



# mrl.news

**Ausgabe 2025.02**

**Seite 2**

Editorial

**Seite 3**

Der Cyber Resilience Act und die neue EU-Maschinenverordnung

**Seite 6**

IO-Link Safety: Wegbereiter für die nächste Generation sicherer Maschinen

**Seite 10**

Marktzugang für Sicherheitsschaltgeräte in Südkorea: die KC-Zertifizierung

**Seite 11**

Tiepner GmbH: Maschinensicherheit im Sondermaschinenbau

**Seite 14**

Neue Sicherheitslichtvorhänge / -gitter mit ATEX-Zertifizierung

**Seite 15**

tec.nicum – excellence in safety

**Seite 17**

Das Seminarprogramm 2026 der tec.nicum academy



**mrl.news bleibt Ihr Kompass im Wandel – praxisnah, verständlich und zukunftsorientiert.**

**Liebe Leserinnen und Leser,**

**seit vielen Jahren erscheint die mrl.news als verlässliche Informationsquelle rund um die Maschinenrichtlinie, jenes zentrale Regelwerk, das die Sicherheit von Maschinen in Europa entscheidend geprägt hat. Doch wie das Umfeld, in dem Maschinen konstruiert, betrieben und vernetzt werden, entwickeln sich auch die entsprechenden Normen und gesetzlichen Grundlage kontinuierlich weiter.**

Im Jahr 2027 wird die bisherige Maschinenrichtlinie 2006/42/EG in der Praxis abgelöst durch die neue Maschinenverordnung, die Verordnung (EU) 2023/1230. Diese Änderung erscheint auf den ersten Blick formaler Natur, bedeutet in Wirklichkeit jedoch einen grundlegenden Wandel. Wie alle Verordnungen der EU wird die Maschinenverordnung direkt und einheitlich in allen Mitgliedstaaten der Europäischen Union gelten, ohne dass sie in nationales Recht umgesetzt werden muss.

Wir haben diskutiert, abgewogen, Alternativen geprüft. Und uns bewusst entschieden: mrl.news bleibt mrl.news. Denn dieser Titel steht für mehr als nur ein Akronym. Er

steht für Fachkompetenz, für Orientierung im Maschinenrecht, für ein Magazin, das seit Jahren verlässlich informiert, einordnet und Impulse gibt.

Die neue Maschinenverordnung bringt mehr Klarheit und Verbindlichkeit, eröffnet aber auch neue Herausforderungen, insbesondere im Hinblick auf digitale Sicherheitsaspekte, künstliche Intelligenz, Software und vernetzte Systeme.

Als Ihr Partner in allen Fragen der Maschinensicherheit begleiten wir Sie auch in dieser neuen Ära. In dieser und in den kommenden Ausgaben der mrl.news zeigen wir praxisnah, was sich für den Maschinenbau und die Komponentenhersteller ändert. Einen ersten Beitrag finden Sie dazu auf Seite 3.

Eines bleibt unverändert: Unser Ziel ist es, Wissen zu teilen, Orientierung zu geben und gemeinsam sichere Lösungen zu gestalten – für Menschen, Maschinen und die Zukunft.

Mit besten Grüßen  
Ihr mrl.news Redaktionsteam

# Rechtssicher in die Zukunft

## Der Cyber Resilience Act und die neue EU-Maschinenverordnung

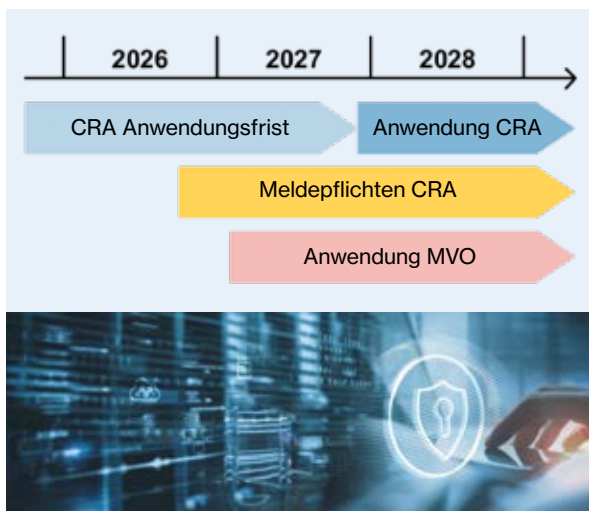
### Welche Anforderungen ergeben sich aus dem Cyber Resilience Act (CRA) und der neuen EU-Maschinenverordnung für den Maschinenbau und die Komponentenhersteller?

Die neue Maschinenverordnung (MVO), die ab 20. Januar 2027 rechtsverbindlich für alle EU-Staaten gilt, regelt unter anderem auch die Anforderungen für den Maschinenbau, die sich aus dem Cyber Resilience Act (CRA) der EU ergeben.

Der CRA, der am 10. Dezember 2024 in Kraft getreten ist, muss mit dem Stichtag 11. Dezember 2027 vollständig angewendet werden. Zusätzlich gibt es aber Meldepflichten für Schwachstellen und Cybervorfälle, die bereits am 11. September 2026 beginnen.

Ziel des CRA ist es, die Widerstandskraft der EU gegen Cyberattacken auf digitale Systeme, Produkte und Prozesse (Hard- und Software) zu erhöhen. Anlagen und Maschinen sowie die dazugehörigen wirtschaftlichen Prozesse sind schon heute vielfältigen Angriffen über lokale digitale Schnittstellen oder über IT-Netzwerke ausgesetzt. Diese Angriffe zielen im Maschinenbau häufig auf die Integrität und Verfügbarkeit von Produktionsprozessen und weniger auf das Abgreifen von Daten und Informationen aus diesen Prozessen.

Die funktionale Sicherheit von Maschinen und Anlagen ist in besonderer Weise verwundbar, weil Sicherheitssysteme bereits bei geringfügigen Beeinträchtigungen die Maschine in einen sicheren Zustand überführen müssen, d. h. die Maschine muss stillgesetzt werden. Deshalb sind die wirtschaftlichen Auswirkungen derartiger Cyberangriffe so gravierend.



### Pflichten der Hersteller

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

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

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

Zudem wird die Erstellung einer technischen Dokumentation für Hardware und Software gefordert sowie die Beachtung einer Sorgfaltspflicht bei der Integration von Komponenten, die von Dritten bezogen werden. Dies gilt selbstverständlich auch für Softwaremodule, die in Komponenten oder Maschinen integriert werden.

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

### Zum Schwachstellenmanagement zählen (Anhang I / Teil 2):

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

### Meldepflichten bei Sicherheitslücken

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



#### **Zu den Meldepflichten des Herstellers zählen (Artikel 14):**

- Meldung nach Kenntnis jeder aktiv ausgenutzten Sicherheitslücke oder jedes Vorfalls an ENISA & CSIRT
- Meldung mit Information und ggf. Abhilfemaßnahmen innerhalb von 72 Stunden
- Abschlussbericht zu ausgenutzten Sicherheitslücken und Vorfällen mit:
  - Beschreibung, Schweregrad und Auswirkungen der Attacke
  - Möglichen Ursachen und beteiligten Akteuren,
  - Sicherheitsupdates und Bereitstellung von Abhilfemaßnahmen für betroffene Nutzer

Die Meldepflicht tritt bereits 21 Monate nach dem Inkrafttreten der CRA-Verordnung, also im September 2026, in Kraft.

#### **Umsetzung der Anforderungen der Schutzziele und Definition der Security Level:**

Zur Umsetzung der Anforderungen kann der Maschinenbauer auf unterschiedliche Normenwerke zurückgreifen.

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

potenziellen Angreifern mit unterschiedlichem Wissen und Ressourcen an.

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

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

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

Für die Cyber-Security-Aspekte von Komponenten gibt es zusätzlich das Normungsvorhaben der IEC 63208. Der finale Entwurf (FDIS) dieser Norm liegt seit Mai 2025 vor, und mit der Verabschiedung wird spätestens Anfang 2026 gerechnet.

Die IEC 63208 greift die Systematik der IEC 62443 auf und erweitert die Cyber-Security-Anforderungen auf den Produktbereich der kommunikationsfähigen Niederspannungsschaltgeräte. →

### EU Cyber Resilience Act (CRA 2024/2847)

Inkrafttreten: 10.12.2024  
 Start Meldepflichten: 11.09.2026  
 Verbindliche Anwendung: 11.12.2027

### EU Maschinenverordnung (MVO 2023/1230)

Inkrafttreten: 19.07.2023  
 Verbindliche Anwendung: 20.01.2027

### IEC 62443 IT-Sicherheit für industrielle Automatisierungssystem (IACS)

Teil 3-3: IT-Systemanforderungen und Security Level  
 Teil 4-2: Technische Anforderungen an Komponenten  
 Stand: 2019 / 2020

### FDIS\_IEC 63208 Niederspannungsschaltgeräte & -steuerungen und ihre Komponenten – Security Aspekte

Stand: Finaler Entwurf 2025-05

EU-Verordnungen und Normen im Überblick

### Lösungsansätze für den Maschinenbau

Es ist hilfreich, im ersten Schritt ein Systemlayout der Maschine zu erstellen, um die Netzwerktopologie zu analysieren. Hierbei gilt es, sowohl den OT-Bereich der maschinennahen Feldbusssysteme als auch die Einbindung der Maschine in das IT-Netzwerk der Anlage und der Fertigungsstätte zu betrachten.

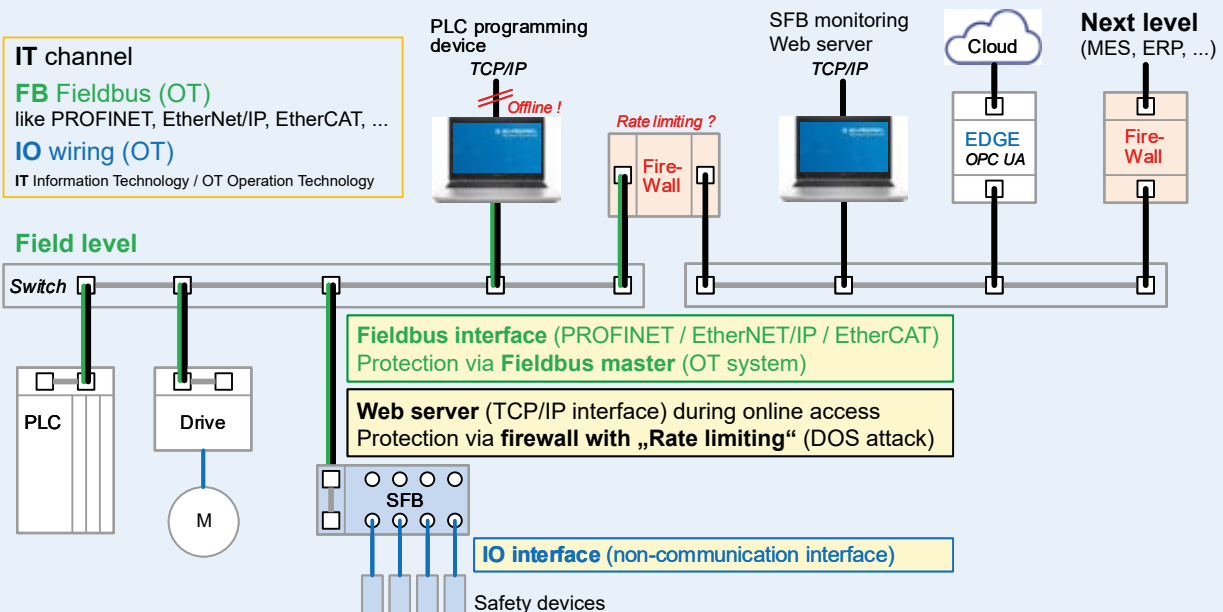
Meist ist es sinnvoll, die unterschiedlichen Netzwerkbereiche zu segmentieren und an den Übergängen mit Hilfe von Firewalls abzusichern. Zusätzlich sollten die Zugriffe auf den OT-Bereich über die IT-Schnittstellen zur Programmierung und zu Servicezwecken abgesichert werden und ggf. nur offline zulässig sein. ■

**Udo Weber**

Produktmanager Sicherheitstechnik der Schmersal Gruppe und Mitglied im DIN-Gemeinschaftsausschuss „Sicherheits-technische Grundsätze – Steuerungen“



### Systemlayout einer Maschine





Die ersten IO-Link-Safety-Produkte von Schmersal sind gegen Ende des ersten Halbjahres 2026 verfügbar: der Sicherheitssensor RSS362 (rechts) und die Sicherheitszuhaltung AZM42 (links) – weitere Produkte wie der IO-Link-Safety-Master und der Sensor RSS262 sind in der Entwicklung.

## Sichere Kommunikation in der Industrie 4.0 IO-Link Safety: Wegbereiter für die nächste Generation sicherer Maschinen

**Mit IO-Link Safety steht erstmals ein herstellerunabhängiges, standardisiertes Kommunikationssystem für funktionale Sicherheit zur Verfügung. Es erweitert die Möglichkeiten der Industrie 4.0 um eine sichere Punkt-zu-Punkt-Kommunikation zwischen Sensoren, Aktoren und Steuerungen.**

Im Gespräch erläutert Volker Heinzer, Strategischer Produktmanager bei der Schmersal-Gruppe, wie weit die Technologie ist, welche Chancen sie bietet und warum sie künftig eine Schlüsselrolle in der Maschinensicherheit spielen wird.



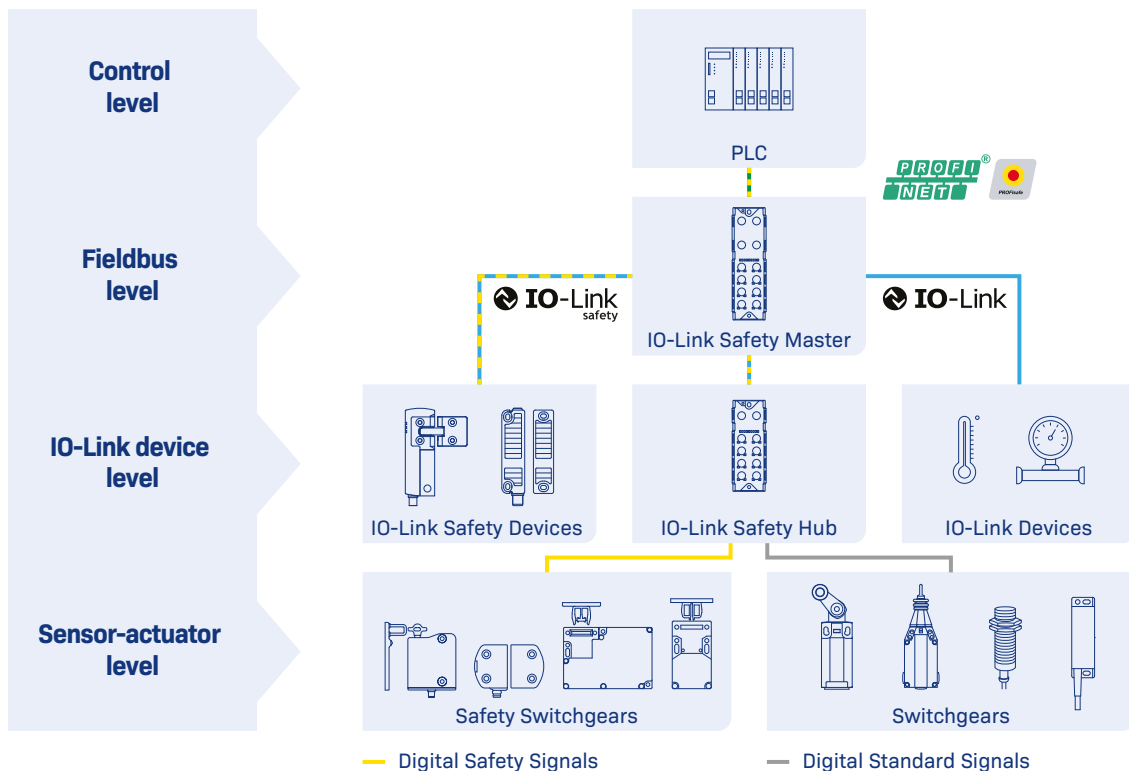
### Ein neuer Standard für Sicherheit und Kommunikation

IO-Link Safety baut auf der bewährten IO-Link-Technologie auf und überträgt deren Prinzipien auf den Bereich der funktionalen Sicherheit. Damit entsteht erstmals ein einheitlicher Standard auf der untersten Automatisierungsebene, der die Integration sicherheitsgerichteter Komponenten erleichtert. „IO-Link Safety ist für uns von großer Bedeutung, da es eine Schlüsseltechnolo-

gie für die Zukunft der Maschinensicherheit darstellt“, erklärt Volker Heinzer. In einer zunehmend vernetzten und automatisierten Industrie komme es darauf an, Sicherheitslösungen flexibel, skalierbar und datenfähig zu gestalten. Der entscheidende Vorteil: IO-Link Safety schafft Transparenz bis in die Feldebene. Sensoren und Aktoren können nicht nur sicherheitsrelevante Signale übermitteln, sondern auch zusätzliche Diagnosedaten und Parameter austauschen. Das eröffnet neue Möglichkeiten für Wartung, Zustandsüberwachung und Prozessoptimierung – ein echter Schritt in Richtung „Safety meets Smart Factory“.

### Normung und Standardisierung auf internationalem Niveau

Ein wichtiger Meilenstein war die Standardisierung von IO-Link Safety in der IEC 61139-2. Diese legt fest, dass das System höchste Sicherheitsanforderungen bis PL e (EN ISO 13849-1) bzw. SIL 3 (IEC 61508/62061) erfüllt. „Mit der Veröffentlichung der ersten Version der IO-Link Safety Extensions im Jahr 2017 wurde der Weg für herstellerübergreifende Sicherheitslösungen geebnet“, so Heinzer. Bis dahin war der Safety-Bereich stark von proprietären Schnittstellen geprägt. IO-Link Safety schafft →



Schematische Darstellung einer IO-Link Safety Systemarchitektur.

hier eine gemeinsame Basis, auf der Geräte unterschiedlicher Hersteller interoperabel zusammenarbeiten können. Das bedeutet: Anwender können künftig Sicherheitskomponenten verschiedener Anbieter flexibel kombinieren, ohne sich auf ein bestimmtes System festlegen zu müssen. Damit wird die Maschinensicherheit nicht nur effizienter, sondern auch wirtschaftlicher und zukunftsfähiger.

#### Mehrwert durch bidirektionale Kommunikation

Zu den zentralen Vorteilen von IO-Link Safety zählt die bidirektionale Kommunikation. Während herkömmliche Sicherheitsverbindungen meist nur einfache Signalübertragungen erlauben, ermöglicht IO-Link Safety einen beidseitigen Informationsaustausch. Das bedeutet: Steuerungen können nicht nur Daten von Sensoren empfangen, sondern auch Parameter, Befehle und Konfigurationen zurücksenden. „Das verbessert die Diagnosemöglichkeiten erheblich“, betont Heinzer. Durch die Kommunikationsfähigkeit der Sensoren und Aktoren eröffnen sich zudem neue Anwendungsfelder, etwa bei der vorausschauenden Instandhaltung oder der Prozessüberwachung. Ein weiterer praktischer Vorteil liegt im reduzierten Installationsaufwand. Statt achtadriger Leitungen reichen bei IO-Link Safety oft dreiadrige Standardkabel mit M12-Steckern aus. Das senkt Material- und Montagekosten, vermeidet Verdrahtungsfehler und beschleunigt die Inbetriebnahme. Das bedeutet einen spürbaren Effizienzgewinn für Maschinenbauer.

#### Integration in die Welt der Industrie 4.0

IO-Link Safety ist nicht nur eine Sicherheitslösung, es ist ein Schlüsselement der digitalen Transformation. Die Technologie fügt sich nahtlos in moderne Industrie-4.0-Umgebungen ein, in denen Daten über alle Ebenen hinweg gesammelt, analysiert und genutzt werden. „Die Möglichkeit, zusätzliche Informationen aus der Feldebene zu gewinnen, führt zu einer höheren Flexibilität und Transparenz in der Produktion“, sagt Heinzer. Damit werde IO-Link Safety zu einem Enabler für smarte, adaptive Fertigungsprozesse, die sich dynamisch an Produktionsanforderungen anpassen können.

#### Herausforderungen auf dem Weg zur Praxistauglichkeit

Neben den vielen Vorteilen sieht Heinzer auch Herausforderungen: „Wir müssen sicherstellen, dass das gesamte Ökosystem von IO-Link und IO-Link Safety interoperabel bleibt.“ Das betrifft sowohl die Geräteentwicklung als auch die Systemintegration. Die Implementierung erfordert ein tiefes Verständnis der Technologie und bringt zunächst zusätzliche Entwicklungsaufwände mit sich. Unternehmen, die bislang keine IO-Link-Erfahrung haben, müssen sich auf ein gewisses Umdenken einstellen. „Es kann anfangs zu höheren Initialkosten kommen“, räumt Heinzer ein, „doch diese amortisieren sich durch langfristige Einsparungen und Effizienzsteigerungen schnell.“ →

## Schmersal bringt die ersten IO-Link-Safety-Produkte auf den Markt

Eine erfreuliche Nachricht für alle Anwender: Schmersal wird in Kürze die ersten beiden IO-Link-Safety-Produkte vorstellen – die Sicherheitszuhaltung AZM42 und den Sicherheitssensor RSS362. Damit zählt das Unternehmen mit zu den Pionieren der IO-Link-Safety-Integration und unterstreicht seine führende Rolle in der funktionalen Sicherheit. Beide Geräte erweitern das IO-Link-Safety-Installationssystem von Schmersal für industrielle Sicherheitsanwendungen und bieten eine bidirektionale, sichere Kommunikation über eine 3-adrige Leitung. Damit lassen sich sichere Anwendungen bis Performance Level e, Kategorie 4 bzw. SIL 3 realisieren – bei zugleich hoher Flexibilität und einfacher Integration in bestehende Anlagen.

### AZM42: Sicherheitszuhaltung mit digitalem Mehrwert

Die Sicherheitszuhaltung AZM42 zählt bereits in ihrer ursprünglichen Version zu den besonders kompakten und leistungsfähigen Sicherheitslösungen für den Maschinenbau. In der neuen Variante konnten die Abstände bei Verwendung von zwei nebeneinander montierten Geräten noch einmal verkleinert werden und die Verriegelungs- und Zuhaltfunktion bis PL e, Kat. 4, SIL 3 befindet sich in einem Gerät. Die IO-Link-Safety-Schnittstelle erweitert die Zuhaltung um zahlreiche Industrie-4.0-Funktionen. Neben den bekannten Sicherheitsfunktionen bietet die AZM42 nun Status- und Diagnosedaten in Echtzeit, darunter Informationen über die Versorgungsspannung, die Temperatur und die Güte des RFID-Signals. Außerdem zählt das System Türöffnungs- und Verriegelungszyklen und erkennt zum Beispiel Abstandsüberschreitungen zwischen Sensor und Betätiger.



### RSS362: Sicherheitssensor mit intelligenter Diagnose

Mit dem RSS362 bringt Schmersal nun die IO-Link-Safety-fähige Variante des bereits erfolgreich eingeführten, berührungslosen, RFID-basierten Sicherheitssensors auf den Markt. Auch hier konnten die Abstände zwischen zwei Geräten deutlich verringert werden. Die bekannten Sicherheitsfunktionen stehen weiterhin im Mittelpunkt, ergänzt durch ein umfangreiches Paket an Diagnose- und Betriebsdaten. So liefert auch der RSS362 Informationen über die Anzahl der Schaltzyklen, Informationen über die Versorgungsspannung, die Temperatur und Güte des RFIS-Signals sowie zur Ausrichtung des Sensors zum Betätiger. Über die IO-Link-Safety-Kommunikation können diese Daten an die Steuerung übertragen und dort für vielfältigste Aufgaben, wie zum Beispiel für Predictive Maintenance, genutzt werden.



Wie der AZM42 unterstützt auch der RSS362 die bidirektionale sichere Kommunikation – die Steuerung kann also auch Konfigurationsdaten bzw. Parameter oder Befehle sicher an den Sensor senden. Damit lassen sich etwa neue Betätiger anlernen, ohne dass ein physischer Eingriff erforderlich ist. Dank der implementierten Data-Storage-Funktion können Gerätekonfigurationen bei beiden Geräten automatisch gespeichert und bei einem Austausch wiederhergestellt werden. Damit wird die Wartung deutlich vereinfacht. Die Offline-Konfiguration und -Parametrierung ermöglicht es zudem, Geräte bereits im Büro am PC vorzubereiten – ein echter Vorteil in der Instandhaltung und Serienfertigung.

**Heinzer: „Mit diesen beiden Produkten zeigen wir, dass IO-Link Safety nicht nur ein theoretisches Konzept ist, sondern bereits in der Praxis angekommen ist.“ →**



Neben den bekannten Sicherheitsfunktionen bietet die AZM42 nun Status- und Diagnosedaten in Echtzeit.

### Praxisnahe Anwendungen und Mehrwert für den Betreiber

Die Integration von IO-Link Safety in Sicherheitskomponenten eröffnet Betreibern und Maschinenbauern neue Möglichkeiten. Durch den Zugriff auf zusätzliche Daten lassen sich Wartungsintervalle dynamisch anpassen, Fehlerquellen schneller identifizieren und ungeplante Stillstände vermeiden. Darüber hinaus erleichtert IO-Link Safety die Standardisierung von Systemarchitekturen und die schnelle Inbetriebnahme. Durch den modularen Aufbau können Sicherheitslösungen künftig flexibler erweitert werden – ein entscheidender Vorteil angesichts immer komplexerer Produktionsumgebungen.

### Zukunftsperspektiven: IO-Link Safety als Industriestandard

Der Markt für IO-Link wächst rasant – inzwischen gehören dem IO-Link-Konsortium weltweit über 500 Unternehmen an, darunter viele führende Automatisierungsanbieter. „So wie IO-Link selbst in den letzten Jahren exponentiell an Bedeutung gewonnen hat, wird auch IO-Link Safety eine zentrale Rolle in der nächsten Generation von sicheren Maschinen und Anlagen spielen“, ist Heizer überzeugt. Für Schmersal bedeutet das: kontinuierliche Weiterentwicklung, enge Zusammenarbeit im IO-Link-Konsortium und konsequente Ausrichtung auf datenbasierte Sicherheitstechnologien. Mit der AZM42 und dem RSS362 wird das Unternehmen zu einem der ersten Anbieter, die IO-Link-Safety-fähige Geräte in Serie bringen – und setzt damit ein starkes Signal im Markt.



#### Fazit:

#### Sicherheit wird digital, vernetzt und intelligent

IO-Link Safety markiert einen Wendepunkt in der industriellen Sicherheitstechnik. Der standardisierte Kommunikationsweg verbindet Funktionalität und Sicherheit auf einer Plattform und schafft die Grundlage für intelligente, selbstüberwachende Systeme. Für Maschinenbauer und Betreiber ergeben sich daraus klare Vorteile: geringere Installationskosten, höhere Transparenz, schnellere Diagnose – und eine bislang unerreichte Flexibilität. „IO-Link Safety wird eine zentrale Rolle in der nächsten Generation von sicheren Maschinen und Anlagen spielen – und Schmersal wird ganz vorne mit dabei sein“, unterstreicht Heizer abschließend die unternehmerische Entschlossenheit, diesen technologischen Wandel aktiv mitzugestalten und innovative Sicherheitslösungen voranzutreiben. ■

**Volker Heizer**

Strategischer Produktmanager Industrielle Kommunikationssysteme und Industrie 4.0 bei der Schmersal-Gruppe

## Geprüfte Produktsicherheit

# Marktzugang für Sicherheitsschaltgeräte in Südkorea: die KC-Zertifizierung

Die **Korea Certification (KC)** ist ein zentrales Instrument zur Sicherstellung der Produktsicherheit in Südkorea. Sie ist dort für viele elektrische und elektronische Geräte verpflichtend. Auch für einige sicherheitsrelevante Produkte wie Not-Halt-Taster, Zuhaltungen, Sicherheitskontrolle oder Sicherheitsrelais ist die KC-Zertifizierung unter bestimmten Voraussetzungen verpflichtend und stellt sicher, dass Produkte nach koreanischen Standards sicher und zuverlässig funktionieren. Dabei leiten sich die anzuwendenden nationalen Vorschriften teilweise von den internationalen IEC-Normen ab. Es gibt jedoch bei den koreanischen Standards zum Teil Besonderheiten, die sich von den IEC-Bestimmungen abheben.

Verantwortlich für die Umsetzung ist die Korean Agency for Technology and Standards (KATS). Die KC-Zertifizierung wurde bereits 2009 eingeführt, mit dem Ziel, zahlreiche unterschiedliche Prüfzeichen in Südkorea unter einem einheitlichen System zusammenzufassen.

Für ausländische Hersteller gelten weitere besondere Anforderungen: Ein in Korea ansässiger Bevollmächtigter muss benannt werden, und einige technische Dokumente müssen in koreanischer Sprache vorliegen.

Im Einzelnen muss jeder Hersteller prüfen, welches Zertifizierungsschema für welche Produkte anzuwen-

den ist. Produkte, die eine KC-Zertifizierung besitzen, sind entsprechend zu kennzeichnen. Ergänzend zu dem Zertifizierungslabel „KC“ erhält jeder Hersteller eine Zertifikatsnummer, die ebenfalls auf dem Produkt anzubringen ist. ■

### Der Zertifizierungsprozess läuft wie im Folgenden beschrieben ab:

1. **Antragstellung** bei einer akkreditierten Prüfstelle in Korea.
2. **Einreichung der technischen Dokumentation**, z. B. Schaltpläne, Stücklisten, Risikoanalysen und Prüfberichte (CB-Schema-Berichte können teilweise anerkannt werden).
3. **Durchführung der Typprüfungen** in akkreditierten koreanischen Laboren.
4. **Erstinspektion der Fertigung** (bei Erstanträgen verpflichtend).
5. **Erteilung des Zertifikats** und Veröffentlichung in der KC-Datenbank.

**Dipl.-Ing. (FH) Jörg Eisold**

Head of Standards, Committees and Associations  
Work, K.A Schmersal GmbH & Co. KG



Das Logo für die KC-Zertifizierung.



**Die Herstellung von Werkzeugen und Sondermaschinen für die Verschweißung von Kunststoffen ist seit über 40 Jahren das Spezialgebiet der Tiepner GmbH.**

**Bild 1:** Die kompakte Anlage fertigt ID-Karten aus Schichtkunststoff, die u. a. als Kunden-, Ausweis- oder Scheckkarten genutzt werden. Links im Bild Christian Höltge, Geschäftsführer der Tiepner GmbH.

## Auf die richtige Karte gesetzt Maschinensicherheit im Sondermaschinenbau

Die Bediener der voll automatisierten (Sonder-)Maschinen von Tiepner sind immer bestens informiert sowohl über den Prozess als auch über den Betriebszustand im Sicherheitskreis. Dafür sorgen Schutztüren, die freie Sicht auf die jeweilige Station bieten, und – bei der neuesten Maschine – beleuchtete Türgriffe, die über die Farbe zum Beispiel anzeigen, ob die Tür zum Öffnen freigegeben ist. Eine Safety Fieldbox vereinfacht die Kommunikation im Sicherheitskreis der Maschine, die bis zu 15.000 Kunststoff-ID-Karten pro Stunde erzeugt. Damit setzt Tiepner zwei aktuelle Innovationen von Schmersal ein – und ist mit dem Ergebnis vollständig zufrieden.

Die Kunden der Tiepner GmbH in Dietfurt/Oberpfalz setzen keinesfalls alles auf eine Karte. Im Gegenteil: Mit einer einzigen Anlage von Tiepner produzieren bzw. verarbeiten sie pro Stunde eine fünfstellige Anzahl von Kunststoffkarten, die als ID-, Chip-, Ausweis-, Scheck- oder Kundenkarten universellen Einsatz finden und aus unterschiedlichen Kunststoffen – zumeist PVC oder Polycarbonat – bestehen.

### 15.000 ID-Karten pro Stunde

Kürzlich hat Tiepner eine solche Anlage projektiert, gebaut und ausgeliefert, die Karten im üblichen ID-Format voll automatisiert produziert (siehe Bild 1). Ausgangsmaterial sind laminierte Bögen, die der Anlage zugeführt werden. An unterschiedlichen Stationen werden die Bögen zunächst vereinzelt, dann ausgerichtet und ihre Stärke kontrolliert. Es folgt eine Station, die jeweils drei Karten mit normierten Abmessungen aus dem Grundkorpus ausstanzt. Die einzelnen Karten werden in einem

von mehreren Magazinen abgelegt. Auf diese Weise produziert die Anlage rund 15.000 Karten pro Stunde – mit oder ohne Chip, in Serie oder personalisiert.

Abgesehen von der Entnahme der Magazine arbeitet die Maschine selbsttätig, d. h., ohne dass ein Bediener im wahrsten Sinne des Wortes „eingreifen“ muss. Die Bediener haben freie Sicht auf jede einzelne Station, und die Schutztüren – mit großen Sichtfenstern – sind jeweils durch eine Sicherheitszuhaltung abgesichert.

### Neues Bediensystem

Dieses Konzept ist Standard bei allen Tiepner-Maschinen, ebenso die Tatsache, dass die Sicherheitsschaltgeräte und Bediengeräte an den Schutztüren bei Schmersal bezogen werden. Bei der hier vorgestellten, neuesten Anlage gehörte Tiepner zu den ersten Anwendern einer neuen Generation von Bediensystemen. Geschäftsführer Christian Höltge (siehe Bild 1): „Kurz bevor wir mit →

der Konstruktion dieser Sondermaschine begonnen haben, hatte Schmersal eine neue Türgriff-Baureihe vorgestellt mit beleuchteten Griffen, die den Betriebszustand der Maschine signalisieren. Weil wir großen Wert auf Transparenz an der Mensch-Maschine-Schnittstelle legen, hat uns diese Baureihe direkt gefallen. Sie passt gut in unser Bedienkonzept.“

### Türgriffe, die in verschiedenen Farben leuchten



**Bild 2:** Die Türgriffe des DHS-Systems leuchten großflächig in bis zu sieben Farben und zeigen damit den Betriebszustand der Schutztür an.

Bei der neuen Baureihe handelt es sich um das Türgriffsystem DHS (**Bild 2**), das die Funktionen eines robusten Türgriffs mit der Anzeige verschiedener Maschinenzustände kombiniert: Die Türgriffe leuchten großflächig in bis zu sieben Farben. Die Zuordnung von Farbe und Funktion kann der Anwender selbst konfigurieren. Tiepner nutzt das System unter anderem, um zu signalisieren, ob die Schutztür geöffnet werden kann. Und wenn die Steuerung eine Unregelmäßigkeit erkennt, wird farblich die Schutztür angezeigt, an welcher sie festgestellt wurde.

Zusätzlich ist jeder Türgriff der DHS-Serie mit einem Drucktaster ausgestattet, dessen Funktion ebenfalls frei belegt werden kann – zum Beispiel mit einer Reset-Funktion oder einer Anforderung zum Öffnen der Schutztür.

### Transparenz an der Schutztür

Aus Sicht des Anwenders vereinfacht das Türgriffsystem die Bedienung der Maschine. Der Anwender weiß, woran er ist – zum Beispiel in welcher Betriebsart (Einricht- oder Tippbetrieb) sich die Maschine gerade befindet. Er kann – so hat Tiepner das System konfiguriert – auch über den Drucktaster anfragen, ob die Sicherheitszuhaltung die Tür freigegeben hat, d. h. ob er sie öffnen kann. Damit erübrigt sich die Montage zusätzlicher Türgriffe und Leuchtmelder.

### Kombination mit kompakter Sicherheitszuhaltung

Das gesamte Türgriffsystem ist für die Integration in 40-mm-Profilssysteme ausgelegt – und es kann als Bau-

einheit mit der Sicherheitszuhaltung AZM40 verwendet werden. Genau diese Kombination nutzt Tiepner und kann damit die zentralen Funktionen der Maschinensicherheit und der Mensch-Maschine-Schnittstelle – Stel-



**Bild 3:** Die Türgriffe können als Baueinheit mit der kompakten Sicherheitszuhaltung AZM40 kombiniert werden.

lungsüberwachung der Schutztür, Verriegelung / Zuhaltung / Öffnen der Schutztür und Information über den Betriebszustand – in einer kompakten Einheit realisieren (**Bild 3**).

Mit diesem neuen System sind die Konstrukteure von Tiepner und auch die Anwender der ersten damit ausgerüsteten Maschine vollständig zufrieden. Christian Höltge: „Der Bediener ist immer bestens informiert: Kann die Schutztür geöffnet werden? An welcher Tür hat die Steuerung eine Unregelmäßigkeit erkannt? Das schafft Transparenz.“



**Bild 4 links:** Für zusätzliche Bedienfunktionen wird ein separates Bedienfeld aus der BDF 100-Serie von Schmersal genutzt (oben im Bild).

**Bild 5 rechts:** Der separate Not-Aus-Taster, ebenfalls aus der BDF 100-Serie, ist dort montiert, wo er im Blickfeld und im Notfall schnell erreichbar ist.

Für zusätzliche Bedienfunktionen wird ein separates, ebenfalls Bedienfeld aus der BDF 100-Serie von Schmersal genutzt (**Bild 4**). Die Serie BDF 100 umfasst eine Auswahl von Bedienfeldern für weitere Funktionen. Sie lassen sich mit geringem Aufwand dort installieren, wo sie im Bedarfsfall schnell erreichbar sind – auch als separater Not-Aus-Taster. (**Bild 5**). Außerdem sind sie sehr kompakt und passen perfekt an die 40-mm-Profile der Maschinenumhausung. →

**Bild 7:** Als Spezialist für die Produktion von Kunststoffkarten konstruiert und baut Tiepner auch komplexere Anlagen, die vorgelagerte Prozessschritte wie z. B. die Herstellung des aus bis zu acht Lagen bestehenden Schichtwerkstoffs übernehmen.



### Premiere für die Safety Fieldbox

Auf der Ebene der sicherheitsgerichteten Kommunikation setzt Tiepner – zum ersten Mal – die Safety Fieldbox von Schmersal ein (siehe Bild 6). Über die universellen Geräteschnittstellen für achtpolige M12-Stecker lassen sich u. a. elektronische und elektromechanische Sicher-



**Bild 6:** Die Safety Fieldbox vereinfacht die Integration von Sicherheitsschaltgeräten in den Sicherheitskreis

heitszuhaltungen, Sensoren, Bedienfelder, Lichtvorhänge oder Schalter in den Sicherheitskreis integrieren. Dabei benötigen Sicherheitszuhaltungen oder auch Sicherheitslichtgitter nur einen M12-Steckplatz.

Auch Bedienfelder mit Not-Halt-Funktion sowie bis zu drei nicht sichere Befehls- und Meldegeräte können direkt und ohne zusätzliche Hardware an einem Port der Safety Fieldbox angeschlossen werden. Über ein sicheres Ethernet-Protokoll werden die Daten an die Steuerung übermittelt. Damit wird für die Modularisierung der Sicherheitstechnik eine gute Grundlage geschaffen – auch aus wirtschaftlicher Sicht, denn diese universelle Geräteschnittstelle ist kostengünstiger als Einzelgeräte mit Busschnittstelle.

Bei größeren Anlagen können auch mehrere miteinander verbundene Feldboxen für eine Vereinfachung der sicherheitsgerichteten Kommunikation sorgen.

### Anschlussfertig mit konfektionierten Leitungen

Für Tiepner war die Montage der Sicherheitsschaltgeräte an dieser Anlage besonders einfach. Christian Höltge: „Wir haben bei der Bestellung die Leitungslängen angegeben, und Schmersal hat die konfektionierten Leitungen gleich mitgeliefert. Das hat nochmals Zeit gespart, und die Installation der Fieldbox selbst hat auch nur sehr wenig Aufwand erfordert.“

### Fazit: Komplettlösung für die Maschinensicherheit

Somit hat Tiepner bei der Konstruktion und Fertigung dieser Maschine mit der DHS-Serie auf eine Komplettlösung für die Maschinensicherheit gesetzt. Der Spezialist für die Herstellung von Kunststoff-ID-Karten setzt mit der DHS-Serie zudem eine Neuheit von Schmersal ein, die für Transparenz an der Schutztür sorgt, und die Safety Fieldbox vereinfacht die Kommunikation im Sicherheitskreis sowie die Installation der Sicherheitsschaltgeräte. ■

### Ein Spezialist für die ID-Karten-Fertigung

Die Tiepner GmbH projiziert und fertigt auch deutlich größere Anlagen als die hier beschriebene. Mit ihnen wird der Schichtwerkstoff erzeugt, aus dem die Karten gestanzt werden (siehe Bild 7). Bis zu acht Folien aus Polycarbonat oder PVC als Bogen- oder Rollenmaterial werden erst einzeln vollautomatisch bereitgelegt, ggfs. beschnitten und dann gestapelt. Kameras unterstützen die Stapelbildung, bei der es u. a. auch auf die exakte Ausrichtung der Bedruckung ankommt. Dann folgt das Ausstanzen der einzelnen Karten. Speziell für diesen Arbeitsgang fertigt Tiepner – wie hier beschrieben – auch separate und extrem kompakte Maschinen.

## Höchste Anforderungen

# NEUE SICHERHEITSLICHTVORHÄNGE / -GITTER MIT ATEX-ZERTIFIZIERUNG (FÜR ZONE 1 / 2G UND ZONE 21 / 2D)



Um Zugänge in explosionsgefährdeten Bereichen zuverlässig abzusichern, hat Schmersal das Programm an optoelektronischen Schutzeinrichtungen erweitert. Mit der neuen Baureihe EX-SLC/SLG440 stehen nun Sicherheitslichtvorhänge und -gitter in Ex-Ausführung zur Verfügung. Dadurch lassen sich höchste Sicherheitsstandards mit bewährter Qualität kombinieren.

In zahlreichen Fertigungsbereichen besteht eine erhöhte Explosionsgefahr, beispielsweise in der Chemieindustrie, in Raffinerien oder in Lackierereien, wo entzündbare – Beschichtungsstoffe verarbeitet werden. Auch in Branchen, in denen Schüttgüter verarbeitet werden – etwa in

der Futtermittel- oder Recyclingindustrie, in Sägewerken oder in Betrieben der Getreideverarbeitung – kann Staub zu einer Explosionsgefahr führen.

Für diese anspruchsvollen Einsatzbereiche wurden die Sicherheitslichtvorhänge und -gitter **SLC/SLG440** nun auch in Ex-Ausführung entwickelt. Die optoelektronischen Schutzeinrichtungen können in besonders explosionsgefährdeten Gas- und Staub-Atmosphären der Zonen **1 und 21** zur Absicherung von Gefahrstellen eingesetzt werden.

### Sicherheitslichtvorhänge EX-SLC440 zur Finger-, Hand- und Körpererkennung

- ATEX-zertifiziert für 2G / D, Zone 1 / 21
- Finger- und Handschutz mit Auflösung 14 mm und 30 mm
- Körperschutz für Gliedmaßen mit 2 bis 4 Strahlen
- Reichweiten: 0,3 bis 20 m
- Staubdicht
- Geeignet für den Einsatz im Außenbereich
- Schutzgehäuse mit Metallkappen
- Einfache Installation und Handhabung mit geringem Gewicht ■



Broschüre bestellen oder online einsehen



## ATEX CATEGORY

Zone 1 Gas	Zone 21 Dust	Zone 2 Gas	Zone 22 Dust
2G	2D	3G	3D
✓	✓	✓	✓



## excellence in safety

tec.nicum ist in der Schmersal Gruppe der Geschäftsbereich für Lösungen und Dienstleistungen, die im Kontext mit der Maschinen-, Anlagen- und Arbeitssicherheit stehen.

2024 hat Schmersal sein Dienstleistungsgeschäft neu strukturiert. Das Angebot an Safety Services des tec.nicum wurde deutlich erweitert – vor allem im Hinblick auf Digitalisierung und Komplettlösungen für die Maschinensicherheit – und die globalen Aktivitäten und Kompetenzen wurden stärker integriert.

Im April 2024 gründete Schmersal die tec.nicum – Solutions & Services GmbH als neue Tochtergesellschaft, in die auch die omnicon engineering GmbH eingegliedert wurde, die Schmersal bereits 2019 erworben hatte. Der Sitz der neuen Tochtergesellschaft befindet sich in Kirkel-Limbach, Deutschland.

Die vier Säulen, auf denen das Angebot von tec.nicum bisher aufgebaut war – academy, consulting, engineering und integration – wurden um zwei weitere ergänzt: digitalisation und outsourcing.

**digitalisation:** tec.nicum bietet verstärkt neuentwickelte Software-Lösungen an, wie beispielsweise ein neues Tool zur Durchführung von Risikobeurteilungen, aber auch neue digitale Technologien wie etwa Cloud-Lösungen, IIoT-Anwendungen, digitalisierte Lockout-Tagout-Verfahren oder Instrumente für das Energiemanagement.

**outsourcing:** tec.nicum bietet den Anwendern die Möglichkeit, alle Aufgaben im Zusammenhang mit der Maschinensicherheit komplett auszulagern, von der Konzeption von Sicherheitslösungen bis hin zur Planung und Installation von Schaltschränken. tec.nicum stellt dem Anwender bei Bedarf anschlussfertige Plug-and-Play-Produkte zur Verfügung.

Die Dienstleistungen von tec.nicum sind dank des weltweiten Beratungsnetzwerks rund um den Globus verfügbar. tec.nicum berät Kunden kompetent, produkt- und herstellerneutral und unterstützt sie bei der sicherheitstechnischen Gestaltung ihrer Maschinen und Produktionslinien.

**tec.nicum**  
Schmersal Group

**tec.nicum – Solutions & Services GmbH**  
**Standort Kirkel**

Friedrichstraße 65  
66459 Kirkel-Limbach

Telefon: +49 6841 77780-0  
E-Mail: [europa@tecnicum.com](mailto:europa@tecnicum.com)  
Web: [www.tecnicum.com](http://www.tecnicum.com)

**tec.nicum – Solutions & Services GmbH**  
**Standort Wuppertal**



Möddinghofe 30  
42279 Wuppertal

Telefon: +49 202 6474-932  
E-Mail: [europa@tecnicum.com](mailto:europa@tecnicum.com)  
Web: [www.tecnicum.com](http://www.tecnicum.com)





Das Dienstleistungsangebot von tec.nicum umfasst sechs Bereiche: **academy (Wissenstransfer), consulting (Beratung), engineering (technische Planung), integration (Ausführung und Implementierung), digitalisation (Softwarelösungen und neue digitale Technologien) und outsourcing (Komplettlösungen).**

<p><b>academy</b> </p> <p><b>Weiterbildungszentrum</b></p> <ul style="list-style-type: none"> <li>■ Schulungen</li> <li>■ Kundenspezifische Workshops</li> <li>■ Inhouse-Trainings</li> <li>■ Zertifizierte Kurse (mce.expert und FSE)</li> </ul>	<p><b>consulting</b> </p> <p><b>Analyse und Dokumentation</b></p> <ul style="list-style-type: none"> <li>■ Technische Unterstützung</li> <li>■ Risikobeurteilungen</li> <li>■ CE-Konformitätsbewertung</li> <li>■ Bewertungen von Maschinen und Produktionslinien</li> <li>■ Technische Dokumentationen</li> </ul>
<p><b>engineering</b> </p> <p><b>Planung und Konstruktion</b></p> <ul style="list-style-type: none"> <li>■ Technische Projektierungen</li> <li>■ Konzeptionelle Projektentwicklung</li> <li>■ Elektronische und mechanische Konstruktion</li> <li>■ Projektmanagement</li> </ul>	<p><b>integration</b> </p> <p><b>Praktische Anwendung</b></p> <ul style="list-style-type: none"> <li>■ Turnkey-Lösungen</li> <li>■ Installation</li> <li>■ Retrofit</li> </ul>
<p><b>digitalisation</b> </p> <p><b>Software-Integration</b></p> <ul style="list-style-type: none"> <li>■ tec.<b>ps</b> (Product Service System)</li> <li>■ tec.<b>ssm</b> (Schmersal Smart Machine)</li> <li>■ tec.<b>cvs</b> (AI and Computational Vision Solutions)</li> <li>■ tec.<b>dloto</b> (Digital Lockout Tagout)</li> <li>■ tec.<b>ems</b> (Energy Monitoring System)</li> </ul>	<p><b>outsourcing</b> </p> <p><b>Serielle Lösungen</b></p> <ul style="list-style-type: none"> <li>■ Plug-and-Play-Produkte</li> <li>■ Engineer-to-Order-Projekte</li> <li>■ Systeme und Schaltschränke</li> </ul>

**tec.nicum**

# tec.nicum academy

## Das Seminarprogramm 2026

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

Besuchen Sie uns unter [www.technikum.com](http://www.technikum.com) und finden Sie aktuelle Detailinformationen und Buchungsoptionen zu allen Seminaren und Sonderveranstaltungen.

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

Wir beraten Sie gerne persönlich.  
Sprechen Sie uns an:

**Tobias Keller**  
**Head of Administration**  
Tel. +49 202 6474 897  
[tkeller@schmersal.com](mailto:tkeller@schmersal.com)



Seminarthemen	Wuppertal	Wettenberg	Kirkel	Online	Inhouse
<b>Recht</b>					
Maschinenverordnung 2023/1230 (Kompaktseminar) <span style="float: right;">NEU</span>	23.04.2026 19.11.2026	21.05.2026	12.02.2026 23.11.2026	auf Anfrage	auf Anfrage
Maschinenverordnung 2023/1230 (Intensivseminar – 2-Tages-Seminar) <span style="float: right;">NEU</span>	16.-17.06.2026 20.-21.10.2026	10.-11.03.2026	16.-17.03.2026 31.08.- 01.09.2026	auf Anfrage	auf Anfrage
Grundlagen des Arbeitsschutzes für Führungskräfte	22.10.2026	20.05.2026	07.05.2026	auf Anfrage	auf Anfrage
Rechtliche Aspekte der Maschinensicherheit für Führungskräfte (1/2-Tages-Seminar)	-	-	-	auf Anfrage	auf Anfrage

**tec.nicum**

(Fortsetzung auf Seite 18)

## Seminarprogramm 2026 (Fortsetzung von Seite 17)

Seminarthemen	Wuppertal	Wettenberg	Kirkel	Online	Inhouse
<b>Normen – Verordnungen</b>					
Risikobeurteilung gemäß EN ISO 12100	15.01.2026	25.08.2026	04.05.2026	auf Anfrage	auf Anfrage
Gefährdungsbeurteilung für Maschinen und Anlagen gemäß Betriebs-sicherheitsverordnung	23.06.2026	13.10.2026	18.03.2026 24.11.2026	auf Anfrage	auf Anfrage
Technische Dokumenta-tion / Betriebsanleitung	21.-22.07.2026	14.-15.10.2026	09.-10.02.2026	auf Anfrage	auf Anfrage
Anwendung der EN ISO 13849-1 und Einstieg in SOFTEMA	–	–	–	auf Anfrage	auf Anfrage
Anwendung der EN ISO 13849-1 und Einstieg in SISTEMA und die Validierung	07.10.2026	11.02.2026	06.05.2026	auf Anfrage	auf Anfrage
Elektrische Ausrüs-tung von Maschinen gemäß EN 60204-1 (VDE 0113-1) <b>(2 Tage)</b> <span style="background-color: #0070c0; color: white; padding: 2px;">NEU</span>	11.-12.08.2026	–	03.-04.03.2026	auf Anfrage	auf Anfrage

Seminarthemen	Wuppertal	Wettenberg	Kirkel	Online	Inhouse
<b>Qualifizierungskurse mit besonderem Abschluss</b>					
Qualifizierung zum TÜV zertifizierten „Machinery CE Certified Expert® – mce.expert“	27.-30.10.2026	27.-30.01.2026	13.-16.07.2026	–	auf Anfrage
Grundlehrgang Sicherheitsbeauftragte(r) <b>(2 Tage)</b>	08.-09.06.2026	04.-05.08.2026	30.06.-01.07.2026	–	auf Anfrage



**Seminarprogramm 2026** (Fortsetzung von Seite 18)

Seminarthemen	Wuppertal	Wettenberg	Kirkel	Online	Inhouse
<b>Anwendung</b>					
Grundlagen der Sicherheitstechnik – trennende und nicht trennende Schutzeinrichtungen	in Planung (i.P.)	i.P.	i.P.	auf Anfrage	auf Anfrage
Sicherheitsgerichtete Auslegung von Batteriefertigungsanlagen	i.P.	i.P.	i.P.	auf Anfrage	auf Anfrage
Fahrerlose Transportsysteme und ihre Integration in die Produktionsumgebung	i.P.	i.P.	i.P.	auf Anfrage	auf Anfrage
Sicherheit in integrierten Roboterfertigungsanlagen	i.P.	i.P.	i.P.	auf Anfrage	auf Anfrage
Mensch-Roboter-Kollaborationen	i.P.	i.P.	i.P.	auf Anfrage	auf Anfrage
Elektrotechnisch unterwiesene Person (EUP)	23.07.2026	–	11.02.2026	auf Anfrage	auf Anfrage
Lockout / Tagout (LOTO)	24.06.2026	12.03.2026	05.05.2026	auf Anfrage	auf Anfrage
Befähigung Kranführer (flurgesteuerte Krane)	–	–	–	–	auf Anfrage
Sicherer Umbau von Maschinen und Anlagen	18.06.2026	19.05.2026	02.07.2026	auf Anfrage	auf Anfrage
Psychische Gesundheit am Arbeitsplatz	26.08.2026	–	24.02.2026	auf Anfrage	auf Anfrage

Seminarthemen	Wuppertal	Wettenberg	Kirkel	Online	Inhouse
<b>Produkte</b>					
Grundlagen und Inspektion von opto-elektronischen Schutzeinrichtungen gemäß BetrSichV (Seminarziel: Befähigte Person)	i.P.	i.P.	i.P.	i.P.	i.P.

(Stand November 2025)

Weitere Seminartermine folgen. Die aktuelle Übersicht finden Sie unter [www.tecnicum.com/academy](http://www.tecnicum.com/academy)

Fotos: K.A. Schmersal GmbH & Co. KG (shutterstock.com,  
Annette Kradisch, Fotografin für Anwenderbericht Tiepner

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

Die bei der Produktion dieser Broschüre entstandenen Treib-  
hausgasemissionen 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