

Manipulationsschutz im Fokus

Hersteller von Maschinen für die Produktion von Medizintechnik werden ab 2027 die neue EU-Maschinenverordnung einhalten müssen. Bei der funktionalen Sicherheit gilt es nachzubessern – durch effektiven Manipulationsschutz an der Maschine.



Protokollierung des Manipulationsschutzes und der Codes. Nach der Inbetriebnahme der Anlage oder des Systems können die Codes protokolliert werden um zu kontrollieren, ob die Anlage manipuliert worden ist.

Hersteller von medizinischen Produkten und Geräten unterliegen verschiedenen – branchentypisch strengen – Regularien. Für Maschinenbauer, deren Anlagen in der Fertigung von Medizintechnik zum Einsatz kommen, galt bisher unter anderem die Maschinenrichtlinie 2006/42/EU, deren Ursprung mittlerweile 20 Jahre zurückreicht. Am 20. Januar 2027 wird die neue Maschinenverordnung EU 2023/1230 verbindlich anzuwenden sein.



Autor:
Matthias Höhl
Country Sales Manager Deutschland
Pizzato Deutschland GmbH
www.pizzato.com/de

Ziel ist es, europaweit einheitliche Sicherheitsstandards für Maschinen und Software zu schaffen. Die neue Verordnung soll auch neue Risiken abdecken, die sich unter anderem durch die jüngsten Fortschritte in der Mensch-Roboter-Zusammenarbeit ergeben.

Die neue EU-Maschinenverordnung verknüpft erstmals die funktionale Betriebssicherheit eng mit der Cybersicherheit. Dies betrifft somit die sogenannte Safety, also funktionale Sicherheit oder Betriebssicherheit, und Security, in diesem Fall Cybersicherheit. Die auf aktuellen Stand gebrachte Verordnung fordert, dass Sicherheitsfunktionen und Schutzvorrichtungen sowohl physisch gegen mechanisches Umgehen als auch gegen unbefugte digitale Zugriffe, also Cyberangriffe oder Softwaremanipulation, geschützt sein müssen.

Betroffene

Zu beachten ist ebenso, dass nicht nur Hersteller, sondern sämtliche Akteure, die Maschinen in der EU auf dem Markt bereitstellen, in Verkehr bringen oder in Betrieb nehmen, betroffen sind, also auch Händler, Importeure und Bevollmächtigte. Wenn also ein Hersteller oder Marktakteur ab dem 20. Januar 2027 eine Maschine in Verkehr bringt, muss diese die neue EU-Maschinenverordnung erfüllen. Dies unabhängig davon, ob die verbauten Komponenten bereits zu einem früheren Zeitpunkt entwickelt oder zertifiziert wurden.

Neue Verordnung regelt Manipulationsschutz detaillierter

Wesentliche Säulen in der neuen Regelung betreffen neben der Verzahnung von Safety und Security die technische Umsetzung an Hardware und Software sowie die Risikobeurteilung. Im Idealfall sollten Maschinenhersteller die Anforderungen der kommenden Verordnung jetzt schon berücksichtigen.

Was die Verzahnung von Safety und Security betrifft, verlangt die neue EU-Maschinenverordnung Schutz vor „Korrumpierung“, in der IT-Sprache in Zusammenhang mit Datenbeschädigung auch als „Korruption“ bekannt. Im Safety-Bereich bedeutet dies, dass Funktionen wie beispielsweise Not-Halt oder Schutztüren gegen vorsätzliche oder versehentliche Änderungen und Manipulation physisch resistent sein müssen. Hinsichtlich Cybersicherheit wird ab 2027 eine Maschine nur dann als CE-konform gelten, wenn die Steuerungssoftware und Datenkommunikation gegen digitale Manipulationen, also Cyberangriffe, die den Betrieb gefährden, abgesichert sind.

Begrenzung des „Manipulationsanreizes“

Die technische Umsetzung an Hardware und Software erfordert zunächst eine Begrenzung des „Manipulationsanreizes“, ein Begriff, den das Berufsgenossenschaftliche Institut für Arbeitsschutz (BGIA) geprägt hat. Bei der Hardwarekonstruktion muss hierbei der Hersteller evaluieren, ob die Bauweise einer Maschine, etwa durch unpraktische Ergonomie, Mitarbeiter dazu verleitet, aus Gründen der Bequemlichkeit oder Zeiteinsparung, Schutzvorrichtungen zu umgehen. Entscheidend ist hierbei, es künftig zu erschweren, dass durch Manipulation eine Umgehung sinnvoller Maßnahmen für die Arbeitssicherheit möglich ist. Sensorik und Verriegelungseinrichtungen (gemäß ISO 14119) müssen so installiert und codiert sein, wie im Fall von hochcodierten RFID-Schaltern, dass sie nicht einfach mit Werkzeugen oder simplen Ersatzmagneten überlistet werden können. Sicherheitskritische Änderungen oder Eingriffe in die Steuerungssoftware müssen zudem für Sicherheits- und Wartungszwecke nachvollziehbar protokolliert werden.

Hinsichtlich der Risikobeurteilung werden die Hersteller gesetzlich verpflichtet sein, Cyber-Risiken und potenzielle Missbrauchsszenarien bereits vor dem Inverkehrbringen der Maschine in ihrer Risikobeurteilung zu erfassen und entsprechende Schutzmaßnahmen zu implementieren.

Problem: Bewusste Manipulation

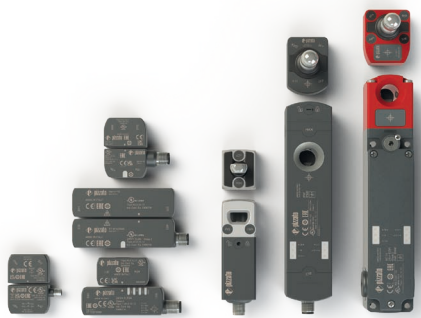
Bewusste Manipulation von Maschinen ist ein bekanntes Problem. Der Manipulationsschutz ist ein entscheidender Aspekt der neuen EU-Maschinenverordnung und verdient besonderes Augenmerk. Wie bereits skizziert, geht es darum, das bewusste Umgehen oder Deaktivieren von Schutzvorrichtungen, wie etwa das Überbrücken von Sicherheitsschaltern an Schutztüren, zu verhindern. Ziel ist es, folgenschwere Arbeitsunfälle zu vermeiden.



Anschlussleitungen mit Manipulationsschutz. Dieser Manipulationsschutz muss zerbrochen werden und demnach wird ersichtlich, dass manipuliert wurde.



Verschiedene Türzuhaltungssysteme mit codiertem Manipulationsschutz der Verschraubungen und hochcodierten RFID-Verriegelungen



Auszug Türzuhaltung Portfolio mit Manipulationsschutz und hochcodierten Zuholdungen

Diese gehen laut Branchenexperten auch darauf zurück, dass ein Viertel aller Maschinen in Betrieben bewusst manipuliert werden.

Die Manipulation und Umgehung von Sicherheitssystemen wie Sicherheitsschaltern und -sensoren gehört somit auch zu den Hauptursachen für Arbeitsunfälle. Mit diesem Thema, das ab 2027 noch strenger geregelt sein wird, befasst sich bereits die Norm DIN EN ISO 14119 im Kapitel „Minimierung von Manipulationen“. Diese zentrale Norm für Verriegelungseinrichtungen enthält konkrete Vorgaben und Klassifizierungen, um das Umgehen und die Fehlermaskierung von Sicherheitsschaltern zu verhindern. So verlangt sie, dass die Befestigungssysteme von Sicherheitsgeräten an Schutzvorrichtungen selbst nicht leicht zu entfernen sind, und schlägt Lösungen wie One-Way-Schrauben, Nieten oder andere nicht herkömmliche Befestigungssysteme vor. Für Maschinenhersteller ist dies nicht immer einfach zu bewerkstelligen und erweist sich in der Praxis zudem nicht immer als effektiv.

Diese bestehende, hier entscheidende Norm DIN EN ISO 14119 entstand in enger Zusammenarbeit mit Maschinensicherheitsexperten, woraus zugleich marktreife Lösungen für den Manipulationsschutz hervorgegangen sind. Diese gewinnen nun zunehmend an Bedeutung, je näher der Stichtag für die Umsetzung der neuen EU-Maschinenverordnung rückt.

Alternativer Ansatz für Manipulationsschutz

Ein alternativer Ansatz für den Manipulationsschutz sind nicht entfernbare Schraubenabdeckungen. Hierbei sind Kunststoffabdeckungen so konzipiert, dass sie die Befestigungsschrauben der Sicherheitseinrichtung abdecken und nach dem Anbringen am Gerät nicht mehr entfernt werden können. Dies wäre zwar durch physische Zerstörung oder anderweitige Beschädigung der Schutzabdeckung nach wie vor möglich, würde aber deutliche Spuren von Manipulation verursachen. Um die Manipulation zusätzlich zu erschweren, sind Schutzabdeckungen dieser Art nicht als Ersatzteil erhältlich, da damit Eingriffe vertuscht werden könnten. Nach einer Wartung wird die Maschine mit neuen ordnungsgemäß kodierten Abdeckungen wieder in Betrieb genommen. Es geht hierbei um Abdeckungen von Maschinen oder Gefahrenbereichen, die mit einer individuellen, eindeutigen elektronischen oder physischen Kennung (z. B. RFID, Magnetcodierung) versehen sind.

Manipulationsschutz erhöhen

Der Ansatz der nicht entfernbaren Schraubenabdeckungen hat sich in der Praxis bereits bewährt, sodass sich auf Betriebssicherheit spezialisierte Anbieter Lösungen dieser Art gewidmet haben. Bei der jüngsten Weiterentwicklung dienen kodierte Schraubenabdeckungen für Schalter und Betätiger dazu, den Manipulationsschutz bestehender Standard-Schraubenabdeckungen zu erhöhen. Jede kodierte Schutzabdeckung ist mit einem anderen alphanumerischen Code gekennzeichnet. Zwei kodierte Abdeckungen für die beiden Befestigungsschrauben, die auf dem Produkt angebracht werden, ergeben jedes Mal einen anderen Code. Wird eine Schutzabdeckung entfernt und anschließend eine neue angebracht, entsteht nicht derselbe Code, so dass eine Manipulation erkennbar wird. Durch die Erfassung der Daten der Schutzabdeckungen während der Fertigstellung der Maschine, z. B. durch Fotografieren der installierten Produkte, kann jeder Austausch im Nachhinein erkannt werden. Kodierte Schutzabdeckungen dieser Art können



Beispiel des Manipulationsschutzes: Kabelstecker und Befestigungsschrauben sind durch codierte Abdeckungen gesichert, welche nur durch Beschädigung der Abdeckung lösbar sind.

daher auch als Ersatz für Standardabdeckungen, falls diese verloren gehen, verwendet werden, ohne dass dadurch der Manipulationsschutz beeinträchtigt wird.

Kodierung

Die Kodierung, die auf jeder Schutzabdeckung angebracht ist, besteht aus einer Folge von alphanumerischen Zeichen, wobei jedes Zeichen verschiedene Werte annehmen kann, was insgesamt eine fünfstellige Anzahl von Kombinationen pro Schutzabdeckung ergibt. Bringt der Maschinenhersteller zwei Schutzabdeckungen an, entsteht ein Code mit mehr als einer Milliarde Kombinationen. Zur Verbesserung der Lesbarkeit der Codes wurden optisch ähnliche Zeichen wie die Zahl Null/0 und der Buchstabe O entfernt. Laserbeschriftung garantiert maximale Haltbarkeit und Widerstandsfähigkeit der Kodierung.

Maschinenbauer müssen zeitnah nachbessern

Die neue EU-Maschinenverordnung verknüpft erstmals funktionale Betriebssicherheit eng mit Cybersicherheit. Somit werden auch Hersteller von Maschinen für die Produktion von Medizintechnik ab Januar 2027 die neue EU-Maschinenverordnung einhalten müssen. Dies erfordert es, bei der Safety zeitnah nachzubessern. Lösungen für effektiven Manipulationsschutz an der Maschine gibt es bereits – und mit strengeren Anforderungen werden hier praxistaugliche neue Ansätze an Bedeutung gewinnen. ◀



Beispiel Schutzbereich einer Produktion bzw. Gefahrenbereiches mit abgesicherten Zugangstüren