mrl.news

Ausgabe 2023.02

tec.nicum

Neue Herausforderungen –
von kollaborierenden Robotern bis Cybersecurity

Ausnahmen bestätigen nicht nur die Regel, sondern können auch vernünftig sein. Wenn die britische Regierung beschließt, dass eine EU-Regelung nach dem Brexit ausnahmsweise beibehalten wird, ist das eine gute Nachricht, mit der wir diese Ausgabe der MRL News gewissermaßen eröffnen. Großbritannien will das europäische CE-Kennzeichen nach dem Brexit nun doch beibehalten – das erleichtert den Warenverkehr. Nicht alle neuen Regeln der EU sind durchweg positiv: Die neue Fassung der Maschinenverordnung wird voraussichtlich eine Hürde für Betreiber darstellen, die ihre Maschinen modernisieren möchten oder müssen. Erfahren Sie mehr dazu auf Seite 19.

Welche Regeln und Normen bei der Einrichtung eines Arbeitsplatzes mit einem kollaborierenden Roboter zu beachten sind, damit beschäftigt sich der Beitrag auf den Seiten 4 bis 7. Die schutzzaunlose Zusammenarbeit von Mensch und Roboter birgt ein hohes Gefahrenpotenzial, daher gelten hier spezielle Anforderungen.

Ebenfalls hoch ist das Gefahrenpotenzial in der Intralogistik. In diesem Heft stellen wir Ihnen einige neue Automatisierungs- und Sicherheitslösungen vor, die sowohl die Sicherheit als auch die Produktivität der Prozesse erhöhen.

Herausforderungen ganz anderer Art ergeben sich bei der Fernwartung von Maschinen. Hier gilt es, Safety und Security im Blick zu haben. Externe Zugriffe auf die IT-Infrastruktur eines Unternehmens könnten als Einfallstor für Cyberattacken missbraucht werden. Selbst direkte Angriffe auf Steuerungssysteme (SPS) stellen heute eine reale Gefahr dar. Prominentes Beispiel: Der Angriff auf die iranischen Atomanlagen 2010 mithilfe des Computerwurms Stuxnet.

Noch eine gute Nachricht zum Schluss: Das tec.nicum bietet seinen Kunden verstärkt Turnkey Solutions an – Komplettlösungen für die Maschinensicherheit. Welche Leistungen dieses Angebot umfasst, lesen Sie auf der Seite 8.

Viel Vergnügen bei der Lektüre!

Herzlichst

Ihr Redaktionsteam

Großbritannien will europäisches CE-Kennzeichen nach dem Brexit doch beibehalten

Großbritannien erklärte Anfang August dieses Jahres, dass es die europäische CE-Kennzeichnung für Produkte nach dem Austritt des Landes aus der Europäischen Union nun doch auf unbestimmte Zeit beibehalten und nicht abschaffen wird.

Eigentlich sollte von Ende 2024 an das CE-Symbol von einem neuen, britischen Sicherheitssiegel namens UKCA (UK Conformity Assessed) für in Großbritannien verkaufte Produkte ersetzt werden. Allerdings hatten Unternehmen über enorme Zusatzkosten geklagt und die Regierung mit Nachdruck aufgefordert, ihre Pläne aufzugeben, die zunächst lediglich eine Spiegelung der EU-Vorschriften bedeutet hätten.

Laut Presseberichten nannte der Chef des britischen Herstellerverbands Make UK, Stephen Phipson, den Verzicht auf die Umstellung „pragmatisch und vernünftig". Unternehmen können nun wählen, ob sie von Ende 2024 an das UKCA-Zeichen, das in der EU nicht anerkannt wird, für den Verkauf ihrer Produkte in Großbritannien nutzen wollen.

Auch die britischen Handelskammern begrüßten die unbefristete Beibehaltung des CE-Zeichens. Eine Umfrage aus dem Jahr 2021 ergab, dass nur 8 % der Unternehmen das EU-Kennzeichnungssystem aufgeben wollten, während 59 % der von der Entscheidung betroffenen Unternehmen es beibehalten wollten.

Schmersal hatte bereits im Jahr 2022 das erste UKCA-Zertifikat für seine Sicherheitszuhaltungen AZ300, AZM300 und AZM300-AS vom TÜV Rheinland erhalten. Bis Anfang 2023 sollten die gängigsten und am häufigsten nachgefragten Produkte von Schmersal mit dem UKCA-Zertifikat ausgestattet werden, damit die Kunden von Schmersal ihre Maschinen richtlinienkonform in Großbritannien in Verkehr bringen können.

Der Richtungswechsel der britischen Regierung erleichtert den Export von Produkten nach Großbritannien, weil die Unternehmen nun zwischen CE- und UKCA-Siegel wählen können. Doch ob in Fragen des Warenverkehrs zwischen UK und EU das letzte Wort gesprochen ist, lässt sich momentan schwer beurteilen. Die MRL News wird Sie in jedem Fall auf dem Laufenden halten! ■

Die sichere Zusammenarbeit von Mensch und Robotern in kollaborativen Arbeitssystemen ist erstens möglich und bringt zweitens klare Vorteile – auch bei Verpackungsprozessen. Allerdings müssen einige Voraussetzungen geschaffen und diverse Normen der Maschinensicherheit berücksichtigt werden.

Planung und Konstruktion einer kollaborativen Roboterzelle

Auf gute Zusammenarbeit!

Vom Roboter zum Cobot: Dieser Schritt bietet sich in vielen Anwendungsbereichen der industriellen Automation an – beispielsweise in der Verpackung von Lebensmitteln, wenn es sich um kleinere Stückzahlen oder Sonderverpackungen handelt.

Die Kollaboration, sprich Zusammenarbeit, von Mensch und Roboter ohne trennende Schutzeinrichtungen kann hier die Flexibilität deutlich erhöhen, und eben das ist gefragt, wenn immer häufiger kleine Serien produziert werden oder wenn auf einer Linie verschiedene Produkte gefertigt werden sollen.

Was ist bei der Konstruktion von Roboterzellen mit Mensch-Roboter-Kollaboration zu beachten? Deren Grundkonzept sieht vor, dass Mensch und Roboter gleichzeitig in einem Arbeitssystem tätig sind und zusätzlich durch trennende Schutzeinrichtungen von der Außenwelt abgeschirmt sind. Das heißt: Die Zelle braucht einen Schutzzaun mit Schutztüren, und sie braucht Zuführmöglichkeiten in den Gefahrbereich hinein und aus ihm heraus – z. B. Förderanlagen oder Übergabestationen für die zu bearbeitenden Produkte. Was die Zelle hingegen nicht (mehr) braucht, ist eine physische Trennung zwischen den Arbeitsbereichen von Mensch und Roboter. Das ist aus Sicht der Robotik und der Automatisierungstechnik ein echter Einschnitt: Jahrzehntelang durften Roboter und Bediener niemals in Kontakt kommen, und der Roboter musste seine Tätigkeit „hinter Schloss und Riegel“ verrichten.

Jetzt ist die gleichzeitige Tätigkeit von Mensch und Roboter in einem Arbeitssystem Teil der „Smart Factory“. Es gibt viele Hersteller von kollaborativen Robotern (Cobots) und mindestens ebenso viele Systemintegratoren, deren Anlagen auch dank der Cobots hoch produktiv kleinere Stückzahlen von Produkten und auch Verpackungen erzeugen. Bei jeder einzelnen Applikation werden die Stärken des menschlichen Bedieners (Geschick, Kraftdosierung, selbstständige Problemlösung) mit denen des Roboters (Präzision, Ermüdungsfreiheit, Wiederholgenauigkeit) kombiniert. →

Klare Grundsätze für die Kollaboration

Natürlich mussten für diese neue Art der Zusammenarbeit erst die normativen Grundlagen geschaffen werden – mit dem Ziel, den Roboter mit Sicherheitseinrichtungen zum Schutz des Menschen auszustatten und ihn zum kollaborierenden Roboter zu machen. Das ist geschehen und soll hier kurz vorgestellt werden.

Wie generell in der Maschinensicherheit (und das heißt: im Geltungsbereich der Maschinenrichtlinie) gilt in der kollaborativen Robotik die „Normenpyramide“ von harmonisierten Typ-A-, Typ-B- und Typ-C-Normen.

Als Typ-A-Normen bezeichnet man die Sicherheitsgrundnorm EN ISO 12100 (Risikobeurteilung). Etwas konkreter werden die Typ-B1-Normen, die sich mit speziellen Sicherheitsaspekten befassen. Beispiele sind die bekannte EN ISO 13849 (Sicherheitsbezogene Teile von Steuerungen) und EN ISO 11161 (Integrierte Fertigungssysteme). Die Typ-B2-Normen treffen Aussagen zu einzelnen Arten von Sicherheitsgeräten, z. B. zu Not-Halt-Einrichtungen (EN ISO 13850).

Speziell für die Robotik gibt es mehrere Fachnormen oder Typ-C-Normen. Dazu gehören:

- EN ISO 10218 „Industrieroboter – Sicherheitsanforderungen“, gegliedert in
  - Teil 1 („Roboter“) und
  - Teil 2 („Robotersysteme und Integration“). Hier werden Sicherheitsanforderungen an Roboterzellen definiert.
- ISO/TS 15066 „Roboter und Robotikgeräte – kollaborierende Roboter“.

Die „Technische Spezifikation“ ISO/TS 15066 ist allerdings nicht harmonisiert, d. h. nicht unter der MRL gelistet. Darüber hinaus steht die Normenreihe EN ISO 10218 kurz vor der Veröffentlichung einer überarbeiteten Version. Teil zwei der Normenreihe wird ab diesem Zeitpunkt die Anforderungen der ISO/TS 15066 beinhalten, sodass die Anforderungen an kollaborierende Robotersysteme bald vollständig der EN ISO 10218-2 entnommen werden können und somit auch erstmals unter der MRL harmonisiert sind.

Neben den Normen gibt es weitere hilfreiche Dokumente zum Thema „Maschinensicherheit bei kollaborativen Robotern“ – z. B. die DGUV-Information 209-074 „Kollaborierende Robotersysteme“ samt Checkliste sowie ein VDMA-Positionspapier „Sicherheit bei der Mensch-Roboter-Kollaboration“ und mehrere nützliche Whitepapers vom TÜV Austria.

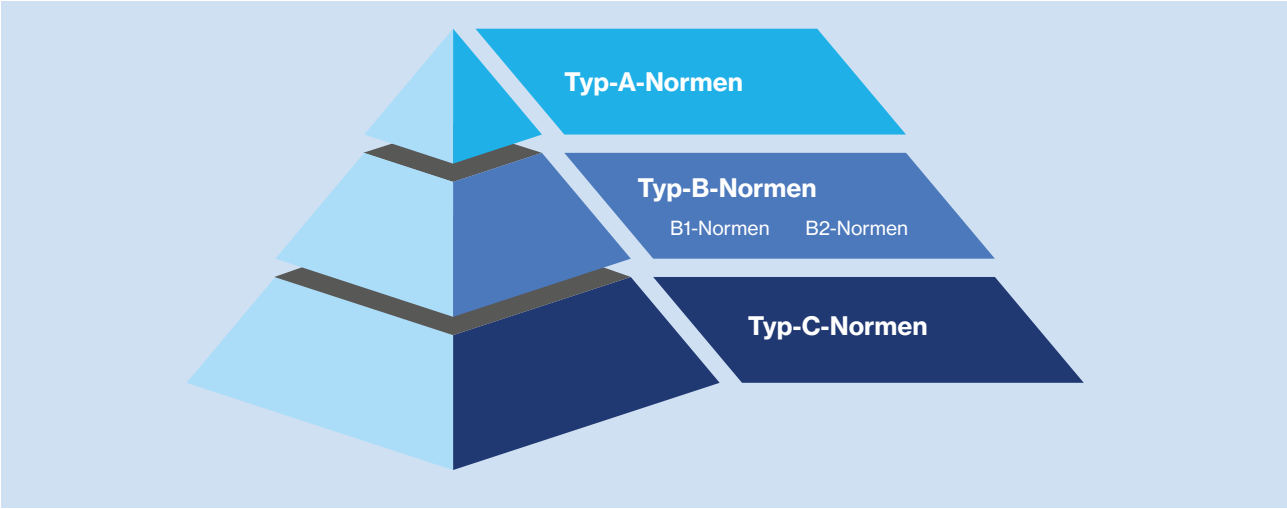
Der Weg zum kollaborativen Arbeitssystem nach ISO/TS 15066

In drei Schritten kann ein kollaborierendes Robotersystem erreicht werden:

1. Verwendung eines mit der EN ISO 10218-1 konformen Roboters.
2. Integration des Roboters in eine Roboterzelle entsprechend den Anforderungen der EN ISO 10218-2, dabei ggf. Anwendung der EN ISO 11161.
3. Gestaltung des Kollaborationsraumes entsprechend ISO/TS 15066.

Die EN ISO 10218 definiert die Räume, die bei der Gestaltung der Sicherheitsmaßnahmen von Roboterzellen zu berücksichtigen sind (maximaler Raum, eingeschränkter Raum, Betriebsraum, geschützter Bereich). Darüber hinaus gibt es bei kollaborierenden Robotern einen Kollaborationsraum, der sowohl in EN ISO 10218-1 als auch in ISO/TS 15066 beschrieben wird. In ihm können sich Mensch und Roboter gleichzeitig aufhalten und Aufgaben ausführen. Die entsprechende Betriebsart nennt sich „kollaborierender Betrieb“.

Welche Anforderungen gelten nun konkret für Entwurf und Planung einer Roboterzelle als „kollaboratives →



Arbeitssystem“ gemäß ISO/TS 15066? Wenn das Layout der Zelle definiert ist, sollte der Konstrukteur die Gefährdungen ermitteln und eine Risikobeurteilung durchführen. Daraus ergeben sich die notwendigen Maßnahmen zur Risikominderung. Welche Maßnahmen für ein kollaboratives Arbeitssystem zulässig sind, wird in der ISO/TS 15066 beschrieben und mit den entsprechenden Anforderungen definiert.

Kernprozess: Gestaltung des Layouts der Roboterzelle

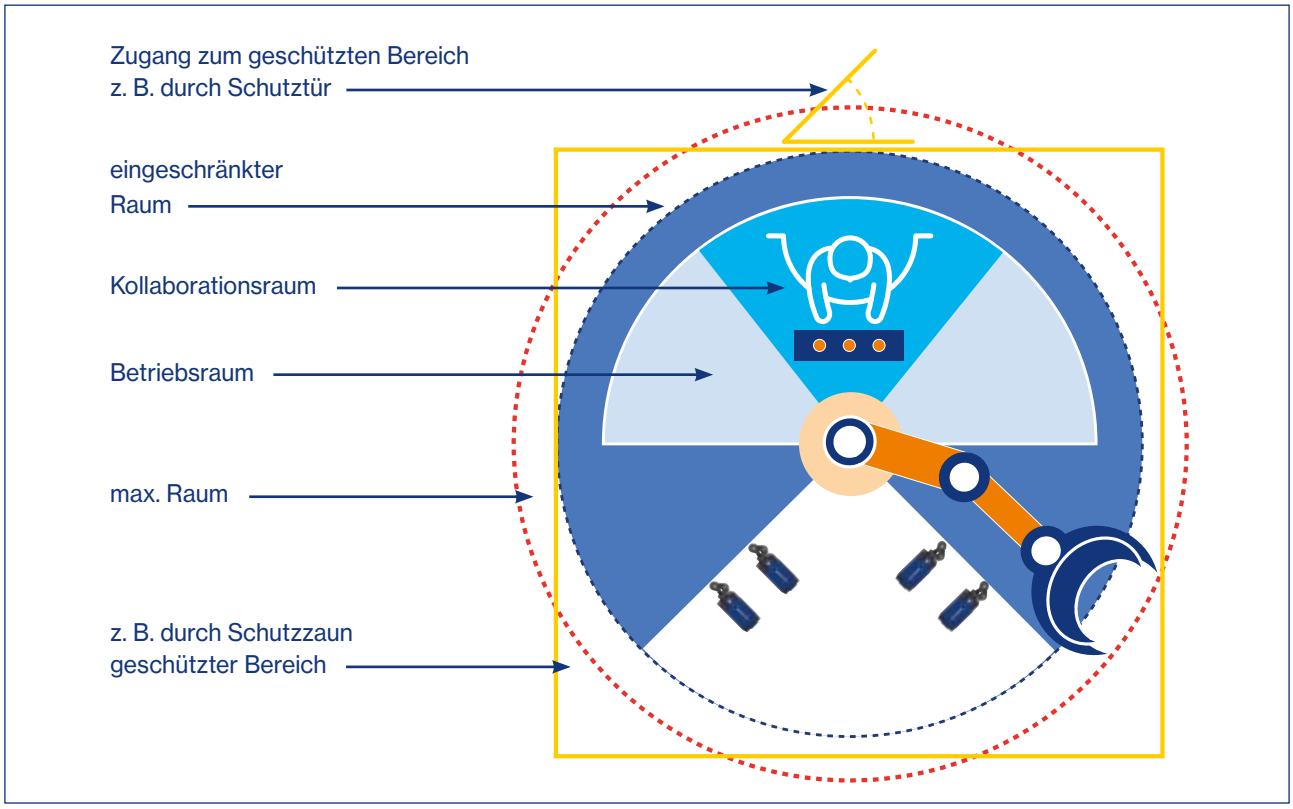
Die Gestaltung des Layouts ist ein Kernprozess bei der Risikominderung in kollaborativen Roboterzellen. Mit dem Layout werden die oben genannten Räume, einschließlich des Kollaborationsraums, festgelegt und auch die Zugänge zu den Gefahrenbereichen. Bei diesem entscheidenden Schritt sollte sowohl die Ergonomie an der Mensch-Maschine-Schnittstelle bedacht werden als auch der zusätzliche Raum, der ggfs. für Nachlaufbewegungen des Roboters (z. B. nach der Betätigung der Not-Halt-Einrichtung) benötigt wird.

Zu den Aufgaben des Konstrukteurs bzw. Sicherheitsingenieurs gehört die Berücksichtigung des besonderen Gefährdungspotenzials durch Roboter und deren Betrachtung im Rahmen der Risikobeurteilung. Schließlich war es nicht ohne Grund so, dass die Arbeitsbereiche von Mensch und Roboter jahrzehntelang strikt getrennt werden mussten. Hilfreich sind in diesem Zusammenhang die Gefährdungslisten im Anhang A der EN ISO 10218-1 und EN ISO 10218-2, die speziell auf die Gefährdungen von Robotern und in Roboterzellen eingehen.

Konkret besteht das Gefährdungspotenzial u. a. darin, dass Roboter Bewegungen mit hoher Energie und Reichweite ausführen und dass ihr Verfahrweg nur schwer vorhersehbar ist. Unter Umständen muss auch damit gerechnet werden, dass mehrere Roboter in einem gemeinsamen Betriebsraum arbeiten. Deshalb muss der Kollaborationsraum eindeutig festgelegt werden, und darüber hinaus muss jede Bedienperson in diesem Raum, d. h. im Arbeitsbereich des Roboters, ein eigenes Steuerungselement mit sich führen. Ebenfalls vorgeschrieben ist der Einsatz einer sicheren Software zur Achs- und Raumbegrenzung, die in der Regel vom Hersteller des Roboters bereitgestellt wird.

Möglichkeiten zur Gestaltung eines kollaboratives Betriebes

Die ISO/TS 15066 stellt vier Möglichkeiten in den Mittelpunkt, wie die Kollaboration zwischen dem Bediener und dem Roboter realisiert werden kann. Zu diesen gehören die Handführung des Roboters (Bewegung des Roboterarms durch menschliche Krafteinwirkung), die Geschwindigkeits- und Abstandsüberwachung (Einhalten des Abstands durch Verringerung der Geschwindigkeit), →



Bei kollaborierenden Robotern gibt es einen Kollaborationsraum, der sowohl in EN ISO 10218-1 als auch in ISO/TS 15066 beschrieben wird. In ihm können sich Mensch und Roboter gleichzeitig aufhalten und Aufgaben ausführen.

der sicherheitsbewerte überwachte Halt (Stoppkategorie 2, Wiederanlauf beim Verlassen des Kollaborationsraums) und die Leistungs- und Kraftbegrenzung (durch Reduktion der Kräfte gemindertes Risiko). Fast alle diese Methoden bedingen eine steuerungstechnische Realisierung, sodass zusätzliche Sicherheitsfunktionen zu realisieren und zu bewerten sind.

Beispiel: Leistungs- und Kraftbegrenzung

Die wesentliche Gefährdung bei der Zusammenarbeit von Mensch und Roboter ist der unbeabsichtigte Kontakt von beiden. Mit der Leistungs- und Kraftbegrenzung sollen daher die Folgen eines solchen Kontaktes minimiert werden. Kann es im Kollaborationsraum zu einem Kontakt kommen, gibt es auf die einzelnen Körperteile bezogene Belastungsgrenzwerte, die einzuhalten sind. Das kann durch passive Schutzmaßnahmen geschehen, zum Beispiel durch Schaumstoffpolster, eine Vergrößerung der Kontaktfläche oder eine Begrenzung der bewegten Massen. Oder aber der Konstrukteur der kollaborativen Roboterzelle beugt hier aktiv, per Steuerungstechnik, vor – zum Beispiel durch eine Begrenzung von Kraft oder Drehmoment oder durch die Integration von Sensorik, die den Bediener detektiert.

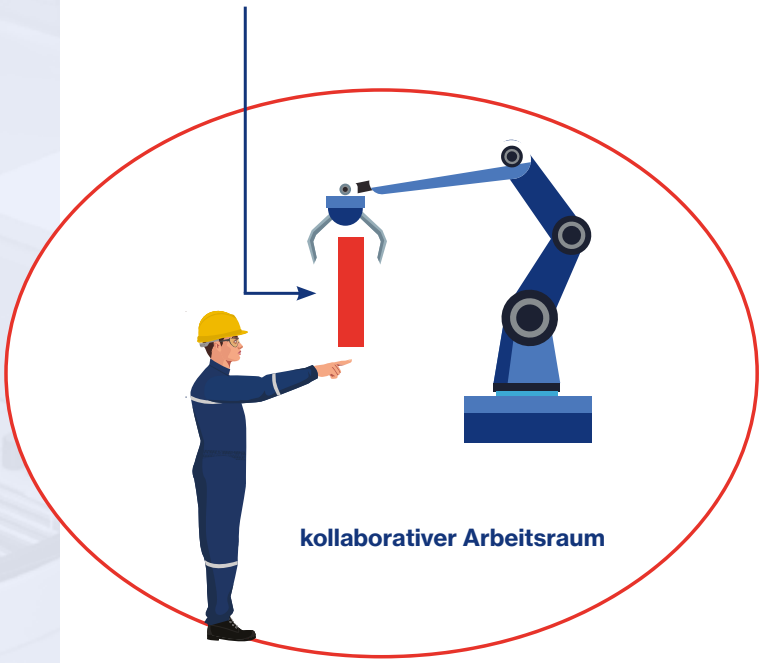
Somit sind beim kollaborativen Betrieb von Roboterzellen verschiedene Sicherheitsfunktionen zu realisieren. Je nach gewählter Realisierung des kollaborativen Betriebs sind z. B. Drehmoment, Kraft, Geschwindigkeit oder Position der Roboterachse sicherheitsgerichtet zu überwachen. Auch ein Betriebsartenwahl- und Zustimmungsschalter gehört in der Regel zur sicherheitsbezogenen Ausstattung. Die entsprechenden Produkte bzw. Systemlösungen sind – zum Beispiel im Schmersal-Programm – verfügbar und in solchen Anwendungen bewährt.

Nach der Gestaltung: Verifizierung und Validierung

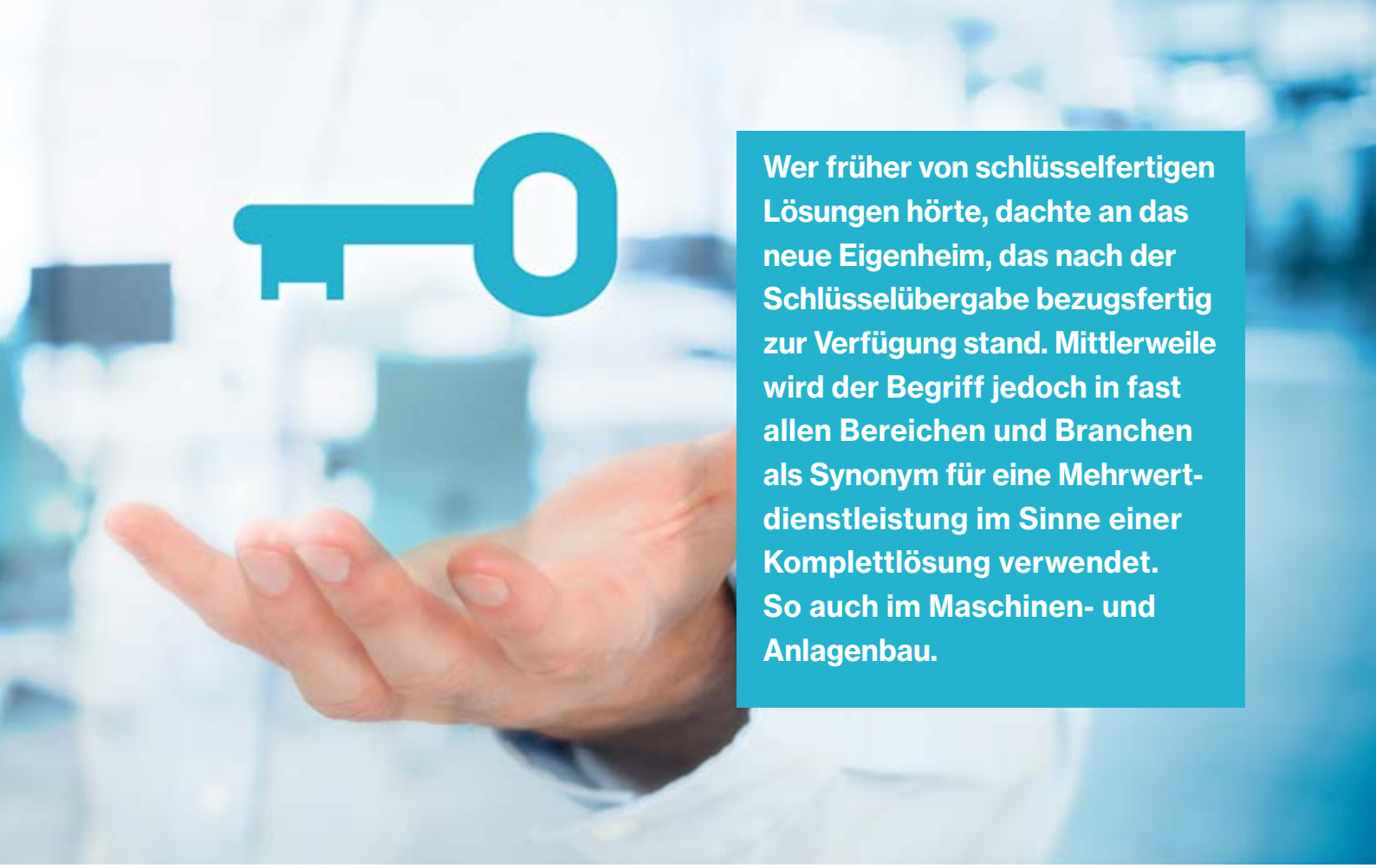
Gemäß ISO/TS 15066 muss das Ergebnis der Gestaltung einer kollaborativen Roboterzelle abschließend verifiziert und validiert werden. Dieser Schritt ist aufgrund des hohen Gefahrenpotenzials im Robotersystem elementar, um die Sicherheit abschließend zu bestätigen und die Konformität mit der Maschinenrichtlinie zu erreichen. Hierbei – und auch bei den weiteren notwendigen Arbeitsschritten wie Konformitätsbewertung, Risikobeurteilung, Kraft- und Druckmessung – kann der Anwender die qualifizierten Dienstleistungen des tec.nicum von Schmersal in Anspruch nehmen. Die Safety Consultants des tec.nicum bringen die nötige Expertise mit und auch ein hohes Maß an Branchenkompetenz in der Verpackungstechnik. ■

Benjamin Bottler
Safety Consultant,
Schmersal Gruppe

Sicherheitslichtgitter überwachen den Kollaborationsraum für den sicheren Eintritt einer Person.



Beim kollaborativen Betrieb von Roboterzellen sind verschiedene Sicherheitsfunktionen zu realisieren, z. B. müssen Drehmoment, Kraft, Geschwindigkeit oder Position der Roboterachse sicherheitsgerichtet überwacht werden.



Wer früher von schlüsselfertigen Lösungen hörte, dachte an das neue Eigenheim, das nach der Schlüsselübergabe bezugsfertig zur Verfügung stand. Mittlerweile wird der Begriff jedoch in fast allen Bereichen und Branchen als Synonym für eine Mehrwert-dienstleistung im Sinne einer Komplettlösung verwendet. So auch im Maschinen- und Anlagenbau.

Turnkey Solutions – der Schlüssel zum Erfolg

Hocheffiziente sicherheitstechnische Modernisierung von Maschinen und Anlagen aus einer Hand

Die Maschinen- und Anlagensicherheit unterliegt heute einer ständigen Weiterentwicklung und einer daraus resultierenden kontinuierlichen Anpassung an den technischen Fortschritt. Die immer umfangreicher werdenden Anforderungen erschweren es den Betreibern zunehmend, sich auf ihre Kernaufgabe, die Aufrechterhaltung der Produktionsprozesse mit komplexen und qualitativ hochwertigen Präzisionsmaschinen und -anlagen, zu konzentrieren.

Das Sicherheitskonzept einer Maschine ist ein integraler und zwingend notwendiger Aspekt im Rahmen des Betriebes derartiger Produktionsmaschinen und -anlagen. Dabei spielt es zunächst keine Rolle, ob es sich um eine neue oder bereits in Betrieb befindliche Anlage handelt. Eine Maschine muss muss auch bei den erhöhten heutigen Anforderungen zu jedem Zeitpunkt sicher sein!

Turnkey Solutions gewinnen daher auch im Bereich der Maschinen- und Anlagensicherheit immer mehr an Bedeutung. Turnkey Safety Solution Provider übernehmen dabei für den Kunden den gesamten Bereich der Maschinensicherheit und liefern ihm eine komplette Herstellungskette bis hin zur Übergabe einer sicheren Gesamtlösung. Dies reicht von der sicherheitstechnischen Analyse und Bewertung über die Entwicklung von Sicherheitskonzepten und deren Engineering bis hin zur schlüsselfertigen Übergabe nach der Installation der Sicherheitslösungen.

Auch das tec.nicum der Schmersal Gruppe hat sich auf diese Entwicklung eingestellt und bietet seinen Kunden genau solche ganzheitlichen Dienstleistungen an.

Bereits seit der Gründung des tec.nicum im Januar 2016 hat Schmersal auch Safety Services in sein Angebotsportfolio aufgenommen. Zunächst nur in Form von Einzelleistungen wie Risikobeurteilungen, Berechnungen von Sicherheitsfunktionen oder auch Validierungen von Sicherheitsfunktionen.

Doch getreu dem Motto „Stillstand bedeutet Rückschritt“ stellt sich das tec.nicum den Herausforderungen der Zukunft und entwickelt sich stetig weiter, um seinen Kunden bestmöglichen und maßgeschneiderten Service bieten zu können. →

Vom Komponentenhersteller zum System- und Lösungsanbieter

Genau diesem Selbstverständnis folgend, gehören Turnkey-Projekte mittlerweile zum festen Repertoire der tec.nicum-Dienstleistungen. Wir bieten unseren Kunden und Partnern Komplettlösungen, die alle gesetzlichen und kundenseitigen Anforderungen erfüllen und somit einen sicheren Betrieb der Anlage gewährleisten. Um eine möglichst kosteneffiziente und prozessoptimierende Wirkung zu erzielen, stehen unsere Projektkoordinatoren und -ingenieure ständig in engem Kontakt mit den verantwortlichen Mitarbeitern des Auftraggebers. Nur so lassen sich zukunftssichere Lösungen im Sinne unserer Kunden erzielen. Unsere Projektpartner bekommen genau das, was sie brauchen, und nicht einfach das, was wir haben!

Sollte sich im Laufe eines Projektes herausstellen, dass spezielle Tätigkeiten nicht von den Experten des tec.nicum selbst durchgeführt werden können oder von diesen nicht durchgeführt werden dürfen, kümmern wir uns selbstverständlich auch hier um eine entsprechende Umsetzung. Ein breit gefächertes Netzwerk an spezialisierten Partnern ermöglicht es uns, auf jede Aufgabenstellung schnell reagieren zu können.

Bei offenen Projekten bleibt es unserem Auftraggeber überlassen, welche Gewerke er in Eigenleistung erbringen möchte und welche er an uns vergibt. Am Ende übergeben wir aber auch hier das Projekt schlüsselfertig zum vereinbarten Zeitpunkt an unseren Kunden.

Der große Vorteil unserer Turnkey-Komplettlösungen liegt für unsere Kunden darin, dass die Maschinen und Anlagen nach der schlüsselfertigen Übergabe sofort und ohne weitere Anpassungen genutzt werden können.

Genau das ist auch der entscheidende Vorteil gegenüber allgemeinen Standardlösungen, die in der Regel vom Betreiber selbst mit relativ hohem Aufwand an die eigenen Bedürfnisse und Anforderungen angepasst werden müssen. Nicht bei uns! tec.nicum liefert immer maßgeschneiderte Individuallösungen, die zu 100 % auf die Prozesse und Bedürfnisse des Kunden abgestimmt sind!

Um unnötige Produktionsstillstände im Projektverlauf zu vermeiden, werden alle Umbaumaßnahmen an der Maschine mit den Wartungs- und Instandhaltungszyklen des Auftraggebers abgestimmt und entsprechend im Projektplan hinterlegt. So wird ein möglichst reibungsloser Projektablauf gewährleistet.

After-Sales-Service mit dauerhafter professioneller Betreuung

Auch nach einem Umbau muss die Sicherheitstechnik gewartet werden. Der Umfang dieser Maintenance-Services richtet sich immer nach den Anforderungen und Bedürfnissen des Kunden sowie eventuellen externen Auflagen und kann verschiedene Leistungen im Zusammenhang mit der sicherheitstechnischen Ausrüstung der Maschine oder Anlage umfassen. So sind z. B. wiederkehrende Prüfungen von optoelektronischen Schutzeinrichtungen (Lichtschranken oder Lichtvorhänge) in regelmäßigen Abständen erforderlich, oder einzelne Komponenten müssen ausgetauscht werden, weil sie das Ende ihrer Lebensdauer erreicht haben. Mit einem zuverlässigen Partner, der das Sicherheitskonzept Ihrer Anlage bis ins letzte Detail kennt und dieses stets im Blick hat, ist das kein Problem. ■

Fazit:

Turnkey Solutions stellen für die Betreiber von Maschinen und Anlagen, die einer sicherheitstechnischen Modernisierung bedürfen, einen hohen Mehrwert dar. Alle relevanten Arbeiten, von der ersten Analyse bis hin zur kompletten technischen Umsetzung, werden von nur einem einzigen Auftragnehmer übernommen und ausgeführt.

Der Betreiber kann sich auf eine fachgerechte und qualitativ hochwertige Projektausführung nach dem Stand der Technik verlassen. Da er hier keine eigenen Mitarbeiter einsetzen muss, kann er diese folglich für andere Aufgaben und Projekte einplanen. Alle projektbezogenen praktischen und organisatorischen Aufgaben werden von unseren Mitarbeitern professionell und zuverlässig umgesetzt.

Der Schlüssel zu Ihrem Erfolg ist unsere Turnkey-Lösung!

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

Sprechen Sie uns einfach an. Wir sind überzeugt, dass wir Ihnen die Unterstützung bieten können, die Sie benötigen!

Tobias Keller
Business Development Coordinator
Solutions & Services im tec.nicum der
Schmersal Gruppe

Erfordert die Fernwartung von Maschinen eine Risikobeurteilung? Welche Herausforderungen stellen Industrie 4.0 und neue Vorschriften an die Security? Welche Schritte sind notwendig, um die IT-Sicherheit zu gewährleisten? Welche Normen sind für die Fernwartung relevant? Dieser Artikel möchte einen Anstoß geben, sich speziell mit dem Thema Cyber-Security auseinanderzusetzen.

Herausforderungen und Chancen beim Remote-Zugriff auf Maschinen

Safety und Security bei der Fernwartung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bezeichnet Fernwartung als einen „räumlich getrennten Zugriff auf IT-Systeme und die darauf laufenden Anwendungen. Der Zugriff kann z. B. dazu dienen, Konfigurations-, Wartungs- oder Reparaturarbeiten durchzuführen“ [1].

Die Vorteile der Fernwartung sind vielfältig. Sie spart vor allem Zeit und Kosten, beispielsweise entfallen die Aufwendungen und die Wegzeiten für Reisen. Ein Techniker kann sich in Sekunden auf die gestörte Anlage aufschalten, kann dann den Fehler lokalisieren und entweder beheben oder einen Techniker des Betreibers anleiten. Dadurch können die Servicemitarbeiter beim Maschinenbauer zentralisiert werden, und durch diese Zentralisierung ist der Zugriff auf weitere Spezialisten im Unternehmen oftmals einfacher und schneller möglich.

Die Covid-19-Pandemie und die damit verbundenen Reisebeschränkungen haben den Bedarf an Remote-Lösungen noch verstärkt. Dies gilt nicht nur für die Fernwartung zur Fehlerbehebung oder als geplante Revision, sondern beispielsweise auch für die Inbetriebnahme einer Maschine.

Technisch ist der Zugriff über das Internet in Zeiten von Breitbandverbindungen kein Problem, es gibt unzählige Softwaretools, die den Zugriff auf PCs ermöglichen. Auch sind viele Steuerungen über ihre IP-Adressen einfach zu erreichen. Im Zusammenhang mit Remotezugriffen müssen allerdings zwei wichtige Aspekte berücksichtigt werden: Safety und Security. Da beide Begriffe sich in der deutschen Übersetzung „Sicherheit” nicht unterscheiden, bietet es sich an, die englische Nomenklatur zu übernehmen. Safety bezeichnet hierbei den Schutz des Menschen vor der Maschine im Sinne der Maschinenrichtlinie, dies wird auch als funktionale Sicherheit bezeichnet. Im Gegensatz dazu beschreibt Security den Schutz der Maschine vor dem Menschen.

Hinzu kommen noch rechtliche Fragen z. B. bezüglich der Haftung, wenn Personal des Betreibers vor Ort mit einem online verbundenen Service-Techniker zusammenarbeitet. Diese Fragen sollen an dieser Stelle nicht betrachtet werden, es sei nur beispielhaft auf das Angebot des VDMA verwiesen. Der Verband der Maschinen- und Anlagenbauer bietet Vertragsentwürfe an, die bei der gegenseitigen (haftungs-)rechtlichen Absicherung von Betreiber und Maschinenbauer helfen [2]. →

Bei Remotezugriffen sollte zwischen reinen Lese- und Lese-/Schreibzugriffen unterschieden werden. So erfolgt bei der Ferndiagnose nur ein lesender Zugriff. Auch der im Kontext der Industrie 4.0 oft verwendete Begriff des Condition Monitoring erfordert prinzipiell zunächst nur einen lesenden Zugriff auf Maschinen- bzw. Prozessdaten. Aus dem Blickwinkel der Maschinensicherheit ist dies in der Regel unkritisch, da nicht von außen in den Prozess eingegriffen wird, die Maschine also ihren Betriebszustand nicht verlässt und alle Sicherheitsfunktionen regulär ausgeführt werden. Mit Blick auf die Security lassen sich rein lesende Zugriffe oft relativ einfach über sogenannte Datendioden absichern. Letztlich ist aber zu bewerten, welche Daten gelesen werden, und ob diese Daten in falsche Hände gelangen können. Hier sind dann ggf. entsprechende Maßnahmen zu ergreifen.

Safety

Sowohl Inbetriebnahmen als auch Fehlersuche und geplante Wartungen erfordern häufig das Verfahren der Maschine bei deaktivierten Schutzeinrichtungen, beispielsweise um Einstell- oder Reinigungsarbeiten möglichst effizient durchführen zu können. Auch unter diesen Bedingungen muss der Schutz des Bedieners sichergestellt sein, unabhängig davon, ob gerade ein Fernzugriff auf die Maschine erfolgt.

Um diesen Schutz sicherzustellen, sind geeignete Maßnahmen zu treffen, insbesondere zur Vermeidung des unerwarteten Anlaufs [3]. Es bietet sich zudem eine gesonderte Betriebsart an, die durch das Maschinenpersonal aktiv initiiert werden muss. Weiterhin sollte sichergestellt sein, dass insbesondere Not-Halt-Einrichtungen immer Vorrang haben und nicht durch Remote-Befehle überschrieben werden können. Auch das Rücksetzen von Sicherheitsfunktionen sollte nicht aus der Ferne möglich sein. Idealerweise wird an der Maschine zudem deutlich kenntlich gemacht, dass aktuell ein Remote-Zugriff erfolgt. Nicht zuletzt sollte auch durch technische und organisatorische Maßnahmen verhindert werden, dass Dritte unbefugt in den Prozess der Fernwartung eingreifen und damit gefährliche Maschinenzustände initiieren können.

Letztlich ist der Fernzugriff eine weitere Betriebsart der Maschine, die im Rahmen der Risikobeurteilung bewertet werden muss und für die geeignete Sicherheitsfunktionen definiert und implementiert werden müssen, um den Schutz des Bedieners zu gewährleisten. Die EN ISO 13849 [4], aber auch die EN ISO 12100 [5] geben hier wichtige Hinweise, wenn auch nicht explizit mit Blick auf die Fernwartung.

Bei allen Änderungen an der Sicherheitsapplikation oder Änderungen von sicherheitsrelevanten Parametern, wie zulässigen Geschwindigkeiten, Drücken, Temperaturen etc., stellt sich auch die Frage, ob eine wesentliche Veränderung vorliegt. Einen Leitfaden hierfür bietet das Interpretationspapier des BMAS [6], aber auch der Blue Guide [7] der Europäischen Union. Im Zweifel wird dann derjenige, der die Änderung vornimmt, zum neuen Hersteller der Maschine mit allen zugehörigen Pflichten, wie beispielsweise der Aufgabe, eine neue Konformitätsbewertung nach aktueller Maschinenrichtlinie durchzuführen. Bei Maschinen nach Anhang IV sind solche Änderungen auch mit der benannten Stelle abzustimmen, wenn eine Baumusterprüfung als Konformitätsverfahren angewendet wurde. Andernfalls kann die Prüfbescheinigung unwirksam werden. Aber auch wenn es sich nicht um eine wesentliche Veränderung handelt, muss der Betreiber gemäß Betriebssicherheitsverordnung [8] die Änderung bewerten und gegebenenfalls Maßnahmen ergreifen. Immer sollte auch eine umfassende Validierung der Sicherheitsfunktionen jeder Änderung folgen.

Security

Externe Zugriffe auf die IT-Infrastruktur des Unternehmens waren und sind für die verantwortlichen Administratoren seit jeher eine große Herausforderung. Ging es zunächst vor allem um den Schutz des Intellectual Property (IP), steht man heute vielfach der Gefahr von Ransomware gegenüber. →

In einer Studie des Security-Anbieters Sophos von 2022 [9] geben 67 % der befragten deutschen Unternehmen an, Opfer von Ransomware-Angriffen gewesen zu sein. Im Schnitt entstand dabei ein Schaden von 1,6 Mio. €, nicht nur durch das Zahlen des Lösegeldes, sondern auch durch Produktionsausfälle, gestörte Lieferketten, Regressansprüche etc.

Sogar der direkte Angriff auf Steuerungssysteme (SPS) ist heute eine reale Gefahr. Der Angriff auf die iranischen Atomanlagen 2010 mittels des Computerwurms Stuxnet ist hier nur ein prominentes Beispiel [10]. So wurde die Malware Industroyer2 2022 für einen Angriff auf die ukrainische Energieversorgung genutzt. Diese Malware ist auch auf ICS-Systemen (Industrial Control System) lauffähig [11]. Im Zuge der Industrie 4.0 verschwinden die Grenzen zwischen der Feldebene und der Ebene des ERP (Enterprise-Resource-Planning) durch die fortschreitende vertikale Vernetzung dieser Bereiche immer mehr. Damit verschwindet auch das sogenannte Air Gap, also die physische Trennung von OT (operative Technologie) und IT (Informationstechnologie). So bietet beispielsweise die Verwendung IP-basierter Feldbusse neue Einfallstore für Angreifer. Darüber hinaus schaffen neue Vorschriften wie die Maschinenverordnung [12], der EU Cyber Resilience Act [13] oder die Neufassung der NIS-Richtline [14] weiteren Handlungsdruck. Gerade die Richtlinie NIS 2, die spätestens im Oktober 2024 in Kraft treten wird, bedarf hier besonderer Beachtung, denn die Kriterien, ab wann für ein Unternehmen die Richtlinie Anwendung findet, wurden überarbeitet und erweitert.

Was sollte man tun?

Erster Schritt sollte eine Einschätzung der eigenen Situation sein, also eine Risikoanalyse ähnlich wie bei der funktionalen Sicherheit. Eine Hilfestellung bietet hier die Normenreihe IEC 62443. Insbesondere die Teile 2-1 [15], 2-4 [16] und 3-3 [17] sind für Betreiber und Integratoren relevant. Sie definieren für den Prozess sogenannte Maturity Level (Reifegrade). Technische Anforderungen an Systeme werden durch vier Security Level (SL) bewertet. Die verschiedenen Level geben dabei die Widerstandsfähigkeit gegenüber verschiedenen Angreiferklassen an d. h., wie viele Ressourcen aufgewendet werden müssten. Auch wenn es hier auf den ersten Blick viele Analogien zur funktionalen Sicherheit zu geben scheint, so bietet diese Norm, anders als beispielsweise die EN ISO 13849, keine „einfachen" Handlungsanweisungen dafür, ein bestimmtes Sicherheitsniveau zu erreichen. Es gibt nicht die eine Lösung, die für alle Anwendungen und Netzwerktopologien optimal ist – sowohl vom zu erreichenden Schutz als auch mit Blick auf die Kosten und den administrativen Aufwand. →

Grundlegende Sicherheitsprinzipien

Eine der Grundforderungen für eine sichere IT-OT-Topologie ist die Segmentierung der Netzwerke mit zwischengeschalteten sogenannten demilitarisierten Zonen (DMZ). Diese DMZ schützen die Übergänge zwischen den verschiedenen Netzbereichen z. B. mittels Firewalls. Mindestens die verschiedenen Level nach dem Purdue-Referenzmodell [18] sollten entsprechend geschützt sein. Je nach Netzwerk-Topologie oder dem ermittelten Risiko kann es sinnvoll sein, auch einzelne Fertigungsabschnitte oder gar einzelne Maschinen in einem eigenen Segment zu kapseln.

Die Fernwartung sollte immer unter Kontrolle des Betreibers stehen. Dies bedeutet zum einen, dass die Fernwartung nur durch den Betreiber initiiert oder zumindest autorisiert werden kann. Zum anderen sollte auch die verwendete Hardware unter der Kontrolle des Betreibers stehen. Nur so kann er sicherstellen, dass Zugänge zu seinem Netz immer auf dem aktuellen Stand sind, d. h. alle bekannten Sicherheitslücken zeitnah geschlossen werden.

Es ist zudem eine zeitliche Limitierung anzuraten, um zu verhindern, dass für die Fernwartung geöffnete Zugänge zum Netzwerk, beispielsweise VPN-Zugänge, nach Beendigung der Fernwartung geöffnet bleiben. Remotesitzungen sollten immer auch geloggt werden, um Zugriffe und gegebenenfalls durchgeführte Änderungen nachvollziehen zu können.

Im Unterschied zur funktionalen Sicherheit, bei der man zu Beginn die Grenzen der Maschine definiert und eine Laufzeit von 20 Jahren betrachtet, ist Security ein andauernder Prozess. Mit der ständigen Weiterentwicklung Schritt zu halten, erfordert ein kontinuierliches Updaten (Patchen) der entsprechenden Komponenten und der verwendeten Software, um einmal entdeckte Schwachstellen umgehend schließen zu können. Derzeit ist die Fernwartung nur in wenigen Normen beschrieben. Eine davon ist die Norm EN ISO 10218-2 [19]. Für Robotersysteme ist hier festgelegt, dass eine Fernsteuerung nur dann möglich sein soll, wenn sich die Maschinensteuerung in der manuellen Betriebsart befindet. Darüber hinaus können sicherheitsrelevante Parameter, Achs- und Raumbegrenzung, Bahnänderungen usw. nur dann verändert werden, wenn die Änderungen vom Bediener vor Ort akzeptiert und bestätigt werden. ■

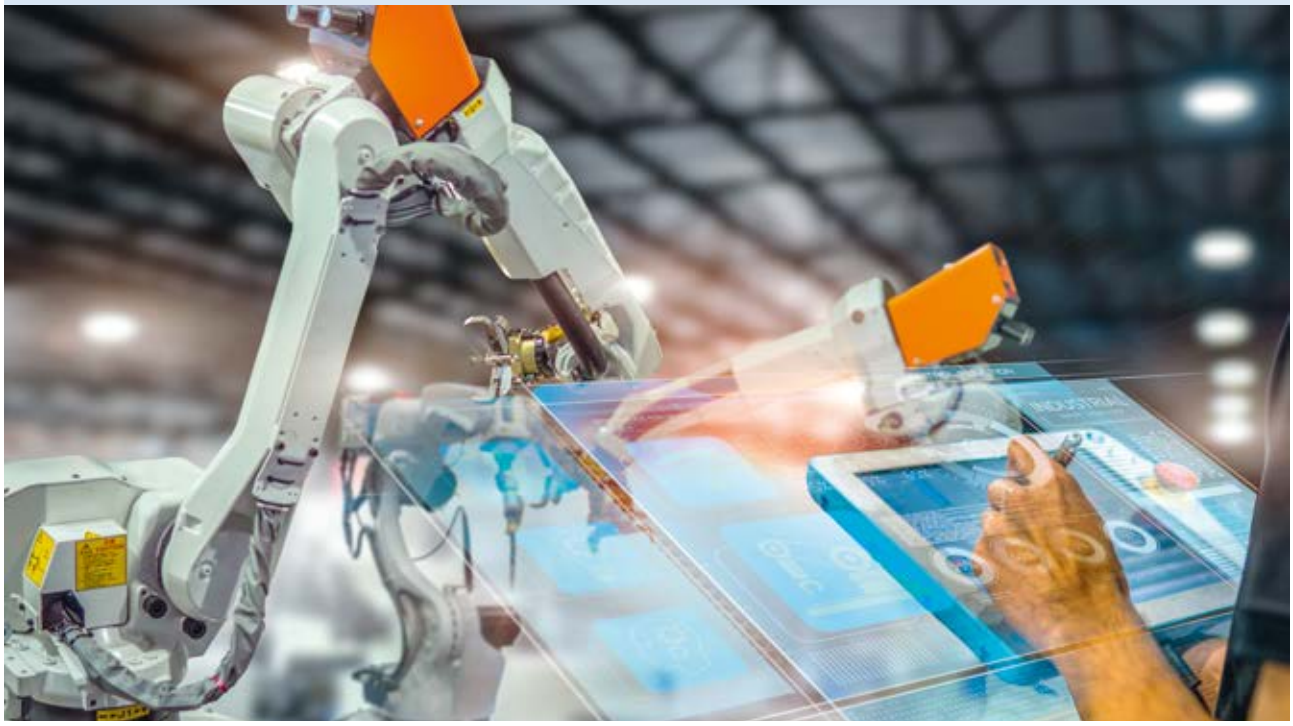
Fazit

Remote-Zugriffe auf Maschinen sind ein zeitgemäßes Werkzeug, um effizient Inbetriebnahmen oder Wartungsarbeiten durchzuführen. Wichtig ist es aber, sich der Risiken bewusst zu sein, sowohl bezüglich der IT-Sicherheit als auch im Hinblick auf die funktionale Sicherheit für den Bediener.
Dieser Text kann und will keine umfassende Darstellung bieten, vielmehr möchte er Anstoß sein, sich insbesondere mit dem Thema Cybersecurity zu befassen. Gerade hier erwachsen mit den neuen EU-Richtlinien neue Herausforderungen sowohl für Maschinenbauer als auch für Betreiber. Herausforderungen, die durch die Veränderungen im Zusammenspiel von IT und OT im Zuge der Industrie 4.0 aktuell noch drängender werden.

Christian Lumpe
Produktmanager Steuerungen,
Schmersal Gruppe

Literatur

1. Bundesamt für Sicherheit in der Informationstechnik. OPS.1.2.5: Fernwartung
2. VDMA Verlag. Remote-Inbetriebnahme. EAN 4250697525225
3. EN ISO 14118: Sicherheit von Maschinen. Vermeidung von unerwartetem Anlauf
4. EN ISO 13849-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze
5. EN ISO 12100: Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung
6. Bundesministerium für Arbeit und Soziales. Interpretationspapier „Wesentliche Veränderung von Maschinen“
7. Bekanntmachung der Kommission: Leitfaden für die Umsetzung der Produktvorschriften der EU 2016 („Blue Guide“) (2016/C 272/01)
8. Verordnung über Sicherheit und Gesundheitsschutz bei der Verwendung von Arbeitsmitteln (Betriebssicherheitsverordnung – BetrSichV)
9. Sophos Ltd. „State of Ransomware 2022“.
10. Produktmitteilung Beitrags-ID: 43876783, Beitragsdatum: 01.04.2011. „SIMATICWinCC/SIMATIC PCS 7: Information bezüglich Malware / Virus / Trojaner“
11. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
12. Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates
13. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen
14. Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union
15. IT-Sicherheit für industrielle Automatisierungssysteme – Teil 2-1: Anforderungen an ein IT-Sicherheitsprogramm für IACS-Betreiber
16. IT-Sicherheit für industrielle Automatisierungssysteme – Teil 2-4: Anforderungen an das IT-Sicherheits-programm von Dienstleistern für industrielle Automatisierungssysteme
17. Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme – Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level
18. Theodore J. Williams: The Purdue Enterprise Reference Architecture: A Technical Guide for CIM Planning and Implementation
19. EN ISO 10218-2 „Industrieroboter – Sicherheitsanforderungen – Teil 2: Robotersysteme und Integration“



Die neue Magnetspur-Sensorbox SSB-R von Schmersal.

Neue Automatisierungs- und Sicherheitslösungen für die Intralogistik

Innerbetrieblicher Materialfluss: sicher – produktiv – vernetzt

Die Intralogistik gewinnt in vielen Branchen an Bedeutung. Aufgrund von Lieferengpässen und Materialmangel sind neue Konzepte für Lagerhaltung und Materialfluss gefragt. Und auch die Industrie 4.0 ist ohne eine effiziente und vernetzte Logistik nicht realisierbar. Jetzt gibt es neue technische Lösungen und Systeme für eine sichere und produktive intralogistische Infrastruktur.

In der Intralogistik sind die Anforderungen an die Produktivität und Ausfallsicherheit der Anlagen sehr hoch. Die Kunden erwarten eine immer schnellere und zuverlässigere Auftragsabwicklung, daher werden Prozesse zunehmend automatisiert. Hinzu kommt, dass das Gefahrenpotenzial beim innerbetrieblichen Lagern und Transportieren hoch ist. Doch Unfälle gefährden nicht nur die Gesundheit der Mitarbeiter, sondern stören auch den Betriebsablauf und verursachen hohe Kosten. Bei der Entwicklung neuer Automatisierungs- und Sicherheitslösungen für die Intralogistik hat Schmersal daher immer beides im Blick: Sicherheit und Produktivität.

Preisgünstig und wartungsfrei: die neue Magnetspur-Sensorbox SSB-R für Elektrohängebahnen

Elektrohängebahnen werden branchenübergreifend zum Transport von Werkstücken und Materialien unterschiedlichster Art eingesetzt. Die flurfreie Förderung ist wesentlich effizienter und schneller als flurgebundene Förderung und schafft Platz auf der Bodenfläche in Montage und Lager. In jedem Elektrohängebahn-(EHB-) System sind viele Trolleys auf einer gemeinsamen Hängebahn unterwegs. In einigen Bereichen fahren sie schnell, in anderen Zonen langsamer, und an definierten Punkten halten sie an. Deshalb ist eine Überwachung von Geschwindigkeit und Position jedes einzelnen Trolleys unabdingbar. Dies wurde bisher von mehreren einzelnen Magnetsensoren ausgeführt. Die neue Magnetspur-Sensorbox SSB-R von Schmersal übt diese Funktionen jetzt mit einer deutlich größeren Präzision aus.

Die Sensorbox ermöglicht die Abfrage von vier parallelen und unabhängigen Magnetspuren. Sie erfasst das Magnetfeld der Betätiger und wechselt bei Vorbeifahrten den entsprechenden Signalzustand. Dieser auch bei schneller Vorbeifahrt erzeugte Pegel bleibt bis zur nächsten Ansteuerung erhalten. Eine angeschlossene Steuerung ermittelt aus den Signalen Position und Streckenabschnitt der Trolleys und regelt z. B. Geschwindigkeit (Eilgang / Schleichgang) oder Haltepositionen des Antriebsmotors.

Die Sensorbox ist in vier Varianten verfügbar. Die Variante mit der Bezeichnung SSB-RH ist auf zwei Spuren mit zusätzlicher Sensorik ausgestattet und nutzt ein High-Pegel (für 100 ms). Mit diesen Eigenschaften →

ermöglicht sie eine höhere Positioniergenauigkeit und kann z. B. einen Trolley auf +/– 1,5 mm genau an der gewünschten Stopp-Position zum Halten bringen. Das ist etwa an Roboterarbeitsplätzen von Vorteil, wo Bauteile sehr präzise positioniert werden müssen. Mittels der zweiten Positionierspur lassen sich z. B. bei Nachlauf Start- und Endposition einer Haltezone exakt definieren.

Ein weiterer Pluspunkt für die Produktivität: Die magnetische Signalspeicherung funktioniert auch bei einem Spannungsausfall und ermöglicht einen schnellen Wiederanlauf des Betriebs.

Die Sensorbox kann nicht nur bei der Planung von Neuanlagen für vereinfachte Montage und eine genauere Positionierung der Trolleys sorgen. Da die Magnetschalter und -spuren im üblichen Abstand von 30 mm installiert sind, kann die Box an vorhandenen EHB-Systemen vier einzelne Magnetschalter z. B. der Baureihen BN325 und BN310 von Schmersal ersetzen – bei minimiertem Montageaufwand und höherer Positioniergenauigkeit.

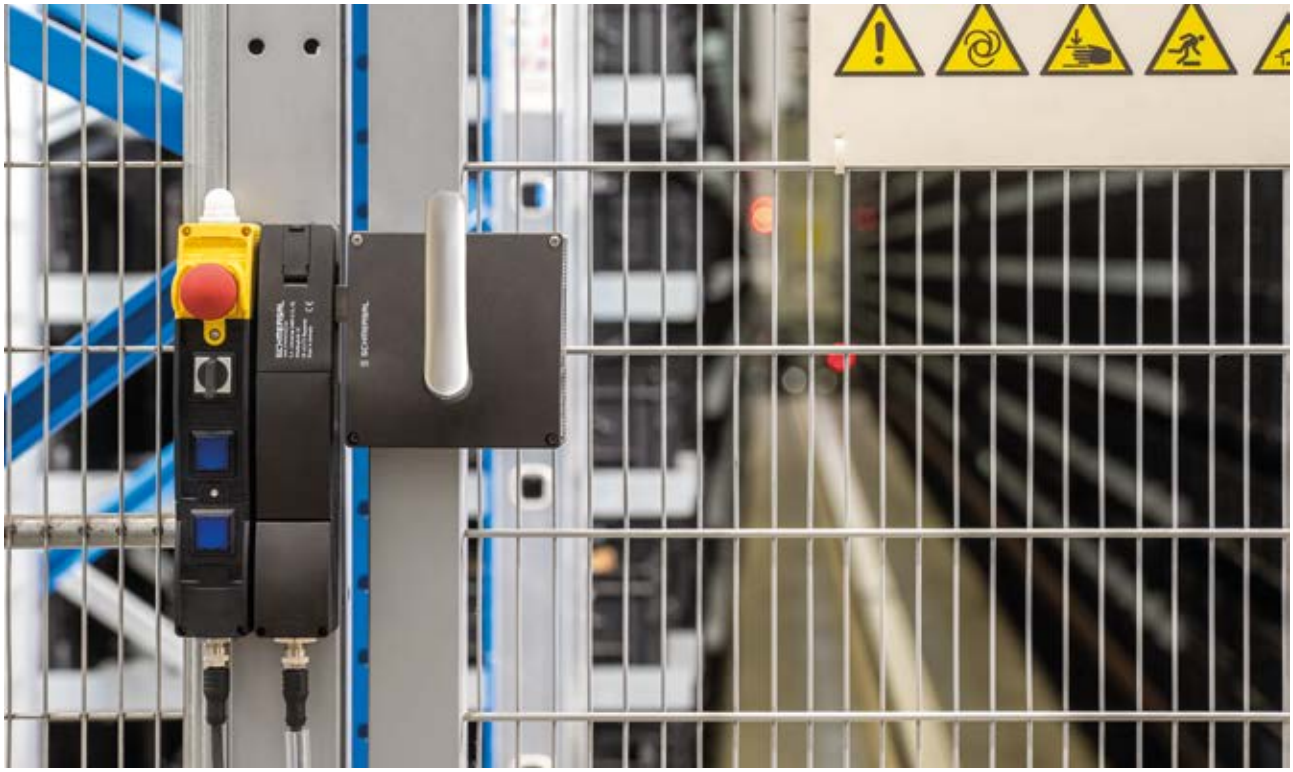
Flexible Einsatzmöglichkeiten ergeben sich auch aus der Tatsache, dass es diverse andere fördertechnische Anlagen gibt, die über Stromschienen mit Energie und Signalen versorgt werden – zum Beispiel Regalbediengeräte, bodengebundene Skids und Shuttles auf den einzelnen Ebenen von Shuttle-AKLs (AKL = Automatisches Kleinteilelager). Bei diesen und weiteren Anlagen bietet der Einsatz der Magnetspur-Sensorbox die gleichen Vorteile wie bei Elektro-Hängebahnen.

Vernetzte Sicherheitslösungen

In großen Logistikstandorten, z. B. in den Regionallägern der Lebensmittel-Discounter oder Warenverteilzentren der Kontraktlogistiker, ist der Materialfluss weitgehend automatisiert. Für die Maschinensicherheit gelten hier besondere Anforderungen, weil die automatisierten Anlagen weitläufig sind und es viele „Schnittstellen“ zum Personal gibt – zum Beispiel Übergabeplätze. Aus diesen Gründen bietet sich hier die Vernetzung der Sicherheitsschaltgeräte an. Das heißt: Die klassische Einzelverdrahtung jedes Schaltgerätes wird durch effizientere, netzwerkartige Verdrahtungskonzepte ersetzt. Dabei stehen mehrere Optionen zur Auswahl.

Palettierer handhaben schwere Lasten mit großer Geschwindigkeit. Um die Mitarbeiter vor den schnellen Bewegungen z. B. von Portalrobotern zu schützen, sind die Arbeitsbereiche von Mensch und Roboter durch Schutzzäune mit mindestens einer Schutztür getrennt, deren Stellung sicherheitsgerichtet überwacht werden muss. Der Konstrukteur sollte sich vorzugsweise für eine Sicherheitszuhaltung entscheiden, z. B. die Zuhaltung AZM201 von Schmersal. Sie hält die Schutztür so lange verriegelt, bis die gefährliche (Nachlauf-)Bewegung zum Stillstand gekommen ist. Damit dient sie einem unterbrechungsfreien Betrieb, weil der Palettiervorgang nicht durch Öffnen der Schutztür gestoppt werden kann. Das ist umso wichtiger, als Palettierer meist in verkettete Produktions- und Verpackungsprozesse eingebunden sind.

→



Sicherheitszuhaltungen wie die AZM201 von Schmersal dienen der Stellungsüberwachung von Schutztüren, z. B. an Roboterarbeitsplätzen.

Sicherheitszuhaltungen – und auch viele andere Sicherheitskomponenten von Schmersal – können mit einem integrierten Interface für den Sicherheits-Bus AS-i Safety at Work ausgestattet und damit einfach in einen Sicherheitskreis integriert werden. Der AS-i-Safety-Standard ermöglicht nicht nur eine schnelle Montage mit minimalem Verdrahtungsaufwand. Er bietet auch eine hohe Flexibilität, z. B. bei Umbauten an der Anlage oder bei neuen (Sicherheits-)Anforderungen.

Ein wesentlicher Vorteil der Sensorbox sind die umfangreichen Diagnosefunktionen. Sie ermöglichen bei Unregelmäßigkeiten oder Störungen ein schnelles Auffinden der Fehlerquelle, so dass insbesondere bei weitläufigen, komplexen Anlagen die Stillstandszeiten in solchen Fällen erheblich reduziert werden können. Aus diesen Gründen sind viele Intralogistik-Anlagen, die Schmersal mit Sicherheitssystemen ausrüstet, über AS-Interface Safety at Work (AS-i SaW) vernetzt.

Anschaltung über die sichere Feldbox

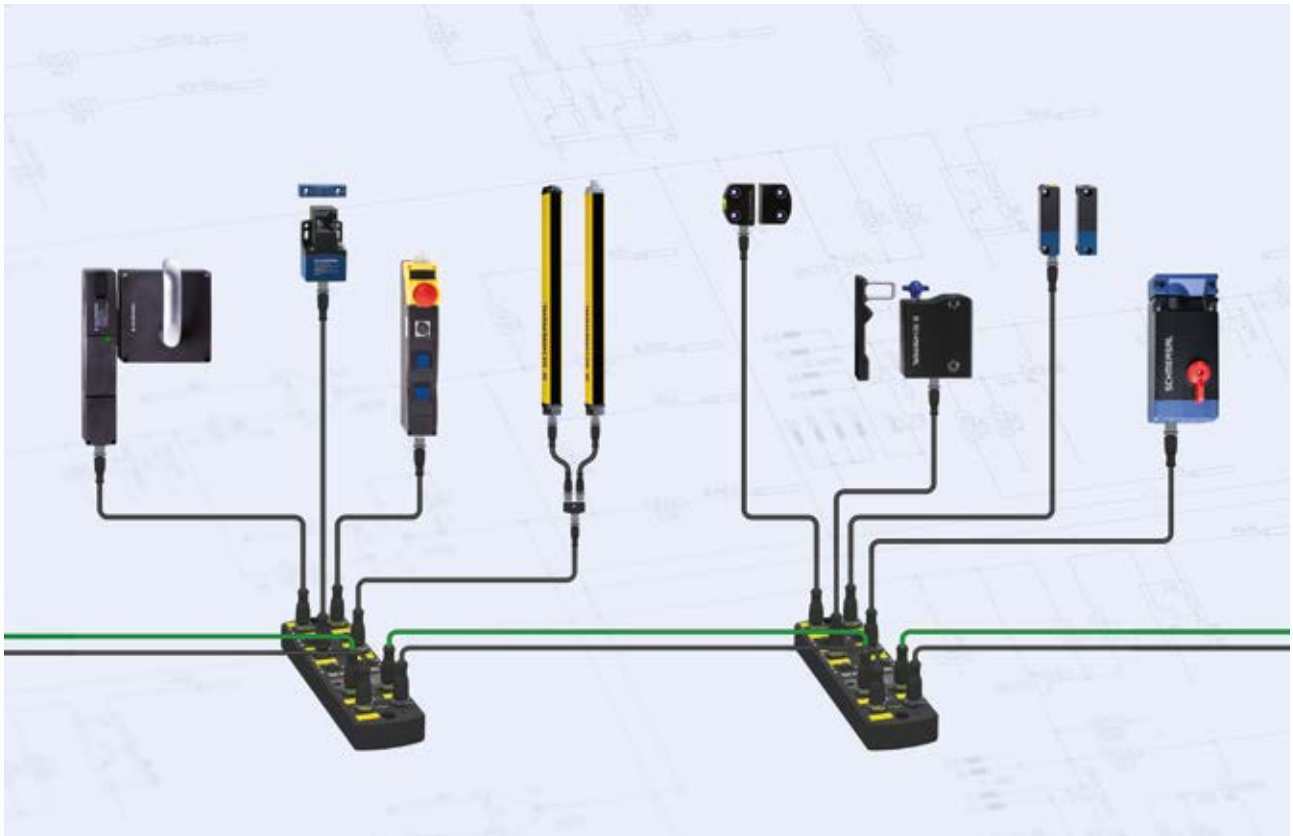
Alternativ kann anstelle von AS-i SaW auch das „Safety Fieldbox"-System (SFB) eingesetzt werden. Eine Safety Fieldbox ermöglicht die Anschaltung von bis zu acht Sicherheitsschaltgeräten verschiedener Bauarten im Feld. Dabei belegen elektromechanische und elektronische Endgeräte jeweils nur einen Geräteanschluss. Sowohl die sicherheitsgerichteten als auch die betriebsmäßigen Signale werden gesammelt und über das PROFINET/PROFIsafe-Protokoll – das heißt: über das in Europa am häufigsten verbreitete Bus-System – mit übergeordneten Steuerungsbausteinen verbunden.

Neues Bussystem SD 4.0

Wenn der Anwender ausschließlich betriebsbezogene, d. h. nicht sicherheitsgerichtete Signale sammeln und auswerten möchte, steht ihm mit SD 4.0 eine dritte Option zur Auswahl. Das ist die neueste Ausprägung eines von Schmersal entwickelten Bussystems, mit dem elektronische Sicherheitssensoren und -zuhaltungen umfassende Status- und Diagnosedaten an eine übergeordnete Maschinensteuerung übertragen.

Ein zentraler Vorteil von SD 4.0 gegenüber dem bisherigen SD-Bus ist die deutlich einfachere Vernetzungsmöglichkeit mit höheren Ebenen. Die Voraussetzung dafür schafft die Anbindung an OPC UA als standardisiertes Protokoll für die M2M-Kommunikation. Das hat zum Beispiel den Vorteil, dass die im Feld gesammelten Diagnoseinformationen besser visualisiert und über mobile Endgeräte wie Tablets oder Handys abgerufen werden können. Das erleichtert die Implementierung von Predictive-Maintenance-Konzepten. ■

Marcel Bogusch
Branchenmanager Logistik,
Schmersal Gruppe



Die Safety Fieldbox ermöglicht vernetzte Sicherheitslösungen.

Hersteller und Betreiber sollten sich frühzeitig mit der neuen Maschinenverordnung (MVO) befassen, denn ab dem 20.1.2027 müssen die Anforderungen umgesetzt werden.

Begriffsbestimmung der „wesentlichen Veränderung“ in der MVO

Welchen Einfluss hat die Einführung der Maschinenverordnung auf bestehende Anlagen oder das Retrofit?

Durch die Begriffsbestimmung der „wesentlichen Veränderung“ in der MVO sind jetzt auch die Betreiber betroffen, die Maschinen umbauen oder verändern.

Die ab 20. Januar 2027 anzuwendende Regelung ist wie folgt in der neuen MVO ausgeführt.

Artikel 3 Begriffsbestimmungen

16. „Wesentliche Veränderung“ bezeichnet eine vom Hersteller „nicht vorgesehene oder geplante physische oder digitale Veränderung“ einer Maschine oder eines dazugehörigen Produkts nach deren bzw. dessen Inverkehrbringen oder Inbetriebnahme, die die Sicherheit der jeweiligen Maschine oder des dazugehörigen Produkts beeinträchtigt, indem eine neue Gefährdung entsteht oder sich ein bestehendes Risiko erhöht, wodurch es erforderlich wird,

a. die Maschine oder das dazugehörige Produkt um trennende oder nichttrennende Schutzeinrichtungen zu ergänzen, deren Einbindung eine Anpassung des bestehenden Sicherheitssteuerungssystems erforderlich macht, oder
b. zusätzliche Schutzmaßnahmen zur Gewährleistung der Stabilität oder der Festigkeit der jeweiligen Maschine oder des dazugehörigen Produkts zu ergreifen.

Die Aussage „nicht vorgesehene oder geplante physische oder digitale Veränderung“ bedeutet zunächst für 99,9 % der Fälle eine „wesentliche Veränderung“, denn kaum ein Hersteller plant eine physische oder digitale Veränderung nach dem Inverkehrbringen. Dazu kommt, dass die „wesentliche Veränderung“ gemäß aktueller Fassung der MVO **zu einer „neuen Maschine“ führt.** Die Erleichterung bei „Teil einer Gesamtheit von Maschinen“ wird nicht viel Jubel auslösen. Zu den weiteren Pflichten des Herstellers wird erläutert:

Artikel 18 Sonstige Fälle

„Eine natürliche oder juristische Person, die eine wesentliche Veränderung an einer Maschine oder einem dazugehörigen Produkt vornimmt, gilt für die Zwecke dieser Verordnung als Hersteller und unterliegt den in Artikel 10 genannten Pflichten des Herstellers für diese Maschine bzw. dieses dazugehörige Produkt oder, wenn sich die wesentliche Veränderung wie in der Risikobeurteilung gezeigt **nur** auf die Sicherheit einer Maschine oder eines dazugehörigen Produkts, das Teil einer Gesamtheit von Maschinen ist, auswirkt, für die **betroffene Maschine** bzw. das betroffene dazugehörige Produkt.“

„Die Person, die die wesentliche Veränderung vornimmt, muss insbesondere, jedoch unbeschadet anderer Verpflichtungen nach Artikel 10, sicherstellen und auf ihre alleinige Verantwortung erklären, dass die betroffene Maschine bzw. das betroffene dazugehörige Produkt den geltenden Anforderungen dieser Verordnung entspricht, und muss das einschlägige Konformitätsbewertungsverfahren nach Artikel 25 Absätze 2, 3 und 4 dieser Verordnung anwenden.“ →

Ein nichtprofessioneller Nutzer, der eine wesentliche Veränderung an seiner Maschine oder seinem dazugehörigen Produkt für den Eigengebrauch vornimmt, gilt für die Zwecke dieser Verordnung nicht als Hersteller und unterliegt nicht den Pflichten des Herstellers nach Artikel 10.

Die im Erwägungsgrund (26) aufgeführte „Verhältnismäßigkeit“ ist in den Artikeln für uns nicht wirklich herauszulesen, zumindest nicht für gewerbliche Betreiber von Maschinen und Anlagen.

Da in der Praxis viele Betreiber ihre Maschinen modernisieren oder auf betriebliche Anforderungen umbauen, wird die aktuelle Fassung der MVO sicher eine große Hürde darstellen. Betreiber müssen sich gut überlegen, wie „zukunftssicher“ ihre nächsten Anschaffungen sind und ob Umbauten unter der MVO unter wirtschaftlichen Gesichtspunkten vertretbar bleiben.

Das tec.nicum unterstützt Hersteller und Betreiber bei der Umsetzung der Herausforderungen der neuen MVO, von der Beratung über Schulungen bis zu „schlüsselfertigen“ Maschinen oder Anlagen. So werden beispielsweise auch Turnkey-Projekte mit Umbaumaßnahmen begleitet oder im Rahmen eines GU-Auftrags komplett übernommen. ■

Jürgen Heimann
Dozent, omnicon engineering GmbH,
member of tec.nicum

Personelle Verstärkung für das tec.nicum

Die Serviceleistungen des tec.nicum werden immer stärker nachgefragt. Deshalb werden die personellen Kapazitäten ausgebaut. Zwei neue erfahrene Experten verstärken seit Anfang des Jahres das tec.nicum-Team.

Thilo Potthast ist seit dem 01.04.2023 neuer Mitarbeiter für die Projektbearbeitung in Wuppertal. Als staatlich geprüfter Techniker der Fachrichtung Elektrotechnik/Automatisierungstechnik verfügt Thilo Potthast über große Kompetenz bei der Erstellung von Steuerungsapplikationen und Visualisierungssystemen im Automatisierungsbereich. Auch Roboteranwendungen und deren Programmierung sowie die Umsetzung industrieller Prozesse gehören zu seinen beruflichen Erfahrungen.

Als Projektleiter im Maschinen- und Anlagenbau wird er seine Expertise im Bereich Solutions & Services einbringen und sein umfangreiches Wissen im neuen Aufgabengebiet der Maschinensicherheit vertiefen und anwenden.

Seit dem 01.07.2023 verstärkt **Matthias Wellandt** das Team des tec.nicum. Er verfügt über langjährige Erfahrung in der Konstruktion und Entwicklung sowie im Projektgeschäft. Als Diplom-Ingenieur mit der Fachrichtung Elektro- und Automatisierungstechnik konnte Matthias Wellandt bereits seit 2011 als Projektingenieur Erfahrungen auf dem Gebiet der funktionalen Sicherheit in der Nukleartechnik sammeln. In der Konstruktions- und Entwicklungsabteilung eines mittelständischen Maschinenbauunternehmens war er seit 2017 für elektrotechnische Produkte und Entwicklungen verantwortlich und erwarb 2019 die Qualifikation zum Functional Safety Engineer. Bei tec.nicum wird er seine Expertise bevorzugt in der Beratung einsetzen und auch den Bereich Solutions and Services sowie die tec.nicum academy unterstützen.

tec.nicum academy

Das Seminarprogramm 2024

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.

Sprechen Sie uns an:

Jasmin Ruda
Tel. +49 202 6474-804, jruda@tecnicum.com

Agnes de Castro
Tel. +49 202 6474 864, adecastro@tecnicum.com

Seminarthemen	Wuppertal	Ulm	Wettenberg	Hamburg	Online	Inhouse
Recht						
Maschinenrichtlinie 2006/42/EG – CE-Konformitäts-bewertungsverfahren	07.11.2024	auf Anfrage	18.03.2024	auf Anfrage	11.01.2024	auf Anfrage
Rechtliche Aspekte der Maschinensicherheit für Einkäufer, Konstrukteure, Projektkoordinatoren **(Halbtags-Seminar)**	24.10.2024	auf Anfrage	23.04.2024	auf Anfrage	08.02.2024	auf Anfrage
Grundlagen des Arbeitsschutzes für Führungskräfte	04.06.2024	auf Anfrage	22.03.2024	auf Anfrage	02.09.2024	auf Anfrage

Recht	Wuppertal	Ulm	Wettenberg	Lübeck	Online	Inhouse
Rechtliche Aspekte der Maschinensicherheit für Führungskräfte **(Halbtags-Seminar)**	27.02.2024	auf Anfrage	auf Anfrage	auf Anfrage	20.09.2024	auf Anfrage

(Fortsetzung auf Seite 22)

Seminarprogramm 2024 (Fortsetzung von Seite 21)

Seminarthemen	Wuppertal	Ulm	Wettenberg	Lübeck	Online	Inhouse
Normen – Verordnungen						
Gefährdungsbeurteilung zur Infektionsprävention	Termine auf Anfrage					
Risikobeurteilung und Betriebsanleitung	21.02.2024	auf Anfrage	19.03.2024	02.12.2024	07.10.2024	auf Anfrage
Validierung gemäß EN ISO 13849-2 **(Halbtags-Seminar)**	22.02.2024	auf Anfrage	25.04.2024	03.12.2024	–	auf Anfrage
Grundlagen der Betriebssicherheits-verordnung (BetrSichV)	13.06.2024	auf Anfrage	20.03.2024	auf Anfrage	25.11.2024	auf Anfrage
Gefährdungsbeurteilung für Maschinen und Anlagen	05.06.2024	auf Anfrage	19.04.2024	auf Anfrage	28.08.2024	auf Anfrage
Technische Dokumentation von Maschinen und Anlagen	auf Anfrage	auf Anfrage	21.03.2024	auf Anfrage	03.09.2024	auf Anfrage
Neubau, Umbau, Retrofitting – vom Hersteller zum Betreiber? **(Halbtags-Seminar)**	14.03.2024	auf Anfrage	24.04.2024	auf Anfrage	29.11.2024	auf Anfrage

Normen – Verordnungen	Wuppertal	Ulm	Wettenberg	Hamburg	Lübeck	Inhouse
Anwendung der EN ISO 13849-1 Einstieg in SISTEMA	19.06.2024	auf Anfrage	11.09.2024	20.11.2024	12.03.2024	auf Anfrage
Praxisworkshop Arbeiten mit SISTEMA **(Halbtags-Seminar)**	20.06.2024	auf Anfrage	12.09.2024	21.11.2024	13.03.2024	auf Anfrage

Normen – Verordnungen	Wuppertal	Ulm	Wettenberg	Hamburg	Online	Inhouse
NEU Anwendung der EN ISO 13849-1 Einstieg in SOFTEMA	29.02.2024	12.06.2024	04.12.2024	18.09.2024	–	auf Anfrage

Normen – Verordnungen	Wuppertal	Kirkel	Wettenberg	Lübeck	Inhouse
Qualifizierung zum TÜV-zertifizierten „Machinery CE Certified Expert® – mce.expert“	29.01.2024 bis 01.02.2024	08.04.2024 bis 11.04.2024	02.12.2024 bis 05.12.2024	auf Anfrage	auf Anfrage

Seminarprogramm 2024 (Fortsetzung von Seite 22)

Seminarthemen	Wuppertal	Ulm	Wettenberg	Lübeck	Online	Inhouse
Anwendung						
Grundlagen der Sicherheitstechnik – trennende und nicht trennende Schutzeinrichtungen	16.05.2024	auf Anfrage	25.09.2024	auf Anfrage	22.11.2024	auf Anfrage
Elektromagnetische Verträglichkeit EMV / EMVU in der Praxis	Termine auf Anfrage					
Sichere Fluidtechnik – EN ISO 13849-1 sicher umsetzen	Termine auf Anfrage					
Brandschutz im Maschinenbau	Termine auf Anfrage					
Fahrerlose Transportsysteme und ihre Integration in die Produktionsumgebung	10.09.2024	auf Anfrage	20.02.2024	auf Anfrage	auf Anfrage	auf Anfrage
Sicherheit in integrierten Roboterfertigungsanlagen	11.09.2024	auf Anfrage	21.02.2024	auf Anfrage	auf Anfrage	auf Anfrage
Mensch-Roboter-Kollaborationen	12.09.2024	auf Anfrage	22.02.2024	auf Anfrage	auf Anfrage	auf Anfrage
Anwendung	**Wuppertal**	**Ulm**	**Wettenberg**	**Bremen**	**Online**	**Inhouse**
Kompaktseminar Explosionsschutz	Termine auf Anfrage					
Anwendung	**Wuppertal**	**Ulm**	**Wettenberg**	**Lübeck**	**Online**	**Inhouse**
Sicherheitsgerichtete Auslegung von Batteriefertigungsanlagen	09.09.2024	auf Anfrage	19.02.2024	auf Anfrage	auf Anfrage	auf Anfrage
Produkte	**Wuppertal**	**Ulm**	**Wettenberg**	**Bremen**	**Online**	**Inhouse**
Basis-Workshop Sicherheitssteuerung PSC1	auf Anfrage	auf Anfrage	11.06.2024	auf Anfrage	auf Anfrage	auf Anfrage
Experten-Workshop Sicherheitssteuerung PSC1	auf Anfrage	auf Anfrage	12.06.2024	auf Anfrage	auf Anfrage	auf Anfrage
Produkte	**Wuppertal**		**Mühldorf**		**Inhouse**	
Grundlagen und Inspektion von optoelektronischen Schutzeinrichtungen gemäß BetrSichV **(Seminarziel: Befähigte Person)**	24.04.2024		26.09.2024		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
info-de@tecnicum.com
www.tecnicum.com