-Strahlung, die Sonnenbrand auslöst, verantwortlich, sondern auch die UV-A-Strahlung. Deren negative Wirkung macht sich vor allem in Form von Langzeitschäden wie Falten und Pigmentflecken bemerkbar, aber im schlimmsten Fall auch als Hautkrebs. Deswegen müssen Sonnenschutzmittel auch gegen UV-A-Strahlen schützen. In der Europäischen Union sollte der UVA-Schutzfaktor eines Sonnenschutzmittels mindestens ein Drittel des auf der Packung angegebenen Lichtschutzfaktors (LSF) betragen. Dieses Verhältnis basiert auf einer Empfehlung der EU-Kommission von 2006. Da der LSF primär den Schutz gegen UVB-Strahlen (Sonnenbrand) misst, stellt diese Regel sicher, dass auch ein proportional steigender Schutz gegen UVA-Strahlen (Hautalterung und langfristige Schäden) gewährleistet ist. Profimittel für den täglichen Gebrauch sollten jedoch weit darüber hinausgehen (**Bild 3**).

Bei der Auswahl der Sonnenschutzmittel sollte man sich zudem die Inhaltsstoffe anschauen. Enthalten die Produkte Parfüm ist das problematisch, weil Parfüm für die Hautverträglichkeit nicht unumstritten ist und grundsätzlich Allergien auslösen kann. Das ist ein Problem, das sich in Verbindung mit der Sonneneinstrahlung noch verschärfen kann, weil einige Parfüminhaltstoffe Sonnenallergien fördern können. Mittel für den professionellen Gebrauch sollten daher auf Parfüm verzichten.

## Die korrekte Dosierung ist entscheidend

Mindestens genauso wichtig wie die Auswahl des richtigen Produkts ist die korrekte Dosierung und Anwendung. Denn das größte Problem beim Sonnenschutz – und beim Hautschutz insgesamt – ist, dass die Beschäftigten die Produkte nicht oder falsch anwenden und die Anwendung nicht zur Routine wird. Deswegen sind praktische Unterweisungen und Hilfsmittel wie Poster und Infokarten wichtig, wie sie Profianbieter bereitstellen. Die richtige Dosierung funktioniert am besten mit Spendersystemen, die den Sonnenschutz automatisch richtig dosieren und so optimalen Schutz bieten. Man kann die Spender beispielsweise im Servicefahrzeug oder im Bauwagen anbringen oder an strategischen Punkten auf dem Werksgelände platzieren. So ist man zugleich abgesichert, dass das Sonnenschutzmittel immer vor Ort ist. Tuben und Sprays hingegen können die Beschäftigten leicht mitnehmen, wenn sie unterwegs sind.

Abschließend stellt sich die Frage, wie die neue ASR A5.1 zu bewerten ist. Zum einen nehmen die verschärften Regeln die Arbeitgeber noch stärker in die Pflicht als sie es ohnehin schon sind. Zu den Pflichten gehören etwa die Unterweisungspflicht und das Bereitstellen geeigneter Sonnenschutzmittel. Gleichzeitig werden aber auch die Beschäftigten ausdrücklich eingespannt, indem ihre Mitwirkungspflicht betont wird. Insgesamt wird die neue Regelung den UV-Schutz auf der Agenda der Berufsgenossenschaften noch weiter nach oben schieben, verstärkte Kontrollen eingeschlossen. ■ TS1136

*www.pgp-hautschutz.de*

**Anja Dick**
ist Apothekerin und Expertin für UV-Schutz bei Peter Greven Physioderm (PGP).

Die neuen Hybrid-Hosen sind das Highlight-Produkt der erweiterten Multinormschutz-Kollektion BP Multi Protect Plus. Sie vereinen Leichtigkeit und technische Finesse in bislang ungekanntem Maße. *Foto: BP – Bierbaum-Proenen*

# Die PSAisierung der Workwear

Einer der großen Trends derzeit ist, dass moderne Workwear heute auch Schutzfunktionen erfüllt. Besonders zeigt sich das aktuell beim Thema Sichtbarkeit und der Norm EN 17353. Hersteller wie BP – Bierbaum-Proenen befassen sich intensiv mit dem Thema. Das macht das Arbeiten für Menschen in unterschiedlichen Einsatzbereichen viel sicherer.

**TEXT**: *Jan-Frederic Sielemann*

Früher war die Unterscheidung deutlich, waren die Welten klar abgegrenzt. Auf der einen Seite gab es die Workwear, auch Berufsbekleidung genannt. Sie wurde und wird in vielen Berufen in der Industrie, im Handwerk, in der Gastronomie oder im Dienstleistungssektor getragen und dient vorwiegend dazu, den Arbeitsalltag der Trägerinnen und Träger zu erleichtern. Ihr Fokus liegt daher vor allem auf dem Tragekomfort, der Funktionalität und dem Auftritt nach außen – Workwear fungiert also als Visitenkarte eines Unternehmens. Sie muss keine Normen und keine Schutzfunktionen erfüllen (**Bild 1**).

Auf der anderen Seite stand und steht die Schutzkleidung oder Persönliche Schutzausrüstung (PSA). Sie wird in Arbeitsumgebungen mit potenziellen Gefahren getragen: vom Elektro-Handwerk über die Baubranche, den Verkehrssektor

**Bild 2** Workwear, die nach EN 17353 Typ B2 zertifiziert ist, wird, je nach Ausführung, mit unterschiedlich vielen und breiten Reflexstreifen an Armen und Beinen ausgestattet. *Foto: BP – Bierbaum-Proenen*

**Bild 3** Das Herzstück der Workwear-Kollektion von BP sind die Hybrid-Hosen, bei denen BP die besten Eigenschaften von Superstretch- und robustem Gewebe in Einklang gebracht hat, um maximale Bewegungsfreiheit und höchsten Tragekomfort mit Langlebigkeit zu vereinen. *Foto: BP – Bierbaum-Proenen*

und viele industrielle Bereiche bis zum Straßenbau und zur Abfallwirtschaft. Der Hauptfokus liegt hier auf dem Schutz und der persönlichen Sicherheit der Trägerinnen und Träger. Welche Schutzkleidung die Beschäftigten tragen müssen, ergibt sich aus der Gefährdungsbeurteilung. Im Gegensatz zur Workwear muss Schutzkleidung von den Arbeitgebenden kostenlos bereitgestellt und von den Arbeitnehmenden getragen werden. Je nach Einsatzgebiet schützt die PSA vor potenziellen Gefahren wie dem Übersehen-Werden im Straßenverkehr, vor Störlichtbögen, Schweißspritzern, Chemikalien, zündfähiger Entladungen in explosionsgefährdeter Umgebung, Hitze, Wind/Regen oder vor Kälte. Warnschutzkleidung gehört also ebenso zur PSA wie Schweißerschutz- oder Multinormschutzkleidung.

## Workwear und PSA nähern sich einander immer weiter an

Soweit zur Unterscheidung von Workwear und Schutzkleidung. Nun bemerken wir seit einiger Zeit den starken Trend, dass sich Workwear und PSA einander immer weiter annähern. Konkret haben wir es mit einer PSAisierung der Workwear und einer Casualisierung der PSA zu tun. Befassen wir uns zunächst mit der PSAisierung der Workwear. Was verstehen wir darunter? PSAisierung der Workwear meint, dass auch Workwear zunehmend Schutzfunktionen erfüllt. Besonders zeigt sich dieser Trend gerade beim Thema Sichtbarkeit. Hintergrund ist die Norm EN 17353, die für mittlere Risikosituationen gilt.

Seit 2020 ersetzt die EN 17353 zwei Normen, die EN 1150, die sich mit Schutz- und Warnkleidung für den nicht professionellen Gebrauch befasste; und die EN 13356:2001, die Warn-Zubehör für den nicht professionellen Gebrauch regelte. Die EN 17353 bewegt sich im professionellen Bereich. Nach EN 17353 zertifizierte Kleidung eignet sich für Berufsgruppen mit einem mittleren Risiko, bei der Arbeit übersehen zu werden – also zum Beispiel für Beschäftigte auf dem Bau, in der Logistikbranche oder in der Industrie. Stark gefährdete Berufsgruppen, wie etwa Mitarbeitende im Straßenbau, die im fließenden Verkehr tätig sind, müssen auch weiterhin Warnkleidung nach EN ISO 20471 tragen. Ob eine mittlere oder eine hohe Gefährdung vorliegt, ergibt die Risikoanalyse, die ein Betrieb in den Einsatzbereichen der Beschäftigten durchführen muss. Bei der EN 17353 gibt es drei Typen: Produkte des Typs A sind fürs Tageslicht geeignet, solche des Typs B für die Dunkelheit und der Typ AB schließlich eignet sich für alle Lichtverhältnisse inklusive der Dämmerung (**Bild 2**).

## Mehr Sicherheit, eine bessere Sichtbarkeit und ein spürbares Upgrade der Kleidung

Es hat etwas gedauert, bis sich die EN 17353 am Markt durchgesetzt hat. Jetzt spüren Hersteller wie der Kölner Berufsbekleidungsspezialist BP – Bierbaum-Proenen aber eine verstärkte Nachfrage. Das Interessante: Immer mehr Arbeitgebende möchten ihre Beschäftigten mit Workwear ausstatten, die nach EN 17353 Typ B2 zertifiziert ist.

Von der aufgewerteten Workwear versprechen sich die Arbeitgebenden mehr Sicherheit, eine bessere Sichtbarkeit und ein spürbares Upgrade der Kleidung für ihre Beschäftigten. Dahinter steht ein ganzes Büdel an Gründen. Kein Unternehmen möchte heute mehr irgendein Risiko eingehen und sich im Falle eines Unfalls Vorwürfe machen lassen müssen. Zum einen kostet jeder Betriebsunfall Geld, senkt die Produktivität und kratzt nicht zuletzt auch am Image des Unternehmens. In der Folge tun die Unternehmen alles, um mögliche Gefährdungen auszuschließen. Ein weiterer und kaum zu überschätzender Treiber für die gestiegene Nachfrage nach Workwear mit Schutzfunktion ist der Fach- und Arbeitskräftemangel. Unternehmen, die ihren Mitarbeitenden komfortable und professionelle Workwear bieten, die darüber hinaus auch noch eine Schutzfunktion bietet, erweisen ihren Be-

schäftigten Respekt, erhöhen ihre Motivation und Identifikation. So wird aufgewertete Workwear zum Werkzeug der Mitarbeiterbindung und -gewinnung und zur Trumpfkarte im Spiel um die begehrten Fach- und Arbeitskräfte (**Bild 3**).

## Wirtschaftlich attraktive Lösung für mittlere Risikosituationen

Workwear, die nach EN 17353 Typ B2 zertifiziert ist, wird, je nach Ausführung, mit unterschiedlich vielen und breiten Reflexstreifen an Armen und Beinen ausgestattet. Das bringt zusätzliche Sichtbarkeit bei Dunkelheit und in schlecht beleuchteten Innenbereichen – ohne dazu Warnschutzkleidung der EN ISO 20471 einsetzen zu müssen. Deswegen handelt es sich um eine wirtschaftlich attraktive Lösung für mittlere Risikosituationen. Die Kleidung eignet sich beispielsweise für all jene, die hauptsächlich drinnen, aber immer wieder auch draußen arbeiten, und dabei Gefahr laufen, übersehen zu werden. Die reflektierenden Elemente verbessern die Sicherheit auf innerbetrieblichen Verkehrswegen, etwa in der Industrie, Logistik, im Lager, der Gebäudereinigung oder bei kommunalen Dienstleistern. Ein großer Vorteil ist zudem, dass sich bestehende Bekleidungssysteme im Workwear-Sektor durch Typ-B2-Elemente erweitern lassen, ohne Farb- oder Designkonzepte zu verändern. Die dezenten Reflektoren sind optisch wenig auffällig und lassen sich daher gut in sämtliche Arbeitsbereiche integrieren. Das erhöht die Trageakzeptanz und schafft so mehr Sicherheit. In diesem Sinne ist die EN 17353 ist ein echter Gamechanger. Viele Experten vertreten daher die Meinung, dass es künftig keine Workwear mehr geben wird und geben darf, die nicht nach EN 17353 zertifiziert ist.

Kommen wir zum zweiten Trend, der Casualisierung der PSA. Damit ist gemeint, dass die Menschen heute nicht mehr nur an ihre Workwear, sondern selbst an Schutzkleidung dieselben Maßstäbe anlegen wie an Freizeitkleidung. Die Menschen wollen sich wohlfühlen in ihrer PSA, sie soll bequem und leicht sein. Beim Design äußert sich das in

**Bild 3** Die Warnschutz-Kollektion BP Hi-Vis Stretch bietet eine breite Auswahl an Produkten, in der neben den Klassikern wie Warnschutzhosen und -jacken auch viele casualisierte Kleidungsstücke wie T-Shirts, kurze Hosen oder Troyer erhältlich sind. *Foto: BP – Bierbaum-Proenen*

sportiven Schnitten, die für ein zeitgemäßes und professionelles Auftreten sorgen. Die Palette an Passformen, Funktionen und Farben ist sehr groß geworden, was eine Vielzahl an Kombinationsmöglichkeiten eröffnet. So finden Trägerinnen und Träger für jede Körperform, jede Arbeitssituation und jedes Wetter die beste Lösung. Es äußert sich aber auch darin, dass heute Kleidungsstücke im Arbeitskontext eine Rolle spielen, bei denen das früher nicht denkbar war, wie etwa Hoodies und Sweatjacken.

## Tragekomfort und Bewegungsfreiheit sind so wichtig wie nie zuvor

Der Tragekomfort und die Bewegungsfreiheit sind so wichtig wie nie zuvor, niemand hat mehr Lust auf Kleidung, die zwickt und zwackt, die unbequem ist und die Arbeit erschwert. Deswegen geht der Trend ganz klar zu Hybrid-Styles, die robuste und strapazierfähige Gewebe mit Stretch-Elementen verbinden. Das können Stretch-Einsätze sein, die an den richtigen Stellen dafür sorgen, dass der Stoff immer fließend den Bewegungen des Körpers folgt. Das können aber auch Stretch-Fasern sein, die für ein bequemes Tragegefühl sorgen. Dazu trägt auch die Leichtigkeit der Gewebe bei – das ist ein Punkt, der vor allem vor dem Hintergrund des Klimawandels und der immer heißeren Sommer stetig wichtiger wird. Bei aller Leichtigkeit muss Berufsbekleidung aber immer auch robust und strapazierfähig sein. Deswegen sind Hybrid-Lösungen so wichtig. Die Folge der Casualisierung der PSA ist, dass sich heute selbst Hightech-Produkte wie Multinorm- oder Warnschutzkleidung leicht und bequem wie Workwear anfühlt – obwohl sie vor lebensgefährlichen Risiken schützt.

Man sieht: Die ehemals getrennten Welten von Workwear und Schutzkleidung nähern sich einander immer mehr an. Bei beiden Entwicklungen stehen die Wünsche der Trägerinnen und Träger im Mittelpunkt. Schutzfunktion, Tragekomfort, Bequemlichkeit und Leichtigkeit sind also längst keine Gegensätze mehr – sondern zwei Seiten einer Medaille. Dabei haben die Hersteller immer sowohl das Wohl der Menschen als auch die Bedürfnisse der Unternehmen im Blick.

■ TS1137

**Jan-Frederic Sielemann**
ist Marketing-Leiter beim Kölner Hersteller BP – Bierbaum-Proenen.

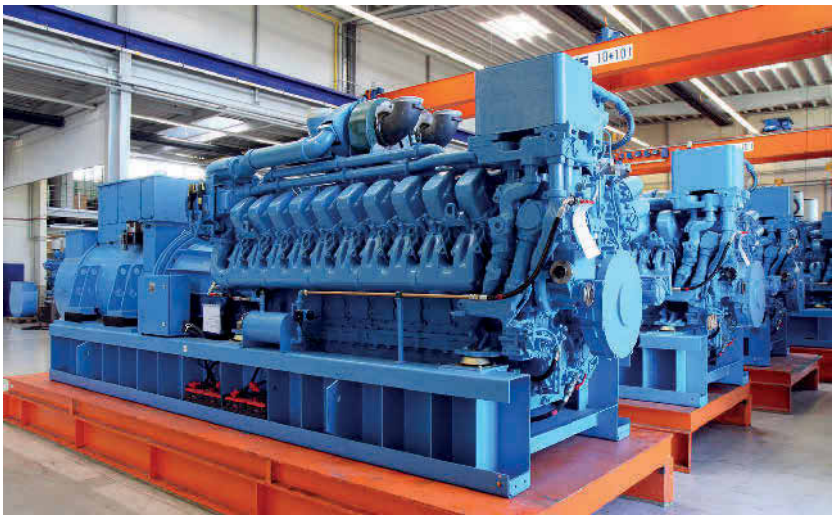
## KI-Überwachung wird zum Business-Tool

Reolink verstärkt seine Offensive im Markt für kleine und mittlere Unternehmen (KMU): Gestützt auf leistungsstarke Produkte wie die RP-PCB8MZ, RP-PCT16MD und RP-WCB8MZ Kameras aus dem Professional Series Portfolio und ein stetig wachsendes Distributionsnetzwerk, baut das Unternehmen seine Position im gewerblichen Bereich gezielt aus. Mit der Professional Series schließt Reolink die Lücke zwischen einfachen Sicherheitssystemen und komplexen Enterprise-Lösungen. Dabei wird klassische Videoüberwachung zum proaktiven Business-Tool, das präzise, KI-gestützte Sicherheitsfunktionen mit intelligenten Analyse-Werkzeugen kombiniert. Die einfache Verwaltung erfolgt über das zentrale Video Management System (VMS) von Reolink.

Reolink bietet auch im Professional Segment eine große Bandbreite an Kameras und NVRs für unterschiedlichste Anforderungen – von vandalismusgeschützten Dome-Varianten bis hin zu Kameras mit UHD-Auflösung, starkem optischem Zoom und ColorX-Vollfarb-Nachtsicht. Über die klassische Gefahrenabwehr hinaus macht ReoNeura die Sicherheitslösungen von Reolink zum strategischen Instrument moderner Unternehmensführung.

**www.Reolink.com**

## Neues Planerhandbuch „Notstromversorgung“



**Neues Planerhandbuch** „Notstromversorgung“ der DGWZ. *Foto: Piller Power Systems*

Die Deutsche Gesellschaft für wirtschaftliche Zusammenarbeit erstellt ein neues Planerhandbuch zur Notstromversorgung. Die Veröffentlichung ist im September 2026 geplant. Das Planerhandbuch enthält Informationen über die führenden Hersteller aus dem Bereich der Notstromversorgung sowie deren Produkte. Außerdem werden Ansprechpartner für Planer mit Kontaktdaten aufgeführt. Das Planerhandbuch „Notstromversorgung“ kann ab sofort kostenlos bei der DGWZ über die Website *www.dgwz.de/notstromversorgung-uebersicht* oder per E-Mail an *planerhandbuch@dgwz.de* vorbestellt werden. Das Planerhandbuch bietet Fachplanern, Ingenieurbüros, Elektrofachbetrieben, Betreibern und Bauherren einen kompakten Überblick über Anbieter, Produkte und Lösungen im Bereich der Notstromversorgung.

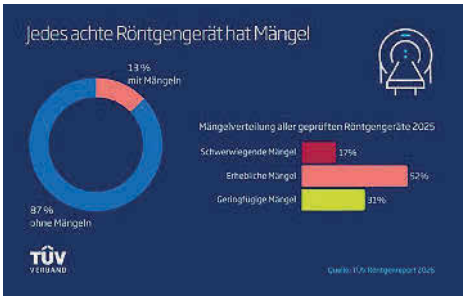
*www.dgwz.de/presse*

## Weniger Fahrraddiebstähle – Schäden bleiben auf Rekordniveau

Die Zahl der versicherten Fahrraddiebstähle ist weiter zurückgegangen. Nach aktuellen Zahlen des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) wurden 2025 rund 115 000 (2024: 135 000) versicherte Fahrräder gestohlen. Die Hausratversicherer zahlten dafür wie im Vorjahr insgesamt rund 150 Millionen Euro. Fahrräder haben in vielen Haushalten inzwischen einen deutlich höheren Wert als noch vor einigen Jahren. Hochwertige E-Bikes kosten oft mehrere tausend Euro und sind damit nicht nur attraktive Mobilitätsmittel, sondern auch ein lukratives Ziel für Diebstähle. Gleichzeitig steigt mit den höheren Anschaffungskosten auch das finanzielle Risiko. Fahrräder sind über die Hausratversicherung grundsätzlich gegen Einbruchdiebstahl abgesichert, etwa wenn sie aus der Wohnung, dem Keller oder einer verschlossenen Garage gestohlen werden. Für einfachen Diebstahl unterwegs ist jedoch häufig ein zusätzlicher Fahrradbaustein erforderlich. Rund 27 Millionen Haushalte in Deutschland verfügen über eine Hausratversicherung. Etwa die Hälfte dieser Verträge enthält eine Fahrradklausel. Versicherer empfehlen, Kaufbelege, Rahmennummer und aktuelle Fotos des Fahrrads aufzubewahren, um die Schadenregulierung im Ernstfall zu erleichtern. Hochwertige Bügel- oder Kettenschlösser sowie gut sichtbare Abstellorte können zudem helfen, das Diebstahlrisiko zu senken. Langzeitstatistiken zum Thema Fahrraddiebstahl finden Sie unter: *www.gdv.dex*

# TÜV Röntgenreport: Jedes achte Röntgengerät hat Mängel

Die Mängelquote bei Röntgengeräten in Deutschland ist im Jahr 2025 leicht gestiegen. Gut jede achte Röntgeneinrichtung (13 Prozent) weist bei den unabhängigen Sicherheitsprüfungen Mängel auf. Im Vergleich zum Vorjahresreport ist die Mängelquote um einen Prozentpunkt gestiegen. Das ist ein Ergebnis des „TÜV Röntgenreport 2026". Insgesamt haben die Sachverständigen der TÜV-Organisationen bundesweit 15 333 Röntgengeräte geprüft. Dabei stellten sie an 2 037 Geräten Mängel fest und dokumentierten 2 794 einzelne Beanstandungen. „Röntgen ist ein unverzichtbares Werkzeug der Medizin und Technik, aber jede Aufnahme bedeutet auch eine Strahlenbelastung", sagt Dr. Alexander Schröer, Strahlenschutzexperte des TÜV-Verbands. „Deshalb müssen Geräte und Anwendung besonders sorgfältig kontrolliert werden."




Mängelverteilung an Röntgengeräten.
*Foto: TÜV-Verband*

Von den festgestellten Mängeln waren 17 Prozent „schwerwiegend". Schwerwiegende Mängel sind Mängel, die das Patientenrisiko stark erhöhen, wie zum Beispiel eine zu hohe Dosis, mangelhafte Strahlfeldbegrenzung oder fehlende Bildqualität. Aber auch formale Punkte wie das Fehlen der CE-Kennzeichnung oder die Nichteinhaltung von gesetzlichen Vorgaben bei der Patientendosiserfassung gehören dazu. Schwerwiegende Mängel schließen einen Weiterbetrieb der Anlage grundsätzlich aus, bis der Mangel behoben und das Gerät erneut geprüft wurde. Mehr als jeder zweite Mangel (52 Prozent) entfiel auf die Kategorie „erheblicher Mängel". Erhebliche Mängel müssen zeitnah von Fachpersonal beseitigt werden. Fast ein Drittel (31 Prozent) wurden als „geringfügige" beziehungsweise formale Mängel eingestuft, die mit geringem Aufwand von den Betreibern selbst behoben werden können.

Die meisten geprüften Röntgengeräte stammen aus der Human- und Dentalmedizin und werden unmittelbar in der Diagnostik am Menschen eingesetzt. Gut die Hälfte der Anlagen (53 Prozent) entfällt auf die Dentalmedizin und knapp jede fünfte (19 Prozent) auf die Humanmedizin. „Röntgenbilder sind die Grundlage medizinischer Entscheidungen und müssen daher korrekt sein", sagt Schröer. „Schon kleine Fehler können die Aussagekraft beeinträchtigen und damit direkte Folgen für die Behandlung haben."

Mit 8 144 geprüften Röntgenanlagen stellt die Dentalmedizin die größte Gerätegruppe. 16 Prozent der Geräte weisen Mängel auf. Die Quote entspricht damit dem Niveau des Röntgenreports aus dem Jahr 2022 (16 Prozent). An 1 333 Anlagen wurden insgesamt 1 748 Mängel festgestellt. Erhebliche Mängel dominieren mit 49 Prozent, schwerwiegende Mängel machen 16 Prozent aus, geringfügige beziehungsweise formale Mängel 35 Prozent.

In der Humanmedizin wurden 2 939 Geräte geprüft, davon weisen 14 Prozent Mängel auf. Die Mängelquote bei humanmedizinischen Röntgengeräten ist in den vergangenen Jahren deutlich gesunken – um 8 Prozentpunkte seit 2022. Im Jahr 2025 stellten die Sachverständigen an den humanmedizinischen Röntgenanlagen 698 Mängel fest. Der Großteil entfällt auf erhebliche Mängel (71 Prozent), schwerwiegende Mängel machen 17 Prozent aus, geringfügige Mängel 12 Prozent.

Auffällig sind Defizite rund um die Röntgenaufnahme selbst. Viele der festgestellten Mängel an Geräten aus der Human- und Dentalmedizin betreffen zentrale Elemente der Bildgebung, insbesondere Bildwiedergabesysteme sowie beschädigte oder unzureichend geprüfte Speicherfolien. „Kratzer, Knicke oder Verschmutzungen auf Speicherfolien können als Artefakte auf Röntgenbildern sichtbar werden und die Befundung erschweren oder verfälschen", sagt Schröer. „In der Human- und Dentalmedizin ist eine verlässliche Diagnose nur anhand technisch einwandfreier Bilder möglich." Mit der zunehmenden Digitalisierung und dem Einsatz von KI in der Bildauswertung gewinnt die Qualität der zugrunde liegenden Röntgenaufnahmen weiter an Bedeutung. Artefakte oder Qualitätsmängel in den Bildern können die automatisierte Auswertung erschweren und die diagnostische Sicherheit beeinträchtigen.

Neben Defiziten bei der Bildqualität treten auch Mängel im Bereich des Strahlenschutzes auf, etwa bei Dosisindikatoren, Patientenschutzmitteln oder der Kennzeichnung von Expositionsparametern. Fehlende oder fehlerhafte Dosisindikatoren erschweren die Kontrolle der Strahlenexposition und können dazu führen, dass unnötige Belastungen nicht erkannt werden. Mängel bei den Schutzmitteln für Patient:innen und Personal, wie Bleischürzen, führen dazu, dass Menschen während einer Röntgenaufnahme unnötig Strahlung ausgesetzt sind. Und Mängel bei den Expositionsparametern können die Nachvollziehbarkeit der Strahlenbelastung erschweren und eine optimale Einstellung der Geräte beeinträchtigen. „Strahlenschutz ist Voraussetzung für den sicheren Einsatz von Röntgentechnik", sagt Schröer. „Röntgen ist nur dann sinnvoll, wenn der Nutzen klar überwiegt und Risiken konsequent minimiert werden."

Um diesen Anspruch im Praxisalltag sicherzustellen, sind regelmäßige und unabhängige Prüfungen unverzichtbar. „Unabhängige Prüfungen sind kein bürokratischer Aufwand, sondern eine zentrale Voraussetzung für sicheren Strahlenschutz", sagt Schröer. „Sie sorgen dafür, dass technische Standards im Betrieb tatsächlich eingehalten werden."

Der TÜV Röntgenreport 2026 zeigt, dass sich die Mängelquoten in den vergangenen Jahren insgesamt verbessert, zuletzt aber auf einem relevanten Niveau stabilisiert haben. Entsprechend hoch bleibt der Handlungsbedarf. Aus Sicht des TÜV-Verbands besteht insbesondere beim Strahlenschutz und im Umgang mit Bildgebungssystemen Qualifizierungsbedarf. „Viele der festgestellten Mängel betreffen den praktischen Umgang mit den Geräten sowie die Umsetzung von Sicherheitsanforderungen", sagt Schröer. „Aus- und Weiterbildungsangebote für Betreiber, Servicefirmen und Aufsichtsbehörden sind daher notwendig." Zudem sollte die Abstimmung bei der praktischen Umsetzung regulatorischer Vorgaben zwischen Bund und Ländern verbessert werden, um einheitliche Standards sicherzustellen. Nur so lassen sich die Qualität der Bildgebung und die Sicherheit von Patientinnen und Patienten dauerhaft gewährleisten.

Der vollständige Röntgenreport 2026 ist abrufbar unter:
*www.tuev-verband.de/presse/publikationen/reporte/roentgenreport*

# Deutscher Goldstandard für Cloud-Sicherheit

Kiteworks hat das BSI C5 (Cloud Computing Compliance Criteria Catalogue) Typ-2 Testat erhalten. Der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Kriterienkatalog bildet den Goldstandard für Cloud-Sicherheit in Deutschland. Das BSI C5 Testat ist ein essenzielles Auswahlkriterium für Unternehmen, die hohe Sicherheitsanforderungen an ihre Cloud-Anbieter stellen. Es bietet eine Compliancebasis, die weltweit gilt. Das BSI C5 Framework umfasst 121 Sicherheitskontrollen in 17 Domänen, abgeleitet von international anerkannten Standards wie BSI IT-Grundschutz, ISO/IEC 27001 und der CSA Cloud Controls Matrix. Die Prüfung von Kiteworks erfolgte vom 1. August bis 31. Oktober 2025 und umfasste sowohl das Design als auch die operative Wirksamkeit der Sicherheitskontrollen. Sie wurde durch ein unabhängiges Prüfungsurteil der HKKG GmbH vom 19. Dezember 2025 attestiert. Es bestätigt die Sicherheit von Kiteworks in den Bereichen Identity & Access Management, Kryptografie und Schlüsselmanagement, Security Incident Management, Business Continuity und weiteren – und adressiert damit das gesamte Spektrum der Cloud-Sicherheitsanforderungen.

Das BSI C5 Typ-2 Testat erweitert das umfassende Compliance-Portfolio von Kiteworks und ergänzt die bestehenden Zertifizierungen wie SOC 2 Typ II, ISO 27001, 27017 und 27018, die FedRAMP Moderate Authorization sowie den FedRAMP High Ready-Status und die IRAP-Zertifizierung. So können Kunden auf eine zentrale Plattform setzen, die regulatorische Anforderungen in Europa, Nordamerika und dem asiatisch-pazifischen Raum unterstützt.

Das Testat hat besonders für regulierte Branchen einen hohen strategischen Wert. Unternehmen aus Bereichen wie öffentliche Verwaltung, Gesundheitswesen, Finanzdienstleistungen oder kritische Infrastrukturen müssen robuste Sicherheitskontrollen nachweisen. BSI C5 Typ-2 liefert dafür eine unabhängige Bestätigung, dass zertifizierte Unternehmen wie Kiteworks die notwendige Transparenz sowie Sicherheitskontrollen und operative Resilienz für den Schutz sensibler Daten in Cloud-Umgebungen gewährleisten. Das Testat verkürzt Sicherheitsüberprüfungen von Anbietern und beschleunigt so Beschaffungsprozesse. Compliance-Teams erhalten auditfähige Unterlagen, die direkt die Einhaltung von DSGVO, NIS2 und DORA unterstützen. Und besonders relevant für den deutschen Markt: Kiteworks unterstützt deutsche und europäische Unternehmen dabei, Anforderungen an Datensouveränität umzusetzen, etwa durch On-Premises- oder Private-Cloud-Bereitstellungen vollständig zertifizierter Software. „Deutsche Unternehmen brauchen erprobte Plattformen, die ihre robuste Abwehr unter realen Bedingungen unter Beweis stellen“, sagt Nadine Hoogerwerf, Global IT CISO bei Kiteworks. Weitere Informationen zum BSI C5 Testat von Kiteworks finden sich im Solution brief.

*www.digitalk-pr.de*

IMPRESSUM

**Technische Sicherheit**
ISSN 2191-0073, 17. Jahrgang 2026

**Herausgeber**
VDI Fachmedien GmbH und Co. KG
Düsseldorf

**Redaktion**
Annika Hilse M.Sc., Chefredakteurin
Telefon: +49 0211 6103-343
*ahilse@vdi-fachmedien.de*
Ines Henning, Redaktionsassistenz
Telefon: +49 211 6103-311
Fax: +49 211 6103-148
ts*@vdi-fachmedien.de*
Dipl.-Phys.-Ing. Udo Schnell
Redaktionsleitung VDI Fachmedien
Telefon: +49 211 6103-104
*uschnell@vdi-fachmedien.de*

Autorenhinweise/Veröffentlichungsgrundlagen: *www.technische-sicherheit.de*

**Verlag**
VDI Fachmedien GmbH & Co. KG
Unternehmen für Fachinformationen
VDI-Platz 1, 40468 Düsseldorf
Postfach 10 10 22, 40001 Düsseldorf
Commerzbank AG
SWIFT/BIC-Code: DRES DE FF 300
IBAN: DE69 3008 0000 0212 1724 00

**Geschäftsführung**
Beatrice Gerner

**Layout**
Ulrich Jöcker

**Leitung Sales Solutions**
Petra Seelmann-Maedchen
Telefon +49 211 6188-191
*pmaedchen@vdi-nachrichten.com*

**Anzeigenverkauf**
Arnd Walgenbach
Telefon +49 211 6103-199
*awalgenbach@vdi-fachmedien.de*
Es gilt der Anzeigentarif Nr. 13
vom 1. Januar 2026.

**Vertrieb und Leserservice**
Leserservice VDI Fachmedien
65341 Eltville
Telefon: +49 6123 9238-202
Fax: +49 6123 9238-244
*vdi-fachmedien@vuservice.de*

**Bezugspreise**
6 Ausgaben jährlich (1/2, 3/4, 5/6, 7/8, 9/10, 11/12 als Doppelausgaben)
Jahresabonnement: € 295,– (E-Paper € 253,–)
VDI-Mitglieder: € 265,50(E-Paper € 227,70)
nur für persönliche Mitglieder
Studenten: € 134,– (E-Paper € 115,–)
gegen Studienbescheinigung
Preise Inland inkl. MwSt., Ausland exkl. MwSt. zzgl. Versandkosten (Inland: € 14,–, Ausland: € 23,–, Luftpost auf Anfrage)
Einzelheft: € 51,– Inland inkl. MwSt., Ausland exkl. MwSt. zzgl.Versandkosten

Die Mindestlaufzeit beträgt 12 Monate. Im Anschluss an die Mindestlaufzeit ist das Abonnement jeweils zum Monatsende kündbar.

**Satz**
Medienpartner Mäurer GmbH
Auf dem Feldchen 14, 41849 Wassenberg

**Druck**
Möller Pro Media GmbH
Zeppelinstraße 6, 16356 Ahrensfelde



**Weitere Informationen:**
www.technische-sicherheit.de

Auflage IVW-geprüft

# Die erste Adresse für Technikwissen: VDI Fachmedien

VDI Fachmedien

Jetzt bestellen

## VDI Fachmedien E-Paper-Abonnements 2026

**Preise in EUR**

| Zeitschrift \| Digital | Ausgaben/Jahr | Jahresabo | Upgrade | Probeabo |
|---|---|---|---|---|
| Bauingenieur | 10 | 491,00 | 99,00 | 100,00 |
| Gefahrstoffe | 6 | 444,00 | 89,00 | 150,00 |
| HLH | 9 | 233,00 | 58,00 | 53,00 |
| Konstruktion | 9 | 525,00 | 84,00 | 118,00 |
| Lärmbekämpfung | 6 | 257,00 | 51,00 | 88,00 |
| Technische Sicherheit | 6 | 261,00 | 51,00 | 89,00 |
| VDI energie + umwelt | 6 | 334,00 | 71,00 | 113,00 |
| VDI-Z | 9 | 279,00 | 59,00 | 63,00 |

Alle Preise brutto | Preisänderungen vorbehalten | Stand: Januar 2026
Kündigungsbedingungen: Die Mindestlaufzeit beträgt 12 Monate. Im Anschluss an die Mindestlaufzeit kann das Abonnement jederzeit mit einer Frist von einem Monat gekündigt werden.
VDI Fachmedien GmbH & Co. KG | AG Düsseldorf HRB 33854 | Geschäftsführung: Beatrice Gerner

### Preisnachlässe:

- Mitglieder des Vereins Deutscher Ingenieure e.V. (VDI) erhalten 10% Rabatt auf das Jahresabo
- Studentenpreise auf Anfrage


**Kontaktieren Sie uns:**
Leserservice VDI Fachmedien | 65341 Eltville
T +49 6123 9238-202
F +49 6123 9238-244
E vdi-fachmedien@vuservice.de

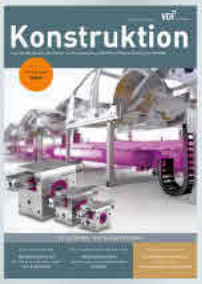
VDI Fachmedien

Alle auch als E-Paper


10 Ausgaben pro Jahr
Jahresabopreis: 573,00 EUR
zzgl. Versandkosten
E-Paper-Abo: 491,00 EUR


6 Ausgaben pro Jahr
Jahresabopreis: 517,00 EUR
zzgl. Versandkosten
E-Paper-Abo: 444,00 EUR


9 Ausgaben pro Jahr
Jahresabopreis: 271,00 EUR
zzgl. Versandkosten
E-Paper-Abo: 233,00 EUR




9 Ausgaben pro Jahr
Jahresabopreis: 612,00 EUR
zzgl. Versandkosten
E-Paper-Abo: 525,00 EUR


6 Ausgaben pro Jahr
Jahresabopreis: 299,00 EUR
zzgl. Versandkosten
E-Paper-Abo: 257,00 EUR

**Die erste Adresse für Technikwissen: VDI Fachmedien**


6 Ausgaben pro Jahr
Jahresabopreis: 304,00 EUR
zzgl. Versandkosten
E-Paper-Abo: 261,00 EUR


6 Ausgaben pro Jahr
Jahresabopreis: 388,00 EUR
zzgl. Versandkosten
E-Paper-Abo: 334,00 EUR


9 Ausgaben pro Jahr
Jahresabopreis: 324,00 EUR
zzgl. Versandkosten
E-Paper-Abo: 279,00 EUR

**Die VDI Fachmedien bieten Ihnen eine breite Palette renommierter Fachzeitschriften aus den Bereichen Bau, Konstruktion/Produktion, Logistik, Energie und Umwelt.** In direkter Anbindung an den VDI, das größte technisch-wissenschaftliche Netzwerk für Ingenieur*innen Deutschlands. Unsere Autor*innen berichten über Innovationen und Hintergrundwissen in ihrem jeweiligen Fachgebiet. Und das jederzeit praxisorientiert, ohne den wissenschaftlichen Background aus dem Blick zu verlieren.

**Technikwissen für Ingenieur*innen – jetzt auswählen und bestellen:**

**T** +49 6123 9238-202
**E** vdi-fachmedien@vuservice.de
**vdi-fachmedien.de**

Inlandsbruttopreise – Ausland auf Anfrage