Fit für 2027: Was sich mit der neuen EU-Maschinenverordnung wirklich ändert

Cybersicherheit, KI und Cobots im Fokus. Mehrschichtiges Sicherheitskonzept Defense-in-Depth kombiniert verschiedene Schutzebenen.

Bild 1: Die neue EU-Maschinenverordnung rückt Cybersicherheit und digitale Risiken stärker in den Fokus.

In rund einem Jahr ist es soweit: Ab dem 20. Januar 2027 gilt die neue EU-Maschinenverordnung 2023/1230. Um die Betriebssicherheit zu erhöhen und eine verlässliche Basis für zukunftsfähige Automatisierungslösungen in einer immer vernetzteren Industrie zu schaffen, sollten sich Unternehmen jetzt intensiv mit den neuen Anforderungen auseinandersetzen. Der Übergang von der bisherigen Maschinenrichtlinie 2006/42/EG zur neuen Verordnung markiert einen bedeutenden Wandel in den rechtlichen Vorgaben für Maschinen, Anlagen und zugehörige Produkte.

Für Systemintegratoren beinhaltet das strengere Anforderungen bei der Integration von KI-basierten Systemen, autonomen Maschinen und vernetzten Geräten. Aber auch Endnutzer, etwa die Betreiber komplexer Maschinensysteme, sollten sich auf die Änderungen vorbereiten, um einen reibungslosen Übergang sicherzustellen. Denn auch wenn grundlegende Sicherheitsziele bestehen bleiben, rücken digitale Aspekte vermehrt in den Fokus. Cybersicherheit, KI-basierte Funktionen und vernetzte Systeme werden verbindlicher Bestandteil der Maschinensicherheit (Bild 1).

© OMRON

Autor:
Peter Goebbels
Marketing Specialist Safety
OMRON
Industrial Automation Europe
http://industrial.omron.de

Harmonisierung mit anderen Vorgaben wie Cyber Resilience Act

Das oberste Ziel: Maschinen sollen sicher konstruiert, gebaut und betrieben werden können. Neu ist jedoch der Ansatz. Als Verordnung gilt das Regelwerk unmittelbar in allen EU-Mitgliedstaaten, ohne nationale Umsetzung. Zudem orientiert sich die Maschinenverordnung am New Legislative Framework (NLF) und schafft so einheitlichere Prozesse für Konformitätsbewertungen, vor allem bei Hochrisikomaschinen und neuen Technologien. Durch die Harmonisierung mit anderen EU-Rechtsakten, etwa KI-Verordnung oder Cyber Resilience Act (CRA), entsteht ein kohärenter Rechtsrahmen, der Sicherheit und Digitalisierung in der industriellen Praxis vereint.

Cybersicherheit als Pflichtbestandteil

Maschinen müssen künftig so ausgelegt sein, dass Manipulationen, unbefugter Zugriff oder Cyberangriffe sicherheitskritische Funktionen nicht beeinträchtigen können. Das betrifft sowohl physische Schnittstellen wie USB-Ports als auch digitale Angriffsflächen in vernetzten Systemen. Der Cyber Resilience Act (CRA) ergänzt hier die Maschinenverordnung: Er fordert „Security by Design" und „Security by Default" für alle Produkte mit digitalen Inhalten, also auch für Steuerungen, Sensoren und Aktoren im industriellen Umfeld.

Aktuelle Zahlen zeigen, wie dringlich das Thema ist: Nach Angaben des Branchenverbands Bitkom verursachten Cyberangriffe auf industrielle Systeme 2024 weltweit Schäden von über 178 Milliarden Euro, rund 30 Milliarden mehr als im Vorjahr, Tendenz steigend (Bild 2). Ein einzelner Angriff kann Produktionslinien lahmlegen, Lieferketten unterbrechen und Umsätze massiv beeinträchtigen. Unternehmen müssen deshalb Schutzmaßnahmen auf allen Ebenen etablieren, von der Produktentwicklung bis zum laufenden Betrieb.

Auf Sicherheit von der Steuerung bis zur Cloud setzen

Omron hat frühzeitig auf die neuen Anforderungen reagiert und umfangreiche Maßnahmen umgesetzt, um sowohl die Vorgaben der

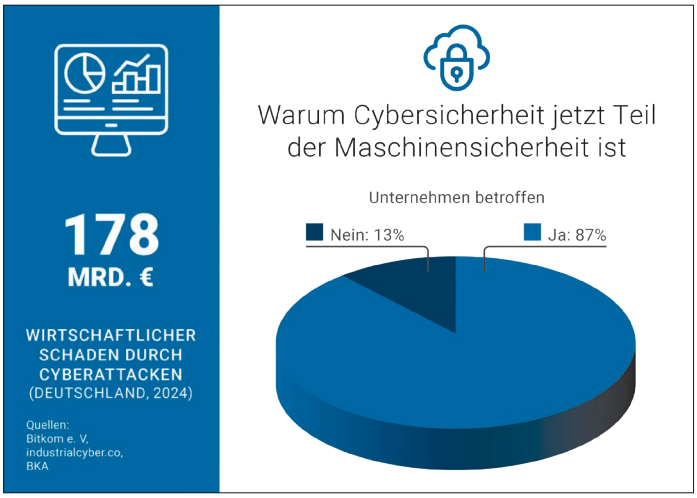

Bild 2: Kumulierte Schäden und hohe Betroffenheit zeigen die wachsende Relevanz von Cybersicherheit als Bestandteil der Maschinensicherheit.
© BKA, Urheber: OMRON

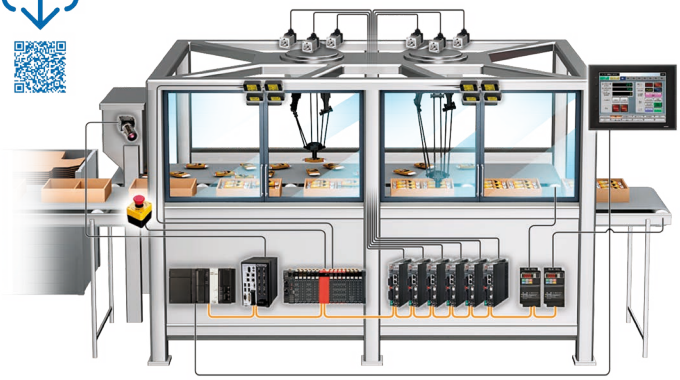

Bild 3: Ein mehrschichtiges Defense-in-Depth-Konzept schützt industrielle Systeme ganzheitlich, von der Steuerungsebene über das Netzwerk bis hin zur Cloud. © OMRON

Maschinenverordnung als auch die Anforderungen des Cyber Resilience Acts zu erfüllen. Im Zentrum steht dabei das Defense-in-Depth-Prinzip, ein mehrschichtiges Sicherheitskonzept, das mehrere Schutzebenen kombiniert (Bild 3). Dazu gehören:

- Netzwerksegmentierung und Firewall-Management zur Begrenzung von Zugriffsrechten
- Verschlüsselte Kommunikation mittels TLS und Zertifikaten (z. B. OPC UA-Server-Funktionen)
- Zugriffskontrolle mit Benutzer- und Rollenmanagement
- Integritätsprüfungen über Hashcodes und Schreibschutzfunktionen
- sowie ein kontinuierliches Schwachstellenmanagement mit transparentem Patch-Prozess

Security Guideline

Hilfreich ist zudem eine Security Guideline für Steuerungen und Automatisierungssysteme, die Schritt für Schritt zeigt, wie sich bestehende Maschinen auf den neuesten Sicherheitsstandard bringen lassen. Ergänzend bietet ein Vulnerability Advisory Service eine zentrale Plattform, über die Schwachstellen gemeldet, bewertet und kommuniziert werden. So entsteht eine durchgängige Transparenz über den gesamten Produktlebenszyklus hinweg, zentraler Baustein des CRA.

In der Produktentwicklung ist „Security by Design“ empfehlenswert: Sicherheitsfunktionen werden nicht nachträglich ergänzt, sondern sind integraler Bestandteil jeder neuen Hardware- und Softwaregeneration. Dazu zählen Funktionen wie sichere Boot-Prozesse, manipulationssichere Firmware-Updates und kryptografisch signierte Kommunikationsprotokolle.

KI-gestützte Prozessoptimierung gepaart mit Sicherheitsmechanismen

Besonders anspruchsvoll sind die neuen Anforderungen für Maschinen mit KI-basierten oder adaptiven Funktionen. Systeme mit Lernfähigkeit müssen nachweisen, dass sich ihr Verhalten nicht sicherheitskritisch verändert. Ratsam ist es hierbei, KI-gestützte Prozessoptimierung mit umfassenden Sicherheitsmechanismen zu kombinieren, um Risiken frühzeitig zu erkennen (Bild 4). Dazu gehören integrierte Überwachungsfunktionen, die Änderungen im Systemverhalten automatisch prüfen und protokollieren, ein entscheidender Schritt in Richtung „sichere KI“.

Keine Übergangsfrist

Die Risikoanalyse dient als Startpunkt. Da es keine Übergangsfrist gibt, muss die vollständige Konformität bis Januar 2027 erreicht sein. Unternehmen sollten daher so schnell wie möglich mit einer Risikoanalyse beginnen und prüfen, welche Komponenten und Systeme bereits die Anforderungen von Maschinenverordnung und CRA erfüllen. Eine enge Zusammenarbeit mit Herstellern kann hier entscheidende Vorteile bieten, etwa durch vorkonfigurierte Sicherheitsfunktionen, Schulungsangebote und praxisorientierte Leitfäden.

Digitale und physische Sicherheit aus einem Guss

ist das oberste Ziel. Die neue EU-Maschinenverordnung ist weit mehr als ein juristisches Update. Sie leitet eine Ära ein, in der digitale und physische Sicherheit untrennbar miteinander verbunden sind. Innovative Hersteller zeigen, wie moderne Automatisierungslösungen nicht nur effizient, sondern auch resilient werden. Digitale Schutzmaßnahmen werden dabei erstmals ganzheitlich in die Maschinensicherheit integriert. Durch sichere Steuerungssysteme, verschlüsselte Kommunikation und klar definierte Zugriffskontrollen lässt sich so ein umfassendes Sicherheitskonzept schaffen. Hierdurch können Maschinenbauer und Betreiber ihre Anlagen zuverlässig vor unbefugtem Zugriff und Manipulation schützen und gleichzeitig regulatorische Anforderungen wie Maschinenverordnung oder Cyber Resilience Act erfüllen.

Fazit

Worauf in Sachen EU-Maschinenverordnung jetzt zu achten ist: Ab Januar 2027 gilt die neue EU-Maschinenverordnung 2023/1230. Dies markiert einen bedeutenden Wandel in den rechtlichen Vorgaben für Maschinen, Anlagen und zugehörige Technologien. Für Systemintegratoren beinhaltet das strengere Anforderungen bei der Integration von KI-basierten Systemen, autonomen Maschinen und vernetzten Geräten. Aber auch Endnutzer müssen sich vorbereiten, um einen reibungslosen Übergang sicherzustellen. Denn auch wenn grundlegende Sicherheitsziele bestehen bleiben, rücken digitale Risiken vermehrt in den Fokus. Cybersicherheit, KI-basierte Funktionen und vernetzte Systeme werden verbindlicher Bestandteil der Maschinensicherheit.

Besonders betroffen sind kollaborative Roboter, autonome Maschinen und Anwendungen mit selbstlernenden Systemen. So müssen Hersteller und Betreiber künftig nachweisen, dass Manipulationen, unbefugter Zugriff oder Cyberangriffe sicherheitskritische Funktionen nicht beeinträchtigen können. Für KI-Systeme mit adaptivem Verhalten steigen die Anforderungen an Risikobeurteilung, Validierung und an Konformitätsbewertungen durch Dritte. Da es keine Übergangsfrist gibt, ist Handeln angesagt. Die Bestandsaufnahme bestehender Maschinen, die Einführung neuer Sicherheits- und Cybersecurity-Standards sowie gezielte Schulungen sind wichtige erste Schritte.

Wer schreibt:

Omron ist ein führendes Automatisierungsunternehmen mit den Kernkompetenzen „Sensing and Control + Think Technology“. Omron ist in zahlreichen Geschäftsfeldern tätig, darunter Industrieautomatisierung, Gesundheitswesen, soziale Systeme, Geräte- und Modullösungen. Omron wurde 1933 gegründet und beschäftigt weltweit rund 28.000 Mitarbeiter, die in mehr als 130 Ländern Produkte und Dienstleistungen anbieten und so zur Schaffung einer besseren Gesellschaft beitragen. ◄

Bild 4: Kollaborative Roboter und KI-basierte Systeme unterliegen künftig strengeren Anforderungen: Ihr Verhalten darf sich auch bei lernenden Funktionen nicht sicherheitskritisch verändern. © OMRON