

Sichere Maschinen mit – oder trotz – künstlicher Intelligenz

Die Europäische Kommission hat im April nicht nur einen Vorschlag für eine Verordnung zur künstlichen Intelligenz vorgelegt, sondern auch einen Vorschlag für eine Verordnung über Maschinenprodukte mit rechtlich verbindlichen Rahmenbedingungen für die Verwendung künstlicher Intelligenz, welche die Maschinen-Richtlinie 2006/42/EG ablösen soll. Ob diese Rahmenbedingungen vollständige, klare und verifizierbare Anforderungen dafür enthalten, in welchen Fällen und unter welchen Voraussetzungen sicherheitsrelevante Funktionen einer Maschine von Methoden der künstlichen Intelligenz beeinflusst oder automatisiert ausgeführt werden dürfen, muss nun geprüft werden. Dieser Artikel will hierzu einige Hinweise und Anregungen liefern.

CORRADO MATTIUZZO

Kommission Arbeitsschutz und Normung (KAN), Sankt Augustin.

SILVIA VOCK

Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA), Dresden.

THOMAS MÖSSNER

Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA), Dresden.

STEFAN VOß

Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA), Dresden.

I. Rechtliche Rahmenbedingungen

In der Europäischen Union müssen die Hersteller einer Maschine die von ihr ausgehenden Risiken beurteilen und so weit wie möglich verringern. Dazu müssen sie:

- die von ihnen vorgesehene Verwendung der Maschine eindeutig bestimmen und die bei vernünftiger Betrachtung möglichen Fehlanwendungen vorhersehen,
- die damit verbundenen Gefährdungen ausschalten oder die mit diesen Gefährdungen verbundenen Risiken nach einer festgelegten Rangfolge mindern,
- die Schwere möglicher Verletzungen oder Gesundheitsschäden und die Wahrscheinlichkeit ihres Eintretens berücksichtigen.

Auch darf von der Maschine während ihrer gesamten voraussichtlichen Lebensdauer kein höheres Risiko aus-

gehen, als das vor dem Inverkehrbringen im Rahmen der Risikobeurteilung als akzeptabel ermittelte. Insofern muss das Zusammenwirken der beiden neuen Rechtsakte sicherstellen, dass die darin enthaltenen Anforderungen an die Risikobeurteilung bzw. das Risikomanagement diesem Anspruch angemessen Rechnung tragen.

Unabdingbar ist also, dass Hersteller in der Lage sind, die von ihren Produkten ausgehenden Risiken zu beurteilen. Und genau dies wäre die Herausforderung, wollte man sich etwa auf eine durch maschinelles Lernen unterstützte Steuerung verlassen, z.B. um zu verhindern, dass Personen von beweglichen Teilen einer Maschine gefährdet werden: Die Designer von Systemen, die auf den komplexeren Methoden der künstlichen Intelligenz basieren (wie etwa maschinelles Lernen mit neuronalen Netzen), können bisher oftmals selbst im Nachhinein nicht zufriedenstellend erklären, warum sich ihr System auf eine bestimmte Weise verhalten hat. Darüber hinaus ist es schwierig, einen Nachweis über die Korrektheit des erlernten Modells zu erbringen. Dies ergibt sich unter anderem daraus, dass die Trainingsdaten nur eine Teilmenge aller möglichen Eingabewerte repräsentieren. Somit kann nicht sicher ausgeschlossen werden, dass bestimmte, während der Laufzeit des Systems auftretende Eingaben, zu falschen Entscheidungen führen.

Diese Herausforderung kann sogar im Einzelfall bei sehr komplexen transparenten und nachvollziehbaren Model-

len, z. B. bei Entscheidungsbäumen, entstehen, so dass ihre Ergebnisse nicht mit traditionellen Verfahren vorab bewertet werden können.

II. Die Rolle von Maschinensteuerungen

Einen wesentlichen Anteil an der Sicherheit einer Maschine haben Steuerungen, wenn sie dazu eingesetzt werden, Sicherheitsfunktionen auszuführen. Moderne, automatisierte Maschinen führen häufig ohne direktes menschliches Zutun Anwendungen aus und sind über Sensoren und Aktoren mit der Umgebung und/oder mit anderen Geräten verbunden. Für die dazu notwendigen Entscheidungen sind in ihre Steuerungssysteme Verlaufsstrategien programmiert. Diese können einfach oder aber sehr komplex sein, unabhängig davon, ob sie auf traditioneller Software oder auf Methoden der künstlichen Intelligenz beruhen.

Die einprogrammierten Verlaufsstrategien und Funktionalitäten können abhängig von ihrer Komplexität überprüfbar und nach bereits bewährten Verfahren bewertbar sein – dies gilt auch für weniger komplexe Methoden der künstlichen Intelligenz. Die technischen Grundlagen und Annahmen, auf denen die traditionellen, bewährten Verfahren aufbauen, um die Sicherheitstechnik des Systems zu bewerten, sind jedoch nicht für komplexere Methoden der künstlichen Intelligenz geeignet. Ein Beispiel dafür ist, dass man bisher das Auftreten von zufälligen Fehlern nur bei Hardware-Komponenten von Steuerungen annahm und man den Ausfall von Software-Komponenten nur systematischen Fehlern zuschrieb. Dieses Konzept ist für die meisten Methoden des maschinellen Lernens (ML) nicht mehr haltbar. Ein ML-Algorithmus kann beispielsweise im Betrieb anhand erfasster Daten weiterlernen und sich so an neue Gegebenheiten anpassen. Damit sind die zugrundeliegenden Programme bzw. Verlaufsstrategien in der Steuerung nicht mehr statisch und vollumfänglich festgeschrieben, Fehler können dann nicht mehr nur durch eine falsche Programmierung, sondern auch durch eine fehlerhafte, das heißt nicht im Sinne des Entwicklungsziels, erlernte Strategie verursacht werden. Auf der anderen Seite, können selbst statische und damit festgelegte Verlaufsstrategien in der Steuerung, wie sie z. B. im Falle von ML-Methoden auftreten, die nicht im Betrieb weiterlernen, ebenfalls zu Herausforderungen an die Bewertbarkeit und Überprüfbarkeit führen.

Die Bedeutung der oben besprochenen Verlaufsstrategien und Funktionalitäten können somit im Verhältnis zur Maschinen-Sicherheit wie folgt eingeordnet werden:

- **Fall 0:** Kein Einfluss auf die Maschinen-Sicherheit

Das Design des Steuerungssystems schließt mit der im Rahmen der Risikobeurteilung als erforderlich festgelegten Zuverlässigkeit¹ aus, dass die auf den Verlaufsstrategien beruhenden Entscheidungen direkt oder indirekt sicherheitsrelevante Auswirkungen haben können.

- **Fall 1:** Im Rahmen der Maschinen-Richtlinie² uneingeschränkt lösbar

Die sicherheitsrelevanten Entscheidungen des Steuerungssystems hängen ausschließlich von Verlaufsstrategien ab, welche mit Verfahren bewertbar sind, die für solche Verlaufsstrategien bereits bewährt sind.

- **Fall 2:** Im Rahmen der Maschinen-Richtlinie nur eingeschränkt lösbar

Die sicherheitsrelevanten Entscheidungen des Steuerungssystems hängen auch von Verlaufsstrategien ab, die nicht oder noch nicht mit bereits bewährten Verfahren bewertbar sind.

- **Fall 2a:** Unter bestimmten Bedingungen mit den Anforderungen der Maschinenrichtlinie vereinbar

Das Design der Maschine schließt mit der im Rahmen der Risikobeurteilung als erforderlich festgelegten Zuverlässigkeit aus, dass die auf den Verlaufsstrategien basierenden Entscheidungen zu Auswirkungen führen, die das im Rahmen der Risikobeurteilung als akzeptabel ermittelte Risiko erhöhen oder neue Risiken entstehen.

- **Fall 2b:** Mit den Anforderungen der Maschinenrichtlinie nicht vereinbar

Das Design der Maschine kann nicht mit der im Rahmen der Risikobeurteilung als erforderlich festgelegten Zuverlässigkeit ausschließen, dass die auf den Verlaufsstrategien basierenden sicherheitsrelevanten Entscheidungen zu Auswirkungen führen können, die das im Rahmen der Risikobeurteilung als akzeptabel ermittelte Risiko erhöhen, oder dass neue Risiken entstehen.

¹ Wahrscheinlichkeit, unter gegebenen Bedingungen für ein gegebenes Zeitintervall die Bedingung zu erfüllen.

² Sofern im Text der Begriff der Maschinenrichtlinie verwendet wird, ist damit die gegenwärtige Richtlinie 2006/42/EG sowie der Anspruch der Autoren an die – auf der Grundlage des am 21. April 2021 veröffentlichten Kommissionsvorschlags – nun vom Europäischen Parlament und Rat endgültig zu vereinbarende Verordnung zu Maschinenprodukten gemeint.

III. Fallbeispiele

1. Beispiele für Fall 0 aus ISO/TR 22100-5³

a) *Optimiertes Verpacken (ISO/TR 22100-5, 4.2.1.1)*

Ein Roboter belädt, optimiert durch maschinelles Lernen, eine Palette mit regellos unterschiedlich großen Teilen. Hier wird durch das im Design der Maschine vorbestimmte Einhalten der Maß- oder Gewichtsgrenzen sicher ausgeschlossen, dass durch die über maschinelles Lernen *optimierte Beladestrategie* zusätzliche Gefährdungen entstehen oder sich das Ausmaß bereits bestehender Gefährdungen erhöht. Dazu müssen allerdings z. B. Anforderungsraten für die nachgelagerten Sicherheitsfunktionen (etwa für das Einhalten der Maß- und Gewichtsgrenzen) in die Risikobeurteilung eingegangen sein, die durch die Beladestrategie nicht überschritten werden können.

b) *Optimiertes Versprühen von Pflanzenschutzmitteln (ISO/TR 22100-5, 4.2.1.2)*

Eine Bildverarbeitung mit Verwendung von KI-Verfahren des maschinellen Lernens ermöglicht es, Nutzpflanzen und Unkraut besser zu identifizieren und dadurch genauer zu entscheiden, an welcher Stelle und wieviel Herbizid versprüht wird. Hierzu werden die Maschinen zum Ausbringen der Herbizide mit Kameras ausgestattet, die mit den Sprühdüsen verbunden sind. Basierend auf dem erkannten Bild wird die optimale Herbizidmenge durch die einzelnen Sprühdüsen an den Stellen ausgebracht, an denen Unkraut erkannt wurde. Das arbeits-sichere Sprühen von Herbiziden wird durch eine Kabine (mit Filter oder Überdrucksystem) an der Spritzmaschine selbst oder dem die Spritzmaschine ziehenden Acker-schlepper gewährleistet. Es ist sichergestellt, dass durch das mit maschinellem Lernen *optimierte Identifizieren des Unkrauts* im Vergleich zur konventionellen Maschinenfunktion keine zusätzlichen Gefährdungen entstehen oder sich das Ausmaß bereits bestehender Gefährdungen erhöht.

c) *Optimierte Entnahme von Teilen aus einer Laserschneidmaschine (ISO/TR 22100-5, 4.2.1.3)*

Eine Anlage schneidet mit Laserstrahlen aus Blechen vollautomatisch Teile in einer fast unendlichen Auswahl an Formen, Größen und Dicken und entnimmt sie mithilfe von 2.500 Saugnäpfen und 180 Stiften. Gelingt die Entnahme nicht schon beim ersten Versuch, drückt die Maschine das Teil so lange mit wechselnden und durch maschinelles Lernen optimierten Methoden aus dem Schrottskelett, bis sie Erfolg hat. Trennende Schutzvorrichtungen verhindern den Zugang zum Schneidetisch und der Teileentnahme. Die durch ma-

schinelles Lernen *optimierten Entnahmestrategien* verursachen im Vergleich zur konventionellen Maschinenfunktion weder zusätzliche Gefährdungen noch erhöhen sie das Ausmaß bereits bestehender Gefährdungen. Auch hier müssen allerdings Anforderungsraten für diese trennenden Schutzvorrichtungen (z. B. Zutritt durch Personal, um Blockaden durch nicht entfernte Teile zu beheben) in die Risikobeurteilung eingegangen sein, welche durch die Entnahmestrategien nicht überschritten werden können.

2. Beispiele für Fall 1

a) *Komplexe „traditionelle“ Software in einem Sicherheitsbauteil, bewertbar nach den Konzepten der funktionalen Sicherheit*

Mittels optischer Sensoren wird ein räumlicher Gefahrenbereich überwacht. Dabei werden durch eine Software die aufgenommenen Bilddaten von drei räumlich getrennt angeordneten Sensoren zu einem dreidimensionalen Abbild des Gefahrenbereiches zusammengesetzt und auf das Eindringen von Objekten überwacht. Beim Eindringen eines Objektes in den Gefahrenbereich wird ein sicherheitsgerichteter Stopp ausgelöst. Die komplexe sicherheitsgerichtete Software wurde mit bewährten Methoden entwickelt und bewertet.

b) *Weniger komplexe Methode künstlicher Intelligenz, die nach bewährten Verfahren bewertbar ist*

Die sicherheitsrelevanten Parameter einer Aluminium-Druckgussanlage werden mittels Sensoren erfasst und in Echtzeit ausgewertet, um die Anlage abzuschalten, wenn Druck oder Temperatur außerhalb des zugelassenen Sicherheitsbereiches liegt. Ein übergeordneter Anomaliedetektor auf Basis eines Entscheidungsbaum-Algorithmus erkennt Sensor-, Netzwerk-, oder Hardwarefehler und löst einen sicherheitsgerichteten Stop aus. Durch die zusätzliche Verwendung des Anomaliedetektors können Redundanzen im Sicherheitssystem reduziert werden, ohne dass die Sicherheitsintegrität des Gesamtsystems verringert wird. Da bei der Anomaliedetektion ein erklär- und interpretierbares Modell verwendet wird und während der Laufzeit des Systems der Algorithmus als austrainiertes Modell ohne ein Weiterlernen im Betrieb verwendet wird, kann die Software des Anomaliedetektors mit anerkannten Software-Qualitätsmanagement-Methoden entwickelt, verifiziert und validiert werden. Damit kann auch die Risikobeurteilung der Druckgussanlage mit bewährten Methoden erfolgen.

³ ISO/TR 22100-5 (2021-01) „Safety of machinery — Relationship with ISO 12100 — Part 5: Implications of embedded Artificial Intelligence-machine learning“

3. Beispiele für Fall 2a

a) *Mit der Maschinen-Richtlinie vereinbares fahrerloses Transportsystem (inspiriert aber abweichend von ISO/TR 22100-5, 4.2.2)*

Ein fahrerloses Transportsystem arbeitet in einem nicht zutrittsgesicherten, aber klar abgegrenzten Bereich und optimiert seine Navigation über maschinelles Lernen selbst. Kollisionen werden technisch durch sensitive Schutzvorrichtungen und traditionell programmierte Geschwindigkeitsanpassung vermieden. Gegenüber fahrerlosen Transportsystemen, die nur in vorgegebenen Bahnen oder gar nur in zutrittsgesicherten Bereichen arbeiten, sind die Anforderungen an das Vermeiden von Kollisionen erhöht. Es entstehen aber keine neuen Gefährdungen, und die Risiken können mit bewährten Methoden bewertet und auf ein akzeptables Maß verringert werden.

b) *Ergänzende signalisierende Assistenzsysteme*

Eine große Werkzeugmaschine ist entsprechend dem Stand der Technik mit trennenden und sensitiven Schutzausrüstungen versehen, um Bedien- und dritte Personen zu schützen. Ergänzend zu diesen, nach geltendem Produktsicherheitsrecht bereits ausreichenden Maßnahmen warnt ein Assistenzsystem akustisch, wenn sich eine Person in den Gefahrenbereich begibt, ohne dabei selbstständig in die Maschinensteuerung einzugreifen. Das Assistenzsystem lernt maschinell während des laufenden Betriebs weiter, um das Erkennen von Personen stetig zu optimieren und um mit den so gewonnenen Daten Praxiserfahrungen für evtl. zukünftige Anwendungen zu sammeln⁴.

4. Beispiel für den Fall 2b

Mit der Maschinen-Richtlinie (gegenwärtig) nicht vereinbares fahrerloses Transportsystem (inspiriert aber abweichend von ISO/TR 22100-5, 4.2.2)

Ein fahrerloses Transportsystem arbeitet in einem nicht zutrittsgesicherten, aber klar abgegrenzten Bereich und optimiert seine Navigation über maschinelles Lernen selbst. Kollisionen werden technisch durch sensitive Schutzvorrichtungen und, abweichend vom 1. Beispiel unter Fall 2a, durch *über maschinelles Lernen optimierte Geschwindigkeitsanpassung* vermieden. Das verwendete maschinelle Lernverfahren ist weder interpretier- noch erklärbar und lernt dynamisch während des Betriebes weiter. Zwar entstehen auch hier nicht zwangsläufig neue Gefährdungen, jedoch können die Risiken nicht mehr mit bewährten Methoden bewertet und dadurch sicher auf

ein akzeptables Maß verringert werden. Diese Unmöglichkeit, die Risiken zu bewerten, macht die beschriebene Fallkonstellation unvereinbar mit den Anforderungen der Maschinen-Richtlinie.

IV. Folgerungen

Einerseits gibt es auch für sehr komplexe, gegenwärtig nicht bewertbare technische Konstellationen Ansätze, die Sicherheit vertrauenswürdig zu belegen, indem „Argumente“ definiert werden, die (induktiv hergeleitete) "starke" Indizien (nicht den absoluten Beweis) liefern sollen. Solche Ansätze werden schon lange beispielsweise in der Nukleartechnik oder der Luft- und Raumfahrt angewendet, aber auch um zu prüfen, ob Software für den sicherheitsrelevanten Einsatz geeignet ist.

Gegenwärtig wird deswegen angestrebt, mit solchen eher aus dem Risikomanagement kommenden Ansätzen auch für Methoden der künstlichen Intelligenz Kriterienkataloge für das Erreichen eines akzeptablen Risikoniveaus aufzustellen. Diese Kriterienkataloge können Festlegungen zu Spezifikation und Modellierung, Erklärbarkeit und Nachvollziehbarkeit von Entscheidungen, Übertragbarkeit auf unterschiedliche Situationen, Verifizierung und Validierung des Systems, Überwachung während der Laufzeit, Mensch-Maschine-Interaktion, Prozesssicherung und Zertifizierung sowie sicherheitsbezogener Ethik und Datensicherheit enthalten. In diese Richtung geht offenbar auch der Vorschlag der EU-Kommission zur künstlichen Intelligenz. Ein solcher Ansatz bedeutet, dass Sicherheit nicht vorwiegend durch nachprüfbar Produkt-eigenschaften definiert wird, sondern durch nachprüfbar Prozesskriterien.

Andererseits muss, um sich einem hohen Sicherheitsniveau im Sinne der europäischen Produktsicherheitsvorschriften und des Grundgedankens der Prävention am Arbeitsplatz anzunähern, aber erst einmal nachgewiesen werden, dass die Kriterien für die oben genannten „Argumente“ vollständig und verlässlich sind. Konservativ betrachtet, dürfen daher auch Vorschriften, die hierfür den Rahmen und grundlegende Anforderungen vorgeben sollen, erst festgelegt werden, wenn sich die ihnen zu Grunde liegenden Annahmen verlässlich bewährt haben. Dafür bestand aber aus Sicht der europäischen Gesetzgeber kein zeitlicher Spielraum: die Kommissionsvorschläge zur Überarbeitung der Maschinen-Richtlinie und zur künstlichen Intelligenz liegen jetzt zeitgleich vor.

⁴ Das Beispiel adressiert nicht die Aspekte von möglichen Auswirkungen auf das Bedienerverhalten, die im Rahmen dieses Artikels nicht thematisiert werden.

Inwieweit die beiden Verordnungsvorschläge vollständige, klare und verifizierbare Anforderungen dafür enthalten, in welchen Fällen und unter welchen Voraussetzungen sicherheitsrelevante Steuerungsfunktionen einer Maschine von Methoden der künstlichen Intelligenz beeinflusst oder automatisiert getroffen werden dürfen, bzw. ob damit eine ausreichende rechtliche Grundlage für Verfahren und Bewertungsansätze für eine sachgerechte Risikobetrachtung vorliegen, gilt es nun zu prüfen. Genügen die beiden Rechtsakte am Ende des Gesetzgebungsverfahrens diesen Anforderungen nicht, würde ihre Anwendung zu erheblichen Unsicherheiten für die beteiligten Akteure im Markt führen. Es lässt sich feststellen, dass noch Interpretations-, Forschungs- und Normungsbedarf vorliegt und die Bearbeitung durch den interdisziplinären Ansatz des Themas für die einzelnen Fachdisziplinen mit großen Herausforderungen verbunden ist.

V. Ausblick

Sowohl die im Entwurf der neuen Maschinenprodukteverordnung enthaltenen grundlegenden Sicherheits- und Gesundheitsschutzanforderungen als auch die im Entwurf zur Verordnung über Künstliche Intelligenz enthaltenen Anforderungen sind als technologieneutrale Schutzziele formuliert. Spezifische Festlegungen zur Erfüllung dieser Schutzziele erfolgen in den harmonisierten Normen unter den beiden künftigen Verordnungen.

Für die Anwendung von Verlaufsstrategien für sicherheitsrelevante Steuerungsfunktionen sind folgende Prämissen von Bedeutung:

- Die auf den Verlaufsstrategien basierenden sicherheitsrelevanten Steuerungsfunktionen dürfen nicht zu einem Überschreiten der durch die Risikobeurteilung festgelegten Grenzen führen.
- Die auf den Verlaufsstrategien beruhenden sicherheitsrelevanten Steuerungsfunktionen müssen mit der in der Risikobeurteilung für die jeweilige Sicherheitsfunktion festgelegten Zuverlässigkeit erfolgen.
- Es müssen Methoden existieren, mit der im Rahmen der Risikobeurteilung die Zuverlässigkeit der auf den Verlaufsstrategien beruhenden sicherheitsrelevanten Steuerungsfunktionen bewertet werden kann.

Anforderungen an Software für Sicherheitsfunktionen sind in den Normen der Reihe DIN EN 61508⁵ sowie in DIN EN 62061:2016-05⁶ zu finden. Auch in den Entwurf der DIN EN ISO 13849-1:2020⁷ sind jetzt Anforderungen an Software zum Einsatz für Sicherheitsfunktionen in Maschinen aufgenommen worden. Es ist also zu prüfen, ob

diese Normen für die Entwicklung von Software, die mit künstlicher Intelligenz ausgestattet ist, ausreichend sind und verwendet werden können.

Da Sicherheitsfunktionen einen nicht unerheblichen Beitrag zur Risikominderung leisten, wird von ihnen auch ein hohes Maß an Zuverlässigkeit erwartet, der durch die erforderlichen Performance Level (PL) oder Sicherheitsintegritätslevel (SIL) ausgedrückt wird. Sollen Verfahren der Künstlichen Intelligenz in Software für Sicherheitsfunktionen eingesetzt werden, müssen diese natürlich die geforderten hohen Zuverlässigkeitswerte erreichen. Hier besteht zum einen noch ein Bedarf nach Steigerung der Zuverlässigkeit der KI-Verfahren. Zum anderen ist es notwendig Methoden zur Überprüfung dieser Zuverlässigkeit soweit zu entwickeln, dass sie allgemein anerkannt sind und für die Überprüfung der Zuverlässigkeit von Sicherheitsfunktionen mit KI-Komponente standardisiert werden können.

Bezogen auf das Beispiel 2b wären folgende Voraussetzungen notwendig, damit es als mit der Maschinenrichtlinie vereinbar angesehen werden kann:

- Die Software für die Sicherheitsfunktion Geschwindigkeitsanpassung, die mit maschinellem Lernen optimiert wird, kann mit einem, z. B. in harmonisierten Normen, anerkannten Verfahren entwickelt werden.
- Die Zuverlässigkeit des KI-Algorithmus ist überprüfbar, z. B. mittels harmonisierter Normen.
- Die Sicherheitsfunktion erreicht die für sie erforderliche Zuverlässigkeit (PL, SIL) auch mit der enthaltenen KI-Komponente.
- Durch eine Überprüfung nach einem Optimierungsschritt ist sichergestellt, dass die in der Risikobeurteilung festgelegten Grenzen nicht überschritten werden.

Es muss weiterhin geklärt werden, inwieweit bestehende Risikobewertungsverfahren dafür geeignet sind, Methoden der künstlichen Intelligenz in Verbindung mit entsprechenden Anwendungsszenarien sachgerecht zu beurteilen. Hierbei besteht der Bedarf Risikobewertungsverfahren weiterzuentwickeln, um das bestehende hohe Schutzniveau des europäischen Binnenmarktes auch für die Zukunft sicherzustellen. ■

⁵ Normenreihe DIN EN 61508 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“.

⁶ DIN EN 62061 (2016-05) „Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme“.

⁷ DIN EN ISO 13849-1 (2020) „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsgrundsätze“.