

# Auswirkung der neuen gesetzlichen und normativen Regelungen auf Industrieroboter-Systeme

V. Malisa<sup>1</sup>, J. Reiff-Stephan<sup>2</sup>

## Zusammenfassung

EU-Verordnungen und ISO-Normen verändern die Nutzung von Industrierobotern und beeinflussen deren Integration in effiziente Produktionssysteme. Die rasante Entwicklung der Digitalisierung und die Notwendigkeit einer umfassenden Vernetzung haben Auswirkungen auf die Sicherheit von Maschinen, die Gestaltung von Arbeitsplätzen und die Anforderungen an die Ausbildung der Beschäftigten. Mit einer Reihe von Gesetzen und Richtlinien schafft die EU einen Ordnungsrahmen für die aktuellen Technologien und versucht, die Rahmenbedingungen für weitere Entwicklungen festzulegen. Gleichzeitig ist die Industrie gefordert, zusätzliche Kompetenzen in bestimmten Bereichen der Digitalisierung aufzubauen. Einige Herausforderungen sind jedoch noch zu bewältigen, z. B. wie der Sicherheitsnachweis für in Maschinen integrierte Künstliche Intelligenz für autonome mobile Roboter erbracht werden kann, wie die Zertifizierung von Software als Sicherheitselement und dessen Integration in die Automatisierungssysteme und wie die Behandlung von Industrierobotern als vollständige und nicht mehr als unvollständige Maschinen erfolgen wird.

## Stichwörter

Industrieroboter, EU-Maschinenverordnung, Normungen, kollaborierende Anwendungen

## 1 Einleitung

Die industrielle Produktion befindet sich in einer Phase des tiefgreifenden Wandels, der durch die sogenannte Zwillingstransformation geprägt ist [1]. Diese umfasst sowohl die Digitalisierung als auch den ressourcenschonenden Umgang mit Produktionsmitteln, die als zentrale Herausforderungen für eine zukunftsfähige und effiziente Produktion betrachtet werden. Ein entscheidender Aspekt ist die Integration von Menschen und Maschinen in gemeinsamen Arbeitsumgebungen, um Synergien zwischen menschlicher Expertise und maschineller Präzision zu schaffen [2]. Insbesondere die Robotik übernimmt dabei eine Schlüsselrolle, da sie nicht nur die Effizienz und Flexibilität der Produktion steigert, sondern sich gleichzeitig an neue gesetzliche Normen und regulatorische Rahmenbedingungen anpassen muss, die diesen Wandel begleiten.

Im Rahmen dieser Arbeit werden Komponenten zur Umsetzung der neuen Verordnungen auf Industrierobotern zusammengefasst. Die seit langem überfällige Überarbeitung der Roboternormen ISO 10218 Teil 1 und Teil 2 steht kurz vor der Veröffentlichung. Im Rahmen der Überarbeitung wurden insbesondere die Aspekte der Mensch-Roboter-Kollaboration (MRK) und des Fernzugriffs auf die Robotersteuerung neu definiert. Die geänderte Definition der "unvollständigen Maschine" hat

---

<sup>1</sup> V. Malisa, F-AR Förderung der Automation und Robotik, Wien, Österreich

<sup>2</sup> J. Reiff-Stephan, TH Wildau, FG: iC3@Smart Production, Wildau, Deutschland

Auswirkungen auf die Behandlung von Industrierobotern und nachfolgend von Robotersystemen. Im Folgenden werden Systeme mit integrierten Robotern als "Roboteranwendungen" gemäß den neuen Roboternormen bezeichnet.

Die EU-Maschinenverordnung 2023/1230 (EU-MVO) [3], die auf die Digitalisierungszeitalter angepasst wurde und die ab dem 20. Januar 2027 rechtlich bindend wird, verändert die Herstellung und den Betrieb von Maschinen. Die neue EU-MVO wird die bis dahin gültige Maschinenrichtlinie 2006/42/EG (EU-MRL) [7] ablösen. Folglich müssen die grundlegenden Sicherheits- und Gesundheitsschutzanforderungen sowie die Konformitätsbewertungsverfahren für alle Akteure in allen EU-Ländern einheitlich Anwendung finden. Eine abweichende Umsetzung, wie sie derzeit bei der Maschinenrichtlinie erfolgt, ist somit nicht zulässig.

Neu ist auch, dass es zwischen neuen und alten Regelungen keine Übergangsfrist gibt, sondern die MRL bis zum 19. Januar 2027 gültig bleibt und ab dem 20. Januar 2027 die neue EU-MVO von den Herstellern der Maschinen und unvollständigen Maschinen berücksichtigt werden muss.

## 2 Normative Regelungen

Es ist vorgesehen, dass die überarbeiteten Fassungen der Roboternormen ISO 10218-1 und ISO 10218-2, welche auf Basis der noch gültigen Maschinenrichtlinie erarbeitet wurden, Anfang des Jahres 2025 veröffentlicht werden. Die neue Norm ISO 10218-2 fasst die bisherige ISO 10218-2 und die ISO/TS 15066 für kollaborierende Roboteranwendungen zusammen. Der Begriff "Cobot", abgeleitet aus dem Englischen für "**collaborating robot**", füllte im letzten Jahrzehnt die technischen Fachzeitschriften und vermittelte den Eindruck eines sicheren Industrieroboters, den man einfach kaufen und ohne systemabhängige Sicherheitskomponenten sicher betreiben kann. Die kommenden Roboternormen nach ISO FDIS 10218-1/-2:2024 [5][6] sprechen nur noch von "kollaborierenden Anwendungen", da nur eine Anwendung entwickelt, verifiziert und validiert werden kann. Die für die Anwendungen erforderlichen Sicherheitselemente werden entweder im Roboter integriert, extern angebracht oder als Kombination aus beidem realisiert. Der missverständliche Begriff "kollaborierender Roboter" wird daher in den Normen nicht mehr verwendet. Auch der „kollaborierende Betrieb“ wird in den Roboternormen nicht behandelt. Ebenso wird der kollaborierende Raum als Raum, in dem sich Roboter und Bediener gleichzeitig befinden, definiert und in den Roboternormen behandelt (siehe Bild 1).

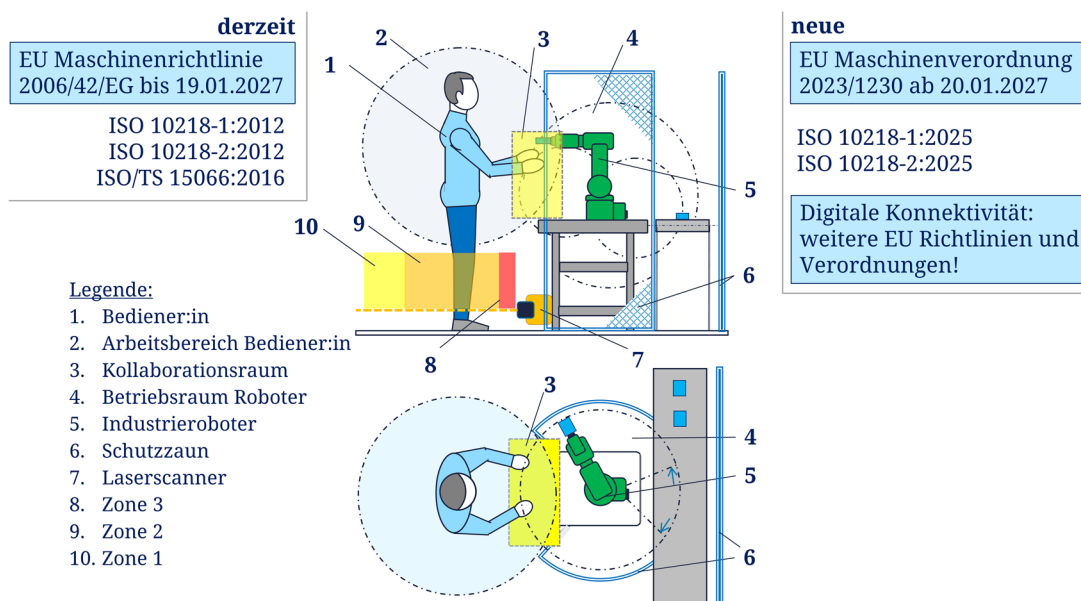


Bild 1: Überblick der Regelungen für MRK derzeit und zukünftig, [nach [4]]

## Klassifizierung von Industrieroboter

In den ISO 10218 wurden Industrieroboter in zwei Klassen aufgeteilt:

„Roboter der Klasse I ...- Die Masse pro Manipulator darf höchstens 10 kg; die maximal erreichbare Geschwindigkeit darf höchstens 250 mm/s; und die maximale Kraft pro Manipulator... darf höchstens 50 N betragen.“ [5]. Alle anderen Industrieroboter mit darüber liegenden Werten fallen in die Klasse II.

Obwohl für diesen Robotertyp die Masse des Manipulators, Geschwindigkeit und Kraft beschränkt ist, kann es auch bei diesen Werten zu bedeutenden Unfällen kommen. Es ist daher ebenso darauf zu achten, bei diesen Roboterzellen die Risikobeurteilung sorgfältig umzusetzen.

Für Roboter der Klasse I gelte wesentlich geringere Anforderungen an die Sicherheitsfunktionen, [11] jedoch müssen bei Anwendungen mit scharfkantigen Werkstücken die gleichen Sicherheitsmaßnahmen wie bei Robotern der Klasse II angewendet werden. Die Versuche Industrieroboter zu klassifizieren gab es zuletzt bei der Einführung von kollaborierenden Anwendungen, für welche die Grenze bis zu einer maximalen Kraft von 70 N im Gespräch war.

## Roboter Programmierung

„Das Programmierhandgerät kann mit dem Endeffektor und anderen Teilen des Robotersystems verbunden werden.“ [5] Beispielsweise kann eine 6D-Maus, die zur Führung des Roboters an der fünften Achse angebracht ist, zur manuellen Führung des Roboters in schwer zugänglichen Bereichen verwendet werden. Mit einem am Endeffektor angebrachten Handgriff kann ein Lackierer die Bewegungen eines Lackierroboters programmieren.

## Fernzugriff auf Robotersteuerung

Die Bezeichnung "Remote Control" wird durch den Begriff "Externe Steuerung" ersetzt, welcher in der Regel als neuer Schalter in der Robotersteuerung integriert wird. Die Funktion "Extern Ein/Extern Aus" erlaubt beispielsweise die Durchführung von Fernwartungsmaßnahmen oder die Programmierung des Roboters über einen externen Personal Computer. Es ist jedoch nach wie vor sicherzustellen, dass zu jedem Zeitpunkt lediglich eine Steuerung – sei es direkt oder extern – für die Steuerung des Roboters zuständig ist (siehe Bild 2).

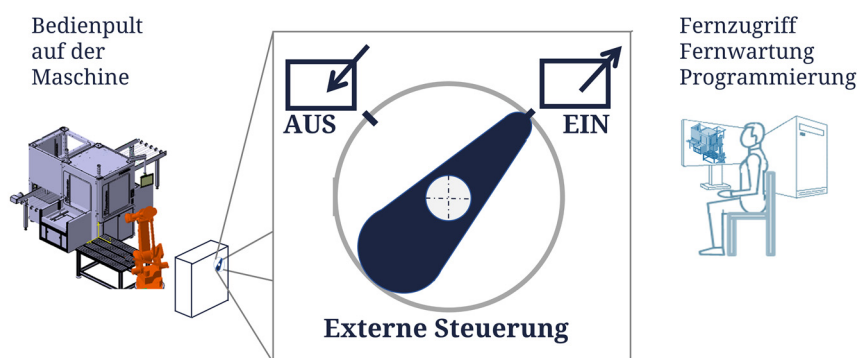


Bild 2: Schalter Externe Steuerung - EIN oder - AUS

In der Betriebsanleitung sind die Betriebsverfahren für den Fernzugriff festzulegen, die vom Fernwartungspersonal und vom Betriebspersonal vor Ort zu befolgen sind. Um das Verfahren in der Organisation zu etablieren, empfiehlt es sich, regelmäßige halbjährliche Übungen durchzuführen, in denen das beteiligte Personal die Rollen übt und die Kommunikation zwischen den Abteilungen getestet wird. Darüber hinaus ist es erforderlich, die für den Fernzugriff benötigte Technik und Software regelmäßig zu testen, um im Bedarfsfall die Fernwartung erfolgreich durchführen zu können [4].

### Präzisierung bei funktionaler Sicherheit

Wenn die Bewegung gestoppt wurde und der Antrieb noch aktiv ist, muss der Stillstand des Roboters überwacht werden. Beispielsweise kann bei einer MRK-Anwendung der Mensch den Arbeitsbereich des Roboters betreten und der Roboter stoppt. In diesem Fall spricht man von sicherheitsgerichtetem, überwachtem Stillstand. Andererseits ist die Geschwindigkeit im Kollaborationsraum, in dem sich Mensch und Roboter gleichzeitig aufhalten, häufig auf einen konfigurierten Wert begrenzt. Auch diese begrenzte Geschwindigkeit muss überwacht werden. In dem manuellen Betrieb wird die Geschwindigkeit des Industrieroboters auf 250 mm/s begrenzt und ebenfalls sicherheitsgerichtet überwacht.

### Cybersicherheit

Die Roboternormen definieren spezifische Anforderungen an die Cybersicherheit, um sicherzustellen, dass die Roboteranwendungen gegen Cyberangriffe geschützt sind. Dies umfasst Maßnahmen zur Authentifizierung, Zugangskontrolle und Datenintegrität. Die ISO/TR 22100-4:2018 [8] bietet Maschinenherstellern Leitlinien zur Berücksichtigung von IT-Sicherheitsaspekten (Cybersicherheit) in Bezug auf die Maschinensicherheit. Die vorliegende Norm verfolgt das Ziel, potenzielle IT-Sicherheitsbedrohungen zu identifizieren und zu bewältigen, welche die Sicherheit von Maschinen, einschließlich Robotern, beeinträchtigen können. Hersteller sind demnach verpflichtet, sicherzustellen, dass Maschinen während ihrer gesamten Lebensdauer sicher bleiben. Dazu gehört die Bereitstellung von Software-Updates, um Sicherheitslücken zu schließen und neue Bedrohungen abzuwehren [10].

Wenn die Beurteilung der Cybersicherheit ergibt, dass durch unbefugten Zugriff auf die Steuerung Sicherheitsrisiken entstehen, müssen geeignete Schutzmaßnahmen getroffen werden. Im Teil 1 werden vom Hersteller des Roboters entsprechende Maßnahmen gefordert und gelistet. Teil 1 verweist für weitere Informationen und Anforderungen auf die Normenreihe IEC 62443 „IT-Sicherheit für industrielle Automatisierungssysteme“ [9]. Grundsätzlich gilt als vernünftige Annahme die Sicherheitsstufe 2 nach IEC 62443 für Teile der Steuerung, die die Sicherheit beeinträchtigen können (Start, Stopp, Änderung der Sicherheitseinstellungen usw.), und die Sicherheitsstufe 1 für andere Teile.

In der IEC 62443 werden Sicherheitsstufen wie folgt definiert:

- SL 1: Schutz gegen beiläufige oder zufällige Verstöße.
- SL 2: Schutz gegen absichtliche Verstöße mit einfachen Mitteln und geringem Aufwand.
- SL 3: Schutz gegen absichtliche Verstöße mit hochentwickelten Mitteln und mittlerem Aufwand.
- SL 4: Schutz gegen absichtliche Verstöße mit hochentwickelten Mitteln und erheblichem Aufwand.

## 3 Umsetzung in der EU-MVO

### 3.1 Einordnung

In der Fachpresse wird der Unterschied zwischen der derzeit gültigen EU-MRL und der neuen EU-MVO pointiert wie folgt diskutiert: Bei der EU-MRL ging es um den Schutz des Menschen vor der Maschine, jetzt bei der EU-MVO muss die Maschine vor dem Menschen geschützt werden, was nur bedingt zutrifft. Denn im Zeitalter von Industrie 4.0 und IoT (Internet of Things) bilden immer mehr Maschinen, PCs, Server, Software, Künstliche Intelligenz, KI-Agenten, Bots ein komplexes System, in dem Cyberkriminalität, vorsätzliche und automatisierte Angriffe von Privatpersonen und Unternehmen weltweit ständig stattfinden. Bild 3 versucht, die miteinander verbundenen Akteure, die die Sicherheit einer Maschine beeinflussen können, grafisch darzustellen.

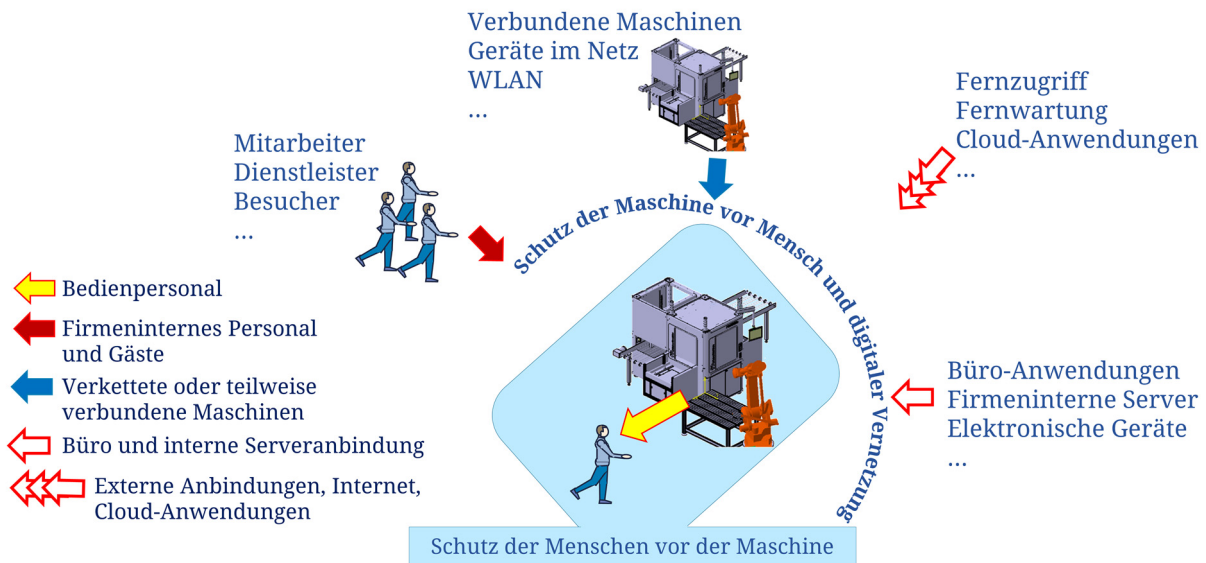


Bild 3: Digitale Konnektivität (Security) der Roboteranwendung beeinflusst Maschinensicherheit (Safety)

### Bedienpersonal

Der Begriff "Bediener" im Sinne der EU-MVO bezeichnet die Person bzw. die Personen, die für die Installation, den Betrieb, die Einrichtung, die Wartung, die Reinigung, die Reparatur oder den Transport von Maschinen oder dazugehörigen Produkten zuständig sind. Es kann angenommen werden, dass in den Normen eine Differenzierung der Tätigkeiten nach einzelnen Personen vorgenommen wird. Der Bediener verfügt über die erforderlichen Qualifikationen und Kenntnisse, um die ihm übertragenen Aufgaben sicher und fachgerecht auszuführen. Dazu gehören eine angemessene Schulung und Unterweisung am Arbeitsplatz sowie die Vertrautheit mit den implementierten Cybersicherheitsmaßnahmen.

### Firmeninternes Personal und Gäste

Der Begriff "firmeninternes Personal" bezeichnet alle Mitarbeiter eines Unternehmens, die innerhalb der Unternehmensstruktur tätig sind. Der Begriff "Gäste" bezeichnet alle Personen, die sich vorübergehend, etwa zu Besuch, in den Räumlichkeiten des Unternehmens aufhalten. Die Mitnahme elektronischer Geräte, Störsender, Smartphones, Tablets, Laptops, USB-Sticks usw. ist in einer Produktion nicht gestattet. Für Besucher, Mitarbeiter von Partnerunternehmen sowie Gäste ist ein Führungsplan zu erstellen, der eine Begleitung durch eine beauftragte Person über einen bestimmten Weg zu den freigegebenen Räumen vorsieht. Der Weg ist so zu gestalten, dass ein sicherer Abstand zu potenziellen Gefahrenstellen und Abstand zu digitalen Schnittstellen gewährleistet ist.

### Verkettete oder teilweise verbundene Maschinen

In einigen Fällen ist eine temporäre Verbindung von Maschinen möglich, beispielsweise mit autonomen mobilen Robotern (AMR) über Lasten-Übergabestellen. Eine weitere Möglichkeit stellt der Austausch von Daten zwischen entfernten Maschinen und der Roboteranwendung zu einem definierten Zeitpunkt über einen festgelegten Port dar. Im Anschluss an die Authentifizierung ist eine kurzzeitige Aufrechterhaltung der Verbindung sowie eine Übertragung von Daten über sichere Protokolle vorgesehen. Die Anwendung setzt voraus, dass die verketteten Maschinen ordnungsgemäß und sicher verbunden sind.

### Büro- und interne Serveranbindung

Um zu gewährleisten, dass ausschließlich autorisierte Verbindungen Zugriff auf die Maschine erhalten, ist es erforderlich, die Maschine in einem separaten Netzsegment zu schützen. Dies kann beispielsweise durch die Einrichtung einer Firewall erfolgen. Von gleicher Relevanz sind die Information und Schulung des Personals außerhalb der Produktionsstätte über den Einsatz von Robotern. Es

ist sicherzustellen, dass sich ausschließlich bestimmte Personen, Programme und Geräte mit der Maschine verbinden können.

### **Externe Anbindungen, Internet, Cloud-Anbindungen**

Im Rahmen der externen Vernetzung ist es unerlässlich, adäquate Maßnahmen zum Schutz vor Cyberangriffen zu implementieren. Dies umfasst die Installation von Firewalls, die Anwendung von Verschlüsselungstechnologien sowie die Durchführung regelmäßiger Sicherheitsupdates. Die Gewährleistung einer stabilen und zuverlässigen Netzwerkverbindung ist von essentieller Bedeutung, um Unterbrechungen im Betriebsablauf zu vermeiden.

## **3.2 Maschinenhersteller und Bewahrung von Dokumenten**

Gemäß der neuen EU-MVO sind die Hersteller dazu verpflichtet, die technische Dokumentation für einen Zeitraum von mindestens zehn Jahren aufzubewahren. Für einige Anforderungen sind lediglich fünf Jahre oder weniger vorgesehen. Dies lässt den Schluss zu, dass eine Wartung von Maschinen über einen Zeitraum von mehr als zehn Jahren mit Schwierigkeiten verbunden sein wird. Dies lässt sich vermutlich auf Software-Updates und die Lieferung entsprechender elektronischer Komponenten zurückführen. Der Gebrauchtmaschinenmarkt sieht sich mit beträchtlichen Herausforderungen konfrontiert, wenn es darum geht, für Maschinen, die älter als zehn Jahre sind, Dokumentationen, Ersatzteile und Unterstützung zu erhalten.

Maschinenhersteller muss für die erwartete Lebensdauer der Maschine für einen Zeitraum von **mindestens 10 Jahren** ab Inverkehrbringen oder der Inbetriebnahme der Maschine folgendes aufbewahren:

- die Betriebsanleitung und Dokumentation können digital bereitgestellt und online zugänglich gemacht werden,
- der Hersteller hält die technischen Unterlagen für Behörden bereit,
- der Hersteller erstellt eine EU-Konformitätserklärung für jedes Maschinenmodell, bewahrt sie mit technischen Unterlagen auf und stellt sie Behörden auf Anfrage zur Verfügung,
- EU-Einbauerklärung und Montageanleitung für unvollständige Maschine online in digitaler Form und technische Unterlagen für Behörden,
- interne Fertigungskontrolle (Konformitätsbewertungsverfahren, Überwachung des Herstellungsprozesses, CE-Kennzeichnung und EU-Konformitätserklärung) und technischen Unterlagen für nationale Behörde.

### **mindestens 5 Jahren:**

- das Rückverfolgungsprotokoll und Versionen der Sicherheitssoftware müssen nach dem Hochladen für Nachweise der Konformität auf Anfrage einer nationalen Behörde zugänglich sein.

### **mindestens 1 Jahr:**

- die Aufzeichnung sicherheitsrelevanter Entscheidungsprozesse bei KI-ähnlichen Steuerungen wird gespeichert, um auf begründetes Verlangen der zuständigen Behörde die Konformität der Maschine oder des Produkts nachzuweisen.

## **3.3 Software als Sicherheitselement**

Software, die eine Sicherheitsfunktion erfüllt und separat in Verkehr gebracht wird, wird gemäß der neuen EU-MVO als Sicherheitsbauteil wie eine Sicherheitslichtschranke betrachtet. Die Frage, welche Zertifizierungsstellen und wie die Zertifizierung solcher Software-Sicherheitselemente erfolgen muss, ist derzeit noch in Klärung. Die Entwicklung sicherheitskritischer Software erfolgt derzeit unter Berücksichtigung etablierter Normen wie IEC 61508, ISO 13849-1 oder IEC 62061 [4]. Maschinen-

hersteller sind dazu verpflichtet, die für den sicheren Betrieb relevante Software sowie die implementierten Maßnahmen zu deren Absicherung zu dokumentieren. Die Maschinensteuerung hat sicherzustellen, dass jegliche Änderungen an der Software und den Daten dokumentiert werden, unabhängig davon, ob diese durch autorisierte oder nicht autorisierte Benutzer vorgenommen wurden. Nach der Implementierung ist eine Speicherung sicherheitsrelevanter Daten zu softwaregestützten Sicherheitssystemen über einen Zeitraum von einem Jahr erforderlich, um die Konformität der Maschine auf Anfrage der zuständigen Behörde nachweisen zu können.

### 3.4 Maschine auch ohne Software

In der neuen EU-MVO steht: „*Maschinen, bei denen lediglich das Aufspielen einer Software fehlt, ... fallen nicht unter die Begriffsbestimmungen ... unvollständige Maschinen.*“ [3] Wird der Industrieroboter mechanisch fertiggestellt z.B. mit angebautem Endeffektor, aber ohne Software, wird der Roboter zur „vollständigen Maschine“. Es stellt sich die Frage, wie mit Softwaresteuerung und funktionaler Sicherheit umgegangen wird. Der Maschinenhersteller stellt dem Anwender nicht unbedingt die Risikobeurteilung zur Verfügung, sodass der Anwender sehr leicht zum Systemintegrator mit eigener Interpretation der Applikation werden kann. Ein sicherer Weg ist, dass der Anwender die eigens erstellte Software vor der Installation durch den Maschinenhersteller prüfen lässt.

„*die Grenzen der Sicherheitsfunktionen ... keine Änderungen der durch die Maschine oder das dazugehörige Produkt oder den Bediener generierten Einstellungen oder Regeln, auch während der Lernphase der Maschine ..., vorgenommen werden dürfen, wenn solche Änderungen zu Gefährdungssituationen führen könnten.*“ [3] Dieser Absatz aus der EU-MVO besagt, dass die Grenzen der Maschine weder automatisch noch manuell verändert werden dürfen. Die „Lernphase der Maschine“ bezieht sich im Wesentlichen auf das Anlernen der Künstlichen Intelligenz, die auch als neue Betriebsart verstanden werden kann und daher keine Gefahrensituationen für den Bediener hervorrufen darf.

„*Steuerungssysteme für Maschinen ... deren Verhalten oder Logik sich vollständig oder teilweise selbst entwickelt ... müssen so konzipiert und gebaut sein, dass ... es jederzeit möglich ist, die Maschine oder das dazugehörige Produkt zu korrigieren, um seine inhärente Sicherheit zu wahren.*“ [3] Zur Umsetzung dieser Anforderung muss ein Monitoring, z. B. durch die Sicherheitssteuerung des Robotersystems, eingerichtet werden, das bei unerwünschten Ergebnissen im Automatikbetrieb einen Maschinenstopp oder z. B. bei kollaborierenden Anwendungen eine Warnung auslöst, damit der Bediener die inhärente Sicherheit des Systems wiederherstellen kann. In diesem Fall muss der Bediener mit der selbstlernenden Steuerung und den Auswirkungen auf das Robotersystem vertraut sein und seine Kenntnisse regelmäßig auffrischen.

### 3.5 Überwachung autonomen mobilen Robotern (AMR)

Im Bereich Intralogistik werden derzeit sowohl Fahrerlose Transportsysteme (FTS) als auch AMR verstärkt eingesetzt. Der Unterschied zwischen den FTS und AMR liegt in dem Automatisierungsgrad.

FTS (Fahrerlose Transportsysteme) fahren auf vorprogrammierten Strecken und benötigen oft eine feste Infrastruktur wie Markierungen oder Reflektoren zur Navigation. Sie erfordern eine exakte Routenplanung. Im Gegensatz dazu sind AMR flexibler und können ihre Routen dynamisch anpassen. Sie nutzen fortschrittliche Technologien wie SLAM (Simultaneous Localization and Mapping), um sich selbstständig in ihrer Umgebung zu orientieren und auf unvorhergesehene Hindernisse zu reagieren.

„*Autonome mobile Maschinen ... müssen gegebenenfalls mit einer speziellen Überwachungsfunktion für die autonome Betriebsart ausgestattet sein. Diese Funktion muss es der Aufsichtsperson ermöglichen,*

aus der Ferne Informationen von der Maschine zu erhalten. Die Überwachungsfunktion darf es nur ermöglichen, die Maschine ... aus der Ferne stillzusetzen und in Gang zu setzen oder sie in eine sichere Position und einen sicheren Zustand zu bringen, damit keine weiteren Risiken entstehen. ... Diese Informationen müssen die Aufsichtsperson auf gegenwärtige oder bevorstehende unvorhergesehene oder gefährliche Situationen aufmerksam machen, die ihr Eingreifen erfordern.“

In der EU-Maschinenrichtlinie wird der Begriff "autonome mobile Maschinen" (AMR) verwendet, um allgemein Maschinen zu beschreiben, die sich selbst bewegen und Aufgaben ohne menschliches Eingreifen ausführen können. Dies können z.B. autonome Baumaschinen zum Verputzen oder Streichen von Wänden sein. Es kann sich aber auch um landwirtschaftliche Maschinen zur Bodenbearbeitung, Aussaat, Unkrautbekämpfung, Ernte usw. handeln. Die Überwachung durch eine Aufsichtsperson kann stationär über einen Leitreechner oder durch eine Aufsichtsperson mit einem tragbaren Bediengerät (Laptop, Pad, Smartphone, AR-Brille etc.) erfolgen (siehe Bild 4).

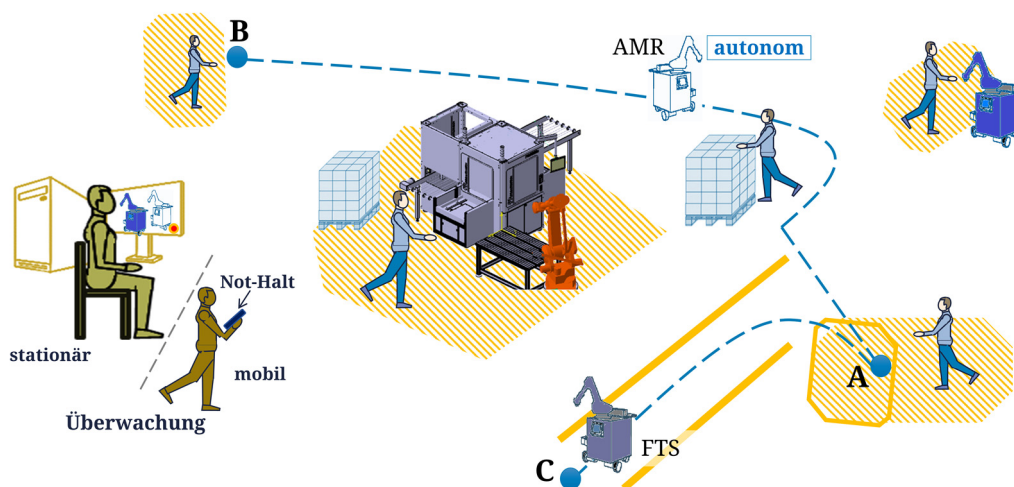


Bild 4: Überwachung von FTS und AMR

Um eine rechtzeitige und angemessene Reaktion der Aufsichtsperson zu gewährleisten, ist eine Übermittlung aller relevanten Daten über den Zustand und das Umfeld der Maschine erforderlich. Sofern die definierten Grenzwerte überschritten oder Anomalien innerhalb der Daten identifiziert werden, erfolgt eine Warnung an die Aufsichtsperson. Eine deaktivierte Überwachungsfunktion muss dazu führen, dass die Maschine nicht im Automatikmodus versetzt werden kann, sondern lediglich in einen untergeordneten Betriebsmodus, welcher die Anwesenheit einer Bedienperson direkt an der Maschine erfordert, wie etwa im manuellen Betrieb.

„Neue Vorschriften, wie die EU-Maschinenverordnung, stellen zusätzliche Herausforderungen dar, etwa durch die Notwendigkeit einer kabellosen Not-Halt-Kommunikation für mobile Maschinen. Die Umsetzung solcher Anforderungen kann für Unternehmen, die nicht auf diese Bereiche spezialisiert sind, einen erheblichen Mehraufwand bedeuten. Insbesondere für exportierende Unternehmen, weil es zusätzlich oft sehr länderspezifische Normen und Vorschriften bezüglich der Kommunikationstechnologie gibt.“ [12]

### 3.6 Cybersicherheit

Aus dem Cybersecurity Act sollte das Leitmotiv für die Unternehmen abgeleitet werden: "Befugte Personen, Programme oder Maschinen haben ausschließlich Zugriff auf diejenigen Daten, Dienste oder Funktionen, zu denen sie zugangsberechtigt sind." [17]

Die EU-MVO legt erstmals verbindliche Cybersicherheitsanforderungen für Maschinen und Anlagen fest, um der zunehmenden Vernetzung und den damit verbundenen Risiken zu begegnen. Diese Anforderungen umfassen Maßnahmen zur sicheren Konnektivität, um sicherzustellen, dass durch den Anschluss externer Geräte keine gefährlichen Situationen entstehen. Darüber hinaus müssen Hersteller sicherstellen, dass ihre Maschinen vor Cyberangriffen geschützt sind, indem sie geeignete Sicherheitskonzepte implementieren und regelmäßig aktualisieren.

## 4 Weitere EU normative und gesetzliche Regelungen

Unternehmen sehen sich neben den technischen Standards mit einer Vielzahl von Normen sowie europäischen und nationalen gesetzlichen Vorgaben konfrontiert, welche den Rahmen für Kommunikationslösungen und digitale Vernetzung vorgeben. In diesem Kontext sind insbesondere die folgenden Regelwerke von grundlegender Bedeutung: die IEC 62443, der Cyber Resilience Act, die NIS2-Richtlinie, der EU-AI Act sowie der EU-Data Act. Diese legen die Vorgaben für die Umsetzung von Sicherheit in der industriellen Kommunikation fest. Die genannten Anforderungen umfassen sowohl die funktionale Sicherheit (Safety) als auch den Schutz vor Cyberangriffen (Security).

Die internationale Normenreihe **IEC 62443** [9] definiert technische und prozessuale Anforderungen zur Cybersicherheit in industriellen Automatisierungs- und Steuerungssystemen, die auch Industrieroboter betreffen. Sie beschreibt Rollen wie Betreiber, Hersteller und Integratoren sowie Sicherheitsstufen, die abhängig von Bedrohungsszenarien angewendet werden.

Der **Cyber Resilience Act** [13] legt verbindliche Cybersicherheitsanforderungen für digitale Produkte, einschließlich Industrierobotern, fest. Hersteller sind über den gesamten Lebenszyklus für die Cybersicherheit verantwortlich, inklusive Software-Updates und der Unterstützung bei Sicherheitsfragen. Die CE-Kennzeichnung zeigt die Konformität mit diesen Anforderungen an.

Die Network and Information Security (**NIS-2**) **Richtlinie** [14] fordert von Unternehmen und Lieferanten wie Maschinenherstellern hohe Sicherheitsstandards. Besonders relevant für Industrieroboter ist die Sicherung der Lieferkette, um Angriffe über Drittanbieter zu verhindern. Zudem gelten Meldepflichten bei Sicherheitsvorfällen, um schnelle Reaktionen zu gewährleisten.

Der **EU-AI Act** [15] regelt KI-Systeme anhand ihres Risikograds, wobei Hochrisiko-Systeme wie KI-gestützte Industrieroboter strengen Anforderungen unterliegen. Hersteller müssen Transparenz über die Funktionsweise der KI sicherstellen, umfangreiche Dokumentationen vorlegen und ein kontinuierliches Risikomanagement implementieren. Ziel ist es, Sicherheit und Zuverlässigkeit während der gesamten Nutzung zu gewährleisten. KI-gestützte Technologien, darunter humanoide Roboter und autonome mobile Systeme, haben das Potenzial, Logistikprozesse und Lieferketten zu optimieren. Ihre vollständige Integration in industrielle Anwendungen wird jedoch voraussichtlich mindestens ein Jahrzehnt in Anspruch nehmen.

Der **EU-Data Act** [16] sichert Anwendern das Recht auf Zugang zu Daten, die von vernetzten Produkten wie Industrierobotern generiert werden. Dies umfasst Informationen zu Diagnostik, Wartung und Betrieb, etwa zu Verschleiß, Logfiles oder Nutzerinteraktionen. Maschinenhersteller sind verpflichtet, ihre Produkte so zu gestalten, dass Daten in Echtzeit verfügbar sind, Dritten auf Anfrage zugänglich gemacht werden können und Datenschutz sowie Datensicherheit gewährleistet bleiben. Die Regelung erstreckt sich auf alle robotergestützten Plattformen und autonomen Roboter, die Daten erfassen und auswerten, um beispielsweise den Betrieb zu optimieren oder Wartung zu erleichtern.

## 5 Zusammenfassung

Die neue EU-MVO berücksichtigt die aktuellen Entwicklungen in der Digitalisierung und Vernetzung von Software und Maschinen sowohl auf nationaler als auch auf internationaler Ebene. Ein besonderes Augenmerk gilt dabei der Cybersicherheit, welche eine umfassende Risikobeurteilung erforderlich macht. Dadurch soll sichergestellt werden, dass Maschinen und Anlagen gegen Cyberangriffe geschützt sind und ein sicherer Betrieb gewährleistet werden kann. Die implementierten Maßnahmen dienen der Gewährleistung der Sicherheit und Zuverlässigkeit von Maschinen in einer zunehmend vernetzten Welt. Die EU-MVO statuiert, dass technische Dokumente sowie eine Vielzahl weiterer Unterlagen für einen Zeitraum von mindestens zehn Jahren aufzubewahren sind. Für Software, Elektronik und Cybersicherheit erscheint diese Zeitspanne angemessen, für Maschinen und Produktionslinien jedoch zu kurz bemessen, da Maschinen üblicherweise über einen Zeitraum von mehr als 20 Jahren in Betrieb sind. Die fortschreitende Digitalisierung führt offenbar auch zu einer Verringerung der Nutzungsdauer von Maschinen. Bis Ende 2026 ist die Überarbeitung von hunderten Normen vorgesehen, die an die neue EU-MVO angepasst werden sollen.

Die neue Roboternormen ISO 10218-1/-2, welche auf der EU-MRL basieren, konkretisieren unter anderem kollaborative Roboteranwendungen sowie die Nutzung externer Steuerungen. Des Weiteren werden Aspekte der Cybersicherheit integriert. Dies kann als wesentlicher Schritt in Richtung der neuen EU-MVO bezeichnet werden. Die Einteilung von Industrierobotern in zwei Klassen kann als Experiment bezeichnet werden, dessen erfolgreiche und insbesondere sichere Umsetzung mehr als fraglich ist. Die Integration von KI-Anwendungen, Cloud-Computing und umfangreicher Vernetzung von Roboteranwendungen birgt das Risiko, dass kleine Unternehmen als Systemintegratoren nicht in der Lage sind, mit den technologischen Entwicklungen Schritt zu halten.

## 6 Literatur

- [1] Schumacher, S., Hall, R., Rapp, S., Bildstein, A. und Bauernhansl, T. (2021). Ganzheitliche Produktionssysteme 4.0 - Anforderungen an die Gestaltung von Methoden und Werkzeugen in Ganzheitlichen Produktionssystemen. Fraunhofer IPA, Stuttgart
- [2] Reiff-Stephan, J. (2024) "Humanity-Centered Production - Automatisierung für die Gesellschaft". Tagungsband der Konferenz der Mechatronik Plattform Österreich 2024: Smart Technologies in Mechatronics S. 36
- [3] EU-Parlament 2023. EU-Maschinenverordnung (EU-MVO) 2023/1230, Online: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32023R1230>, Zugriff am 14.12.2024
- [4] Hesse, S. und Malisa, V. (2016) Taschenbuch Robotik - Montage – Handhabung, ISBN 978-3-446-44365-5, Hanser Verlag
- [5] ISO FDIS 10218-1 (2024) Robotics — Safety requirements — Part 1: Industrial robots. Austrian Standards.
- [6] ISO FDIS 10218-2 (2024) Robotics — Safety requirements — Part 2: Industrial robot applications and robot cells. Austrian Standards.
- [7] EU-Parlament (2006) EU-Maschinenrichtlinie (EU-MRL) 2006/42/EG, Online: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:de:PDF>, Zugriff am 12.12.2024
- [8] ISO/TR 22100-4 (2018) Sicherheit von Maschinen – Zusammenhang mit ISO 12100 Teil4: Leitfaden für Maschinenhersteller zur Berücksichtigung von Aspekten der IT-Sicherheit (Cybersicherheit)
- [9] IEC 62443-3-3 (2019) Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme -- Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level
- [10] Maurer, E. (2024) Die neue Maschinenverordnung, Weka Media, online: <https://www.weka.de/produktsicherheit/die-neue-maschinenverordnung-eu-verordnung-2023-1230-ab-wann-gilt-sie/>, Zugriff am 14.12.2024
- [11] Görnemann, O. (2023) Überarbeitung der EN ISO 10218 zu Sicherheitsanforderungen an Roboter. KANBrief 2/23. Online: <https://www.kan.de/publikationen/kanbrief/2/23/ueberarbeitung-der-en-iso-10218-zu-sicherheitsanforderungen-an-roboter>, Zugriff am 11.12.2024

- [12] Vilsbeck, Ch. (2024) Kostenfalle Cybersecurity & Co. A&D. Online [https://www.industr.com/de/A-und-D-Magazin/\\_storage/asset/2768766/storage/master/file/24777687/E-Paper\\_AuD%20Okt24.pdf](https://www.industr.com/de/A-und-D-Magazin/_storage/asset/2768766/storage/master/file/24777687/E-Paper_AuD%20Okt24.pdf), Zugriff am 16.10.2024
- [13] EU Parlament (2024) Cyber Resilience Act 2024/2847. Amtsblatt der Europäischen Union. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847>, Zugriff am 15.12.2024
- [14] EU-Parlament (2022) NIS-2 Richtlinie 2022/2555. Amtsblatt der Europäischen Union. Online: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2555>, Zugriff am 15.12.2024
- [15] EU-Parlament (2024) EU-AI Act 2024/1689. Amtsblatt der Europäischen Union. Online: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>, Zugriff am 15.12.2024
- [16] EU-Parlament (2023) EU-Data Act 2023/2854. Amtsblatt der Europäischen Union. Online: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>, Zugriff am 15.12.2024
- [17] EU Parlament (2019). Cybersecurity Act 2019/881. Amtsblatt der Europäischen Union. Online: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>, Zugriff am 15.12.2024