Maschinenverordnung 2027: Die Zeit läuft

Der Countdown läuft: Am 20. Januar 2027 wird die EU-Maschinenverordnung 2023/1230 verbindlich. Doch wie weit ist die Industrie bei der Umsetzung? Das SPS-MAGAZIN hat bei Herstellern, Safety-Spezialisten und Automatisierungsanbietern nachgefragt. Die Antworten zeigen: Viele Unternehmen haben intern bereits konkrete Maßnahmen eingeleitet, im Markt insgesamt gibt es jedoch noch deutliche Unterschiede beim Reifegrad. Als größte Herausforderungen gelten Cybersecurity, offene Normungsfragen, neue Verantwortlichkeiten sowie der Umgang mit Software und KI. Klar ist: Die Verordnung verändert nicht nur die CE-Praxis, sondern die Automatisierung insgesamt. (Teil 1 von 2)

INES STOTZ
Leitende Redakteurin

Der Stichtag der EU-Maschinenverordnung 2023/1230 rückt näher: Wie bewerten Sie den aktuellen Umsetzungsstand – sowohl in Ihrem eigenen Unternehmen als auch im Markt insgesamt?

SANDRA HAGIUS, EUCHNER: Als die Maschinenverordnung Mitte 2023 im Amtsblatt der EU veröffentlicht wurde und in Kraft trat, hörte man sehr häufig das beruhigende Argument: „Wir haben ja 42 Monate Zeit." Doch von diesen dreieinhalb Jahren sind heute nur noch rund acht Monate übrig. Wer bislang noch keine Maßnahmen ergriffen hat, sollte jetzt dringend starten. Der erste Schritt für Hersteller ist aus meiner Sicht, sich klarzumachen, was die MVO konkret verlangt. Ab dem 20. Januar 2027 gilt ausschließlich die Maschinenverordnung. In klassischen Safety-Themen sind viele Unternehmen bereits gut aufgestellt. Neu hinzu kommen jedoch deutlich erweiterte Anforderungen, beispielsweise im Bereich Security. Genau hier sehe ich in vielen Unternehmen noch erheblichen Nachholbedarf, der jetzt aktiv angegangen werden sollte. Wir beschäftigen uns bereits seit längerem intensiv mit diesen neuen Herausforderungen, um unsere Kunden auch künftig mit sicheren

Produkten und passenden Dienstleistungen unterstützen zu können.

HASAN SÜLÜK, PEPPERL+FUCHS: Der Umsetzungsstand ist aus unserer Sicht noch ziemlich uneinheitlich. Wir haben früh angefangen, die Anforderungen in unsere Entwicklungs- und Qualitätsprozesse zu integrieren, und merken dabei, dass das Thema deutlich tiefer in die Organisation eingreift als zunächst gedacht. Gerade die Verzahnung von Software und Safety erfordert neue Abläufe. Im Markt sieht man ein ähnliches Bild: Größere Unternehmen sind oft schon strukturiert unterwegs, während viele Mittelständler noch dabei sind, sich einen klaren Überblick zu verschaffen. Das Bewusstsein ist mittlerweile vorhanden, aber konkrete Maßnahmen fehlen häufig noch. Insgesamt bewegt sich der Markt, aber mit sehr unterschiedlicher Geschwindigkeit.

CARSTEN GREGORIUS, PHOENIX CONTACT: Insgesamt sind die Vorbereitungen bei uns im Hinblick auf die MVO weit fortgeschritten. Wir kennen die Anforderungen und wissen, was zu tun ist. Unsere Spezialisten befinden sich in der finalen Umsetzungsphase für die relevanten Safety-Produkte. Auf der Anwenderseite sehen wir ebenfalls Aktivitäten. Aufgrund der unklaren Normenlage gibt es jedoch noch einige Verunsicherungen.

MARCEL WÖHNER, PILZ: Aus unserer Sicht fehlen an einigen Stellen noch abschließende, verbindliche Interpretationen und Klarstellungen, insbesondere zu Detailfragen. Grundsätzlich ist der deutsche Maschinenbau jedoch sehr gut aufgestellt. Unternehmen verfügen über langjährige Erfahrung im Umgang mit CE-Themen und regulatorischen Anforderungen. Die bewährten Vorgehensweisen bleiben auch unter der neuen Maschinenverordnung weitgehend gültig. Zwar wurden einzelne Aspekte ergänzt oder präzisiert, im Kern geht es jedoch eher um Klarstellungen und eine stärkere EU-weite Vereinheitlichung als um einen grundlegenden Paradigmenwechsel. Vor diesem Hintergrund sehe ich Deutschland insgesamt gut vorbereitet auf die Umsetzung der MVO.

FRANZ DOLD, SICK: Bei Sick haben wir uns frühzeitig, strukturiert und konzernweit mit den Anforderungen der MVO auseinandergesetzt. Insbesondere die neuen Cybersecurity-Anforderungen wurden organisatorisch und technisch zeitnah adressiert und konsequent in unsere Entwicklungs- und Produktprozesse integriert. In diesem Kontext konnten bereits mehrere Produkte erfolgreich durch Drittstellen nach den MVO-Vorgaben bewertet und zugelassen werden. Weitere Produktzulassungen befinden sich aktuell in Vorbereitung. Im Markt insgesamt zeigt sich derzeit noch ein uneinheitliches Bild. Insbesondere im Automatisierungsumfeld sind bislang nur wenige Hersteller mit bereits MVO-konformen Produkten bei den Prüfstellen gelistet. Viele Unternehmen befinden sich noch in der Analyse- und Übergangsphase. Insgesamt besteht hier weiterhin ein erheblicher Aufholbedarf – sowohl in der praktischen Umsetzung als auch im Aufbau regulatorischer und organisatorischer Kompetenzen.

MARCEL AULILA, SSP: Für uns ist die Maschinenverordnung längst kein Zukunftsthema mehr, sondern bereits Teil unserer strategischen Ausrichtung. Wir treiben die Umsetzung bewusst nicht als reines Compliance-Projekt, sondern integrieren sie in Produktentwicklung, Prozesse und Kundenprojekte. Im Markt sehen wir ein gemischtes Bild: Das Bewusstsein ist vorhanden, aber die praktische Umsetzung hinkt oft hinterher. Besonders bei vernetzten Anlagen und softwaregetriebenen Sicherheitsfunktionen fehlt es vielerorts noch an klaren Strukturen und Verantwortlichkeiten.

MICHAEL FLESCH, TURCK: Bei Turck liegt der Fokus derzeit klar auf der Umsetzung der Anforderungen in unseren Safety-Modulen, die entweder über Profisafe oder CIP Safety an unterschiedliche Steuerungen angebunden werden kön-

> *„Verantwortlichkeiten müssen künftig klar definiert und organisatorisch sauber abgestimmt werden.“*
>
> **Michael Flesch**
> Turck

nen. Ziel ist es, die betroffenen Module bis Dezember mit den erforderlichen Zertifikaten auszustatten. Dafür prüfen wir die derzeitigen Safety-Bedingungen auf Konformität mit der MVO und setzen die Security-Anforderungen des Anhang III aus der MVO entsprechend um. Hinzu kommt die Überarbeitung der gesamten Gerätedokumentation. Wir konzentrieren uns aktuell stark auf diese internen Maßnahmen, um die Umsetzung fristgerecht sicherzustellen. Der Markt insgesamt befindet sich aus meiner Sicht noch in sehr unterschiedlichen Umsetzungsstadien – von weit fortgeschrittenen Projekten bis hin zu noch sehr frühen Planungsphasen.

Welche Aspekte der MVO stellen Unternehmen derzeit vor die größten praktischen Herausforderungen – und wo sehen Sie noch Interpretationsspielräume oder Unsicherheiten?

SANDRA HAGIUS, EUCHNER: Aktuell sehen wir vor allem drei Themenfelder, die Unternehmen in der Praxis beschäftigen: Cybersecurity, die Frage der wesentlichen Veränderung sowie die neuen Rollen der sogenannten Wirtschaftsakteure. Mit der Maschinenverordnung werden diese Akteure erstmals klar definiert. Dazu zählen Hersteller, Bevollmächtigte, Einführer und Händler. Der Hersteller bleibt weiterhin der zentrale Verantwortliche – etwa für Konstruktion, Risikobeurteilung, technische Dokumentation, Konformitätsbewertung und EU-Konformitätserklärung. Das gilt auch für Unternehmen, die Maschinen für den Eigenbedarf herstellen. Neu und für viele noch ungewohnt sind insbesondere die Pflichten von Einführern und Händlern. Sie werden ausdrücklich als Teil der Lieferkette adressiert. Wer Maschinen aus Nicht-EU-Ländern einführt, muss sicherstellen, dass diese den Anforderungen der Maschinenverordnung entsprechen. Zusätzlich müssen neben den Herstellerdaten auch die Angaben des Einführers dauerhaft an der Maschine angebracht werden. Gerade an diesen Schnittstellen der Lieferkette sehen wir derzeit noch Interpretationsbedarf und praktischen Klärungsbedarf.

> *„Wer bislang noch keine Maßnahmen ergriffen hat, sollte jetzt dringend starten.“*
>
> **Sandra Hagius**
> Euchner

HASAN SÜLÜK, PEPPERL+FUCHS: Die Herausforderung liegt weniger im ‘Was’, sondern im ‘Wie’. Viele Anforderungen sind bekannt, aber ihre praktische Umsetzung ist nicht immer eindeutig. Das gilt vor allem für Software in der Risikobeurteilung und die Frage, wann eine ‘wesentliche Veränderung’ vorliegt, das ist in der Praxis alles andere als trivial. Auch die Verantwortlichkeiten entlang der Lieferkette sind nicht immer klar, insbesondere bei komplexen Softwarelösungen. Dazu kommt, dass sich die MVO mit anderen Themen wie Cybersecurity überlagert. Genau in diesen Schnittstellen entstehen aktuell die meisten Unsicherheiten.

CARSTEN GREGORIUS, PHOENIX CONTACT: IDie größten Herausforderungen liegen sicherlich in der Bewertung des Aspekts Korrumpierung aus Anhang III 1.1.9 bzw. 1.2.1 der MVO. Plakativer gesprochen geht es um die Frage, welche Bedrohungen sich für Sicherheitsfunktionen im Hinblick auf Cyber Security ergeben? Wie sehen ganzheitliche Konzepte dazu aus? Die hierfür relevante Norm prEN 50742 befindet sich derzeit im Entwurfsstadium und bietet daher noch keine stabile Basis. Wir hoffen, dass die Norm bis spätestens Ende 2026 zur Verfügung steht. Jedoch lassen sich bereits jetzt aus dem Entwurf einige Anforderungen ableiten.

MARCEL WÖHNER, PILZ: Die Herausforderungen unterscheiden sich je nach Unternehmen und danach, wie der eigene Verantwortungsbereich bislang gelebt wurde. Ein zentraler Punkt der MVO ist, dass künftig mehr Maschinen als ‘prüfpflichtige Maschinen’ eingestuft werden. Dabei handelt es sich um Hochrisiko-Maschinen, für die eine zusätzliche, formalisierte Prüfpflicht vorgesehen ist. Für betroffene Hersteller kann das den Zulassungsprozess deutlich verändern. Klarstellungen bringt die MVO auch bei bislang strittigen Auslegungen, etwa bei unvollständigen Maschinen bzw. Anlagen, die nahezu komplett erstellt aber ohne Steuerungssoftware verkauft wurden. Hier war die Verantwortung für ein ganzheitliches Sicherheitskonzept oft unklar – die neue Verordnung schafft mehr Verbindlichkeit. Die größten Unsicherheiten bestehen derzeit bei der Frage, welche Normen konkret für eine sichere Konstruktion anzuwenden sind. Viele Normen müssen noch angepasst oder neu gelistet werden. Schwierig ist das etwa für Maschinenbauer, die derzeit entwickeln und deren Maschinen erst nach dem Stichtag in Verkehr gebracht werden. Dadurch entstehen zahlreiche Detailfragen, während verbindliche Leitlinien teils noch im Entwurf sind.

> *„Im Kern geht es weniger um einen Paradigmenwechsel als um mehr Klarheit und EU-weite Vereinheitlichung.“*
>
> **Marcel Wöhner**
> Pilz

FRANZ DOLD, SICK: Eine der größten praktischen Herausforderungen ist aktuell das Fehlen harmonisierter Normen zur konkreten Umsetzung der MVO. Gerade im Bereich Cybersecurity existiert mit der prEN 50742 zwar ein erster Normentwurf, dieser befindet sich jedoch noch in einem frühen Stadium und ist mit erheblichen Änderungsrisiken verbunden. Dies erschwert eine belastbare und zukunftssichere Umsetzung der Anforderungen. Parallel dazu stehen Prüfstellen vor einer erheblichen Rezertifizierungswelle, die absehbar zu Kapazitäts- und Zeitengpässen führen wird. Neben diesen technischen und organisatorischen Herausforderungen erwarten Maschinenbauer und Betreiber zunehmend frühzeitige Compliance-Aussagen zur Investitionssicherheit. Solange jedoch klare Normen und eine einheitliche Auslegung fehlen, sind solche

Aussagen nur eingeschränkt möglich, was zu Unsicherheiten entlang der gesamten Wertschöpfungskette führt.

MARCEL AULILA, SSP: Die größten Herausforderungen liegen an der Schnittstelle zwischen klassischer Safety und neuen Themen wie Software und Cybersecurity. Genau dort entstehen aktuell die

> *„Die Umsetzung darf kein reines Compliance-Projekt sein.“*
>
> **Marcel Aulila**
> SSP

meisten Unsicherheiten. Besonders kritisch sind aus unserer Sicht drei Punkte: die Abgrenzung von Safety und Security, die Bewertung von Softwareänderungen im Lebenszyklus und die saubere Nachweisführung. Hier gibt es noch Interpretationsspielräume, die Unternehmen aktuell selbst strukturieren müssen

MICHAEL FLESCH, TURCK: Der größte Druck kommt aktuell vor allem von großen Maschinenherstellern und deren Endkunden, die die Anforderungen der MVO möglichst schnell umgesetzt sehen wollen. Für kleinere und mittelständische Unternehmen wird es deutlich anspruchsvoller werden, alle Vorgaben vollständig und korrekt umzusetzen. Besonders bei der Risikobewertung im Bereich Security ist ein nüchterner und strukturierter Ansatz wichtig, um sachgerecht zu bewerten und keinen unnötigen Handlungsdruck zu erzeugen. Positiv ist aus meiner Sicht, dass mit der EN 50742:2025 rechtzeitig eine Norm zur Verfügung steht, die eine solide Grundlage für die sicherheitsbezogene Bewertung von Security-Aspekten bietet und damit mehr Klarheit schafft.

Mit Themen wie Cybersecurity, Software und KI erweitert die Verordnung den klassischen Maschinenbegriff. Welche konkreten Auswirkungen hat das auf Entwicklung, Architektur und Verantwortlichkeiten in der Automatisierung?

SANDRA HAGIUS, EUCHNER: Die neue Maschinenverordnung greift genau die zwei zentralen Zukunftsthemen auf: künstliche Intelligenz und Cybersecurity. Maschinen und Sicherheitsbauteile mit KI, die ein selbstentwickelndes Verhalten in Bezug auf ihre Sicherheitsfunktionen zeigen, werden künftig den Hochrisikomaschinen zugeordnet. Für diese gelten strengere Anforderungen im Konformitätsbewertungsverfahren. Hersteller können dieses Verfahren dann nicht mehr allein durchführen, sondern müssen eine notifizierte Stelle einbeziehen. Damit reagiert der Gesetzgeber auf den zunehmenden Einsatz von KI in sicherheitsrelevanten Anwendungen. Parallel dazu rückt Cybersecurity deutlich stärker in den Fokus. Mit wachsender Vernetzung steigen auch die Risiken durch manipulierte Steuerungen, unbefugte Zugriffe oder stillgelegte Produktionslinien. Die MVO ergänzt den bisherigen Safety-Ansatz daher um verbindliche Security-Anforderungen und fordert eine nachweisbare Widerstandsfähigkeit gegenüber Cyberangriffen. Für Entwicklung und Architektur bedeutet das: Maschinen mit digitalen Schnittstellen oder Fernzugriffen müssen von Anfang an so ausgelegt sein, dass durch Cyberangriffe keine Gefahrensituationen entstehen. Security- und Softwareaspekte werden damit integraler Bestandteil des Maschinenkonzepts – und die Verantwortlichkeiten reichen künftig deutlich über die klassische Functional Safety hinaus.

HASAN SÜLÜK, PEPPERL+FUCHS: Die klassische Trennung zwischen Maschinenbau und IT funktioniert so nicht mehr. Entwicklung wird zwangsläufig interdisziplinärer, weil Safety, Security und Software zusammen gedacht werden müssen. Das hat direkte Auswirkungen auf die Architektur: Systeme müssen modularer, updatefähig und gleichzeitig sicher ausgelegt sein. In der Praxis bedeutet das auch mehr Aufwand in der Entwicklung. Gleichzeitig verschiebt sich die Verantwortung stärker in Richtung Hersteller und zwar über den gesamten Lebenszyklus hinweg. Das endet nicht mehr mit der Inbetriebnahme.

> *„Gerade die Verzahnung von Software und Safety erfordert neue Abläufe.“*
>
> **Hasan Sülük**
> Pepperl+Fuchs

Bild: ©Oliver Farys / Pepperl+Fuchs SE

CARSTEN GREGORIUS, PHOENIX CONTACT: Im Hinblick auf Cyber Security sehen wir tatsächlich aktuell die größten Herausforderungen. Die Auswirkungen von ‘Software als Sicherheitsbauteil’ betrachten wir dagegen als gering. Im Rahmen des ZVEI gab es dazu eine umfangreiche Bewertung mit dem Ergebnis, dass nur ein geringer Anteil der möglichen Use Case davon betroffen ist. Der KI wird hingegen zukünftig auch im Bereich der Si-

> *„Die größte Herausforderung bleibt derzeit Cybersecurity.“*
>
> **Carsten Gregorius**
> Phoenix Contact

cherheitstechnik eine stärkere Bedeutung zukommen. Das kann verschiedene Bereiche betreffen: von der Risikobeurteilung über das Safety Engineering bis zu Aspekten wie Sensor-Fusion. Die normativen Anforderungen stehen diesbezüglich jedoch noch am Anfang.

MARCEL WÖHNER, PILZ: Zunächst ist wichtig, ein Missverständnis auszuräumen: Die MVO führt Themen wie Cybersecurity oder KI nicht neu ein, sondern schafft vor allem Klarheit in der Abgrenzung. Im Fokus steht nicht eine umfassende Cybersecurity, sondern der Schutz der Safety-Funktionen vor Manipulation. Hersteller müssen sicherstellen, dass Sicherheitsfunktionen nicht durch einfache digitale Eingriffe ausgehebelt werden können. Grundlegendere Anforderungen an die OT-Security bringt erst der Cyber Resilience Act, dessen Vorgaben künftig in die Technische Dokumentation zur Maschine einfließen und für die CE-Bewertung relevant werden. Beim Thema Software bleibt das etablierte Vorgehen zur sicheren Entwicklung bestehen. Neu ist jedoch, die klare regulatorische Grundlage für sicherheitsrelevante Applikationssoftware und diese maschinenunabhängig mit eigenständiger Zulassung und Angabe von Sicherheitskennwerten in Verkehr bringen zu können. KI ist nach aktuellem Stand nicht als alleinige Schutzmaßnahme vorgesehen. Sie kann Prozesse unterstützen oder Sicherheitsreaktionen ergänzen – jedoch nur zusätzlich zu klassisch umgesetzten Safety-Funktionen.

FRANZ DOLD, SICK: Die MVO erweitert den Maschinenbegriff deutlich und definiert Cybersecurity und Software ausdrücklich als sicherheitsrelevante Elemente. Sicherheitsrelevante Bauteile müssen gegen unbeabsichtigte oder vorsätzliche Manipulation geschützt sein und dürfen auch im Verbund mit anderen Komponenten keine gefährlichen Situationen verursachen. Steuerungen sind so auszulegen, dass sie böswilligen Angriffen standhalten. Entsprechend müssen Entwicklung und Systemarchitektur von Beginn an Manipulationsschutz, Zugriffskontrolle, Rückverfolgbarkeit und sichere Software-Updates berücksichtigen. Software gewinnt als Sicherheitsbauteil an Bedeutung und unterliegt teils prüfstellenpflichtigen Konformitätsbewertungen,

„Viele Unternehmen befinden sich noch in der Analyse- und Übergangsphase.“

Franz Dold
Sick

insbesondere bei selbstentwickelndem Verhalten. Sie muss korrigierbar, nachvollziehbar und funktional begrenzt sein. Ergänzend gelten Anforderungen aus dem Cyber Resilience Act sowie bei KI-Anwendungen dem AI Act. Insgesamt ergibt sich eine ganzheitliche System-, Prozess- und Lifecycle-Verantwortung.

MARCEL AULILA, SSP: Die wichtigste Auswirkung ist aus unserer Sicht, dass Maschinenentwicklung endgültig nicht mehr nur mechanisch und elektrotechnisch gedacht werden kann. Wer heute Automatisierungslösungen entwickelt, muss Software, Kommunikation, Updatefähigkeit und Zugriffswege von Anfang an als sicherheitsrelevante Architekturentscheidungen verstehen. Die EU-Kommission nennt ausdrücklich KI-gestützte Sicherheitsfunktionen sowie Cyber-Safety für compliance-relevante Softwaredaten und Sicherheitssteuerungen als Teil des neuen Rahmens. Für die Entwicklung bedeutet das: Safety darf nicht erst am Ende über Validierung oder Dokumentation ‘hinzugefügt‘ werden. Sie muss gemeinsam mit Softwarearchitektur, Benutzerrechten, Schnittstellenmanagement und Änderungsprozessen gedacht werden. Für viele Unternehmen ist das ein kultureller Wandel, weil Safety, Automation, Softwareentwicklung, IT und Produktmanagement enger zusammenarbeiten müssen als bisher. Für die Verantwortlichkeiten heißt das auch: Es braucht klar definierte Ownership über den gesamten Entstehungs- und Änderungsprozess hinweg. Gerade in vernetzten Anlagen ist es entscheidend, dass Verantwortlichkeiten nicht zwischen Mechanik, Elektrotechnik, SPS, HMI, Remote Service und IT-Security verloren gehen.

MICHAEL FLESCH, TURCK: In den Risikobeurteilungen sicherer Bauteile spielt die Security-Bewertung nun eine deutlich größere Rolle und wird integraler Bestandteil der Gesamtbewertung. Unsere Geräte werden grundsätzlich unter einer Sicherheitssteuerung innerhalb einer Maschine betrieben, sodass wir sie gezielt auf einen sicheren Betrieb in diesem Umfeld vorbereiten können. Die Gesamtverantwortung liegt jedoch weiterhin beim Maschinenhersteller, der alle Komponenten zusammenführt. Gemeinsam mit dem Endkunden, der die Maschine in seine IT- und Produktionsnetzwerke integriert, müssen die Voraussetzungen für eine durchgängige Cybersecurity geschaffen werden. Damit verschieben sich Verantwortlichkeiten, die klar definiert und organisatorisch sauber abgestimmt werden müssen. n

Sandra Hagius
Safety Consultant
Euchner

Hasan Sülük
Team Leader Safety Services, Global Technical Sales Support, FS Engineer (TÜV Rheinland, #20893/ 20, Machinery)
Pepperl+Fuchs

Carsten Gregorius
Manager Strategic Product Marketing Safety
Phoenix Contact, Bad Pyrmont

Marcel Wöhner
Chief Technical Officer
Pilz

Franz Dold
Vice President R&D - Safety Infrastructure
Sick

Marcel Aulila
Stellvertretender Geschäftsführer SSP Safety System Products

Michael Flesch
Produktmanager Safety-Systeme
Turck