mrl.news

Das Neueste zur Maschinenverordnung

Ausgabe 2026.01

tec.nicum

Sicherheit im Wandel – Chancen gestalten, Zukunft sichern

Liebe Leserinnen und Leser,

die industrielle Automatisierung befindet sich in einer Phase tiefgreifender Veränderungen. Neue regulatorische Anforderungen, innovative Kommunikationstechnologien und die zunehmende Digitalisierung verändern nicht nur Maschinen und Anlagen, sondern auch die Anforderungen an Hersteller, Integratoren und Betreiber.

Mit der ab Januar 2027 rechtsverbindlichen neuen Maschinenverordnung sowie dem Cyber Resilience Act rücken Themen wie funktionale Sicherheit und Cybersecurity noch enger zusammen. Unternehmen stehen vor der Aufgabe, ihre Produkte und Prozesse frühzeitig auf die kommenden Anforderungen auszurichten. Gleichzeitig entstehen dadurch Chancen, Sicherheit ganzheitlich neu zu denken und Wettbewerbsvorteile zu schaffen.

Wie moderne Maschinenkonzepte künftig sicher und flexibel gestaltet werden können, beleuchten wir in unserem Beitrag „Sichere Automation in der Praxis“. Technologien wie die Sichere Feldbox, IO-Link Safety und Single Pair Ethernet schaffen die Grundlage für eine leistungsfähige, durchgängige und zukunftsfähige Automatisierung.

Dass innovative Sicherheitskonzepte bereits heute erfolgreich in der Praxis eingesetzt werden, zeigt unser Praxisbericht zu den TREIF-Maschinen von JBT Marel. Am Beispiel moderner Schneidanlagen wird deutlich, wie intelligente Sicherheitslösungen Produktivität und Bedienerfreundlichkeit miteinander verbinden können.

Ein weiterer Schwerpunkt dieser Ausgabe ist die Digitalisierung von Sicherheitsprozessen. Mit Digital LOTO gewinnt die digitale Verwaltung von Lockout-Tagout-Prozessen zunehmend an Bedeutung. Gerade vor dem Hintergrund steigender Anforderungen an Dokumentation, Transparenz und Effizienz bietet die Digitalisierung erhebliche Potenziale für mehr Sicherheit im täglichen Betrieb.

Auch die rasante Entwicklung im Bereich der Robotik wirft neue Fragen auf. Humanoide Roboter und KI-gestützte Systeme wecken hohe Erwartungen hinsichtlich Flexibilität und Leistungsfähigkeit. Gleichzeitig müssen Sicherheitskonzepte Schritt halten, um das notwendige Vertrauen in den sicheren Einsatz dieser Technologien zu schaffen. Die Verbindung von funktionaler Sicherheit und künstlicher Intelligenz wird daher künftig eine Schlüsselrolle spielen.

Darüber hinaus werfen wir einen Blick auf die Anforderungen für den nordamerikanischen Markt. Die UL-Zulassung bleibt für viele Unternehmen ein entscheidender Faktor bei der internationalen Markterschließung und stellt zugleich wichtige Weichen für die globale Wettbewerbsfähigkeit.

Nicht zuletzt freuen wir uns, Ihnen mitteilen zu können, dass unsere Academy-Seminare mit einem wiederum erweiterten Angebot zur Verfügung stehen. Wissenstransfer und Qualifizierung bleiben zentrale Bausteine, um den Herausforderungen einer zunehmend komplexen Technologiewelt erfolgreich zu begegnen.

Wir wünschen Ihnen eine spannende Lektüre, neue Impulse für Ihre tägliche Praxis und viele Anregungen für die sichere Gestaltung der industriellen Zukunft.

Ihr mrl.news Redaktionsteam

Was Maschinenhersteller und Betreiber jetzt wissen müssen

Die neue EU-Maschinenverordnung (EU) 2023/1230

QUICK-BOX

Am 20. Januar 2027 tritt mit der Verordnung (EU) 2023/1230 ein grundlegend neues Regelwerk für Maschinenhersteller, Importeure und Betreiber in Kraft. Sie löst die seit 2009 gültige Maschinenrichtlinie 2006/42/EG ab – und das ohne Wenn und Aber: Es gibt keinen fließenden Übergang, sondern einen harten Stichtag. Wer nicht vorbereitet ist, riskiert, Maschinen nicht mehr rechtskonform in Verkehr bringen zu können. Höchste Zeit für einen Überblick.

Autor: Tobias Keller

Head of Administration,
tec.nicum

1. Vom Entwurf zur Verordnung – der Werdegang

Die Maschinenrichtlinie 2006/42/EG war lange das Rückgrat der Maschinensicherheit in Europa. Doch die Welt hat sich verändert: Digitalisierung, Vernetzung, künstliche Intelligenz (KI) und Cybersicherheit waren 2006 kaum oder gar nicht im Blick. Zudem führten unterschiedliche nationale Umsetzungen der Richtlinie in den Mitgliedstaaten zu Auslegungsdifferenzen und Wettbewerbsverzerrungen.

Die Europäische Kommission reagierte mit einem neuen Anlauf: Statt die Richtlinie zu überarbeiten, wählte sie das Instrument der Verordnung. Damit gilt das neue Regelwerk ohne nationale Umsetzung unmittelbar und einheitlich in allen 27 EU-Mitgliedstaaten. Das Europäische Parlament nahm die Verordnung am 18. April 2023 mit großer Mehrheit an, der Europäische Rat stimmte am 22. Mai 2023 zu. Die Veröffentlichung im Amtsblatt der EU folgte am 29. Juni 2023, das formale Inkrafttreten am 19. Juli 2023.

Für Hersteller verbindlich wird die Verordnung ab dem 20. Januar 2027, genau 42 Monate nach Inkrafttreten. In Deutschland wird zudem das sogenannte Maschinenverordnung-Durchführungsgesetz (MaschinenDG) die bisherige nationale Umsetzungsregelung (9. ProdSV) ablösen.

2. Was sich grundlegend ändert

Verordnung statt Richtlinie: kein nationaler Spielraum mehr

Der fundamentalste Wechsel ist formaler Natur, aber mit erheblicher praktischer Wirkung. Eine EU-Verordnung gilt direkt, eine Richtlinie muss dagegen erst in nationales Recht umgesetzt werden. Bisher konnten Mitgliedstaaten die Maschinenrichtlinie unterschiedlich interpretieren und umsetzen. Damit ist jetzt Schluss. Die Maschinenverordnung (EU) 2023/1230 wird EU-weit einheitlich angewendet und ist somit ein echter Gewinn für die Rechtssicherheit und für den Binnenmarkt. →

Die neue EU-Maschinenverordnung schafft einen modernen Rechtsrahmen für das Inverkehrbringen von Maschinen in Europa.

Erstmals: Cybersicherheit und künstliche Intelligenz

Das technisch vielleicht bedeutsamste Novum: Die neue Verordnung adressiert erstmals explizit Cybersicherheitsrisiken für Sicherheitssteuerungen und sicherheitsrelevante Software. Hersteller müssen Maschinen und deren Software gegen unbefugten Zugriff und Manipulation schützen. Zusätzlich werden Anforderungen für KI-gestützte Sicherheitsfunktionen eingeführt, abgestimmt mit dem etwa zeitgleich eingeführten EU AI Act. Wer KI in sicherheitsrelevanten Maschinenfunktionen einsetzt, muss künftig beide Regelwerke im Blick haben. Auch autonome und ferngesteuerte Maschinen erhalten eigene Regelungen.

Risikobeurteilung schließt Software ein

Das Grundprinzip der Risikobeurteilung bleibt erhalten, doch der Umfang wächst. Neu ist die explizite Pflicht, auch Risiken aus der Maschinensoftware zu bewerten, einschließlich geplanter künftiger Software-Updates nach der Inverkehrbringung. Hersteller müssen bereits bei der Konzeption festlegen, welche Updates sie planen, und die damit verbundenen Risiken vorab analysieren. Das ist ein Paradigmenwechsel: Die Verantwortung für die Maschinensicherheit endet nicht mehr mit der Auslieferung der Maschine.

Klarheit bei „wesentlichen Änderungen“

Ein bisher häufiger Streitpunkt wird jetzt kodifiziert: Die Verordnung legt präzise fest, wann eine Modifikation an einer bestehenden Maschine als „wesentliche Änderung“ gilt und damit ein neues Konformitätsbewertungsverfahren erforderlich macht. Für Betreiber, die Umbauten oder Retrofits durchführen, hat das direkte Konsequenzen. Im Zweifelsfall übernehmen sie schneller die Herstellerverantwortung – inklusive CE-Kennzeichnung und technischer Dokumentation.

Erweiterte Drittstellenpflicht für Hochrisikomaschinen

Für sechs Produktkategorien mit besonders hohem Risikopotenzial (Anhang I der MVO) wird die Einschaltung einer benannten Stelle (sog. „Notified Body“) für die Konformitätsbewertung verpflichtend.
Darüber hinaus werden Pflichten für Importeure und Händler schärfer gefasst, und die behördliche Meldepflicht bei Sicherheitsmängeln wird erweitert. Auch der Begriff des Sicherheitsbauteils wurde ausgeweitet. Er umfasst nun ausdrücklich auch Software und digitale Komponenten, die Sicherheitsfunktionen erfüllen.

Digitale Betriebsanleitungen erlaubt

Praxisnah und ressourcenschonend. Die Maschinenverordnung erlaubt künftig, Betriebsanleitungen, Montageanleitungen und EU-Konformitätserklärungen vollständig digital bereitzustellen. Betreiber sollten diese digitalen Dokumente allerdings lokal sichern. Der Online-Zugang allein genügt nicht, denn ein Hersteller könnte später nicht mehr erreichbar sein.

3. Die wichtigsten Fristen auf einen Blick

Datum	Ereignis
29.06.2023	Veröffentlichung der MVO (EU) 2023/1230 im EU-Amtsblatt
19.07.2023	Formales Inkrafttreten der Verordnung (freiwillige Anwendung möglich)
20.01.2025	EU-Kommission beauftragt CEN/CENELEC mit der finalen Formulierung der Normen
Ende 2026	Geplante Veröffentlichung harmonisierter Normen (hENs) im EU-Amtsblatt; Durchführungsbeschluss mit vollständiger Normenliste
20.01.2027	**Stichtag:** Maschinenrichtlinie 2006/42/EG tritt außer Kraft. Nur noch MVO (EU) 2023/1230 gilt. Kein paralleler Betrieb möglich.

4. Stand der Normung – die Uhr tickt

Harmonisierte Normen sind das praktische Rüstzeug für Hersteller. Wer eine solche Norm anwendet, darf in der Regel davon ausgehen, dass die gesetzlichen Anforderungen erfüllt werden („Konformitätsvermutung“). Genau hier liegt jedoch aktuell eine der größten Herausforderungen der neuen Maschinenverordnung.

Alle bisher unter der Maschinenrichtlinie harmonisierten Normen (es sind mehrere Hundert) müssen auf die neuen Anforderungen der MVO überprüft und gegebenenfalls angepasst werden. Die EU-Kommission hat am 20. Januar 2025 den finalen Normungsauftrag an CEN und CENELEC erteilt. Der Zeitplan ist allerdings ambitioniert: CEN/CENELEC sollte bis spätestens Juli 2025 einen Entwurf des gemeinsamen Arbeitsprogramms vorlegen, die harmonisierten Normen sollten bis Anfang 2026 verabschiedet und bis Ende 2026 im EU-Amtsblatt veröffentlicht werden – kurz vor dem Stichtag 20. Januar 2027. →

Seit Februar 2025 arbeiten die technischen Komitees an den Normen. Nach Angaben von CEN/CENELEC wurden bis Mitte 2025 die Ergebnisse für rund zwei Drittel aller harmonisierten Normen an die EU-Kommission übermittelt. Ob alle Normen rechtzeitig veröffentlicht werden, ist derzeit offen. Die Verordnung sieht jedoch gemeinsame Spezifikationen (Common Specifications) als Ausweichmöglichkeit vor, falls zum Stichtag 20. Januar 2027 harmonisierte Normen fehlen.

Neu erscheinende Normen, die noch vor dem Stichtag 2027 veröffentlicht werden, müssen sowohl die Anforderungen der alten Maschinenrichtlinie als auch die der neuen Verordnung abdecken. Sie erhalten deshalb nach derzeitigem Stand künftig zwei normative Anhänge, den bisherigen Anhang ZA (für die MRL) und einen neuen Anhang ZB (für die MVO). Zusätzlich erarbeitet die EU-Kommission einen Anwendungsleitfaden zur MVO. Die erste Sitzung der Redaktionsgruppe fand im Januar 2025 statt, erste Entwürfe lagen Anfang 2026 vor. Ein Randaspekt mit praktischer Relevanz: Das EuGH-Urteil „Malamud“ (März 2024) verpflichtet dazu, harmonisierte Normen als Teil des Unionsrechts kostenlos zugänglich zu machen. Erste sogenannte „Readability Platforms“ wurden bereits eingerichtet.

5. Fazit: Jetzt handeln, nicht warten

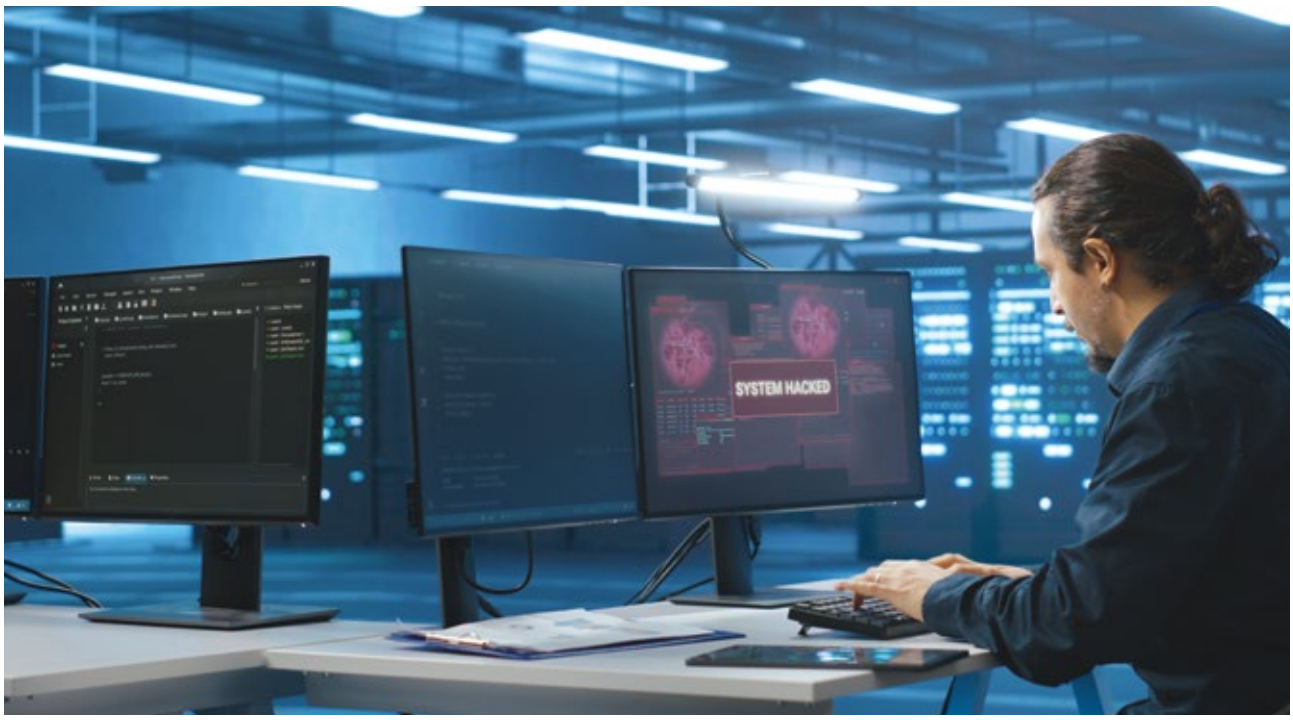
Der 20. Januar 2027 ist näher, als es scheint. Wer heute noch nach der Maschinenrichtlinie arbeitet, sollte parallel beginnen, seine Prozesse auf die neue Maschinenverordnung umzustellen. Risikobeurteilungen müssen Software und Cybersicherheit einschließen, technische Dokumentationen sind zu aktualisieren, und die Frage nach einer möglichen Drittstellenpflicht sollte frühzeitig geprüft werden.

Hersteller, die komplexe Projekte in der Pipeline haben, die erst nach dem Stichtag ausgeliefert werden, sollten die neue Verordnung schon jetzt zugrunde legen. Das spart später aufwendige Nacharbeiten. Eine freiwillige frühzeitige Umstellung auf die Anforderungen der Maschinenverordnung ist bereits möglich und zulässig – etwa durch die frühzeitige Umsetzung der neuen Cybersicherheitsanforderungen.

Die neue Maschinenverordnung ist kein bloßes Behördenpapier. Sie ist eine Antwort auf eine technisch veränderte Welt mit vernetzten, intelligenten und zunehmend autonomen Maschinen. Wer die Anforderungen frühzeitig versteht und umsetzt, schafft sich nicht nur Rechtssicherheit, sondern einen echten Wettbewerbsvorteil. ■

Hinweis zur Normung:
Die Listung harmonisierter Normen nach MVO im EU-Amtsblatt ist für Ende 2026 geplant. Bis dahin können weiterhin die harmonisierten Normen nach Maschinenrichtlinie 2006/42/EG angewendet werden, soweit sie inhaltlich die Anforderungen der MVO erfüllen. Betriebe sollten die Veröffentlichungen von CEN/CENELEC und der EU-Kommission engmaschig verfolgen.

Unternehmen, die frühzeitig handeln, schaffen Planungssicherheit, vermeiden unnötigen Anpassungsdruck und stellen ihre Produkte rechtzeitig auf die neuen Vorgaben ein.



Auswirkungen auf Maschinenbau und Automatisierungstechnik

Cyber Resilience Act (CRA) und OT-Security

Autor: Tobias Keller
Head of Administration, tec.nicum

1. Was ist der Cyber Resilience Act?

Als Cyber Resilience Act (CRA) wird die EU-Verordnung (EU) 2024/2847 bezeichnet, die am 10. Dezember 2024 in Kraft trat. Ziel ist es, Produkte mit digitalen Elementen („Products with Digital Elements“, PDE) über ihren gesamten Lebenszyklus hinweg cybersicher zu machen, von der Entwicklung über den Vertrieb bis zur Außerbetriebnahme.

Der CRA gilt für alle Hersteller, Importeure und Händler, die Hardware oder Software mit Netzwerkfähigkeit oder digitaler Konnektivität auf dem EU-Markt bereitstellen. Für den Maschinenbau bedeutet dies: Sobald eine Maschine, Steuerung, ein Sensor oder ein Antrieb vernetzt ist oder vernetzt werden kann, greift der CRA.

Zeitplan

Okt. 2024:	CRA im EU-Amtsblatt veröffentlicht
Dez. 2024:	Inkrafttreten
Sep. 2026:	Meldepflichten für aktiv ausgenutzte Schwachstellen
Dez. 2027:	Vollständige Anwendbarkeit aller CRA-Anforderungen

2. Relevanz für Maschinenbau und Automatisierungstechnik

Klassische Maschinenkomponenten wie SPS, SCADA-Systeme, Industrieroboter, HMI-Panels, vernetzte Antriebe und IIoT-Gateways fallen unter den CRA, sofern sie netzwerkfähig sind. Damit sind nahezu alle modernen Industrie-4.0-Produkte betroffen.

Kernpflichten für Maschinenbauer

- Secure by Design: Cybersicherheit muss ab der Entwicklungsphase eingebaut sein, nicht nachträglich ergänzt werden
- Schwachstellenmanagement: Sicherheitsupdates müssen über den gesamten Produktlebenszyklus (mind. 5 Jahre) bereitgestellt werden
- Konformitätsbewertung: Je nach Risikoklasse (Standard, Klasse I, Klasse II) unterschiedliche Nachweisverfahren, bis hin zu obligatorischer Drittprüfung
- SBOM (Software Bill of Materials): Vollständige Dokumentation aller Softwarekomponenten und Abhängigkeiten
- Meldeverpflichtung: Aktiv ausgenutzte Schwachstellen müssen innerhalb von 24 Stunden an ENISA gemeldet werden →

3. OT-Security vs. IT-Security: Ein entscheidender Unterschied

Der CRA adressiert erstmals explizit auch Operational Technology (OT), also industrielle Steuerungssysteme und Feldgeräte. Hier gibt es fundamentale Unterschiede zur klassischen IT-Sicherheit:

Kriterium	IT-Security	OT-Security
Schutzziel	Vertraulichkeit, Integrität, Verfügbarkeit (CIA)	Verfügbarkeit, Integrität, Vertraulichkeit (AIC) – Priorität umgekehrt!
Downtime	Kurzfristige Updates möglich	Stillstand = Produktionsausfall; Updates nur in Wartungsfenstern
Lebenszyklen	3–5 Jahre	15–30 Jahre (Maschinen oft älter als Betriebssysteme)
Konnektivität	Vollständig vernetzt	Oft air-gapped oder indirekt vernetzt
Protokolle	TCP/IP-Standard	Profibus, PROFINET, Modbus, OPC-UA, EtherCAT
Patches	Sofortige Verteilung möglich	Validierung, Tests, Herstellerfreigabe erforderlich

4. Das regulatorische Dreieck: CRA – NIS-2 – Maschinenverordnung

Drei EU-Regelwerke greifen im Maschinenbau ineinander und schaffen zusammen ein umfassendes Cybersicherheits-Regime:

Cyber Resilience Act (EU) 2024/2847	**NIS-2-Richtlinie** (EU) 2022/2555 / NIS2UmsuCG	**Maschinenverordnung** (EU) 2023/1230
Fokus: Produkt ■ Pflichten für Hersteller vernetzter Produkte ■ CE-Kennzeichnung für PDE ■ Gilt ab Dezember 2027	**Fokus: Betreiber** ■ Pflichten für Unternehmen kritischer Sektoren (inkl. Fertigung) ■ ISMS, Meldepflichten, Risikomanagement ■ In DE: NIS2UmsuCG / neues BSIG seit Dezember 2025	**Fokus: Maschine** ■ Ersetzt alte Maschinenrichtlinie (2006/42/EG) ■ Cybersicherheit als neues ESHA-Kriterium ■ Gilt ab Juli 2027

Zusammenhang: CRA und Maschinenverordnung wirken auf Produktebene (Hersteller), NIS-2 auf Organisationsebene (Betreiber). Wer Maschinen herstellt und betreibt, unterliegt ggf. allen drei Regelwerken gleichzeitig. CRA-konforme Produkte erleichtern die NIS-2-Compliance beim Betreiber. →

5. Was dies für den deutschen Maschinenbau bedeutet

Deutschland ist mit rund 6.500 Maschinenbauunternehmen und einem Exportanteil von über 70 % besonders stark betroffen. Der VDMA schätzt, dass der Großteil der Branche unter den CRA fällt. Handlungsbedarf besteht auf mehreren Ebenen:

Sofortmaßnahmen bis 2026

- Gap-Analyse: Welche Produkte sind als PDE einzustufen? Welche Risikoklasse gilt?
- Prozesse für Schwachstellenmeldung innerhalb von 24 Stunden etablieren (gilt ab Sept. 2026)
- SBOM-Prozesse aufbauen – Überblick über alle verwendeten Open-Source- und Third-Party-Komponenten schaffen

Kurzfristig bis 2027

- Secure-Development-Lifecycle (SDL) in den Engineering-Prozess integrieren
- OT-spezifische Sicherheitsarchitekturen entwickeln: Netzwerksegmentierung, Defense-in-Depth, IEC 62443 als Referenzrahmen nutzen
- Abstimmung CRA & Maschinenverordnung: CE-Konformitätsbewertung für Cybersicherheit integrieren
- Lieferkette prüfen: Zulieferer müssen ihrerseits CRA-konform sein (Haftung entlang der Supply Chain)

Fazit

Der Cyber Resilience Act markiert einen Paradigmenwechsel: Cybersicherheit wird zur Produkteigenschaft – vergleichbar mit der CE-Kennzeichnung für mechanische Sicherheit. Für den deutschen Maschinenbau bedeutet das erheblichen Aufwand, aber auch eine Chance: Wer frühzeitig investiert, sichert Marktzugang und Wettbewerbsvorteile.

Entscheidend ist die Kombination aus CRA (Produktsicherheit), NIS-2 (Betreiberpflichten) und Maschinenverordnung (Maschinensicherheit). OT-Security ist dabei kein IT-Thema – sie erfordert eigene Methoden, Normen (IEC 62443, ISA/IEC 62443) und Expertise, die im Maschinenbau aufgebaut werden müssen. ■

Sichere Automation in der Praxis:

Sichere Feldbox (SFB), IO-Link/IO-Link Safety und Single Pair Ethernet bei Schmersal

QUICK-BOX

Sichere Automation 4.0:
SFB, IO-Link/IO-Link Safety und zukünftig Single Pair Ethernet bilden bei Schmersal eine integrierte Plattform für modularen Maschinenbau. Sie reduzieren Verdrahtungsaufwand, verbessern Diagnosemöglichkeiten und ermöglichen sichere, IP-basierte Kommunikation ab dem Sensor. Damit entstehen flexible und zukunftssichere Maschinenkonzepte.

Autor: Volker Heinzer

Strategic Product Manager – Industrial Communication Systems and Industry 4.0

„Mit der SFB, IO-Link Safety und Single Pair Ethernet bringen wir die Sicherheitstechnik konsequent in die digitale Zukunft. Diese Technologien schaffen Freiräume für neue Maschinenkonzepte und erleichtern Konstruktion, Inbetriebnahme und Betrieb gleichermaßen."

Der Maschinenbau befindet sich in einer Phase tiefgreifender technologischer Veränderungen. Steigende Flexibilitätsanforderungen, modulare Maschinenkonzepte und die zunehmende Digitalisierung von Fertigungsprozessen verlangen nach neuen Kommunikationslösungen – insbesondere im Bereich der funktionalen Sicherheit. Als Hersteller sicherheitsgerichteter Komponenten und Systeme entwickelt Schmersal Technologien, die sowohl die Konstruktion vereinfachen als auch neue Konzepte der sicheren Automation ermöglichen. **Drei Schlüsseltechnologien stehen dabei im Fokus: die Sichere Feldbox (SFB), IO-Link/IO-Link Safety und zukünftig auch Single Pair Ethernet (SPE).**

Die Sichere Feldbox (SFB) – dezentrale Sicherheit für modulare Maschinen

Modulare Maschinen und flexible Fertigungslinien verlangen nach einer Architektur, die sich einfach anpassen und schnell erweitern lässt. Hier bietet die sichere Feldbox (SFB) von Schmersal einen entscheidenden Vorteil. Als dezentrale sicherheitstechnische Peripherie ermöglicht sie, Sicherheitsfunktionen direkt am Maschinenmodul umzusetzen – ohne zentrale Schaltschränke, ohne aufwendige Parallelverdrahtung und ohne komplexe Verkabelungsstrukturen.

Die SFB kommuniziert über PROFINET / PROFIsafe, EtherNet/IP / CIP-Safety oder EtherCAT / FSoE, integriert sichere Ein- und Ausgänge, Bedienfelder mit sicherer Not-Halt-Funktionalität und ermöglicht über optionale Erweiterungsmodule (Portextender) die Einbindung standardisierter IO-Signale. **Für Konstrukteure bedeutet dies eine klare Vereinfachung:**

- Safety-Funktionalität wird modular, skalierbar und durchgängig digital
- Verdrahtungsaufwand sinkt, Fehlerquellen werden reduziert, und die Inbetriebnahme beschleunigt sich deutlich
- Maschinenmodule können vorkonfiguriert geliefert und im Feld flexibel kombiniert werden

Gerade in Anwendungen mit häufig wechselnden Maschinenkonfigurationen – beispielsweise Verpackungsmaschinen oder Montagezellen – ermöglicht die SFB eine Safety-Lösung mit echtem Plug-and-Play.

IO-Link und IO-Link Safety – Transparenz bis zum Sensor

Während IO-Link als etablierter Kommunikationsstandard auf der Feldebene schon lange seine Stärken ausspielt, geht Schmersal mit IO-Link Safety konsequent den nächsten Schritt. Damit wird die durchgängige, bidirektionale Kommunikation erstmals auch für sicherheitsgerichtete Geräte möglich.

Die Vorteile für Konstruktion und Betrieb sind erheblich:

Vereinfachte Geräteintegration
IO-Link reduziert die Variantenvielfal der Komponenten, ermöglicht die automatische Parametrierung bei →

Produktwechsel und Konfiguration beim Austausch im Servicefall. Geräte müssen nicht mehr manuell eingestellt werden – die Steuerung oder das Maschinenmodul übernimmt dies automatisch.

Transparenz und Diagnose

Bei IO-Link stehen neben dem Status „Tür geschlossen und Zuhaltung aktiviert“ nicht nur ein elektronisches Typenschild, sondern auch umfassende Status- und Diagnosedaten zur Verfügung, darunter Temperaturwerte, Stärke des RFID-Signals, Fehlerzustände sowie Zustandswarnungen. Ergänzend liefern Betriebsdaten wie Zyklen-, Fehler- oder Betriebsstundenzähler wertvolle Informationen für eine vorausschauende Instandhaltung. Sichere Konfiguration und Parametrierung erlauben zusammen mit individuellen Systemkommandos die Integration völlig neuer Funktionen.

Flexible Sicherheitskonzepte

Mit IO-Link Safety wird auch Sicherheitstechnik softwaredefiniert. Geräteparameter, Sicherheitslevel oder Konfigurationen können digital übertragen und zentral dokumentiert werden. Das erleichtert sowohl die Validierung nach ISO 13849 als auch die spätere Erweiterung von Maschinen. Schmersal bringt bereits in der zweiten Jahreshälfte erste Geräte und Komponenten in den Markt, die IO-Link bzw. IO-Link Safety unterstützen – ein wichtiger Schritt hin zu einer durchgängigen Kommunikation bis hinunter zur Sensor-/Aktorebene.

Single Pair Ethernet (SPE) – der Weg zur einheitlichen Infrastruktur

Die wachsende Menge an Daten aus Sensoren, Aktoren und Sicherheitskomponenten verlangt nach leistungsfähigen Kommunikationswegen. Single Pair Ethernet (SPE) gilt bereits heute als „Industrial Ethernet der nächsten Generation“ – und Schmersal öffnet die Sicherheitstechnik gezielt für diese Zukunftstechnologie.

SPE bietet deutliche Vorteile:

Ethernet bis in den Sensor

Mit nur einem verdrillten Adernpaar wird eine durchgängige IP-basierte Kommunikation realisierbar – vom Sensor bis zur Cloud. Das bedeutet: keine Feldbusinseln mehr, kein Medienbruch.

Große Reichweiten und hohe Bandbreiten

Bis zu 1.000 m Reichweite im Feld bei gleichzeitig hoher Datenrate machen SPE ideal für weitläufige Anlagen, intralogistische Systeme oder die Prozessindustrie.

Reduzierte Leitungs- und Steckervielfalt

SPE schafft die Basis für kompakte Steckverbinder und innovative Sensorkonzepte in der Sicherheitstechnik.

Zukunftsorientierte Safety-Konzepte

In Kombination mit sicheren Kommunikationsprotokollen entsteht eine einheitliche und leistungsfähige Plattform für die Übertragung sicherer und nicht sicherer Signale. Für Maschinenkonstrukteure bedeutet dies langfristige Planungssicherheit und die Möglichkeit, Anlagen bereits heute auf zukünftige Ethernet-Architekturen auszurichten.

Synergien im Zusammenspiel der Technologien

Der größte Nutzen entsteht durch das Zusammenspiel aller drei Technologien:

- Die Sichere Feldbox wird zum modularen Safety-Knoten
- IO-Link Safety erweitert sie um flexible sichere Gerätekommunikation
- Single Pair Ethernet schafft den IP-basierten Backbone für hochperformante, echtzeitfähige Datenströme

Damit entsteht eine Architektur, die perfekt zu modernen, skalierbaren Maschinenkonzepten passt, d. h. modular, flexibel, effizient, digital und durchgängig sicher ist. Konstrukteure profitieren durch reduzierte Komplexität, Techniker durch vereinfachte Inbetriebnahme und Entwickler durch neue Freiheiten bei der Gestaltung sicherheitstechnischer Funktionen.

Praktischer Nutzen in der Konstruktion

Weniger Varianten, weniger Aufwand

Durch IO-Link und modulare SFB-Knoten sinkt die Gerätevielfalt, Dokumentation und Verdrahtung vereinfachen sich.

Schnellere Inbetriebnahme

Digitale Parametrierung, automatische Erkennung und verbesserte Diagnose verkürzen Montage- und Servicezeiten erheblich.

Neue Maschinenkonzepte

SPE und dezentrale Safety-Konzepte eröffnen neue Ansätze für mobile, flexible und vernetzte Produktionseinheiten.

Zukunftssicherheit

Planer können Maschinen heute schon für kommende Ethernet-basierte Sicherheitsarchitekturen rüsten. Schmersal versteht Sicherheitstechnik nicht mehr nur als einzelne Komponente, sondern als durchgängiges System – von der Verbindungstechnik über die dezentrale Peripherie bis zur digitalen Integration. ■

Schneiden und würfeln – schnell, präzise und sicher

OEM-Sicherheitssteuerung in Industrie-Schneidemaschinen

QUICK-BOX

JBT Marel und die TREIF-Maschinen im Kurzporträt

Seit mehr als 75 Jahren ist der Name TREIF für Lebensmittel-Schneidemaschinen bekannt. Das Unternehmen in Oberlahr/Westerwald, das seit Anfang 2025 zu JBT Marel gehört, entwickelt und produziert u. a. Slicer (die dünne Scheiben schneiden) sowie Dicer (für das Schneiden von Würfeln) und Portionsschneider in einem breiten Leistungsspektrum. Im Fokus stehen Maschinen für die Lebensmittelindustrie. Aber weil es auch ein breites Programm an Schneidemaschinen für den Einzelhandel – insbesondere für Bäckereien – gibt, sind TREIF Maschinen auch dem Verbraucher bekannt.

JBT Marel entwickelt und fertigt ein sehr breites Spektrum an Maschinen und Anlagen/Systemen für die Lebensmittelverarbeitung (Fleisch, Geflügel, Fisch, Convenience ...). Das Werk in Oberlahr arbeitet mit hoher Fertigungstiefe – auch die Messerherstellung gehört dazu – und beschäftigt rund 370 Mitarbeiter. Dank der Innovationkraft und der hohen Marktdurchdringung gilt das Unternehmen als einer der Hidden Champions des Maschinen- und Anlagenbaus und ist über Vertriebsgesellschaften und Partner weltweit präsent.

Autor: Dirk Plastwich

Systems and Solution Sales Representatives
Functional Safety Engineer (TÜV Rheinland Certified)

Unter der weltweit bekannten Produktlinie TREIF produziert JBT Marel in Oberlahr/Westerwald industrielle Schneidanlagen und setzt dabei baureihenübergreifend eine kundenspezifische Sicherheits-Kompaktsteuerung ein – auch in der neuen Baureihe TREIF PUMA, die kurz vor der Markteinführung steht. Diese Lösung bietet klare Vorteile – nicht nur für Maschinenbauer, sondern auch für das Bedienpersonal.

Steaks, Fleischkäse, Koteletts: Der „TREIF PUMA“ von JBT Marel schneidet Lebensmittel mit hohem Tempo, hoher Präzision und sehr flexibel. Deshalb ist diese Baureihe weltweit vor allem in vielen fleischverarbeitenden Betrieben im Einsatz. Aktuell läuft im Werk Oberlahr/Westerwald die Vorbereitung für die Serienproduktion der neuen PUMA-Generation. **(Bild 1)**

Bild 1: Kurz vor der Markteinführung: Die neue Generation der PUMA-Baureihe wird Maßstäbe beim schnellen und präzisen Schneiden von Fleisch setzen.

Kompakt und kundenspezifisch: die Sicherheits-(Klein-)Steuerung

Auch bei der Höchstleistung von 260 Schnitten pro Minute und vielen (manuellen) Produktwechseln muss sich der Bediener keine Sorgen um die Sicherheit beim Schneidprozess machen. Denn für die Konstrukteure der Maschinen hat die Maschinensicherheit hohe Priorität. Das zeigt unter anderem das durchdachte Bedienkonzept, auf das noch eingegangen wird, sowie die Tatsache, dass der neue TREIF PUMA – wie bereits sein Vorgänger und die meisten anderen Baureihen, die JBT Marel unter der Produktlinie TREIF fertigt – mit einer kompakten Sicherheitssteuerung vom Typ PROTECT SELECT OEM ausgestattet ist. **(Bild 2)** Diese Steuerung wird von Schmersal nach den Wünschen und Anforderungen des Anwenders, d. h. in diesem Fall von JBT Marel, programmiert und validiert. Geliefert wird eine fertig programmierte und validierte Sicherheits-Steuerung mit verschiedenen auswählbaren Applikationsprogrammen. Die IO-Konfigurationen, Sicherheitsschaltgeräte-Kombinationen und Meldungen der unterschiedlichen Maschinentypen werden – gemäß dem Sicherheitskonzept der TREIF-Maschinen – über die verschiedenen Applikationsprogramme der PROTECT SELECT OEM ausgewählt. →

Bild 2: Die Steuerungseinheit der neuen PUMA-Brotschneider. Rechts im Bild: die Sicherheits-Kompaktsteuerung PROTECT SELECT OEM.

Erst sechs, jetzt sieben Applikationsprogramme auf einer Steuerung

Schon seit einigen Jahren setzen die Ingenieure für TREIF-Maschinen diese OEM-spezifische Sicherheitssteuerung ein. Mike Vogelsberg, Leiter Entwicklung Software & E-Technik: „Wir hatten vorher unterschiedliche Steuerungsmodelle für die einzelnen Baureihen. Seit wir auf die PROTECT SELECT umgestellt haben, hat sich die Lagerhaltung deutlich vereinfacht, und die Sicherheitsfunktionen sind perfekt abgestimmt auf das, was wir brauchen – baureihen-übergreifend. Wir müssen die Steuerung nach der Installation nur anmelden und die jeweiligen Applikationen bestimmen."

Ursprünglich gab es sechs solcher Applikationsprogramme, die Software-Spezialisten von Schmersal geschrieben haben. Zu den Funktionen dieser Programme gehören z. B. die sicherheitstechnische Koordination der Überwachung bzw. Betätigung von Schutzhaube, Vorschub (Greifer), Austragband und Messer sowie definierte Wartungspositionen. Auch die optionale nicht-elektrische Deckelöffnung per Federkraft – die eine schnellere Bestückung mit neuem Schneidgut ermöglicht – wird sicherheitstechnisch berücksichtigt.

Für die neue PUMA-Generation haben die Schmersal-Programmierer jetzt eine siebte Applikation in die Steuerung „hineinprogrammiert". Und bei Bedarf können bei neuen Anforderungen problemlos noch weitere Funktionen bzw. Programme hinzugefügt werden. Damit ist diese Art der Sicherheitssteuerung zukunftssicher und auch baureihenübergreifend nutzbar.

Die umfassende Konnektivität der PROTECT SELECT OEM (18 sichere digitale und zwei sichere analoge Eingänge, sechs sichere Ausgänge) schafft die Voraussetzung für vielfältige Einsatzszenarien. Eine unidirektionale Schnittstelle ermöglicht die Signalauswertung und steigert die Nutzbarkeit bei geringem Verdrahtungsaufwand.

Standardfunktion bei allen Maschinen: Safe Torque Off

Eine Applikation, die bei allen Maschinen mit der PROTECT SELECT OEM genutzt wird, betrifft die Not-Aus-Funktion „Safe Torque Off" (sicher abgeschaltetes Drehmoment). Die Applikationsprogramme lassen sich bei Bedarf bzw. bei der Installation einfach auswählen, eine einzige Variante der Sicherheits-Kompaktsteuerung PROTECT SELECT OEM ein breites Maschinenspektrum abdeckt. Mike Vogelsberg: „Wir nutzen die PROTECT SELECT OEM nicht nur für Portionsschneider wie den TREIF PUMA, sondern unter anderem auch für Dicer – das sind Maschinen, die z. B. Speck und Schinken in Würfel schneiden – und für die SB-Brotschneidemaschinen in Supermärkten, die mit Sicherheitszuhaltungen ausgestattet sind. Nur unsere komplexesten Maschinen mit besonders anspruchsvollen Sicherheitsfunktionen, die oft auch sichere Antriebsfunktionen wie Safe Limited Speed fordern, sind mit einer passenden Safety SPS ausgestattet.

Intensive Kooperation in der Programmierphase

Bei der Festlegung der gewünschten Applikationen und der Zuordnung von Ein- und Ausgängen haben die Safety-Experten von Schmersal intensiv mit der TREIF-Entwicklung zusammengearbeitet, mehrfach waren die Schmersal-Programmierer auch in Oberlahr vor Ort. Das Ergebnis: Die Programmlogik ist bestens an die Maschinenfunktionen angepasst, die Programmcodes von mehreren zuvor eingesetzten Steuerungen sind abgebildet und eine kleinere Hardware-Änderung wurde ebenfalls realisiert. Eine Baumusterprüfung der Software gehörte zum Service-Umfang, den Schmersal erledigte.

Hygienegerechte, präzise Schnitte: der neue PUMA

Die stärkere Standardisierung auf der Antriebs- und Maschinenebene war ein zentrales Ziel, das die Konstrukteure im Team um Mike Vogelsberg bei der Entwicklung der neuen PUMA-Generation verfolgten – ein Konzept, das sich bei der Maschinensicherheit bereits bewährt. „Die Antriebe sind drehzahlgeregelt. Der Bediener gibt die Dicke der Scheiben und die Taktrate pro Minute ein, und die Maschine regelt das selbsttätig ein." Die Steuerung koordiniert dabei die Antriebe, und die Betriebsweise der Sicherheits-Kompaktsteuerung wiederum wird mit den betriebsmäßigen Signalen koordiniert.

Bedienung: möglichst intuitiv – und mit dem neuen H-Programm

Bei der Bedienung des PUMA und anderer Maschinen setzen die Konstrukteure auf den Grundsatz „Weniger ist mehr." Mike Vogelsberg: „Die Maschinen stehen oft in kleineren Betrieben. Sie werden in der Regel nicht →

von Elektrofachkräften bedient, sondern von Mitarbeitern in fleischverarbeitenden Betrieben oder Bäckereifilialen.

Bild 3: Alles im Blick: Der Touchscreen des PUMA

Deshalb ist eine einfache, möglichst intuitive Bedienung das Ziel.“ Gewährleistet wird das durch einen Touchscreen **(Bild 3)** in Kombination mit wenigen physischen Bedienelementen. Dabei setzt TREIF auf das H-Programm der Bediengeräte von Schmersal. **(Bild 4 und 5)** Dieses Programm wurde erst vor Kurzem vorgestellt, und es entspricht auch sehr hohen Anforderungen an die Hygiene. Eben dies wird bei TREIF-Maschinen auch verlangt, wie Mike Vogelsberg erläutert: „Wir testen alles, was wir verbauen, sehr intensiv auf die Verträglichkeit gegenüber häufiger und intensiver Reinigung – und vieles testen wir auch buchstäblich kaputt. Mit den Schaltern aus dem vorherigen N-Programm von Schmersal waren wir aber immer zufrieden und werden deshalb jetzt sukzessive auf die Nachfolgebaureihe umstellen.“ Gerade bei Slicern, so Vogelsberg, werden sehr hohe Hygieneansprüche gestellt: „Diese Maschinen schneiden oft rohe Produkte, die auch so gegessen, d. h. nicht mehr gebraten werden. Die Hallen sind hier kälter, der Hygienegrad höher.“

Bild 4: Ergonomisch und hygienegerecht: Die Bedieneinheit der TREIF-Anlagen.

Bild 5: Die Bedieneinheit aus dem H-Programm von Schmersal – hier ein Hauptschalter – erfüllen höchste Anforderungen an die Hygiene.

Im Fokus: Die Manipulationssicherheit

Bei der Entwicklung sowohl der Schutzeinrichtungen als auch des HMI (Human-Machine Interface) der TREIF-Maschinen ist die Manipulationssicherheit ein wichtiger Aspekt – schließlich ist beim Umgehen der Schutzeinrichtungen die Verletzungsgefahr hoch. Deshalb sind z. B. die Magneten von Sicherheitssensoren verdeckt angebracht, und nach dem Einschalten der Maschinen ist ein Testzyklus vorgegeben: Die Schutzhaube muss einmal geöffnet und geschlossen werden, um die einwandfreie Funktion des sicherheitsgerichteten Abschaltens bei geöffneter Haube zu prüfen. Auch dieser Zyklus wird von der OEM-Sicherheits-Kompaktsteuerung überwacht.

Die Vorteile einer kundenspezifischen Sicherheitslösung

Zusammengefasst sind die Vorteile der kundenspezifischen Sicherheits-Kompaktsteuerung aus Sicht der für die Produktlinie TREIF Verantwortlichen offensichtlich: Die Standardisierung nach dem Prinzip „Eine Steuerung für alles“ spart Kosten, reduziert Komplexität und vereinfacht die Lagerhaltung, und die OEM-Variante enthält alle Funktionen, die für eine sichere Maschinenbedienung benötigt werden. Die für die verschiedenen Maschinentypen und Baureihen erforderliche Varianz wurde in die Steuerung integriert; das jeweils benötigte Applikationsprogramm wird bei der Installation über Auswahlbuttons und Touchdisplay aktiviert.

Auch mit den „soft facts“ sind die Verantwortlichen bei TREIF zufrieden: Die kontinuierliche Zusammenarbeit, so Mike Vogelsberg, funktioniert gut. Auch deshalb werden in neuen Maschinengenerationen künftig vermehrt hygienegerechte Schaltgeräte aus dem H-Programm von Schmersal eingesetzt, und die TREIF-spezifische OEM-Variante der Sicherheits-Kompaktsteuerung sowieso. ■

Bild 6: Mike Vogelsberg, Leiter Entwicklung Software & E-Technik, im Technikum für die TREIF-Produktlinie vor dem „LevelUp”-Slicer, der genau wie der PUMA kurz vor der Markteinführung steht.

Die Safety Fieldbox ergänzt seit 2023 das Portfolio von rund 13.000 UL-zertifizierten Schmersal-Produkten.

Normgerecht, zuverlässig und zukunftssicher.

UL-Zertifizierung von Sicherheitsschaltgeräten

QUICK-BOX

UL-Zertifizierung auf einen Blick

- Voraussetzung für viele Anwendungen in Nordamerika
- Zusätzliche Anforderungen über IEC-Normen hinaus
- Fokus auf Produktsicherheit, Materialien und Installation
- Bewertung von Produkt und Fertigung
- Regelmäßige Audits des Produktionsstandorts

Autor: Dipl.-Ing. (FH) Jörg Eisold

Head of Standards, Committees and Association Work

Sicherheitsschaltgeräte sind ein zentraler Bestandteil moderner Maschinen. Ob Positionsschalter, optoelektronische Sensoren oder RFID-basierte Sicherheitssysteme: Sie müssen zuverlässig funktionieren – und vor allem weltweit zugelassen sein.

Während in Europa die CE-Kennzeichnung auf Basis der Normenreihe IEC 60947-5-x etabliert ist, stellt der nordamerikanische Markt zusätzliche Anforderungen. Hier gilt: Ohne Zertifizierung durch eine anerkannte Prüfstelle wie UL (Underwriters Laboratories) ist ein Marktzugang in vielen Fällen praktisch nicht möglich.

Zwar hat UL seine Normen zunehmend an die IEC-Reihe angepasst, doch auch wenn sich die Normen annähern, bleibt die Sicherheitsphilosophie unterschiedlich.

Die Normen der IEC-Reihe 60947-5-x legen fest, wie ein Gerät funktionieren muss – inklusive elektrischer Kennwerte, mechanischer Eigenschaften und Umweltbedingungen. Diese technische Basis wird mit der Überführung in die UL-Normenwelt – etwa als UL 60947-5-1 oder UL 60947-5-2 übernommen, jedoch um nationale Anforderungen ergänzt. Produkte müssen darüber hinaus in Übereinstimmung mit dem National Electrical Code (NEC) installiert werden, was zusätzliche Randbedingungen schafft.

Zusätzliche nationale Anforderungen betreffen etwa das Brandverhalten des Geräts, die eingesetzten Materialien sowie die Sicherheit bei möglichen Fehlinstallationen. Das führt dazu, dass selbst technisch ausgereifte, mit IEC-Normen konforme Produkte nicht automatisch UL-konform sind. Bei klassischen Sicherheitsschaltern nach IEC 60947-5-1 stehen Eigenschaften wie Zwangsöffnung, mechanische Robustheit und Lebensdauer im Mittelpunkt.

Für die UL-Zertifizierung kommen weitere Aspekte hinzu wie die Bewertung von Luft- und Kriechstrecken, der Nachweis von Materialeigenschaften (z. B. Flammbarkeit) und die Prüfung unter UL-spezifischen Last- und Fehlerbedingungen.

Ein entscheidender Punkt hierbei ist, dass zugelassene Materialien (z. B. Kunststoffe mit „UL Yellow Card“) verwendet werden. Damit wird die Materialauswahl zu einem kritischen Faktor im Entwicklungsprozess. Bei berührungslosen Sensoren nach IEC 60947-5-2 verschiebt sich der Fokus noch stärker in Richtung Anwendung. Während die IEC-Norm die Funktion des Sensors beschreibt – etwa Schaltabstände oder EMV-Eigenschaften –, betrachtet UL das Gesamtsystem, also auch die Stromversorgung, die Anschlussleitung, die Absicherung im Schaltschrank sowie die Einsatzumgebung. Ein Sensor wird somit nicht nur isoliert bewertet, sondern zusätzlich gibt es UL-Prüfungen für die Gesamtheit einer Anlage.

Mit modernen Sicherheitssensoren, etwa RFID-basierten Systemen, erreicht die Thematik eine neue Komplexität. Die Norm IEC 60947-5-3 fordert eine definierte Reaktion auf Fehler (deterministisches Verhalten), die Überwachung interner Zustände sowie die Integration funktionaler Sicherheitsprinzipien. Für die UL-Zertifizierung entsteht hieraus eine besondere Herausforderung, da elektronische und softwarebasierte Funktionen bewertet werden müssen. Zusätzlich ist das sichere Verhalten unter Fehlerbedingungen nachzuweisen. Neben der funktionalen Sicherheit spielt hier die klassische Produktsicherheit also eine entscheidende Rolle. Die zusätzlichen Anforderungen müssen frühzeitig im Entwicklungsprozess berücksichtigt werden. Dazu zählt beispielsweise die Auswahl zugelassener Materialien und Komponenten.

Ein weiterer wichtiger Aspekt ist, dass UL nicht allein das Produkt, sondern auch die Fertigung bewertet. Im UL-File des zertifizierten Produkts ist auch der Produktionsstandort genannt. Hierzu finden am jeweiligen Produktionsstandort regelmäßige Audits statt.

Sind alle Anforderungen erfüllt, die notwendigen Prüfungen abgeschlossen und die formalen Nachweise erbracht, steht dem Marktzugang auf dem nordamerikanischen Markt nichts im Wege. ■

Sicherheit bei humanoiden Robotern

Neue Herausforderungen für Sicherheitskonzepte und funktionale Sicherheit

QUICK-BOX

Sicherheit bei humanoiden Robotern:
Wie viele nicht ortsfeste oder interagierende Roboter arbeiten humanoide Roboter direkt mit Menschen zusammen und nutzen zunehmend KI, um ihre Umgebung zu erkennen und eigenständig zu handeln. Dadurch entstehen neue Sicherheitsanforderungen, die klassische Maschinenkonzepte nur teilweise abdecken.

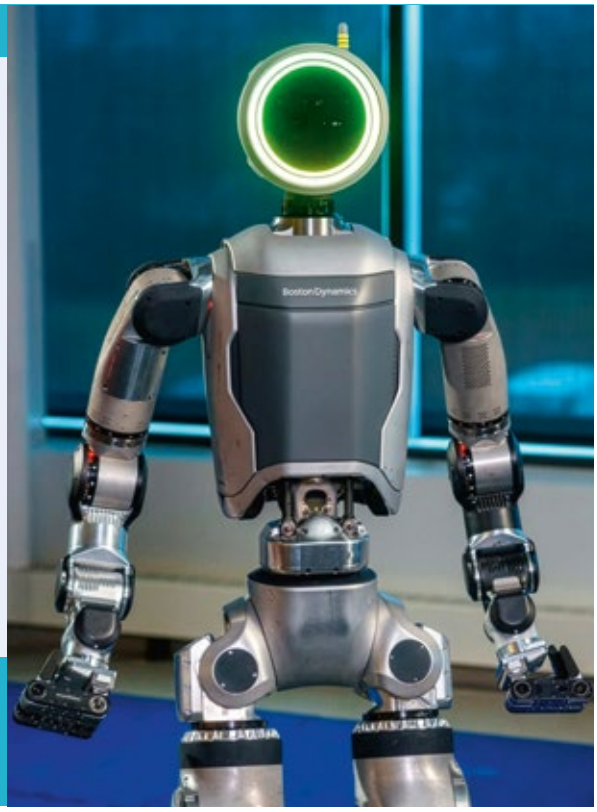
Wichtige Risiken sind:

- Sturzgefahr bei Energieverlust
- Kollisionen durch hohe Bewegungsdynamik
- Schwer vorhersagbares KI-Verhalten
- Cyberangriffe auf vernetzte Systeme

Deshalb gewinnen funktionale Sicherheit, Sensorfusion, sichere Bewegungsfunktionen und Cybersecurity stark an Bedeutung. Bestehende Normen werden derzeit erweitert, um KI-gestützte Robotersysteme besser abzudecken.

Autorin: Katrin Wirz

Product Manager
K.A. Schmersal GmbH & Co. KG



Was ist ein humanoider Roboter?

Humanoide Roboter stehen an der Schwelle vom Forschungslabor zur industriellen Anwendung. Sie versprechen eine neue Form der Automatisierung: flexibel, adaptiv und direkt in menschlichen Arbeitsumgebungen einsetzbar. Gleichzeitig entstehen jedoch sicherheitstechnische Fragestellungen, die mit klassischen Konzepten der Maschinenrichtlinie nur teilweise abgedeckt werden können.

Humanoide Roboter zeichnen sich durch ihre menschenähnliche Bauform und ihre Fähigkeit zur Interaktion mit der Umwelt aus. Sie besitzen in der Regel einen Oberkörper, zwei Arme, verschiedene Sensoren und eine Fortbewegung, die entweder über Beine oder alternative Systeme erfolgt.

Entscheidend ist aber nicht nur ihre äußere Form, sondern ihre funktionale Ausrichtung: Sie sind dafür konzipiert, menschliche Tätigkeiten zu übernehmen und sich in bestehende Arbeitsumgebungen zu integrieren. Diese Eigenschaft unterscheidet nicht ortsfeste Roboter grundlegend von klassischen Industrierobotern, die meist in abgegrenzten Zellen arbeiten und auf spezifische Aufgaben optimiert sind.

Die zunehmende Möglichkeit, künstliche Intelligenz (KI) zu integrieren, verstärkt diese Entwicklung erheblich. Moderne Systeme sind in der Lage, ihre Umgebung wahrzunehmen, Situationen zu interpretieren und darauf basierend Entscheidungen zu treffen. Damit verlassen sie den Bereich strikt deterministischer Systeme und bewegen sich hin zu Entscheidungsprozessen, die auf Wahrscheinlichkeitsberechnungen basieren. Diese neue Qualität eröffnet einerseits weitreichende Möglichkeiten, bringt andererseits aber auch neue Unsicherheiten mit sich, insbesondere im Hinblick auf die Vorhersagbarkeit von Verhalten.

Einsatzfelder und Marktakteure

Die zukünftigen Aufgaben intelligenter Roboter werden sich vor allem dort zeigen, wo Flexibilität und Anpassungsfähigkeit gefragt sind. In der industriellen Produktion können sie Tätigkeiten übernehmen, die bislang Menschen vorbehalten waren, ohne dass bestehende Anlagen grundlegend umgebaut werden müssen. Insbesondere in Zeiten des Fachkräftemangels wird hierin ein erheblicher Nutzen gesehen, da interagierende Roboter körperlich belastende, monotone oder gefährliche Arbeiten übernehmen können. Darüber hinaus eröffnen sich Einsatzmöglichkeiten in der Logistik, →

im Gesundheitswesen sowie im Dienstleistungssektor. Anwendungen reichen von der Unterstützung in der Pflege über Serviceaufgaben bis hin zu Einsätzen in gefährlichen Umgebungen, etwa bei Rettungseinsätzen.

Der Markt speziell für humanoide Robotik wird derzeit von einer Reihe internationaler Akteure geprägt. Unternehmen wie Boston Dynamics und das Toyota Research Institute treiben besonders die Entwicklung hochdynamischer Bewegungsabläufe und KI-basierter Verhaltensmodelle voran. Tesla verfolgt mit dem Optimus-Projekt eine industrielle Skalierungsstrategie, während Firmen wie SoftBank Robotics oder Hanson Robotics ihren Schwerpunkt auf soziale Interaktion legen. Parallel dazu entwickeln Anbieter wie Unitree Robotics oder UBTECH kompakte und vergleichsweise kostengünstige Systeme. Allen Ansätzen gemeinsam ist die Kombination aus fortschrittlicher Aktorik, leistungsfähiger Sensorik und zunehmend komplexer Softwarearchitektur.

Sicherheitsherausforderungen und neue Risikodimensionen

Die Kombination aus physischer Interaktion und intelligenter Steuerung bringt neue sicherheitstechnische Herausforderungen mit sich. Anders als bei klassischen Industrierobotern ist eine räumliche Trennung zwischen „Mensch und Maschine“ oft nicht praktikabel. Stattdessen arbeiten auch humanoide Roboter gezielt in direkter Interaktion mit Menschen, wodurch sich der Fokus von Abschottung hin zu sicherer Zusammenarbeit verlagert. Ein wesentliches Risiko liegt in der mechanischen Ausgestaltung dieser Systeme. Humanoide Roboter etwa sind meist dynamisch instabil und müssen ihre Balance kontinuierlich aktiv regeln. Ein abruptes Abschalten oder ein Energieentzug – wie etwa durch „Safe Torque Off (STO)“ – führt daher nicht in einen sicheren Zustand, sondern kann einen Sturz auslösen. In diesem Moment wird der Roboter zu einem unkontrollierten Objekt mit erheblicher kinetischer Energie, was insbesondere bei größeren Systemen ein hohes Verletzungsrisiko darstellt.

Zusätzlich bestehen erhebliche Kollisionsrisiken. Aufgrund von Dynamik und Masse können selbst kleinere Roboter Kräfte erzeugen, die über den normierten Schmerzgrenzen liegen. Diese Gefahr wird bei humanoiden Robotern durch die hohe Beweglichkeit des gesamten Körpers, einschließlich Beine, Torso und Arme, weiter verstärkt. Neben den physikalischen Risiken treten softwareseitige Herausforderungen auf. Gleichzeitig entstehen neue Anforderungen an die Situations- und Kontexterkennung: Ein Roboter muss nicht nur erkennen, dass sich ein Objekt bewegt, sondern auch verstehen, ob es sich beispielsweise um ein Werkzeug oder eine potenzielle Gefahr handelt.

Auch Aspekte der Cyber- und Datensicherheit gewinnen erheblich an Bedeutung. Roboter verarbeiten oft große Mengen sensibler Daten und sind zunehmend vernetzt, wodurch sie potenziell Ziel von Angriffen werden können. Sicherheitskonzepte müssen daher nicht nur die physische, sondern auch die digitale Integrität berücksichtigen.

Sicherheitskonzepte, Normen und industrielle Einordnung

Vor diesem Hintergrund entstehen neue Sicherheitsarchitekturen, die über klassische Konzepte hinausgehen. Moderne Ansätze kombinieren mehrere Ebenen der Absicherung. Auf der untersten Ebene stehen sichere Antriebs- und Bewegungsfunktionen, die beispielsweise Geschwindigkeiten und Kräfte begrenzen oder aktive Dämpfungsmechanismen bereitstellen. Ergänzt wird dies durch eine umfassende Umfeldüberwachung auf Basis von Sensorfusion, die den Arbeitsraum als dreidimensionales Sicherheitsfeld erfasst und dynamisch bewertet. Darüber hinaus gewinnen übergeordnete Überwachungssysteme an Bedeutung, die das Verhalten der KI selbst analysieren und in kritischen Situationen eingreifen können.

Normativ befindet sich dieser Technologiebereich noch in der Entwicklung. Bestehende Normen wie ISO 12100, ISO 10218 oder ISO 13482 liefern wichtige Grundlagen, sind jedoch nur eingeschränkt auf humanoide Systeme übertragbar. Insbesondere Aspekte wie dynamische Stabilität, KI-basierte Entscheidungsprozesse oder der sichere Zustand bei Energieverlust sind in den bestehenden Regelwerken nicht vollständig adressiert. Parallel dazu gewinnen übergeordnete Regelwerke wie die neue Maschinenverordnung (EU) 2023/1230 an Bedeutung, da sie erstmals explizit Anforderungen an softwarebasierte und KI-gestützte Systeme formulieren.

Funktionale Sicherheit und systematische Sicherheitsbewertung

Ein zentraler Aspekt, der über klassische Sicherheitsbetrachtungen hinausgeht, ist die konsequente Anwendung der funktionalen Sicherheit auf interagierende Robotersysteme. Während bestehende Normen wie ISO 12100 die Risikobeurteilung strukturieren, liefern insbesondere IEC 61508 sowie ISO 13849 die methodische Grundlage für die Entwicklung sicherheitsgerichteter Systeme.

Funktionale Sicherheit umfasst dabei die Analyse, Spezifikation und Validierung sicherheitsrelevanter Funktionen, einschließlich des Nachweises ihrer Zuverlässigkeit. Dies beinhaltet sowohl Hardware- als →

auch Softwarekomponenten und erstreckt sich über die gesamte Systemarchitektur. Bei allen Robotern gewinnt dieser Ansatz an Bedeutung, da sicherheitskritische Funktionen nicht nur klassische Steuerungselemente betreffen, sondern zunehmend durch komplexe Software und KI-Algorithmen realisiert werden.

Ein wesentlicher Bestandteil ist die systematische Bewertung von Ausfallrisiken. Hierbei werden sowohl zufällige Hardwarefehler als auch systematische Fehler – beispielsweise in Software oder KI-Modellen – betrachtet. Ziel ist der Nachweis, dass das Gesamtsystem definierte Sicherheitsniveaus (z. B. SIL oder Performance Level) erreicht und kritische Fehlfunktionen mit ausreichend geringer Wahrscheinlichkeit auftreten.

Darüber hinaus ist eine ganzheitliche Betrachtung des Lebenszyklus erforderlich. Sicherheitsbewertungen müssen nicht nur im Design erfolgen, sondern auch Betrieb, Wartung, Updates und lernendes Systemverhalten berücksichtigen. Gerade bei KI-basierten Systemen kann sich das Verhalten über die Zeit verändern, was kontinuierliche Bewertungs- und Validierungsprozesse erforderlich macht.

Eine besondere Rolle kommt den eingesetzten Halbleiterkomponenten zu. Prozessoren, Sensorchips und KI-Beschleuniger bilden das technische Fundament für Wahrnehmung, Entscheidungsfindung und Aktorik. Fehler in diesen Komponenten können direkt zu sicherheitskritischen Zuständen führen. Daher ist eine spezifische Bewertung dieser Bausteine notwendig, einschließlich ihrer Architektur, ihrer Ausfallmechanismen und ihrer Integration in das Gesamtsystem.

Ergänzend dazu gewinnen KI-spezifische Sicherheitsbewertungen zunehmend an Bedeutung. Normative Ansätze wie ISO/PAS 8800 adressieren die systematische Analyse von KI-Modellen, einschließlich ihrer Robustheit, Generalisierungsfähigkeit und potenzieller Fehlentscheidungen. Ziel ist es, auch nicht-deterministische Entscheidungsprozesse in ein belastbares Sicherheitskonzept zu integrieren.

Neben der Analyse steht die Validierung von risikomindernden Maßnahmen im Fokus. Dazu gehören unter anderem:

- Sensorik und Sensorfusion zur zuverlässigen Umfeldwahrnehmung
- Begrenzung von Geschwindigkeit, Kräften und Arbeitsräumen
- Sichere Bewegungsfunktionen und kontrollierte Stoppstrategien
- Visualisierung und Simulation von Gefahrenräumen

Diese Maßnahmen müssen nicht nur implementiert, sondern auch systematisch geprüft und nachgewiesen wirksam sein.

Schließlich ist die funktionale Sicherheit eng mit Cybersecurity-Aspekten verbunden. Vernetzte humanoide Systeme müssen gegen Manipulation und unbefugten Zugriff abgesichert werden, beispielsweise gemäß der Norm IEC 62443. Nur durch die Kombination aus funktionaler Sicherheit und IT-Sicherheit lässt sich ein durchgängiges Schutzkonzept realisieren.

Neue Märkte erschließen

Für Unternehmen der Sicherheitstechnik ergeben sich daraus sowohl Herausforderungen als auch Chancen. Die Schmersal Gruppe, als etablierter Anbieter von Sicherheitskomponenten und -systemen, verfügt über umfangreiche Kompetenzen in der funktionalen Sicherheit von Maschinen. Diese Kompetenzen lassen sich in vielen Bereichen auf humanoide Anwendungen übertragen, etwa bei der sicheren Signalverarbeitung, der Steuerung sicherheitsgerichteter Funktionen und der Absicherung von Arbeitsbereichen. Gleichzeitig wird es notwendig sein, bestehende Technologien weiterzuentwickeln, um neuen Anforderungen wie dreidimensionaler Umfeldüberwachung oder KI-basierter Sicherheitsbewertung gerecht zu werden.

Zusammenfassend lässt sich feststellen, dass nicht ortsfeste und eben auch humanoide Roboter ein erhebliches Innovationspotenzial bieten, gleichzeitig aber einen Paradigmenwechsel in der Maschinensicherheit erfordern. Klassische Konzepte wie das sichere Stillsetzen oder die physische Trennung von Mensch und Maschine stoßen an ihre Grenzen. Stattdessen rücken adaptive, mehrschichtige Sicherheitsansätze in den Vordergrund, die mechanische, sensorische und informationstechnische Aspekte integrieren. Der Erfolg dieser Technologie wird maßgeblich davon abhängen, inwieweit es gelingt, ein belastbares Sicherheitsniveau zu etablieren und gleichzeitig die wirtschaftlichen Potenziale zu realisieren. ■

Quellen:

- Fraunhofer IPA, Leitfaden Sicherheit Humanoider Roboter, September 2025
- White Paper, Out of the Cage: Advanced Functional Safety for Humanoids – Positron Safety AI Architecture, Synapticon GmbH, Dr.-Ing. Florian Weißhardt, Dr.-Ing. Tim Fröhlich, Dieter Volpert January 23, 2026
- Sicherheitsaspekte bei humanoiden Robotern, 2026, Industriezeitschrift.de
- SGS-Société Générale de Surveillance SA (2026), Flyer „Sicherheitsbewertung für humanoide Roboter“
- [1)] Normen:
  ISO 12100: Safety of machinery – General principles for design – Risk assessment and risk reduction
  ISO 10218: Robotics – Safety requirements, Part 1: Industrial robots, Part 2: Industrial robot applications and robot cells
  ISO 13482: Robots and robotic devices – Safety requirements for personal care robots
  IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems
  ISO 13849: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen
  ISO/PAS 8800:2024: Road vehicles – Safety and artificial intelligence
  IEC 62443: Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme

Humanoide Roboter eröffnen neue Möglichkeiten in der Industrie. Ihr Einsatz erfordert klare Sicherheitsstandards und Normen. Entscheidend ist die sichere Integration in bestehende Prozesse.

Digitales Lockout/Tagout

Sichere Instandhaltung ohne Papierberge

QUICK-BOX

Kernaussagen für Betreiber

- LOTO bleibt ein Kernprozess sicherer Instandhaltung – besonders bei Eingriffen in Energiequellen, Restenergien und Gefahrbereiche.
- tec.dloto ersetzt nicht die physische Verriegelung, sondern macht Vorbereitung, Freigabe, Nachweis und Rücknahme deutlich belastbarer.
- QR-Code-Start, geführte Schritte, Referenzbilder, Foto-Nachweise und Genehmigungen reduzieren die typischen Schwächen papierbasierter Abläufe.
- Zentrale Historien, Dashboards und auditfähige Protokolle geben Sicherheitsverantwortlichen mehr Transparenz im laufenden Betrieb.
- Als tec.nicum-Dienstleistung lässt sich die Lösung mit Beratung, Schulung, Engineering und Integration praxisnah in bestehende Anlagenprozesse einbetten.

Autor: Tobias Keller

Head of Administration,
tec.nicum

Mit tec.dloto bietet tec.nicum, die Dienstleistungssparte der Schmersal Gruppe, eine digitale Lösung, die klassische LOTO-Verfahren in geführte, nachvollziehbare und auditfähige Prozesse überführt.

Instandhaltung ist der Moment, in dem Maschinensicherheit besonders konkret wird. Schutzeinrichtungen werden geöffnet, Antriebe stillgesetzt, Energiequellen getrennt, Restenergien abgebaut. Was im Produktionsbetrieb durch feste Abläufe und technische Schutzeinrichtungen abgesichert ist, hängt bei Wartung, Reinigung, Störungsbeseitigung oder Umbau häufig von sauberer Vorbereitung und konsequenter Durchführung ab. Genau hier setzt Lockout/Tagout an – und genau hier zeigt sich, warum eine digitale Umsetzung wie tec.dloto für Betreiber industrieller Anlagen mehr ist als eine komfortable Software.

Lockout/Tagout, kurz LOTO, bezeichnet ein systematisches Verfahren zur Kontrolle gefährlicher Energien. „Lockout" meint das physische Verriegeln einer Energie-Trenneinrichtung, etwa eines Hauptschalters, Ventils oder Absperrorgans. „Tagout" ergänzt diese Verriegelung um eine klare Kennzeichnung: Wer hat gesichert, warum wurde gesichert, und dass die Anlage nicht wieder in Betrieb genommen werden darf. Das Verfahren stammt begrifflich aus dem angloamerikanischen Arbeitsschutz. Prägend war insbesondere der US-amerikanische OSHA-Standard 29 CFR 1910.147, „The control of hazardous energy", der seit Ende der 1980er-Jahre Anforderungen an Programme, Verfahren, Schulungen und regelmäßige Überprüfungen für Wartungs- und Instandhaltungsarbeiten beschreibt.

Auch im europäischen und deutschen Umfeld ist die dahinterstehende Schutzidee fest verankert, selbst wenn nicht immer der Begriff LOTO verwendet wird. Die ISO 14118 behandelt die Vermeidung unerwarteten Anlaufs von Maschinen und schließt dabei unterschiedliche Energieformen ein: elektrische, hydraulische und pneumatische Energie, aber auch gespeicherte kinetische Energie, zum Beispiel durch Lage, Druck oder Federn. Die Betriebssicherheitsverordnung fordert ebenfalls, dass Arbeitsmittel sicher stillgesetzt und von Energiequellen getrennt werden können. Der praktische Kern ist überall gleich: Eine Maschine darf während gefährlicher Eingriffe nicht unerwartet anlaufen, und gespeicherte Energie darf nicht unkontrolliert frei werden.

Ein klassischer LOTO-Ablauf folgt deshalb einer klaren Logik. Zunächst wird die Arbeit vorbereitet und alle relevanten Energiequellen identifiziert. Danach wird die Maschine geordnet stillgesetzt, von den Energiequellen getrennt und gegen Wiedereinschalten gesichert. →

Anschließend werden Restenergien abgebaut oder zuverlässig beherrscht. Erst wenn die Energiefreiheit beziehungsweise der sichere Zustand verifiziert ist, dürfen die Arbeiten beginnen. Vor der Wiederinbetriebnahme müssen Arbeitsbereich und Maschine kontrolliert, beteiligte Personen informiert und die Sicherungen geordnet zurückgenommen werden. Das klingt einfach, in der betrieblichen Praxis ist es jedoch anfällig für Fehler – besonders bei komplexen Anlagen, Schichtwechseln, Fremdfirmen, Zeitdruck oder häufig wechselnden Instandhaltungsaufgaben.

Grundprinzip LOTO:
Arbeit vorbereiten, Energiequellen ermitteln, Maschine stillsetzen und trennen, verriegeln und kennzeichnen, Restenergie abbauen oder sichern, den sicheren Zustand verifizieren und nach Abschluss kontrolliert wieder freigeben.

Klassische, manuelle Lösungen arbeiten meist mit gedruckten Anweisungen, Formularen, Anhängeschildern, persönlichen Schlössern und handschriftlichen Protokollen. Die physischen Schlösser bleiben für die Absicherung vor Ort unverzichtbar. Der organisatorische Teil ist jedoch oft weniger robust: Papier kann verloren gehen, unleserlich werden oder nicht mehr dem aktuellen Stand entsprechen. Fotos liegen auf privaten oder dezentralen Geräten, Freigaben erfolgen telefonisch oder per E-Mail, und im Audit muss mühsam rekonstruiert werden, wer welchen Schritt wann durchgeführt hat. Noch kritischer ist die fehlende Sichtbarkeit während laufender Arbeiten. Vorgesetzte und Sicherheitsverantwortliche sehen bei rein manuellen Verfahren häufig erst im Nachhinein, ob ein Prozess vollständig und korrekt dokumentiert wurde.

tec.dloto greift genau diese Schwachstellen auf. Die Lösung von tec.nicum ist eine webbasierte und mobile Plattform für das LOTO-Management. Sie digitalisiert den Prozess der Energieisolierung und führt die Anwender durch die erforderlichen Schritte. Der Ablauf beginnt pragmatisch: Der Mitarbeiter scannt einen QR-Code an der Maschine, startet die LOTO-Anforderung und erhält eine schrittweise digitale Anleitung. Referenzbilder helfen, die richtige Trennstelle oder Sicherungsposition eindeutig zu erkennen. Foto-Uploads und Prüfungen dokumentieren den tatsächlichen Zustand vor Ort. Kritische Schritte können über Genehmigungsworkflows abgesichert werden, bevor die Wartung beginnt.

Damit wird aus einer Checkliste ein geführter Prozess. Jede Aktion wird zeitlich nachvollziehbar erfasst, Benutzeraktionen werden zugeordnet, und die LOTO-Historie steht gesammelt zur Verfügung. Für Sicherheitsbeauftragte, Vorgesetzte und Werksleiter entsteht eine Transparenz, die papierbasierte Systeme nur mit hohem Aufwand bieten können. Dashboards, Live-Tracking, Benachrichtigungen und eine zentrale Anlagenübersicht zeigen, welche LOTO-Maßnahmen aktiv sind, welche Genehmigungen ausstehen und wo Arbeiten laufen. Das reduziert nicht nur Audit-Stress, sondern verbessert die operative Steuerung im Alltag.

Der Vorteil gegenüber klassischen manuellen Lösungen liegt deshalb nicht allein im Verzicht auf Papier. Entscheidend ist, dass tec.dloto Verbindlichkeit in den Prozess bringt. Schritte lassen sich nicht so leicht überspringen, veraltete Anweisungen werden zentral ersetzt, und Verantwortlichkeiten sind im System nachvollziehbar. Wo früher verstreute Dokumente, lokale Ordner und mündliche Abstimmungen zusammengeführt werden mussten, entstehen nun auditfähige Datensätze mit Fotos, Zeitstempeln und klaren Rollen. Für neue Mitarbeitende oder externe Dienstleister ist der Einstieg ebenfalls einfacher, weil sie nicht nur eine Anweisung erhalten, sondern durch den Ablauf geführt werden. →

LOTO erhöht die Sicherheit bei Wartungsarbeiten. Digitale Lösungen machen die Prozesse effizient und nachvollziehbar.

Für die Kunden des tec.nicum ist das ein deutlicher Mehrwert. tec.nicum versteht tec.dloto nicht als isoliertes IT-Tool, sondern im Verbund eines umfassenden Dienstleistungsansatzes rund um Maschinen- und Arbeitssicherheit. Die tec.nicum – Solutions & Services GmbH ist Teil der Schmersal Gruppe und bündelt Leistungen aus Academy, Consulting, Engineering, Integration, Digitalisation und Outsourcing. Das ist wichtig, weil ein wirksames LOTO-System nicht mit dem Kauf einer Software endet. Prozesse müssen zur Anlage passen, Rollen müssen geklärt, Mitarbeiter geschult und Verfahren betriebsnah gepflegt werden. Genau dabei kann tec.nicum seine Kunden unterstützen.

In der Praxis bedeutet das: Unternehmen erhalten nicht nur eine digitale Plattform, sondern Hilfe beim Aufbau eines sauberen, skalierbaren und nachweisbaren LOTO-Prozesses. tec.dloto unterstützt den mobilen Zugriff, kann cloudbasiert oder vor Ort bereitgestellt werden und erleichtert den Start durch Massen-Uploads und anpassbare Workflows. Die Lösung wächst also mit den betrieblichen Anforderungen. Perspektivisch können weitere Sicherheitsmodule, etwa Permit-to-Work-Funktionen, ergänzt werden. Für Betreiber mit mehreren Linien, Standorten oder wechselnden Teams ist diese Skalierbarkeit ein wesentlicher Vorteil.

Gerade bei sicherheitskritischen Tätigkeiten ist Digitalisierung nur dann sinnvoll, wenn sie die Arbeit vor Ort einfacher und sicherer macht. tec.dloto erfüllt diesen Anspruch, weil es die bewährten Grundprinzipien von Lockout/Tagout nicht ersetzt, sondern ihre Umsetzung stabilisiert. Die physische Trennung und Verriegelung bleibt der Kern. Die digitale Lösung sorgt dafür, dass Vorbereitung, Freigabe, Nachweis und Rücknahme sauber geführt und dokumentiert werden. Damit entsteht ein praxisnaher Brückenschlag zwischen Arbeitsschutz, Instandhaltung und Compliance. ■

Das Fazit fällt eindeutig aus: LOTO ist kein Formalismus, sondern ein zentrales Element sicherer Instandhaltung. Manuelle Verfahren können funktionieren, verlangen aber hohe Disziplin. Mit tec.dloto bietet tec.nicum seinen Kunden über das Tool hinaus eine Dienstleistung, die diesen Prozess professioneller, transparenter und effizienter macht. Für Kunden bedeutet das weniger Papier, weniger Unsicherheit, schnellere Nachweise und eine deutlich bessere Grundlage, um sicherheitskritische Arbeiten zuverlässig zu steuern.

tec.nicum

tec.nicum academy
Das Seminarprogramm 2026/2027

Auch in den kommenden Monaten erwartet Sie in der tec.nicum academy ein vielseitiges Weiterbildungsprogramm zu aktuellen Themen der Maschinensicherheit.

September 2026:

15.09.2026: Neue Maschinenverordnung (MVO), Wuppertal

16.09.2026: Cyber Resilience Act (CRA), Wuppertal

Darüber hinaus sind bundesweit weitere Seminare und Veranstaltungen an verschiedenen Standorten in Planung.

Neben Fachseminaren umfasst das Angebot auch zertifizierte Qualifizierungsprogramme wie **MCEexpert (Machine CE Expert)** und **FSM tec.nicum (Functional Safety Manager).**

Alle Seminare können bei Interesse auch als Inhouse-Schulung direkt in Ihrem Unternehmen durchgeführt und individuell auf Ihre Anforderungen zugeschnitten werden.

Die aktuellen Seminar- und Veranstaltungstermine sowie alle Informationen zur Anmeldung finden Sie unter www.tecnicum.com.

academy

Weiterbildungszentrum
- Schulungen
- Kundenspezifische Workshops
- Inhouse-Trainings
- Zertifizierte Kurse (MCEexpert und FSE)

consulting

Analyse und Dokumentation
- Technische Unterstützung
- Risikobeurteilungen
- CE-Konformitätsbewertung
- Bewertungen von Maschinen und Produktionslinien
- Technische Dokumentationen

engineering

Planung und Konstruktion
- Technische Projektierungen
- Konzeptionelle Projektentwicklung
- Elektronische und mechanische Konstruktion
- Projektmanagement
- LiDAR-Scan

integration

Praktische Anwendung
- Turnkey-Lösungen
- Installation
- Retrofit

digitalisation

Software-Integration
- tec.**ps** (Product Service System)
- tec.**ssm** (Schmersal Smart Machine)
- tec.**cvs** (Computer Vision Solutions)
- tec.**dloto** (Digital Lockout Tagout)
- tec.**ems** (Energy Monitoring System)

outsourcing

Serielle Lösungen
- Plug-and-Play-Produkte
- Engineer to Order-Projekte
- Systeme und Schaltschränke

Das Serviceangebot des tec.nicum umfasst sechs Bausteine.

Fotos: K.A. Schmersal GmbH & Co. KG, shutterstock.com,
JBT Marel Praxisbericht TREIF-Maschinen

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

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