

mrl.news

Ausgabe 2024.02

Seite 2

Editorial: So wappnen Sie sich gegen Gefahren

Seite 3

Auf dem Weg zu einem nachhaltigeren
Sicherheitsschaltgerät

Seite 6

Wie ein Kunde bei einem internationalen Großprojekt
vom globalen Netzwerk des tec.nicum profitiert

Seite 9

Brandschutz im Maschinenbau –
normative Anforderungen und Praxisbeispiele

Seite 14

Künstliche Intelligenz zur Unfallvermeidung

Seite 16

Cyber-Resilience im Maschinenbau

Seite 20

Lockout-Tagout-Tryout (LOTOTO)

Seite 21

Das Seminarprogramm 2024/25 der
tec.nicum academy



So wappnen Sie sich gegen Gefahren

„Wo aber Gefahr ist, wächst das Rettende auch“, lautet die berühmte Zeile aus einem Gedicht von Friedrich Hölderlin – und könnte auch das Motto dieser Ausgabe der MRL News sein, das sich wie ein roter Faden durch das Heft zieht.

Zum Beispiel in unserem Beitrag über den Cyber Resilience Act der EU: Ganz eindeutig sind die Gefahren für Unternehmen durch Cyber-Attacken in besorgniserregendem Maße gestiegen. Der Cyber Resilience Act, der voraussichtlich im Herbst 2024 vom Europäischen Rat verabschiedet wird, verfolgt das Ziel, die Widerstandskraft der EU gegen solche Angriffe zu erhöhen. Welche neuen Anforderungen und Pflichten damit auf Unternehmen zukommen, beschreibt der Artikel ab Seite 16.

Unbestreitbar sind auch die Gefahren, die durch den Klimawandel entstehen. Auch hier will die EU mit dem Green Deal gegensteuern. Wie Schmersal dazu beiträgt, den CO₂-Fußabdruck entlang der Wertschöpfungskette zu reduzieren, lesen Sie auf der gegenüberliegenden Seite.

Beim Ausstoß von Treibhausgasen sind Elektroautos ein Plus für den Klimaschutz. Doch auch bei der Herstellung von Lithium-Batterien für die Elektromobilität ist Maschinensicherheit ein Muss. Wie ein internationales Team

von Functional Safety Engineers von tec.nicum einen global agierenden Batteriehersteller dabei unterstützt, die Anforderungen der EU-Maschinenrichtlinie zu erfüllen, berichten wir ab Seite 6.

Die enormen Gefahren, die von Bränden ausgehen, werden oft unterschätzt. Das Rettende liegt hier in der Prävention: Ein umfassendes Brandschutzkonzept ist für jedes Unternehmen unerlässlich. Welche Richtlinien und Normen dabei zu berücksichtigen sind, erfahren Sie ab Seite 9.

Potenzielle Gefahren präventiv abwenden – darum geht es auch in dem Beitrag auf Seite 14. Genauer gesagt: Wie man Künstliche Intelligenz zur Unfallvermeidung einsetzen kann.

Das Rettende wächst! In diesem Sinne: Bleiben Sie zuversichtlich!

Eine anregende Lektüre wünscht Ihnen

Ihr Redaktionsteam

Auf dem Weg zu einem nachhaltigeren Sicherheitsschaltgerät Schmersal erforscht Möglichkeiten zur Reduzierung des CO₂-Fußabdrucks

Die EU-Kommission hat einen Vorschlag für eine neue Ökodesign-Verordnung für nachhaltige Produkte (Ecodesign for Sustainable Products Regulation, ESPR) vorgelegt, die zentraler Baustein des European Green Deal werden soll. Auch Schmersal ist bereits auf dem Weg zur Nachhaltigkeit.

Schmersal hat es sich zur Aufgabe gemacht, Kunden nicht nur bei der Einführung von Zukunftstechnologien im Rahmen der digitalen Transformation zu unterstützen, sondern auch dabei, den CO₂-Fußabdruck entlang der Wertschöpfungskette zu reduzieren. Dabei setzt das Unternehmen bei dem Material an, aus dem die meisten Sicherheitsschalter bestehen: Kunststoff.

Bei Produkten im Bereich der Maschinensicherheit besteht die grundsätzliche Herausforderung darin, dass neue, umweltfreundliche Lösungsansätze bei Produktdesign oder Materialeinsatz die Qualität und insbesondere die Sicherheitsfunktionen der Sicherheitsschaltgeräte in keiner Weise beeinträchtigen dürfen. Auch die optimierten Geräte müssen den Normen entsprechen, ihre Eignung muss überprüft und durch Zertifizierungen bestätigt werden.

Um hier Fortschritte erzielen zu können, arbeitet Schmersal seit Langem mit Universitäten und Forschungsinstituten zusammen. Etwa mit dem Kunststoffinstitut Lüdenscheid, mit dem Schmersal aktuell bei einem sehr vielversprechenden Projekt kooperiert. Dabei

geht es um den Einsatz von Recyclingmaterial bei der Herstellung von Sicherheitsschaltgeräten, die über ein Kunststoffgehäuse verfügen. „Unser Ziel ist es, bei den im Spritzgussverfahren hergestellten Schaltern 20 Prozent Regranulat einzusetzen“, sagt Matthias Banaszek, Manager Value Engineering & Expert in Plastics bei Schmersal. „Wir haben deshalb in den vergangenen zwei Jahren rund 30 Tonnen Material aus Produktionsabfällen sortenrein gesammelt, etwa Angüsse oder Anfahrreste, also untaugliche erste Bauteile, die beim Start einer neuen Fertigungscharge anfallen.“

Laut dem Unternehmen UL, das die weltweit anerkannte Sicherheitsprüfzeichen vergibt, ist ein Regranulat-Anteil von 25 Prozent in Sicherheitsschaltern möglich. Dies wird bei eigener Aufbereitung zugelassen. Aus diesem Grund prüfen Abdel El Makrini, Fertigungsmeister Kunststoffbauteile, und Matthias Banaszek aktuell die Möglichkeit, eine eigene Zentralmühle anzuschaffen sowie die entsprechenden Räumlichkeiten und die Infrastruktur einzurichten. Die Planungen dazu sollen in Kürze abgeschlossen sein, sodass mit der Umsetzung begonnen werden kann. →



Schmersal hat sich zum Ziel gesetzt, bei den im Spritzgussverfahren hergestellten Schaltern 20 Prozent Regranulat einzusetzen.



Viele Schalter von Schmersal werden im Spritzgussverfahren hergestellt.

Auch der TÜV würde Sicherheitsschalter mit Recyclinganteil zertifizieren – vorausgesetzt, es kann der Nachweis erbracht werden, dass das eingesetzte Recyclingmaterial keinen Einfluss auf die Qualität der Sicherheitsfunktionen hat.

Zu diesem Zweck führt das Kunststoffinstitut eine Vergleichsprüfung mit den Schaltern von Schmersal durch: Untersucht werden Schalter aus reinem Neumaterial im Vergleich mit Schaltern bestehend aus 80 Prozent Neumaterial und 20 Prozent Regranulat.

Analysiert werden dabei eine Reihe von Parametern mit normgerechten Prüfmethode, wie beispielsweise die Charpy-Schlagzähigkeitsprüfung nach EN ISO 179-1, die zur Charakterisierung eines Kunststoffes bei hohen Dehnraten dient. Oder etwa die Messung der Dichte nach EN ISO 1183-1 sowie das IEC 60093-Prüfverfahren für Durchgangswiderstand zur Beschreibung des elektrischen Isolationsverhaltens. Dabei gilt es nachzuweisen, dass die Schalter aus Mischmaterial widrigen Umwelteinflüssen ebenso gut standhalten wie diejenigen aus reinem Neumaterial.

„Im Grunde kann man schon im Vorhinein ziemlich präzise berechnen, dass dem so ist. Aber natürlich müssen wir auch im konkreten Versuch den Nachweis erbringen“, so Banaszek. Wenn das Ergebnis der Vergleichsprüfung vom Kunststoffinstitut vorliegt und den Erwartungen

entspricht – es also keine Qualitätsbeeinträchtigungen durch den Einsatz von Mischmaterial gibt –, müssen die Schalter im nächsten Schritt vom TÜV zertifiziert werden. Dann wäre der Weg frei für die serienmäßige Produktion der Schalter mit Regranulat-Anteil. Schmersal wäre damit der erste Hersteller, der Recyclingmaterial bei der Herstellung von Sicherheitsschaltern einsetzt.

Poly4Nature – Kunststoffe aus alternativen Rohstoffen

Auch ein weiteres Umweltprojekt kam mittelbar über das Kunststoffinstitut Lüdenscheid zustande: Schmersal hat sich als aktiver Partner dem deutschen Innovationsnetzwerk Poly4Nature angeschlossen, das vom Bundesministerium für Wirtschaft und Klimaschutz gefördert und vom Kunststoffinstitut Lüdenscheid gemanagt wird. Ziel des Innovationsnetzwerks Poly4Nature ist es, Kunststoffe aus alternativen Rohstoffen und mit alternativen Verfahren herzustellen, zum Beispiel durch den Einsatz von Naturfasern oder Vorprodukten aus natürlichen Wertstoff- oder Abfallströmen. Diese Materialien sollen bisher eingesetzte fossile Materialien ersetzen, um eine CO₂-Reduktion bzw. CO₂-Neutralität zu erreichen.

Denn die Bausteine für die Herstellung von Kunststoffen sind Kohlenstoffverbindungen, die aus Erdöl oder Erdgas gewonnen werden. Sowohl bei der Förderung und dem Transport fossiler Brennstoffe wie Erdöl oder Erdgas als auch bei der Herstellung von Kunststoffen werden →

erhebliche Mengen an klimaschädlichen CO₂-Emissionen freigesetzt.

Als Netzwerkpartner hat Schmersal jetzt ein konkretes Projekt mit Poly4Nature vereinbart: die Entwicklung von biologisch abbaubaren Schutzstopfen auf Basis alternativer Rohstoffe. Diese Schutzstopfen werden zum Abdecken von Schrauben und Einschraubblöchern verwendet und kommen bei Schmersal zu Hunderttausenden zum Einsatz – und zwar ausschließlich beim Transport von Schmersal-Schaltern. Sobald der Anwender die Schalter aus der Transportverpackung nimmt, werden die Schutzstopfen entsorgt.

„Bei den Schutzstopfen handelt es sich um nicht sicherheitsrelevante Bauteile. Daher ist der Einsatz alternativer Materialien hier sehr viel einfacher umzusetzen“, erläutert Matthias Banaszek. „Ich könnte mir die Verwendung von Naturpolymeren auch noch bei vielen anderen Verpackungsmaterialien und Bauteilen vorstellen, beispielsweise bei Zubehör wie Schlitzabdeckungen, Schraubstopfen oder bei der Transportsicherung, die wir für unsere Sicherheitszuhaltung AZM40 verwenden.“

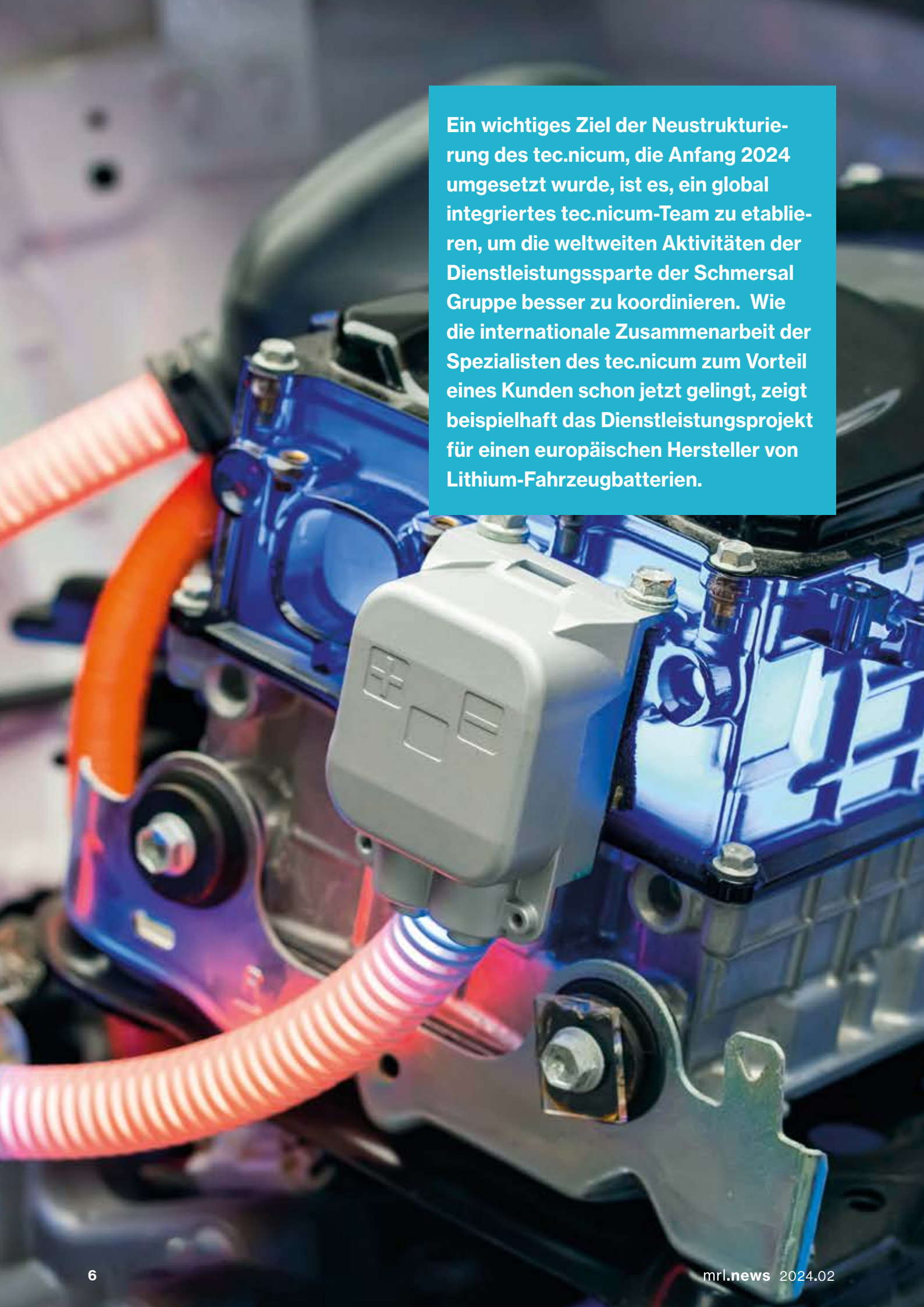
Die alternativen Kunststoffe für diese Verpackungsmaterialien könnten zum Beispiel maritimen Ursprungs sein, wie etwa Algen. Als weitere Möglichkeiten sieht Poly4Nature den „Einsatz von erneuerbarem Kohlenstoff aus Pyrolyseprozessen, auf Lignin basierende Werkstoffsysteme, den Einsatz von Naturfasern oder Vorprodukte aus natürlichen Wertstoff- bzw. Abfallströmen (Side Stream).

Diese Werkstoffe sollen insbesondere bisher eingesetzte fossile Materialien nicht nur ersetzen, sondern in Abhängigkeit von möglichen Eigenschaftsprofilen Produkte mit neuen Funktionen versehen, zumindest jedoch eine CO₂-Reduzierung bzw. -Neutralität bieten.“ Wichtig sei aber auch: „In Abgrenzung zu bisher bekannten Materialien sollen neue Wertschöpfungsketten natürlichen Ursprungs diskutiert werden, die nicht in Konkurrenz zu landwirtschaftlichen Flächen und der Lebensmittelindustrie stehen.“

Ob die Schutzstopfen in Zukunft tatsächlich aus Algen sein werden, bleibt abzuwarten, das Projekt läuft noch bis Anfang 2026. So viel lässt sich aber jetzt schon sagen: Ein Anfang ist gemacht. ■



Schutzstopfen werden zum Abdecken von Schrauben verwendet und sollen künftig aus alternativen Kunststoffen hergestellt werden.



Ein wichtiges Ziel der Neustrukturierung des tec.nicum, die Anfang 2024 umgesetzt wurde, ist es, ein global integriertes tec.nicum-Team zu etablieren, um die weltweiten Aktivitäten der Dienstleistungssparte der Schmersal Gruppe besser zu koordinieren. Wie die internationale Zusammenarbeit der Spezialisten des tec.nicum zum Vorteil eines Kunden schon jetzt gelingt, zeigt beispielhaft das Dienstleistungsprojekt für einen europäischen Hersteller von Lithium-Fahrzeugbatterien.

Zusammenarbeit über vier Kontinente

Bei einem internationalen Großprojekt profitiert ein Kunde vom globalen Netzwerk des tec.nicum

Der globale Markt für Lithiumionen-Batterien boomt: Laut einer Studie soll der Absatz bis 2027 jährlich um rund elf Prozent wachsen. Die Haupttreiber dabei sind zum einen die Produktion von Elektroautos, zum anderen die Elektronikindustrie. Die globale Batterieproduktion wird von einigen Ländern dominiert, allen voran China. Doch verlagert sich die Herstellung von Lithium-Batterien jetzt zunehmend auch nach Europa. Und so ist es kein Wunder, dass der Kontakt zu einem neuen Kunden des tec.nicum – einem europäischen Hersteller von Lithiumionen-Batterien für die Elektromobilität – über ein Projekt in China zustande kam: Dort führte das tec.nicum im Jahr 2023 Risikobewertungen für einen in China ansässigen Maschinenlieferanten durch.

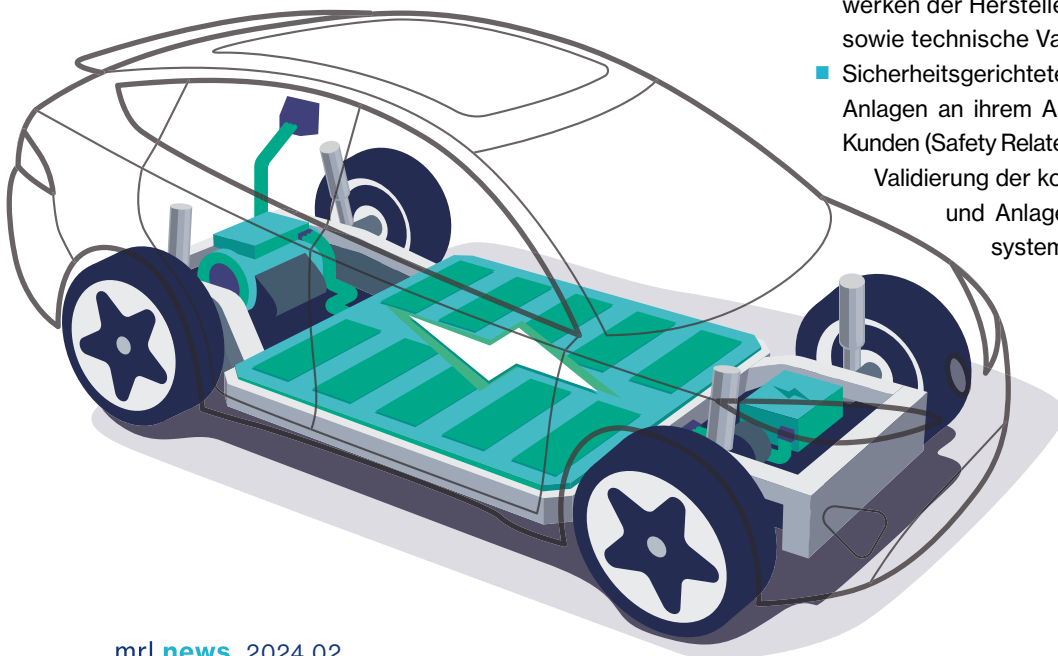
Mit dem neuen Kunden hat das tec.nicum einen Rahmenvertrag mit Wirkung seit Januar 2024 über Beratungsleistungen für dessen Lieferanten geschlossen, die in China, Japan und Südkorea Maschinen zur Batterieproduktion herstellen und nach Europa exportieren. Denn Unternehmen aus diesen asiatischen Ländern gehören nach wie vor zu den führenden Herstellern von Maschinen für die Batterieproduktion. Sie müssen jedoch nachweisen, dass ihre Maschinen die Anforderungen der europäischen Maschinenrichtlinie (MRL) erfüllen und CE-konform sind.

Seit 2024 ist das tec.nicum der exklusive Anbieter für Beratungsleistungen zur CE-Konformität für alle außereuropäischen Maschinenlieferanten des Batterieherstellers. Das bedeutet: Das tec.nicum ist dafür verantwortlich, dass alle Lieferanten, die für den europäischen Kunden tätig sind und ihm ihre Maschinen liefern, die EU-Maschinenrichtlinie einhalten.

Damit erreicht der europäische Batteriehersteller eine effiziente Umsetzung der Sicherheitsanforderungen der MRL und der CE-Kennzeichnung mit einer zentralen Koordination für alle Standorte seiner außereuropäischen Maschinenlieferanten. Der Batteriehersteller profitiert dabei vom globalen Netzwerk des tec.nicum: An dem Projekt sind tec.nicum-Teams aus Deutschland, Schweden, Brasilien, China, Südkorea – wo Schmersal in Kürze eine Niederlassung eröffnen wird – und Indien beteiligt. Da derzeit eine neue Batteriefabrik in Kanada gebaut wird, die künftig von Maschinenlieferanten aus China und Südkorea beliefert werden soll, ist außerdem ein tec.nicum-Team von Schmersal North America involviert.

Die tec.nicum-Dienstleistungen für die Partnerunternehmen des tec.nicum-Kunden in Asien und Kanada werden in fünf Phasen erbracht:

- Schulungen der Partnerunternehmen im Hinblick auf die Anforderungen der europäischen Maschinenrichtlinie, der Normen und der Anforderungen der GTS (General technical specifications) des Kunden
- Prüfung der vorhandenen Dokumentation, Erstellung eines Gap-Reports (Vergleich des aktuellen Status mit dem Zielstatus)
- Bereitstellung von Ingenieurleistungen zur Unterstützung bei der Korrektur von festgestellten Gaps und der Erstellung anderer erforderlicher Dokumente
- Checkliste für die sicherheitsbezogene Werksabnahme (Safety Related Factory Acceptance Test, SR-FAT)
- Prüfung der Sicherheitssysteme und physische Verifizierung ihrer CE-Konformität in den Produktionswerken der Hersteller in China, Südkorea und Japan sowie technische Validierung
- Sicherheitsgerichtete Abnahme der Maschinen und Anlagen an ihrem Aufstellort direkt beim tec.nicum-Kunden (Safety Related Site Acceptance Test (SR-SAT), Validierung der korrekten Montage der Maschinen und Anlagen mit zusätzlichen Sicherheitssystemtests →



Die Service-Pakete, die das tec.nicum an die an die Maschinenhersteller liefert, umfassen darüber hinaus die Überprüfung der Konformität mit verschiedenen EU-Richtlinien.

Dazu zählen:

- Ein Basis-Paket (Maschinenrichtlinie 2006/42/EC, Grundlegende Sicherheits- und Gesundheitsanforderungen, EHSR)
- ATEX (Richtlinie 1999/92/EC und Richtlinie 2014/34/EU)
- Gefährliche Chemikalien (EU-Verordnungen REACH und RoHS)
- EG-Druckgeräterichtlinie PED,
- Sicherheit von Maschinen – Laserbearbeitungsmaschinen (EN ISO 11553)
- Elektromagnetische Verträglichkeit (EMV)
- Spezifische Normen für den Einsatz und die Sicherheit von Hydrauliksystemen in Maschinen
- Integrierte Maschinensysteme (IMS) nach EN ISO 11661

Die tec.nicum-Teams können Beratungsleistungen zum Teil digital ausführen. Die Durchführung der Tests und die Erstellung der Dokumentation erfolgt jedoch überwiegend vor Ort beim Lieferanten. Voraussetzung dafür ist eine gute Kommunikation mit dem Lieferanten in der Landessprache (hauptsächlich Chinesisch, aber auch Koreanisch) und in Englisch. Dies ist durch muttersprachliche Mitglieder des tec.nicum-Teams an den verschiedenen asiatischen tec.nicum-Standorten problemlos gewährleistet.

Auch eine weitere Anforderung des tec.nicum-Kunden – ein sehr gutes technisches Know-how des tec.nicum-Teams, um die Funktionen der vorhandenen Maschinen und deren Dokumentation zu verstehen – kann problem-

los erfüllt werden. Denn die Experten von tec.nicum verfügen über langjährige Erfahrung in der Durchführung technischer Projekte in den unterschiedlichsten Branchen. Zudem sind sie vom TÜV Rheinland zertifizierte Experten, z. B. als Functional Safety Engineer – Machinery oder als IECEx-zertifizierte Fachkraft.

Insgesamt ist das Projekt aufgrund der Vielzahl der Maschinen und Standorte sowie der zu erbringenden Leistungen eine Mammutaufgabe. So werden allein für die Aufgaben der Phase 1.100 Arbeitsstunden für eine mittelgroße Maschine veranschlagt.

Und deshalb gibt es eine weitere essenzielle Anforderung an alle Beteiligten: „We all need a great deal of patience.“

Führende Mitglieder des internationalen tec.nicum-Teams für das Projekt Batterieproduktion:

- Bruno Diniz (tec.nicum Global Director)
- Leo Schytt (Managing Director – Schmersal Nordiska)
- Michele Seassaro (Managing Director – Schmersal China)
- Gary Ferguson (Managing Director – Schmersal North America)
- Sagar Bhosale (Managing Director – Schmersal India)
- Tetsuya Horimoto (Managing Director – Schmersal Japan)
- Uwe Seeger (Director Middle East, Asia & Pacific – Schmersal South Korea)
- Enildo dos Santos (Business Development Manager – tec.nicum Europe)
- Carsten Doll (Site Manager – tec.nicum Germany)
- Girish Alawe (General Manager - tec.nicum Asia)
- Devin Murray (Manager – tec.nicum North America) ■



Der Brandschutz im Maschinenbau ist ein wesentlicher Bestandteil der industriellen Sicherheitstechnik. Maschinen und Anlagen sind besonders durch hochenergetische Prozesse brandgefährdet. Die Brandgefahr kann durch verschiedene Faktoren, wie die Verarbeitung brennbarer Materialien, den Einsatz von Hochtemperaturprozessen (z. B. in Gießereien) sowie durch elektrische Fehlfunktionen oder mechanische Defekte hervorgerufen werden.



Brandschäden und Produktionsausfälle vermeiden

Brandschutz im Maschinenbau – normative Anforderungen und Praxisbeispiele

Beim Brandschutz stehen neben der Vermeidung von Verletzungen der Beschäftigten die Sicherstellung der Betriebskontinuität und der Schutz der hergestellten Produkte im Vordergrund. Produktionsausfälle durch Brandschäden können erhebliche wirtschaftliche Verluste verursachen und die Betriebskontinuität gefährden.

Laut DGUV wurden den Unfallversicherungsträgern in Deutschland in den vergangenen Jahren jeweils etwa 3.500 Arbeitsunfälle gemeldet, deren Ursache auf Brände und Explosionen zurückzuführen war. Ein tragisches Beispiel verdeutlicht die Dringlichkeit effektiver Brandschutzmaßnahmen:

Am 6. Februar 2023 entstand beim Autozulieferer Burgmaier in Allmendingen ein Schaden von rund 200 Millionen Euro, als ein Großbrand die gesamte Fabrikhalle erfasste. Ein Tank mit 50.000 Litern Hydrauliköl entzündete sich. Die Bilanz war verheerend: Fünf Verletzte, ein Schaden in dreistelliger Millionenhöhe sowie rund 250 Menschen ohne Arbeitsplatz und ein Unternehmen, das seinen Hauptsitz verloren hat.

Ein umfassendes Brandschutzkonzept ist daher unerlässlich, um sowohl die Sicherheit der Mitarbeiter als auch die Integrität der Produktionsprozesse zu gewährleisten.

Entstehung und Aufrechterhaltung eines Feuers – Brand-Tetraeder

Der Brand-Tetraeder ist ein erweitertes Modell des traditionellen Branddreiecks und beschreibt die vier wesentlichen Komponenten, die für das Entstehen und die Aufrechterhaltung eines Feuers notwendig sind. Das Verständnis des Brand-Tetraeders ist grundlegend für die Entwicklung effektiver Brandschutz- und Löschrategien, da er zeigt, dass das Entfernen oder Stören einer der vier Komponenten ausreicht, um ein Feuer zu löschen.

Diese vier Komponenten sind:

- **Brennstoff:** Jede brennbare Substanz, die in einem Brand verbraucht wird, sei es fest, flüssig oder gasförmig. Beispiele sind Holz, Papier, Benzin und Methan.
- **Sauerstoff:** Ein Brand benötigt Sauerstoff zur Verbrennung. In der Regel wird dieser aus der Luft entnommen, die etwa 21 Prozent Sauerstoff enthält.
- **Wärme:** Eine ausreichende Menge an Wärme ist erforderlich, um den Brennstoff auf seine Zündtemperatur zu bringen und die Verbrennung aufrechtzuerhalten.
- **Chemische Reaktion:** Die exotherme chemische Reaktion, die zwischen Brennstoff und Sauerstoff abläuft und dabei Wärme und Licht freisetzt. →



Richtlinien und Normen

Die grundlegenden Sicherheits- und Gesundheitsschutzanforderungen finden sich in der gültigen Maschinenrichtlinie 2006/42/EG. Diese fordert unter anderem die Berücksichtigung von Brand- und Explosionsgefahren bereits in der Konstruktionsphase der (ortsfesten) Maschine. Die Anforderungen sind jedoch wenig konkret und geben dem Konstrukteur keine spezifischen Maßnahmen zur Implementierung vor:

„Die Maschine muss so konstruiert und gebaut sein, dass jedes Brand- und Überhitzungsrisiko vermieden wird, das von der Maschine selbst oder von Gasen, Flüssigkeiten, Stäuben, Dämpfen und anderen von der Maschine freigesetzten oder verwendeten Stoffen ausgeht.“

Konkretisiert werden diese grundlegenden Sicherheits- und Gesundheitsschutzanforderungen durch harmonisierte Normen. Die ISO 19353 „Sicherheit von Maschinen – vorbeugender und abwehrender Brandschutz“ ist die zentrale Norm für Brandschutzanforderungen im Maschinenbau. Sie beschäftigt sich umfassend mit dem vorbeugenden und abwehrenden Brandschutz von Maschinen. Ziel der Norm ist es, die von einer Maschine ausgehenden Brandgefahren auf ein akzeptables Niveau zu senken. Hierzu legt die Norm Methoden fest, um Brandgefahren zu erkennen und Risikobeurteilungen durchzuführen. Dabei werden grundlegende Begriffe und Methoden für Brandschutzmaßnahmen definiert.

Darüber hinaus ist im jeweiligen Einzelfall eine weiterführende Normenrecherche für die zu bewertende Maschine unerlässlich! Eine eventuell vorhandene maschinenspezifische C-Norm kann Anforderungen an den maschinenbezogenen Brandschutz enthalten, welche in den weniger detaillierten „Sicherheitsfachgrundnormen“ (Typ-B-Normen) nicht betrachtet sind.

Neben der Verpflichtung der Hersteller, den Brandschutz konstruktiv zu berücksichtigen, gelten ebenso Anforderungen an den Maschinenbetreiber. Die Betriebssicherheitsverordnung verpflichtet Arbeitgeber zur Durchführung von Gefährdungsbeurteilungen und zur Umsetzung geeigneter Schutzmaßnahmen, um die Sicherheit und Gesundheit der Beschäftigten zu gewährleisten. Dazu gehören auch spezifische Brandschutzmaßnahmen. →





ISO 19353 – zentrale Norm für Brandschutzanforderungen im Maschinenbau

Die ISO 19353 liefert dem Maschinenhersteller Methoden zur Identifizierung, Ermittlung und Bewertung sowie Maßnahmen zur Risikominimierung. Wichtig ist, den Anwendungsbereich der Norm zu beachten. Sie gilt ausschließlich für ortsfeste Maschinen. Sie gilt nicht für ortsveränderliche Maschinen, Maschinen für kontrollierte Verbrennungsprozesse, Maschinen für den Einsatz in explosionsgefährdeten Bereichen sowie Brandmelde- und -löschanlagen als Bestandteil von Brandschutzsystemen für Gebäude.

Die wichtigsten Aspekte umfassen:

1. Identifikation von Brandgefahren

- a. Analyse potenzieller Brandquellen:
Diese umfasst die Identifizierung interner und externer Faktoren, die Brände verursachen können, wie elektrische Komponenten, mechanische Reibung oder brennbare Materialien.
- b. Ermittlung von Brandursachen:
Die Norm fordert eine detaillierte Untersuchung der möglichen Ursachen, die zu einem Brand führen können, einschließlich Kurzschlüssen, Überhitzung oder Funkenbildung.
- c. Bewertung der Brandrisiken:
Die Risikobeurteilung erfolgt durch die Abschätzung der Wahrscheinlichkeit und des potenziellen

Schadensausmaßes eines Brandes. Dies erfordert eine systematische und methodische Herangehensweise zur qualitativen und quantitativen Bewertung der Risiken.

d. Dokumentation der Ergebnisse:

Alle identifizierten Risiken und Bewertungen müssen umfassend dokumentiert werden, um eine transparente Nachverfolgung und zukünftige Überprüfungen zu ermöglichen.

2. Risikominderung

- a. Inhärent sichere Konstruktionsmaßnahmen:
Diese beinhalten die Verwendung schwer entflammbarer Materialien und die Minimierung der Anwendung von brennbaren Flüssigkeiten oder Schmierstoffen.
- b. Technische Schutzmaßnahmen:
Hierzu gehören beispielsweise das Kapseln von gefährlichen Komponenten oder Absaugen (z. B. Rauch, Hitze) sowie Maßnahmen gegen den Austritt von Flammen aus produktionsbedingten Öffnungen (z. B. Türspalte, Werkstückzuführung).

Der Prozess zur Risikominderung folgt dem iterativen Drei-Stufen-Verfahren der ISO 12100. Kann das Brandrisiko nicht durch inhärent sichere Konstruktions- und technische Schutzmaßnahmen adäquat vermindert werden, sind ergänzende Schutzmaßnahmen vorzusehen (z. B. NOT-HALT nach ISO 13850, Anschlüsse für die Versorgung mit Löschmitteln etc.). →

In jedem Fall sind integrierte Brandmelde- und Löschanlagen zu bevorzugen.

Das Lösungskonzept bzw. die Auswahl der geeigneten Brandschutzausrüstung richtet sich letztlich nach der definierten Risikohöhe und reicht von automatischen Warn- und Brandmeldungen bis hin zu fest installierten, handbetätigten oder automatischen Löscheinrichtungen. Bei integrierten Löscheinrichtungen sind geeignete Löschmittel entsprechend den vier Brandklassen A, B, C und D nach ISO 3941 festzulegen.

Praxisbeispiel: Brandschutz bei einer ortsfesten Schleifmaschine nach ISO 16089

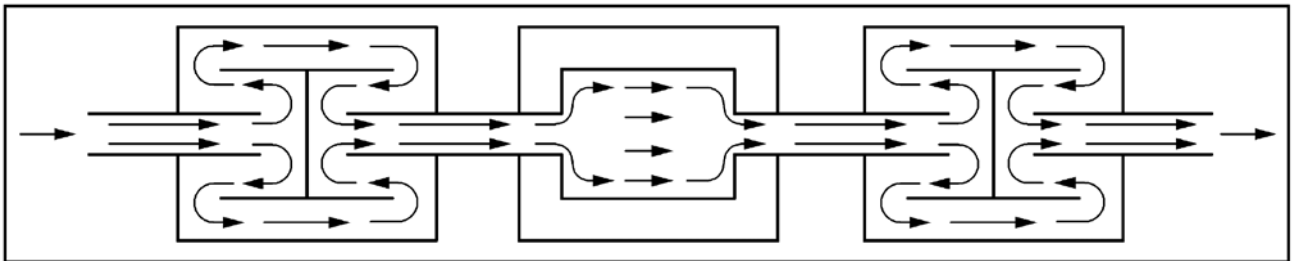
Die ISO 16089 spezifiziert Sicherheitsanforderungen für ortsfeste Schleifmaschinen. Im Rahmen der Norm wird auch der Brandschutz thematisiert, der durch die Umsetzung der Anforderungen der ISO 19353 ergänzt wird. Anhand einer ortsfesten Schleifmaschine sollen die Umsetzung dieser Anforderungen und die Durchführung von Brandschutzmaßnahmen veranschaulicht werden.

Zunächst wird eine detaillierte Risikobeurteilung durchgeführt, um potenzielle Brandgefahren zu identifizieren. Bei Schleifmaschinen besteht eine hohe Wahrscheinlichkeit

von Funkenbildung während des Schleifprozesses. Weitere Gefahrenquellen umfassen die Wärmeentwicklung durch Reibung, die Ansammlung von brennbarem Schleifstaub sowie die Nutzung brennbarer Kühlschmierstoffe.

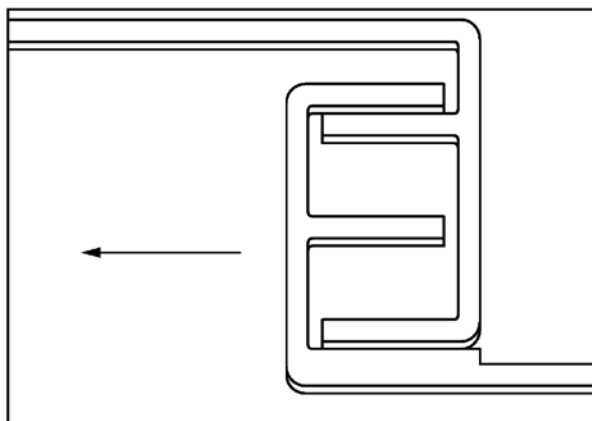
Auf Grundlage der zuvor identifizierten Gefahren werden spezifische technische Schutzmaßnahmen festgelegt. Ein zentrales Element sind automatische Funkenlöschsysteme (vorbeugender Brandschutz). Diese Systeme sind so konzipiert, dass sie Funken unmittelbar nach ihrer Entstehung erkennen und löschen. Automatische Funkenmelder, die in den Absaugsystemen der Schleifmaschine integriert sind, detektieren Funken und aktivieren Wasser- oder Gaslöschdüsen, die den Funken mit einem feinen Wassernebel oder Löschgas ersticken.

Parallel dazu ist die Staubabsaugung entscheidend. Effektive Absaugvorrichtungen entfernen brennbaren Schleifstaub aus dem Arbeitsbereich. Um sicherzustellen, dass Flammen nicht in die Absaugkanäle eindringen, ist die Installation von Flammensperren vorzusehen. Diese Vorrichtungen verhindern die Ausbreitung von Flammen durch die Kanäle. Ergänzend dazu werden Beruhigungsabschnitte in den Absaugkanälen integriert, um heiße Partikel abzukühlen und Funken zu löschen, bevor sie eine Brandgefahr darstellen können. →



Flammensperre (aus ISO 16089)

Ebenfalls eine besondere Bedeutung haben flammendurchschlagsichere Labyrinthdichtungen, die verhindern, dass Flammen aus der Maschine austreten.



Labyrinthdichtung (aus ISO 16089)



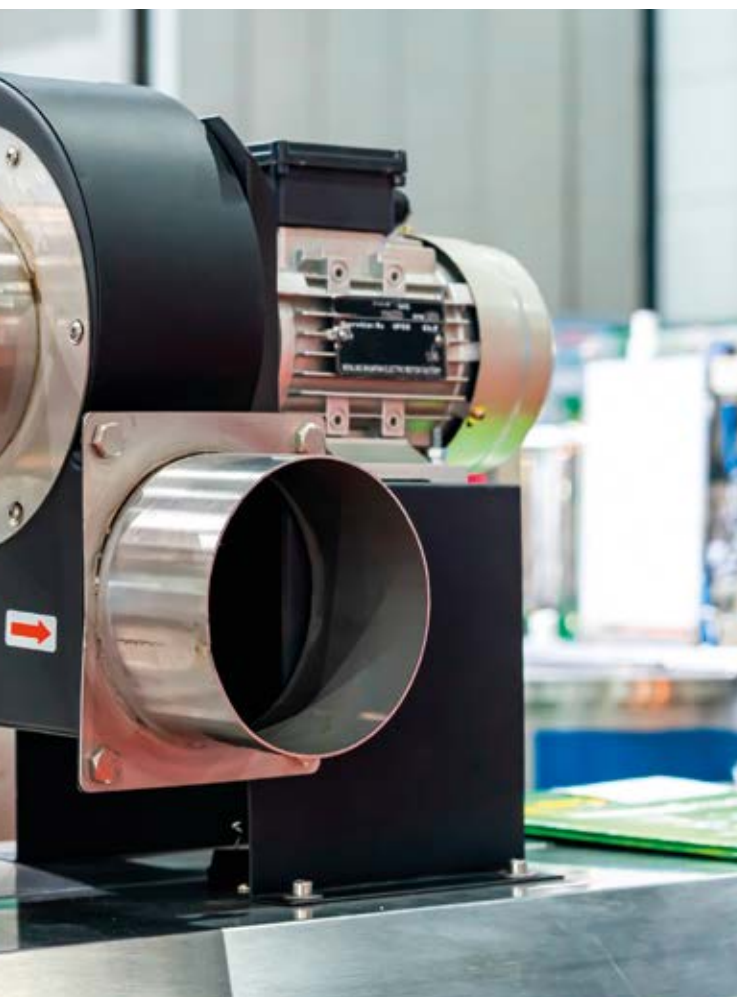
Diese Dichtungen sind beispielsweise an Türen oder Wartungsklappen der Schleifmaschine angebracht und nutzen ein Labyrinthdesign, das Flammen durch mehrfache Umkehrungen im Weg erstickt.

Auch die Gefahr durch brennbare Kühlschmierstoffe wird in der ISO 16089 beschrieben. Generell können Kühlschmierstoffe mit einem Ölanteil von mehr als 15 Prozent zur Gefahr von Bränden oder druckschwachen Explosionen führen. Grundsätzlich sind Kühlschmierstoffe mit geringem Verdampfungsverlust und dem höchsten Flammpunkt bei (nach Möglichkeit) hoher Viskosität zu wählen. Die Wahl erfolgt unter Beachtung der Anforderungen des Bearbeitungsprozesses.

Durch die systematische Identifikation von Brandgefahren, die sorgfältige Auswahl und Implementierung geeigneter technischer Schutzmaßnahmen sowie die regelmäßige Wartung und Überprüfung dieser Systeme können Brandgefahren bei ortsfesten Schleifmaschinen erheblich reduziert und die Sicherheit der Maschinenbediener gewährleistet werden. ■

Tristan Willigsecker

Elektroingenieur, Safety Consultant/
tec.nicum



Fazit:

Der Brandschutz im Maschinenbau erfordert eine ganzheitliche Betrachtung und die Implementierung spezifischer Maßnahmen, die auf einer fundierten Risikobeurteilung basieren.

Durch die Einhaltung normativer Anforderungen, insbesondere der ISO 19353, und die Kombination von technischen und ergänzenden Schutzmaßnahmen kann das Brandrisiko signifikant reduziert werden. Das vorgestellte Beispiel zeigt, dass eine sorgfältige Planung und konsequente Umsetzung von Brandschutzmaßnahmen nicht nur zur Erfüllung gesetzlicher Vorgaben, sondern auch zur Erhöhung der Betriebssicherheit und Effizienz beiträgt.

Die Experten des tec.nicum unterstützen Sie dabei gern mit ihrer langjährigen und breit gefächerten Erfahrung aus unzähligen Projekten im Maschinen- und Anlagenbau.



Seminare der tec.nicum academy

Die tec.nicum academy bietet das Seminar „Brandschutz im Maschinenbau“ sowie das Kompaktseminar „Explosionsschutz“ an.

Termine werden auf Anfrage mitgeteilt.

Ansprechpartnerin:

Melanie Peters-Schuster
Tel. +49 202 6474 864
info-de@tecnicum.com

Künstliche Intelligenz (KI) gilt als zukunftsweisende Technologie, die insbesondere auch die Automatisierung in Industriebetrieben voranbringt, da sie die Auswertung großer Datenmengen ermöglicht. Auch für Maschinensicherheit und Arbeitsschutz eröffnet die KI neue Chancen und Möglichkeiten: tec.nicum bietet im Rahmen seines neuen Angebotsmoduls „digitalisation“ u. a. auch KI-basierte visuelle Sicherheitsüberwachungssysteme an.

Potenzielle Gefahren präventiv abwenden Künstliche Intelligenz zur Unfallvermeidung

Im Zuge der Ausweitung seines Service-Angebots hat tec.nicum die „Digitalisierung“ als einen wichtigen neuen Baustein ins Programm aufgenommen. Zu dem neuen Digitalisierungsangebot gehören im Wesentlichen drei Bereiche:

■ IIoT-Lösungen / Schmersal Cloud-Solution

Dabei geht es um Software-Module, die für die Erfassung, Speicherung, Analyse, Kontrolle und Visualisierung von Safety- und Prozessdaten eingesetzt werden. Es werden z. B. Lösungen für das Safety- und Condition-Monitoring sowie für Predictive Maintenance angeboten, aber auch Software-Lösungen für das Energie- und KPI-Monitoring.

■ tec.dloto – Digital Lockout-Tagout

Die Software bietet eine unterstützende, digitale Überwachung des Lockout-Tagout, das Arbeitsunfälle verhindert, indem Maschinen vorübergehend vollständig von ihren Energiequellen getrennt werden.

■ Computational-Vision-Lösungen

Ein modulares System von Videoanalyselösungen, das Informationen aus verschiedenen industriellen Bereichen in einer Umgebung integriert. Es kann Bilder, Leistungsindikatoren, Verfügbarkeit, Qualität und vor allem die Sicherheit von Menschen und Anlagen messen. Dazu zählt das Videoanalyzesystem „Artificial Intelligence to Reduce Accidents“ (AI.RA).

Visuelle Sicherheitsüberwachung mit intelligenter Datenverarbeitung

Bei dem Videoanalyzesystem **tec.iara – Artificial Intelligence to Reduce Accidents** handelt es sich um eine KI-basierte, visuelle Sicherheitsüberwachung, die Unfallrisiken in Echtzeit erkennen kann, indem das System die Interaktion zwischen Menschen, Objekten und der Arbeitsumgebung beobachtet. Durch die Integration von KI hat sich die Funktionsweise von kameragestützten Überwachungssystemen signifikant geändert. Mithilfe

von maschinellem Lernen und fortschrittlichen Algorithmen sind KI-gestützte Systeme in der Lage, nicht nur statische Bilder und Videos aufzuzeichnen, sondern auch komplexe Analysen durchzuführen. Aufgrund ihrer Fähigkeit zur intelligenten Datenverarbeitung können sie nicht nur Aufnahmen speichern, sondern auch bestimmte vorher gelernte Ereignisse automatisch erkennen und darauf reagieren.

Beispielsweise können diese visuellen Überwachungssysteme erkennen, ob ein Mitarbeiter einen Gefahrenbereich betritt, und ggf. ein Alarmsignal auslösen. Außerdem kann das System die Nähe eines Mitarbeiters zu gefährlichen Gegenständen detektieren sowie die Nähe und Neigung von schwebenden Lasten kontrollieren und einschätzen. Auch kann erkannt werden, ob die Mitarbeiter die vorgeschriebene persönliche Schutzausrüstung wie Helme, Brillen, Handschuhe oder Sicherheitsschuhe tragen.

Das System ermöglicht so eine proaktive Sicherheitsüberwachung und eine unmittelbare Benachrichtigung der verantwortlichen Stellen bei risikobehafteten Aktivitäten, sodass z. B. Stürze oder Unfälle vermieden werden können. Zudem kann überprüft werden, ob Menschen in einem Arbeitsumfeld – etwa in Produktionshallen oder auch im Außenbereich – die vorgeschriebenen, abgesicherten Wege einhalten.

Durch die Fähigkeit des KI-basierten visuellen Überwachungssystems, Bedrohungen oder ungewöhnliche Aktivitäten frühzeitig zu erkennen und in Echtzeit zu analysieren, können potenzielle Gefahren präventiv abgewendet oder es kann zumindest schnell reagiert werden. →

Hybride Architektur

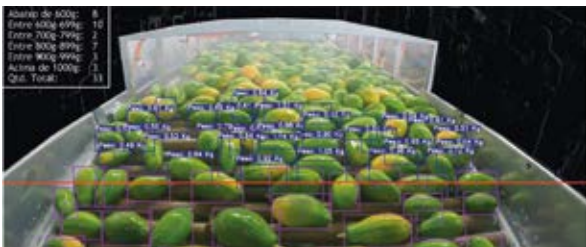


Das Videoanalysesystem tec.iara basiert auf einer hybriden Architektur, die sowohl Cloud- als auch On-Premise-Server nutzt.

Durch die On-Premise-Server können alle Algorithmen lokal ausgeführt werden, was nicht nur zu einer hohen Verarbeitungseffizienz führt, sondern auch zu einem hohen Maß an Datensicherheit. Cloud-Server werden nur zum Hosten von Dashboards und behandelten Daten verwendet. Das bedeutet, dass alle sensiblen Daten (z. B. Bilder) innerhalb des Unternehmens bleiben.

Für das tec.iara-System sind keine besonderen Netzwerke erforderlich, sondern es wird ein normales CC-TV-Netzwerk (Closed-Circuit Television) zur Erfassung und Übertragung von Bilddaten eingesetzt, wie es aus der herkömmlichen Videoüberwachung bekannt ist.

Weitere Computational-Vision-Lösungen: tec.saci und tec.cuca



Zu den weiteren Computational-Vision-Lösungen, die das tec.nicum anbietet, zählen tec.saci, ein System zur Analyse von Verhalten und Interaktion, und tec.cuca (Unified Characteristics Classifier). Für die Implementierung dieser Videoanalyselösungen wird ein IP-Kamera-Bilderfassungssystem eingesetzt. Es ist auch möglich, bereits installierte Geräte zu verwenden. Die Verarbeitung der Daten kann vor Ort (on premise) oder in der Cloud erfolgen; die Berichte werden über eine maßgeschneiderte Dashboard-Plattform zur Verfügung gestellt.

tec.saci – System zur Analyse von Verhalten und Interaktion

Videoanalysesystem zur Erkennung menschlicher Handlungen in Fertigungsbereichen und Werkshallen, das in der Lage ist:

- Eine Echtzeit-Chronoanalyse durchzuführen
- Alle menschlichen Aktivitäten in einem definierten Bereich, getrennt nach Berufsprofilen, zu erkennen
- Die Einhaltung von Routinen, Checklisten und Einrichtungstandards zu bewerten
- Nutzungsmuster und Gerätedefekte zu erkennen
- Die Ausführung und Leistung zu analysieren und zu standardisieren
- Engpässe und ineffiziente Bereiche zu identifizieren

tec.cuca – Unified Characteristics Classifier



tec.cuca ist ein System, das verschiedene Qualitätsstandards erkennen und Informationen sammeln kann:

- Format und Abmessungen
- Anzahl und Verluste
- Erkennung visueller Fehler
- Konformitätsanalysen (z. B. Löcher)
- Aufzeigen von Ursache und Wirkung von Problemen, um eine sofortige Lösung zu ermöglichen
- Trendanalyse

Arbeits- und datenschutzrechtliche Aspekte



Keine Frage: Der Einsatz visueller Überwachungssysteme bietet ein deutliches Plus an Sicherheit und Arbeitsschutz für die Beschäftigten. Dabei empfiehlt es sich, den Einsatz derartiger Systeme sorgfältig zu planen und die Mitarbeiter frühzeitig mit einzubeziehen. Denn es geht dabei nicht nur um Fragen des Arbeits- und Gesundheitsschutzes, sondern auch um Fragen der Leistungs- und Verhaltenskontrolle. Auch datenschutzrechtliche Aspekte müssen berücksichtigt werden. Deshalb sollten arbeits- und datenschutzrechtliche Gesichtspunkte mit den betroffenen Abteilungen und Mitarbeitern im Vorhinein diskutiert und geklärt werden. Das erhöht nicht zuletzt auch die Akzeptanz für den Einsatz dieser KI-Systeme im Unternehmen. ■

Volker Heinzer

Strategischer Produktmanager Programmierbare
Elektronische Systeme und Industrie 4.0 / IIoT,
Schmersal Gruppe

Das Ziel ist ebenso einleuchtend wie begrüßenswert: Die Widerstandskraft von Unternehmen in der EU gegen Cyber-Angriffe auf digitale Produkte und Systeme soll erhöht werden. Dazu hat das Europäische Parlament im März 2024 den Cyber Resilience Act verabschiedet. Damit kommen auf Hersteller von Komponenten und Maschinen sowie auf Maschinenbetreiber neue Anforderungen und Pflichten zu. Welche das sind – und welche Fragen noch offen sind –, beschreiben wir in diesem Beitrag.



Cyber-Resilience im Maschinenbau

Der Cyber Resilience Act der EU bringt neue Pflichten für Maschinenhersteller und -betreiber mit sich

Dass Cyber-Security ein Thema mit absoluter Priorität ist, muss man bei Schmersal niemandem erklären. Die Schmersal Gruppe ist im Mai 2020 selbst Opfer eines Cyber-Angriffs geworden. Ziel solcher Angriffe ist weniger das Abgreifen von Daten und Informationen aus dem Produktionsprozess, sondern vielmehr die Integrität und Verfügbarkeit von Produktionsprozessen. Die funktionale Sicherheit von Maschinen und Anlagen ist in besonderer Weise verwundbar, weil Sicherheitssysteme bereits bei geringfügigen Beeinträchtigungen die Maschine in einen sicheren Zustand überführen müssen, d. h., die Maschine muss stillgesetzt werden. Deshalb sind die wirtschaftlichen Auswirkungen derartiger Cyberangriffe so gravierend.

Der Cyber Resilience Act (CRA), der voraussichtlich im Herbst 2024 vom Europäischen Rat verabschiedet wird, verfolgt das Ziel, die Widerstandskraft der EU gegen Cyber-Attacken auf digitale Prozesse, Systeme und Produkte (Hard- und Software) zu erhöhen. Die neue Verordnung tritt wahrscheinlich im Herbst 2027 in Kraft und ist dann direkt in allen EU-Mitgliedsstaaten gültig. Sie gilt für alle auf dem Markt bereitgestellten Produkte mit digitalen Elementen, die in der Lage sind, mit anderen Produkten zu kommunizieren. Damit ist die Industrie angesichts vernetzter Fertigung im Industrial Internet of Things (IIOT) besonders betroffen: Geräte, Maschinen und Komponenten in der Produktion sammeln und erzeugen Daten mit Sensoren und Aktoren und tauschen sie aus.

Pflichten der Hersteller

Der CRA verpflichtet die Hersteller, Produkte in Übereinstimmung mit den grundlegenden Anforderungen von Anhang I der Verordnung zu entwickeln und herzustellen.

Zu den grundlegenden Anforderungen zählen (Anhang 1 / Teil 1):

- Das Produkt darf nur ohne bekannte Schwachstellen in Verkehr gebracht werden
- Sichere Standardeinstellungen
- Die Bereitstellung von Sicherheitsupdates
- Der Schutz vor unbefugtem Zugriff
- Ein Design mit limitierter Angriffsfläche („Security by Design“)

Zudem wird die Erstellung einer technischen Dokumentation für Hardware und Software gefordert sowie die

Beachtung einer Sorgfaltspflicht bei der Integration von Komponenten, die von Dritten bezogen werden. Dies gilt natürlich auch für z. B. Softwaremodule, die in Komponenten oder Maschinen integriert werden.

Darüber hinaus sind die Hersteller zu einem kontinuierlichen Schwachstellenmanagement verpflichtet. Sie müssen Sicherheitslücken über den gesamten Produktlebenszyklus schließen, mindestens jedoch über fünf Jahre. Und sie müssen Updates mindestens über zehn Jahre zur Verfügung stellen.

Zum Schwachstellenmanagement zählt (Anhang 1 / Teil 2):

- Die Meldung, Behebung und Dokumentation von Schwachstellen
- Die Erstellung einer SBOM (Dokumentation Softwareversionsverlauf)
- Die regelmäßige Überprüfung der Cyber Security
- Meldepflichten gegenüber den EU-Agenturen ENISA und CSIRT

Meldepflichten bei Sicherheitslücken

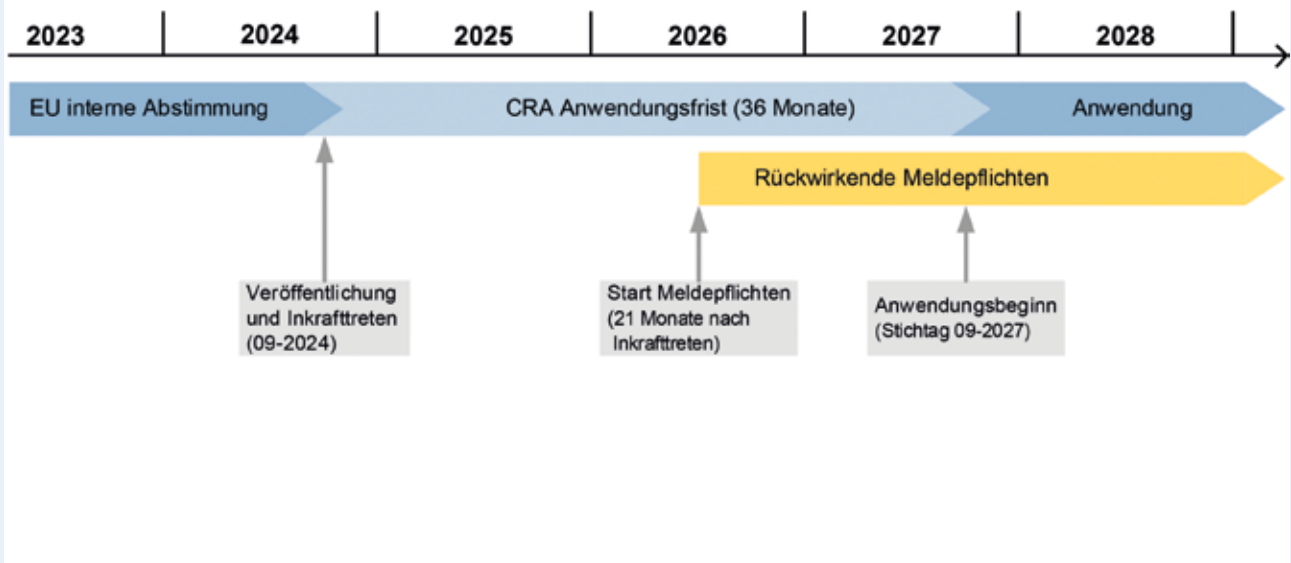
Damit die Nutzer so schnell wie möglich zum Beispiel mit einem Software-Update eine Sicherheitslücke schließen können, müssen die Nutzer, aber auch die Agentur der Europäischen Union für Cybersicherheit (ENISA) informiert werden, wenn eine aktiv ausnutzbare Schwachstelle bekannt wird.

Zu den Meldepflichten des Herstellers zählen (Artikel 14):

- Meldung nach Kenntnis von jeder aktiv ausgenutzten Sicherheitslücke oder Vorfall an ENISA und CSIRT
- Meldung mit Informationen und gegebenenfalls Abhilfemaßnahmen innerhalb von 72 Stunden
- Abschlussbericht über ausgenutzte Sicherheitslücken und Vorfälle
- Beschreibung, Schweregrad und Auswirkungen der Attacke
- Mögliche Ursachen, etwaige Akteure, Sicherheitsupdates
- Bereitstellung von Abhilfemaßnahmen für betroffene Nutzer

Die Meldepflicht tritt bereits 21 Monate nach der Veröffentlichung der CRA-Verordnung in Kraft. →

Cyber Resilience Act (CRA): Roadmap



Security Level definieren Widerstandsfähigkeit gegenüber unterschiedlichem Bedrohungspotenzial

Die normativen Anforderungen für Cyber Security legt die IEC 62443 fest. Sie definiert Schutzziele und Security Level sowie Verfahren, wie die Anforderungen an die Cyber-Security für industrielle Automatisierungssysteme realisiert werden können. Technische Anforderungen an Systeme (IEC 62443-3-3) und Produkte (IEC 62443-4-2) werden in der Norm durch sogenannte Security Level (SL) bewertet. Die verschiedenen Level geben dabei die Widerstandsfähigkeit gegenüber potenziellen Angreifern mit unterschiedlichem Wissen und Ressourcen an.

Die IEC 62443 definiert vier Security Level:

Security-Level 1 (SL1)

die nicht autorisierte Offenlegung von Informationen durch Abhören oder zufälliges Aufdecken verhindern

Security-Level 2 (SL2)

die nicht autorisierte Offenlegung von Informationen an eine mit einfachen Mitteln bei geringem Aufwand, allgemeinen Fertigkeiten und geringer Motivation aktiv danach suchende Person oder Stelle verhindern

Security-Level 3 (SL3)

die nicht autorisierte Offenlegung von Informationen an eine danach aktiv, mit raffinierten Mitteln und moderatem Aufwand, IACS-spezifischen Fertigkeiten und mittlerer Motivation suchende Person oder Stelle verhindern

Security-Level 4 (SL4)

die nicht autorisierte Offenlegung von Informationen an eine mit raffinierten Mitteln und erheblichem Aufwand, IACS-spezifischen Fertigkeiten und hoher Motivation aktiv danach suchende Person oder Stelle verhindern

Der Hersteller von Komponenten und Maschinen muss analysieren, welches Security Level oder Security-Eigenschaften eine Komponente oder Maschine benötigt, um den identifizierten potenziellen Angriffen standzuhalten.

Auf der Basis dieser Risikobewertung müssen geeignete Kontrollmechanismen, die Schutz vor unbefugtem Zugriff bieten, implementiert werden. Das können Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme sein, die die Integrität gespeicherter, übermittelter oder anderweitig verarbeiteter Daten, ob personenbezogener oder sonstiger Daten, Befehle, Programme und Konfigurationen vor einer Manipulation schützen müssen.

Damit ist die IEC 62443 eine gute Orientierungshilfe für Hersteller und Maschinenbetreiber, um Cyber-Security effektiv umzusetzen.

Dennoch wirft der Cyber Resilience Act noch viele unge löste Fragen und Probleme auf. So heißt es in einer Stellungnahme der Deutschen Industrie- und Handelskammer (DIHK): „Der CRA kann sein Potenzial nur entfalten, wenn er Vorgaben macht, die nicht nur dem beabsichtigten Zweck dienen, sondern zugleich auch →

EU Cyber Resilience Act (CRA), EU-Maschinenverordnung (MVO) und Normen (IEC)



angemessen und praktikabel sind. Unternehmen müssen ihre internen Maßnahmen auf CRA-Konformität überprüfen beziehungsweise Prozesse neu etablieren und einen Mechanismus zum Umgang mit Schwachstellen implementieren. Dafür müssen sie sich an europäischen Normen orientieren, die zum großen Teil erst erarbeitet werden müssen. Unternehmen berichten auch sehr häufig, dass sie die dafür erforderlichen Fachkräfte nicht rekrutieren können. Dies trifft gleichermaßen auf den Aufbau von Organisationsstrukturen und Beschäftigten für die Marktüberwachung zu. Insofern wäre eine zeitliche Streckung der Übergangsfrist angezeigt, auch um die sowieso bereits bestehenden Fachkräfteengpässe nicht weiter zu verschärfen.“ ■

Udo Weber

Produktmanager Sicherheitstechnik der Schmersal Gruppe und Mitglied im DIN-Gemeinschaftsausschuss – Sicherheitstechnische Grundsätze – Steuerungen

Lockout-Tagout-Tryout (LOTOTO)

Auf die richtige Umsetzung kommt es an!

Lockout-Tagout – zu Deutsch: Abschalten und Kennzeichnen – verhindert Arbeitsunfälle, indem Maschinen vorübergehend vollständig von ihren Energiequellen getrennt werden. Vor der Durchführung von Instandhaltungsarbeiten an Maschinen oder Anlagen werden diese energielos geschaltet und gegen Wiedereinschalten durch Unbefugte gesichert (Lockout), sodass von ihnen keine Gefahren mehr ausgehen können. Zusätzlich erfolgt eine auffällige Kennzeichnung der abgeschalteten Maschinen (Tagout).

In den vergangenen Jahren haben immer mehr Unternehmen Lockout-Tagout-Prozesse eingeführt oder entsprechende Hilfsmittel zur Verfügung gestellt. Der Begriff Lockout-Tagout taucht jedoch weder in der Maschinenrichtlinie 2006/42/EG noch in der neuen Maschinenverordnung (EG) 2023/1230 auf. Auch in der Betriebssicherheitsverordnung (BetrSichV) ist der Begriff Lockout-Tagout nicht enthalten.

Woher kommt dieser Trend?

Der Ursprung ist in den USA zu finden, denn dort wurde 1973 die erste Norm dazu entwickelt, die heute in der ANSI/ASSP Z244.1-2016 (R2020) „The Control of Hazardous Energy Lockout, Tagout and Alternative Methods“ zu finden ist. Produktsicherheit in Amerika und Produktsicherheit in Europa haben sich jedoch unterschiedlich entwickelt. So wird in Europa primär eine konstruktive und technische Lösung gefordert, während in Amerika auch organisatorische Schutzmaßnahmen einen hohen Stellenwert haben. Weltweit agierende Konzerne sind bestrebt, für ihre Unternehmen einheitliche Standards umzusetzen. So ist es verständlich, dass amerikanische Konzerne die ihnen bekannten Standards auf ihre Unternehmen in Europa übertragen (möchten). Dabei werden jedoch in vielen Fällen die europäischen Anforderungen nicht ausreichend berücksichtigt. Die Produktsicherheit ist in Europa streng geregelt und bietet ausreichenden Schutz. Vorausgesetzt, die erforderlichen Schutzmaßnahmen werden von Herstellern und Betreibern von Maschinen und Anlagen richtig umgesetzt.

Auszug aus der Maschinenrichtlinie 2006/42/EG (Anhang I, 1.6.3.):

Die Maschine muss mit Einrichtungen ausgestattet sein, mit denen sie von jeder einzelnen Energiequelle getrennt werden kann. Diese Einrichtungen sind klar zu kennzeichnen. Sie müssen abschließbar sein, falls eine Wiedereinschaltung eine Gefahr für Personen verursachen kann. Die Trenneinrichtung muss auch abschließbar sein, wenn das Bedienungspersonal die permanente Unterbrechung der Energiezufuhr nicht von jeder Zugangsstelle aus überwachen kann. Darüber hinaus ergänzen harmonisierte Normen diese grundlegenden Sicherheits- und Gesundheitsanforderungen

aus Richtlinien und Verordnungen. Restgefahren und deren Schutzmaßnahmen sind in der Betriebsanleitung zu beschreiben. Damit ist die Maschine oder Anlage aus rechtlicher Sicht vollständig sicher. Nicht selten zeigen sich in Europa Lücken in der Umsetzung der geforderten Schutzmaßnahmen, die auf ganz unterschiedliche Ursachen zurückzuführen sind. Die wohl häufigste Ursache ist die Unkenntnis der rechtlichen Anforderungen und des Standes der Technik.

Wie sieht die Praxis aus?

Wo Lücken im konstruktiven und technischen Bereich zu erwarten sind, macht es Sinn, diese mit organisatorischen oder personenbezogenen Schutzmaßnahmen zu schließen. Hier ist Lockout-Tagout eine sinnvolle und sichere Ergänzung. Vorausgesetzt, die Lockout-Tagout-Prozesse werden ebenfalls richtig umgesetzt! Die Darstellung zeigt: Wer alle Verfahren der Produktsicherheit oder des Arbeitsschutzes, ob europäisch oder amerikanisch, auf Kenntnis (Fachkunde) der jeweiligen Schutzmaßnahmen beruhen, wird das Ziel (Sicherheit) erreichen können.

Was ist der richtige Weg?

Hersteller, die in Europa Maschinen und Anlagen auf den Markt bringen möchten, müssen europäisches Recht anwenden und dessen Anforderungen erfüllen. Gleiches gilt für die Betreiber in Europa. Ergänzend sind Lockout-Tagout-Prozesse hilfreich und schaffen zusätzlich Sicherheit. Voraussetzung ist aber, dass die Verfahren fachkundig umgesetzt und auf ihre Wirksamkeit überprüft werden. In Lockout-Tagout-Prozessen wird hier von „Tryout“ (prüfen, ob das Absperren/Verriegeln erfolgreich war) gesprochen. Daher teils die Abkürzung LOTOTO. So werden z. B. bei der Festlegung von Lockout-Tagout-Prozessen durch fachkundige Personen die bereits vorhandenen Schutzmaßnahmen hinterfragt (Vier-Augen-Prinzip) und ggf. durch Lockout-Tagout-Maßnahmen ergänzt. In unserem Seminar „Lockout-Tagout“ zeigen wir Ihnen, wie Sie in Europa die rechtlichen Anforderungen mit Lockout-Tagout-Prozessen ergänzen können. ■

Jürgen Heimann

Dozent Produktsicherheit und Arbeitsschutz
tec.nicum Solutions & Services GmbH

tec.nicum academy

Das Seminarprogramm 2024/25

Die tec.nicum academy bietet ein umfassendes Schulungs- und Seminarprogramm zu Themen der Maschinen- und Anlagensicherheit.

Besuchen Sie uns unter www.tecnicum.com und finden Sie aktuelle Detailinformationen und Buchungsoptionen zu allen Seminaren und Sonderveranstaltungen.

Gerne gestalten wir ein maßgeschneidertes, auf die individuellen fachlichen Interessen der Teilnehmerinnen und Teilnehmer zugeschnittenes Inhouse-Seminar zu Ihrem Wunschtermin.

Wir beraten Sie gerne persönlich.
Sprechen Sie uns an:

Melanie Peters-Schuster

Tel. +49 202 6474 864

Telefonisch erreichbar:

8.00–11.00 Uhr und 13.30–15.30 Uhr

info-de@tecnicum.com



Seminarthemen	Wuppertal	Wettenberg	Kirkel	Online	Inhouse
Recht					
Maschinenverordnung 2023/1230 (Kompaktseminar) ^{NEU}	29.01.2025	26.06.2025	12.03.2025	auf Anfrage	auf Anfrage
Maschinenverordnung 2023/1230 (Intensivseminar – 2-Tages-Seminar) ^{NEU}	24.06.2025 bis 25.06.2025	29.10.2025 bis 30.10.2025	17.02.2025 bis 08.02.2025	auf Anfrage	auf Anfrage
Maschinenrichtlinie 2006/42/EG – CE-Konformitätsbewertungsverfahren	07.11.2024	–	–	auf Anfrage	auf Anfrage
Grundlagen des Arbeitsschutzes für Führungskräfte	28.03.2025	auf Anfrage	29.04.2024	auf Anfrage	auf Anfrage
Rechtliche Aspekte der Maschinensicherheit für Führungskräfte (1/2-Tages-Seminar)	24.10.2024	–	–	auf Anfrage	auf Anfrage

tec.nicum

(Fortsetzung auf Seite 22)

Seminarprogramm 2024/25 (Fortsetzung von Seite 21)

Seminarthemen	Wuppertal	Wettenberg	Lübeck	Kirkel	Online	Inhouse
Normen – Verordnungen						
Risikobeurteilung und Betriebsanleitung	–	–	02.12.2024	–	auf Anfrage	auf Anfrage
Risikobeurteilung gemäß EN ISO 12100	30.01.2025	02.07.2025	–	05.03.2025	auf Anfrage	auf Anfrage
Gefährdungsbeurteilung für Maschinen und Anlagen gemäß Betriebs-sicherheitsverordnung	28.01.2025	01.07.2025	–	28.04.2025	auf Anfrage	auf Anfrage
Technische Dokumenta-tion / Betriebsanleitung	03.04.2025	03.07.2025	–	06.03.2025	auf Anfrage	auf Anfrage
Anwendung der EN ISO 13849-1 und Einstieg in SOFTEMA	auf Anfrage	–	–	auf Anfrage	auf Anfrage	auf Anfrage
Anwendung der EN ISO 13849-1 und Einstieg in SISTEMA und die Validierung	auf Anfrage	–	–	auf Anfrage	auf Anfrage	auf Anfrage
Elektrische Aus-rüstung von Maschinen gemäß EN 60204-1 (VDE 0113-1) (2 Tage)	01.04.2025 bis 02.04.2025	–	–	–	auf Anfrage	auf Anfrage
Neubau, Umbau, Retrofitting – vom Hersteller zum Betreiber? (Halbtags-Seminar)	–	–	–	–	29.11.2024	–
Validierung gemäß EN ISO 13849-2 (Halbtags-Seminar)	–	–	03.12.2024	–	–	–

Seminarthemen	Wuppertal	Wettenberg	Kirkel	Online	Inhouse
Qualifizierungskurse mit besonderem Abschluss					
Qualifizierung zum TÜV zertifizierten „Machinery CE Certified Expert® – mce.expert“	11.02.2025 bis 14.02.2025	02.12.2024 bis 05.12.2024 13.05.2025 bis 16.05.2025	01.09.2025 bis 04.09.2025	–	auf Anfrage
Grundlehrgang Sicherheitsbeauftragte(r) (2 Tage)	13.02.2025 bis 14.02.2025	–	05.02.2025 bis 06.02.2025	–	auf Anfrage
Elektrotechnisch unterwiesene Person (EUP)	–	04.12.2024	–	–	–

Seminarprogramm 2024/25 (Fortsetzung von Seite 22)

Seminarthemen	Wuppertal	Wettenberg	Kirkel	Online	Inhouse
Anwendung					
Praxisworkshop – Arbeiten mit SISTEMA (Halbtags-Seminar) Hinweis: In Kombination am Folgetag mit dem SISTEMA Einstiegsseminar möglich	auf Anfrage	auf Anfrage	auf Anfrage	–	auf Anfrage
Grundlagen der Sicherheitstechnik – trennende und nicht trennende Schutzeinrichtungen	auf Anfrage	–	auf Anfrage	22.11.2024	auf Anfrage
Sicherheitsgerichtete Auslegung von Batteriefertigungsanlagen	17.03.2025	15.09.2025	auf Anfrage	auf Anfrage	auf Anfrage
Fahrerlose Transportsysteme und ihre Integration in die Produktionsumgebung	18.03.2025	16.09.2025	auf Anfrage	auf Anfrage	auf Anfrage
Sicherheit in integrierten Roboterfertigungsanlagen	19.03.2025	17.09.2025	auf Anfrage	auf Anfrage	auf Anfrage
Mensch-Roboter-Kollaborationen	20.03.2025	18.09.2025	auf Anfrage	auf Anfrage	auf Anfrage
Elektrotechnisch unterwiesene Person (EUP) NEU	04.04.2025	–	27.11.2025	auf Anfrage	auf Anfrage
Lockout / Tagout (LOTO)	09.07.2025	–	18.11.2025	auf Anfrage	auf Anfrage
Befähigung Kranführer (flurgesteuerte Krane)	28.10.2025	–	–	–	auf Anfrage
Sicherer Umbau von Maschinen und Anlagen	08.07.2025	11.11.2025	25.11.2025	auf Anfrage	auf Anfrage

Seminarthemen	Wuppertal	Mühdorf	Wettenberg	Kirkel	Online	Inhouse
Produkte						
Basis-Workshop Sicherheitssteuerung PSC1	auf Anfrage	–	auf Anfrage	auf Anfrage	–	auf Anfrage
Experten-Workshop Sicherheitssteuerung PSC1	auf Anfrage	–	auf Anfrage	auf Anfrage	–	auf Anfrage
Grundlagen und Inspektion von opto-elektronischen Schutzeinrichtungen gemäß BetrSichV (Seminarziel: Befähigte Person)	Mai 2025	September 2025	–	–	–	auf Anfrage

Fotos: K.A. Schmersal GmbH & Co. KG (shutterstock.com)

Diese Broschüre ist auf FSC®-zertifiziertem Papier gedruckt. Das Label auf diesem Produkt sichert einen verantwortungsvollen Umgang mit den Wäldern der Erde zu.

Die bei der Produktion dieser Broschüre entstandenen Treibhausgasemissionen wurden durch Investitionen in das Projekt „LAYA Energieeffiziente Brennholzöfen“ in Indien ausgeglichen.



Herausgeber:

tec.nicum

K.A. Schmersal GmbH & Co. KG

Möddinghofe 30
42279 Wuppertal

Phone: +49 202 6474-932
europe@tecnicum.com
www.tecnicum.com