Methoden zur Risikoeinschätzung

Neue Maschinenverordnung mit zusätzlichen Anforderungen an die Risikoanalyse

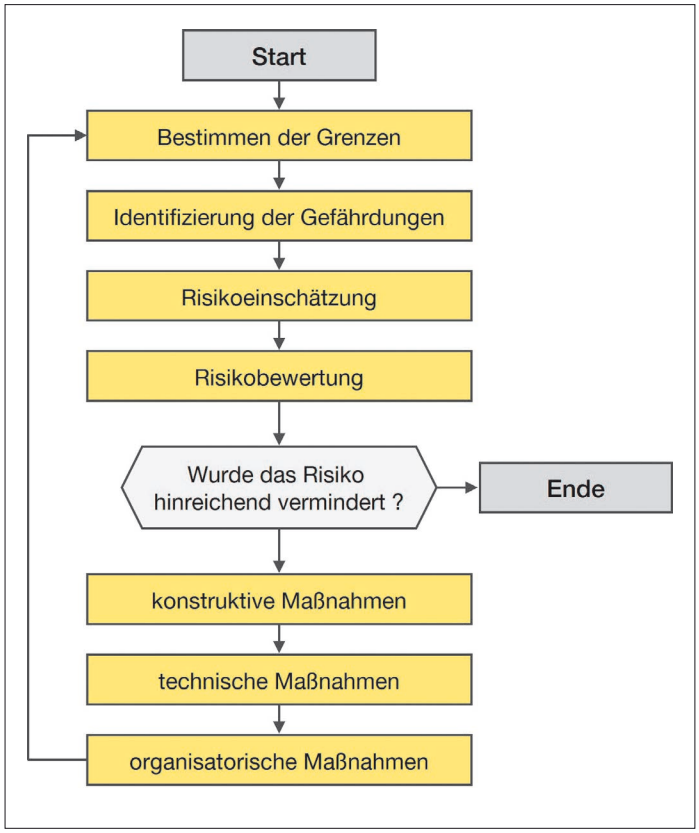

Bild 1: Iteratives Verfahren zur Risikobewertung nach der Norm ISO 12100

Die Europäische Maschinenrichtlinien verlangt, dass für jede Maschine vor dem Inverkehrbringen eine Risikoanalyse durchgeführt werden muss. Durch das Zusammenwachsen von IT und OT sowie die rasante technologische Entwicklung war es notwendig, die Maschinenrichtline zu überarbeiten. Daraus entstand die neue Maschinenverordnung: Sie wird die Maschinenrichtlinie als rechtliche Grundlage ablösen. Sie enthält zusätzliche Anforderungen an die Risikoanalyse. Im Folgenden werden neben dem generellen Vorgehen für die Risikoanalyse verschiedene Verfahren für die Risikoeinschätzung vorgestellt und ihre Eigenschaften erläutert.

Rechtliche Grundlagen

Nach der EU-Maschinenrichtlinie 2006/42/EG darf ein Hersteller von Maschinen keine Maschinen in Verkehr bringen, von denen eine Gefahr ausgeht. Zum Nachweis führt er eine CE-Konformitätsbewertung durch, die das Erstellen einer Risikoanalyse beinhaltet. Maschinen dürfen nur dann ein CE-Zeichen tragen, wenn der Bewertungsprozess komplett durchlaufen wurde und die Risikoanalyse zeigt, dass die Maschine sicher ist.

Die Maschinenrichtlinie beschreibt den Prozess der Risikoanalyse sehr allgemein, selbst wenn sie in einem Anhang mögliche Gefahren auflistet, die bei der Analyse betrachtet werden müssen. Eine genauere Beschreibung des Prozesses der Risikoanalyse findet man in der Norm ISO 12100 - Risikobeurteilung und Risikominderung (Bild 1). Sie definiert ein iteratives Verfahren, bei dem man zuerst die Gefährdungen identifiziert, einschätzt und bewertet. Falls die Bewertung zeigt, dass unzumutbare Gefährdungen vorhanden sind, müssen diese vermindert werden. Das Vorgehen zur Verminderung der Gefährdungen ist in drei Stufen unterteilt, deren Reihenfolge zwingend einzuhalten ist.

Konstruktive Maßnahmen

Die erste Stufe sind konstruktive Maßnahmen. Dies bedeutet, dass die Maschine so gestaltet werden muss, dass sie sicher ist. Sollte das nicht möglich sein, kann der Hersteller technische Maßnahmen einsetzen. Dazu zählen beispielsweise trennende Schutzeinrichtungen wie z. B. Zäune oder nichttrennende Schutzeinrichtungen wie beispielsweise Sicherheits-Lichtvorhänge. Beide sorgen dafür, dass Bediener die Gefährdungen nicht mehr erreichen können. Falls weder technische noch konstruktive Maßnahmen möglich sind, dürfen organisatorische Maßnahmen eingesetzt werden. Eine solche wäre unter anderem die Unterweisung der Mitarbeiter.

Sind die definierten Maßnahmen zur Risikoreduzierung umgesetzt, startet der iterative Prozess erneut. Dadurch identifiziert man eventuelle weitere Gefährdungen, die durch die Maßnahmen nicht vollständig beseitigt wurden oder die durch die Maßnahmen neu entstanden sind. Der iterative Prozess endet erst, wenn alle Gefährdungen genügend vermindert sind.

Die neue Maschinenrichtlinie

Die neue EU-Maschinenverordnung EU 2023/1230 löst die Maschinenrichtlinie am 20.01.2027 ab. Eine Übergangsregelung ist nicht vorgesehen. Eine Überarbeitung der Maschinenrichtlinie war durch den technischen Fortschritt notwendig. Die Maschinenverordnung detailliert nun Anforderungen an die Sicherheit von Maschinen, die in den Bereichen

- Vernetzung von Maschinen
- Digitalisierung und komplexere Steuerungstechnik
- neue Technologien wie z. B. KI oder kollaborierende Roboter
- entstehen.

Anhang III

Im Anhang III – Sicherheitsanforderungen für Konstruktion und Bau von Maschinen – geht die Maschinenverordnung (MVO) auf Gefährdungen ein, die in der Maschinenrichtlinie nicht explizit aufgeführt sind. Die nachfolgenden Abschnitte beschreiben die wesentlichen Änderungen für die Risikoanalyse.

Bei der Vernetzung von Maschinen ist dies der Schutz vor Korrumpierung. Die Anbindung von Hardware bzw. Software darf nicht zu einer Beschädigung führen. Zusätzlich muss ein unbefugter Zugriff auf die Maschine und die

Autor:
Rolf Brunner
Senior Safety Expert
Leuze electronic GmbH + Co. KG
www.leuze.com

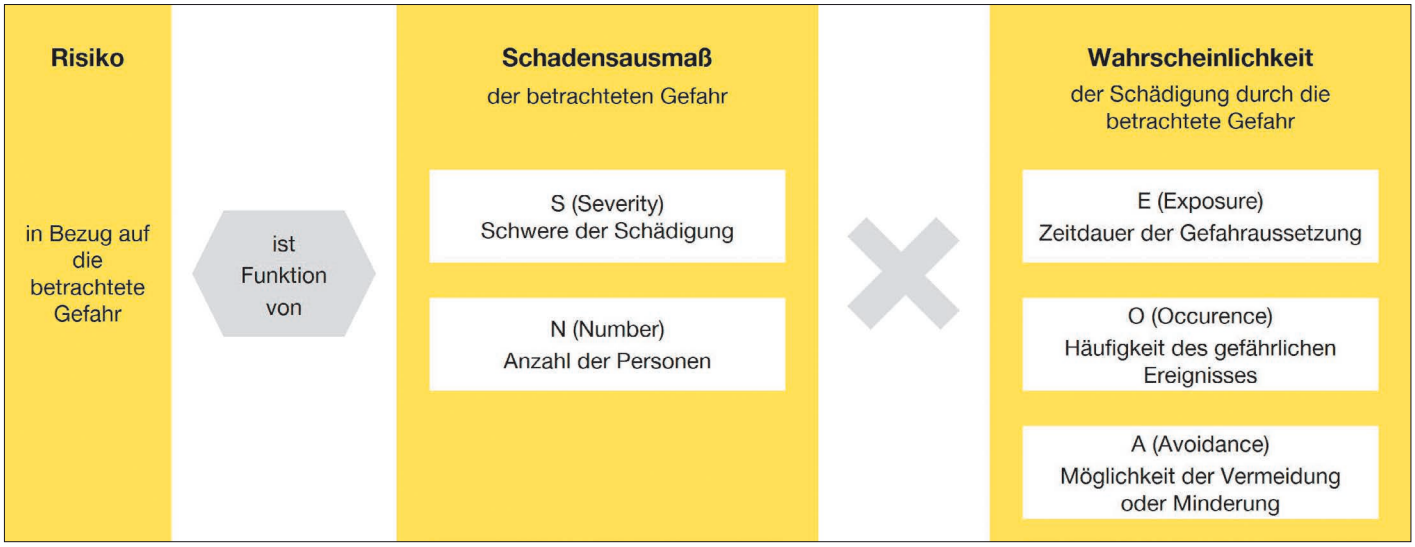

Bild 2: Parameter der Risikoeinschätzung

Möglichkeit zur Manipulation von Daten verhindert werden. Auch der Ausfall oder das Wiederherstellen einer Kommunikationsverbindung darf zu keiner gefährlichen Situation führen.

Die Steuerungen von Maschinen müssen gegen eine Beeinflussung von außen geschützt sein, so dass es zu keiner absichtlichen oder unbeabsichtigten Veränderung der Software oder der Konfiguration kommen kann. Ein Zugriffsprotokoll über Veränderungen der Hardware und/oder Software ist für fünf Jahre zu speichern. Sowohl die Software als auch die Konfiguration müssen eine Identifikation (ID) haben.

Weiterhin regelt die MVO das Thema künstliche Intelligenz von selbst lernenden Systemen. Maschinen dürfen keine Handlungen ausführen, die über ihre festgelegte Aufgabe und Bewegungsbereich hinausgehen. Daten, die zu sicherheitsrelevanten Entscheidungen führen, müssen ein Jahr lang archiviert werden. Weiterhin muss es jederzeit möglich sein, die Maschine zu korrigieren, um die Sicherheit zu wahren. Auch für autonome, mobile Maschinen definiert die MVO zusätzliche Anforderungen. So müssen sie Hindernisse oder Personen erkennen, und bei Kollisionen dürfen Batterien keine Gefährdung verursachen.

Parameter der Risikoeinschätzung

Generell gibt es keine Maßeinheit für ein Risiko. Gebräuchlich ist die Beschreibung des Risikos mit niedrig / hoch, durch eine Risiko-Kennzahl oder durch eine Ausfallwahrscheinlichkeit. Eine textuelle Beschreibung des Risikos ist oft leichter zu verstehen als die Definition mit Kennzahlen. Soll das tatsächliche Risiko anhand einer Kennzahl eingeschätzt werden, so muss deren Wertebereich bekannt sein.

Die Maschinenrichtlinie definiert, dass zur Bestimmung des Risikos einer betrachteten Gefahr zwei Parameter berücksichtigt werden müssen: das Schadensausmaß und die Wahrscheinlichkeit einer Schädigung (Bild 2).

Schadensausmaß

Diese beiden Parameter können – abhängig vom dem zur Risikoeinschätzung verwendeten Verfahren – in weitere Parameter unterteilt sein. Manche Verfahren unterteilen das Schadensausmaß in

- Schwere der Schädigung (S, Severity)
- Anzahl der geschädigten Personen (N, Number).

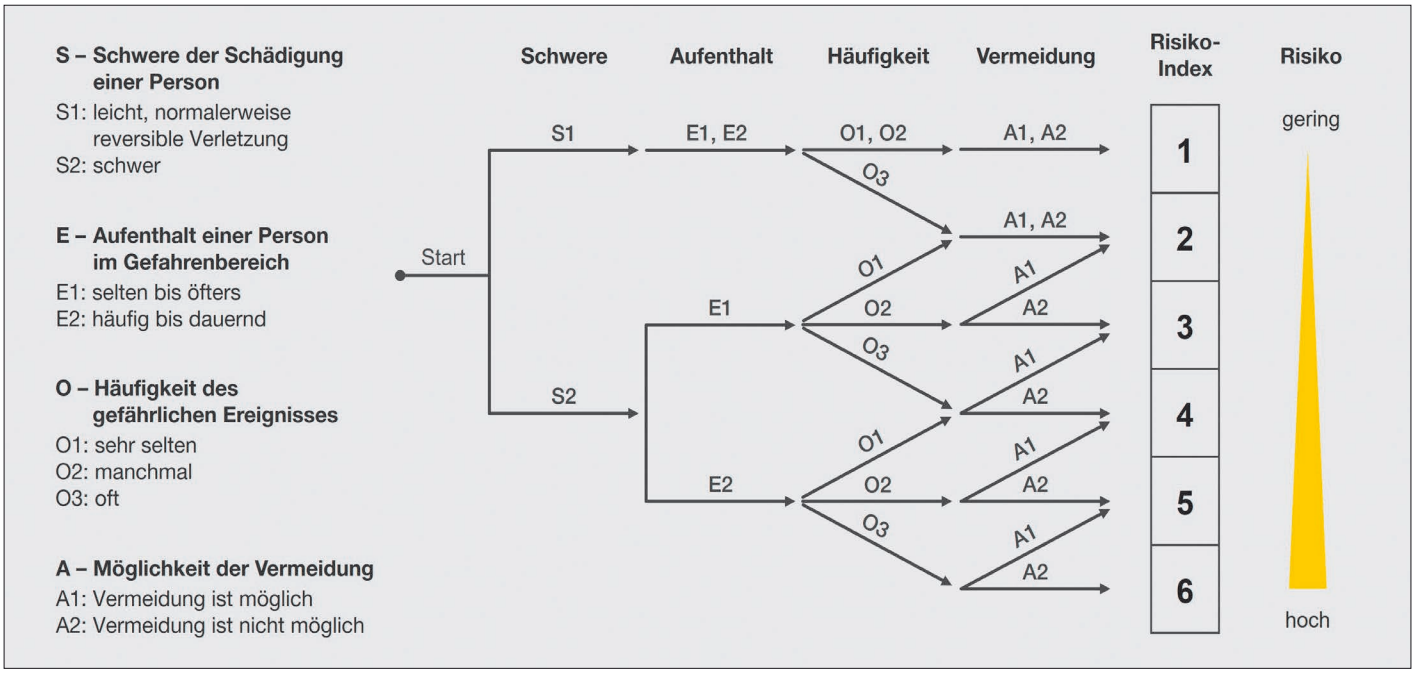

Bild 3: Risikograph nach ISO/TR 14121-2

Kategorie der Wahrscheinlichkeit	Schwere des Schadens			
	1 – Hoch	2 - Mittel	3 – Gering	4 – Unbedeutend
A – Sehr wahrscheinlich	1A	2A	3A	4A
B – Wahrscheinlich	1B	2B	3B	4B
C – Gelegentlich	1C	2C	3C	4C
D – Selten	1D	2D	3D	4D
E – Unwahrscheinlich	1E	2E	3E	4E
F – Sehr unwahrscheinlich	1F	2F	3F	4F

Bild 4: Risikotabelle der ISO 14798

In der Automatisierungstechnik ist von einem Ereignis normalerweise nur eine Person betroffen, so dass der Parameter N dort keine Bedeutung hat. In der Prozesstechnik, wo bei einem Ereignis viele Personen geschädigt werden könnten, ist der Parameter N wichtig zur Beurteilung des Risikos.

Wahrscheinlichkeit

Um die Wahrscheinlichkeit einer Schädigung genauer zu definieren, wird diese oft in die Unterparameter

- Zeitdauer der Gefahraussetzung (E, Exposure)
- Häufigkeit des gefährlichen Ereignisses (O, Occurence)
- Möglichkeit zur Vermeidung des gefährlichen Ereignisses (A, Avoidance)
- unterteilt.

Nicht jedes gefährliche Ereignis führt automatisch zu einem Schaden. Ein Schaden tritt nur ein, wenn sich gleichzeitig zum gefährlichen Ereignis eine Person im gefährdeten Bereich aufhält und nicht in der Lage ist, der Gefahr auszuweichen. In der Praxis minimiert man entweder die Zeitdauer der Gefährdung, E, mit einem Schutzzaun oder die Häufigkeit der Gefährdung, O, durch einen Maschinenstopp mit sicherer Sensorik, um ein sicheres System zu erhalten.

Risikodarstellung

Zusammenfassend kann man das Risiko wie folgt darstellen:

S=f(S, N)* f(E, O, A)

Verfahren zur Risikoeinschätzung

Die Ziele der Risikoeinschätzung sind das Quantifizieren des Risikos mittels der oben angegebenen Parameter und das Darstellen des Risikos durch eine Risikokennzahl als Zahlenwert. Zur Einschätzung des Risikos gibt es keine normativen Vorgaben. Allerdings geben manche Normen ein Verfahren im informativen Anhang an. Weiterhin können Verfahren aus technischen Berichten von Normungsorganisationen oder anderen Veröffentlichungen stammen. Der Maschinenhersteller ist in der Wahl des Verfahrens frei. Generell sollte die Risikoeinschätzung im Team erfolgen, um eine möglichst objektive Bewertung zu erhalten.

Die Verfahren zur Risikoanalyse lassen sich in drei Klassen einteilen:

- graphische Verfahren
- tabellarische Verfahren
- numerische Verfahren

Graphische Verfahren bestimmen das Risiko durch einen Graphen. Jeder Knoten hat meist nur zwei Zweige, die zwei unterschiedliche Parameterwerte repräsentieren. Dabei sind die Auswahlmöglichkeiten textuell beschrieben. Das Risiko ist aufgrund der geringen Auswahlmöglichkeiten meist nur grob klassifiziert, aber leicht verständlich und einfach nachvollziehbar.

Als Beispiel für ein graphisches Verfahren soll der Risikograph nach der Norm ISO/TR 14121-2 - prak-

PE Probability of Exposure			**FE Frequency of Exposure**	
0	Impossible	cannot happen	0,1	Infrequently
1	Unlikely	though conceivable	0,2	Annually
2	Possible	but unusual	1	Monthly
5	Even Chance	could happen	1,5	Weekly
8	Probable	not surprised	2,5	Daily
10	Likely	to be expected	4	Hourly
15	Certain	no doubt	5	Constantly
MPH Maximum Probable Harm			**NP Number of Persons at Risk**	
0,1	Scratch or bruise		1	1 – 2 persons
0,5	Laceration or mild ill health effect		2	3 – 7 persons
1	Break of a minor bone or minor illness (temporarily)		4	8 – 15 persons
2	Break of a major bone or minor illness (permanent)		8	16 – 50 persons
4	Loss of a limb, eye or serious illness (temporarily)		12	50+ persons
8	Loss of limbs, eyes or serious illness (permanent)			
15	Fatality			

HRN = PE x FE x MPH x NP

RISK	Negligible	Very low	Low	Significant	High	Very high	Extreme	Unacceptable
HRN	0 - 1	1 - 5	5 - 10	10 - 50	50 - 100	100 - 500	500 - 1000	Above 1000

Bild 5: Numerisches Verfahren nach HRN

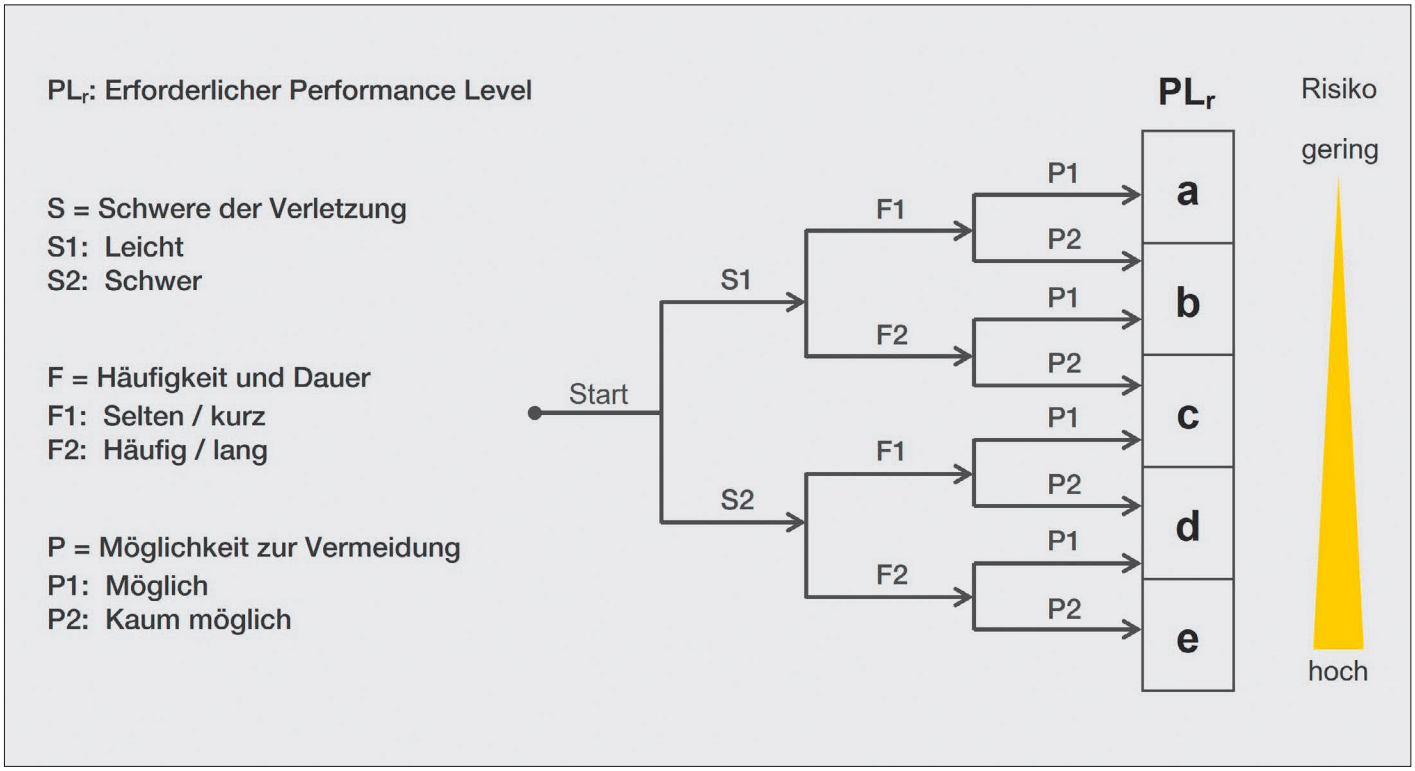

Bild 6: Risikograph nach ISO 13849-1

tischer Leitfaden und Methodenbeispiele, vorgestellt werden (Bild 3). Er wird oft verwendet, um die Wirksamkeit von risikomindernden Maßnahmen darzustellen und hat die vier Parameter S, E, O, A. Der resultierende Risikoindex hat einen Zahlenwert zwischen 1 und 6. Die Werte 1 und 2 repräsentieren einen Zustand geringer Gefahr. Das Beispiel zeigt auch, dass Graphen mit mehr als zwei Zweigen je Knoten unübersichtlich werden.

Tabellarische Verfahren

haben meist mehr als zwei Werte je Parameter, die textuell beschrieben sind. Es gibt mehr Auswahlmöglichkeiten als bei graphischen Verfahren. Die Klassifizierung erfolgt dennoch relativ grob, da die Anzahl der Parameter beschränkt ist, um die Übersichtlichkeit zu erhalten.

Ein einfaches Beispiel für ein tabellarisches Verfahren ist in der Norm ISO 14798 - Aufzüge, Fahrtreppen und Fahrsteige beschrieben (Bild 4). Es hat nur die zwei Parameter ‚Schwere des Schadens' und ‚Wahrscheinlichkeit einer Gefährdung'. Dadurch ist das Verfahren übersichtlich, die Klassifikation erfolgt allerdings wie beim graphischen Verfahren nur grob. Der resultierende Risikoindex ist durch eine Zahl und einen Buchstaben beschrieben, die eine geringe, mittlere oder große Gefährdung ausdrücken.

Numerische Verfahren

bestimmen eine Risikokennzahl durch Addition oder Multiplikation der Parameterwerte. Dadurch sind viele Parameter mit vielen unterschiedlichen Werten möglich, und das Risiko wird feingranularer bestimmt. Dies kann zu einem falschen Eindruck von Genauigkeit führen, da die Parameterwerte immer subjektiv bestimmt werden und von den Fähigkeiten des Anwenders abhängen. Dennoch hilft die feinere Granularität, die Gefährdung unterschiedlicher Risiken miteinander zu vergleichen. Durch die vielen Parameter und Auswahlmöglichkeiten sind numerische Verfahren nicht so einfach und übersichtlich wie graphische oder tabellarische Verfahren.

Durch die feine Granularität ist es möglich, das Risiko verschiedener Gefährdungen miteinander zu vergleichen und die Gefährdung mit dem größten Risiko zu identifizieren. Dies kann wichtig sein, um die Schritte zur Überarbeitung einer Maschine zu priorisieren.

Schwere (S)	Wahrscheinlichkeit (K) = E + O + A				
	3 bis 4	5 bis 7	8 bis 10	11 bis 13	14 bis 15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3	-	(AM)	SIL 1	SIL 2	SIL 3
2	-	-	(AM)	SIL 1	SIL 2
1	-	-	-	(AM)	SIL 1

Bild 7: Risikoeinschätzung nach IEC 62061

Hazard Rating Numbers

Ein Beispiel für ein numerisches Verfahren ist HRN, Hazard Rating Numbers (Bild 5). Es wurde 1990 von Chris Steel veröffentlicht und existiert in mehreren Varianten. Die textuelle Beschreibung der vielen Parameterwerte erschwert jedoch die Auswahl des korrekten Werts. Die ursprüngliche Form besteht aus den vier Parametern S, N, E, O. Der Parameter A für die Möglichkeit des Ausweichens wurde weggelassen. Das resultierende Risiko wird durch Multiplikation ermittelt:

R=S*N*E*O

Risiko R = S x E x O x A			
Risikokennzahl	Bewertung	Entspricht nach ISO 13849-1	Entspricht nach IEC 62061
< 11	Vernachlässigbar	-	-
11 - 60	Gering	PL b	SIL 1
60 - 400	Erhöht	PL c	SIL 1
400 - 1000	Hoch	PL d	SIL 2
> 1000	Extrem	PL e	SIL 3

S (Severity): Schadensausmaß
E (Exposure): Zeitdauer der Gefährdung
O (Occurence): Häufigkeit und Zeitdauer der Gefahr
A (Avoidance): Möglichkeit des Ausweichens

Bild 8: Risikobewertung nach HARMONY

Durch die Multiplikation kann es ausreichen, wenn ein Parameter sehr klein ist oder durch eine Risikominderung sehr klein wird.

Risikoreduzierung durch technische Maßnahmen

Ergibt die Risikobewertung ein zu hohes Risiko, muss es durch passende Maßnahmen reduziert werden. Die Reihenfolge der Maßnahmen ist festgelegt. Technische Maßnahmen können erst realisiert werden, wenn konstruktive nicht möglich sind.

Technische Maßnahmen werden oft mit sicheren Steuerungen realisiert, die Teil einer Sicherheitsfunktion sind. Eine Sicherheitsfunktion besteht aus sicheren Komponenten, d. h. sicheren Sensoren, einer sicheren Steuerung und sicheren Aktoren. Die Komponenten müssen eine bestimmte Zuverlässigkeit erfüllen, welche die Wahrscheinlichkeit eines gefährlichen Ausfalls der Komponente definiert. Sie muss umso höher sein, je größer das Risiko ist, welches sie absichern: bei einem Ausfall der Komponenten ist der Schutz vor der Gefährdung nicht mehr vorhanden. Die Zuverlässigkeit der Komponente wird auch als Sicherheitslevel bezeichnet. Zu seiner Bestimmung muss deshalb eine Risikoeinschätzung durchgeführt werden. Das Ergebnis ist in diesem Fall keine Risikozahl, die das Risiko definiert, sondern einen mindestens notwendigen Sicherheitslevel der Komponenten der Sicherheitsfunktion.

Sicherheitslevel ermitteln

Normen zu sicherheitsbezogenen Steuerungssystemen definieren eigene Verfahren zur Risikoeinschätzung, mit denen man den erforderlichen Sicherheitslevel ermitteln kann.

In der Automatisierungstechnik wird meist die Norm ISO 13849-1 - sicherheitsbezogene Teile von Steuerungen - für die Definition des Sicherheitssystems einer Maschine verwendet. Sie kann für elektronische, mechanische, hydraulische und pneumatische Systeme angewendet werden. Anhang A beschreibt einen Risikograph zur Bestimmung des notwendigen Performance Levels PLr der Sicherheitsfunktion (Bild 6). Der Risikograph enthält drei Parameter: das Schadensausmaß (S), die Aufenthaltsdauer im gefährlichen Bereich (E) und die Möglichkeit der Vermeidung (A). Wie auch andere graphische Verfahren ist es einfach und übersichtlich und arbeitet mit einer groben Klassifikation. Wählen Anwender bei Unsicherheit den höheren Wert, sind die resultierenden Anforderungen zu hoch und die Sicherheitstechnik wird unnötig teuer.

IEC 62061

Eine Alternative für elektrische und elektronische Steuerungssysteme ist die Norm IEC 62061- funktionale Sicherheit sicherheitsbezogener Steuerungssysteme. Anhang A beschreibt eine Kombination aus tabellarischem und numerischem Verfahren zum Ermitteln des erforderlichen Sicherheitslevels SILCL der Sicherheitsfunktion (Bild 7). Das Verfahren ist komplexer als der Risikograph der 13849-1. Allerdings ist eine detailliertere Klassifikation möglich, da für die vier Parameter mehr unterschiedliche Werte zur Auswahl stehen.

Risikoeinschätzung nach HARMONY

Bei den beschriebenen Abläufen führt der Anwender die Risikoeinschätzung zwei Mal mit unterschiedlichen Verfahren und unterschiedlichen Zielen durch: zuerst mit Verfahren 1 für die Einschätzung des initialen und finalen Risikos einer Gefährdung und nachfolgend mit Verfahren 2 zur Bestimmung des Sicherheitslevels der Sicherheitsfunktion.

Dieses Vorgehen erscheint unnötig kompliziert und aufwändig. Eine deutliche Vereinfachung ist möglich, wenn das Verfahren zur Risikoeinschätzung neben der Risikokennzahl automatisch auch ein Sicherheitslevel für technische Maßnahmen definiert.

Aus diesem Grund hat Leuze in seinem Verfahren HARMONY diese Anforderung erfüllt. Der Begriff HARMONY steht für die Kurzform von HAzard Rating for Machinery and prOcess iNdustrY. Das Verfahren ist in der Automatisierungstechnik und der Prozesstechnik einsetzbar.

HARMONY ist eine Anpassung des numerischen Verfahrens HRN und ermittelt eine Risikokennzahl durch Multiplikation der Parameter Schadensausmaß (S), Zeitdauer der Gefährdung €, Häufigkeit des gefährlichen Ereignisses (O) und die Möglichkeit der Vermeidung (A):

R=S*E*O*A

Der Wertebereiche der Risikokennzahl R sind so definiert, dass man ihnen einen Performance Level PLr nach ISO 13849-1 oder einen Safety Integrity Level SILCL nach IEC 62061 zuordnen kann. Bild 8 zeigt diese Zuordnung.

Fazit

Nach der Maschinenrichtlinie und der sie ablösenden Maschinenverordnung muss für jede Maschine vor dem Inverkehrbringen eine Risikoanalyse durchgeführt werden, da von ihr zu keinem Zeitpunkt eine Gefahr ausgehen darf.

Bei der Risikoanalyse ist ein systematisches und sorgfältiges Vorgehen wichtig, um alle Gefährdungen zu identifizieren. Nur wenn die Gefährdung identifiziert ist, kann durch eine entsprechende Maßnahme die Risikoreduzierung erfolgen. Dies ist aufwändig und zeitintensiv. Zur Risikoeinschätzung stehen unterschiedliche Verfahren zur Verfügung, es gibt jedoch keine normativen Vorgaben. Jede Organisation muss selbst die passende Vorgehensweise finden. Kriterien für die Auswahl können die Komplexität der Aufgabe oder das Fachwissen bzw. Vorlieben der Mitarbeiter sein. Das Verfahren HARMONY hilft, das Vorgehen für die Risikoeinschätzung zu vereinfachen und den Aufwand zu reduzieren. ◄