

Ein arithmetisches Mittel zur Sicherheit

Kaum ein Begriff einem so starken Wandel unterworfen, wie Sicherheit. Erkannt hat dies die Europäische Union (EU) auch für den Bereich Antriebstechnik – mit einer Gesetzgebung, die dem Paradigmenwechsel des Sicherheitskonzeptes Rechnung trägt. Auch Hersteller einzelner Komponenten von Sicherheitssystemen, wie etwa Drehgeber, müssen umdenken.

TEXT: Claudia Homburg BILDER: Fritz Kübler GmbH

Schon die „alte“ Maschinenrichtlinie (MSR) 98/37/EG, in Kraft seit dem 1. Januar 1995 und mit dem 30. Dezember 2009 endgültig auslaufend, war in ihrer Art revolutionär. Sie formulierte bereits grundlegende Sicherheitsanforderungen deutlich weniger als Patentformel und Lösung und zunehmend in Form von Schutzziele. Die Zielsetzung: Risiken sollten beherrscht und damit Gefahren für Menschen so weit wie möglich eliminiert werden. Dabei galten drei Grundsätze:

- ▶ Beseitigung oder Minimierung der Gefahren durch die Konstruktion selbst
- ▶ Ergreifen der notwendigen Schutzmaßnahmen gegen nicht zu beseitigende Gefahren und
- ▶ Unterrichtung der Benutzer über Restgefahren

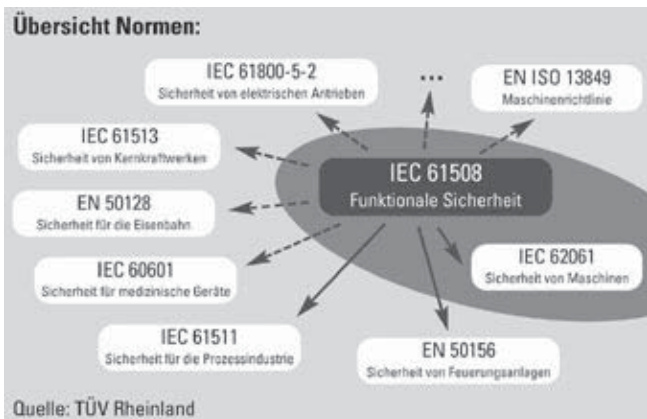
Diese Ziele behalten in der neuen Maschinenrichtlinie, die am 29.12. 2009 bindend in Kraft treten wird, ihre volle Gültigkeit und lassen dabei – wie schon ihre Vorgängerin – den konkreten Weg, wie sie erreicht werden sollen, zu einem großen Teil offen. Hersteller von Maschinen und Anlagen bleiben damit verstärkt eigenverantwortlich in der Pflicht, dieser Trend wird fortgesetzt. Zu den wesentlichen Unterschieden aber, die die neue Maschinenrichtlinie 2006/42/EG mit sich bringt, gehört indes, dass konkrete Zahlen eine entscheidende Rolle spielen. Wahrscheinlichkeitsberechnungen fließen neuerdings in die Ermittlung von Sicherheitsstufen, den so genannten Safety Levels, mit ein.

Safety Integrity Level

Die Betrachtung auf Zahlenbasis offenbart ein neues Verständnis von Sicherheit. War bislang eine rein qualitative Reflexion üblich, so kommt nun eine objektivere, quantitative Sichtweise hinzu. Gerechnet wird im Hinblick auf zwei unterschiedliche Betriebsarten: Eine niedrige Anforderungsrate und eine hohe, respektive kontinuierliche Anforderungsrate.

Wichtig für die Bestimmung des Safety Levels der gesamten Anlage sind die sicherheitstechnisch relevanten Kenndaten der einzelnen verbauten Komponenten. Dabei werden für Anlagen und so genannte risikoreduzierende Maßnahmen vier Sicherheitsstufen unterschieden: Von SIL1 für geringes Risiko bis SIL4 für sehr hohes Risiko. Je höher das Risiko, umso zuverlässiger müssen die Maßnahmen zur Risikoreduzierung durchgeführt werden. Klar, dass hierbei in gleichem Maße die Anforderungen an die verwendeten Komponenten steigen.

Die Analyseverfahren der Wahl heißt FMEDA, oder auch Failure Modes, Effects and Diagnostic Coverage Analysis. Sie definiert mittels formelbasierter Ausfallraten den rechnerischen Anteil ungefährlicher Ausfälle und den Diagnosegrad eines als sicher klassifizierten Systems. Beide zu ermittelnden Kenngrößen laufen im Fachjargon unter ihren englischen Kürzeln: SFF, Safe Failure Fraction und DC, die Diagnostic Coverage. >



Viele Regelungen dienen einem Ziel: Ein Überblick über die wichtigsten Sicherheitsnormen

| Übersicht Safety Levels: | | |
|--|--|--------------------------------------|
| Safety Integrity Level (SIL) EN 62061 | Wahrscheinlichkeit „gefährlicher Fehler“ pro Stunde (1 / h) | Leistungsgrad (PL) EN ISO 13849-1 |
| SIL 0 | $\geq 10^{-5}$ to $< 10^{-6}$ | a |
| SIL 1 | $\geq 3 \times 10^{-6}$ to $< 10^{-5}$ | b |
| SIL 1 | $\geq 10^{-6}$ to $< 3 \times 10^{-6}$ | c |
| SIL 2 | $\geq 10^{-7}$ to $< 10^{-6}$ | d |
| SIL 3 | $\geq 10^{-8}$ to $< 10^{-7}$ | e |

Safety Levels werden nach Wahrscheinlichkeit „gefährlicher Fehler“ pro Stunde berechnet und in Leistungsgrade unterschieden

Sichere Komponenten = sicheres System?

In vielerlei Beziehung knüpft die neue Maschinenrichtlinie an ihre Vorgängerin an. So wird auch weiterhin dem „gesunden Menschenverstand“ in der grundlegenden Annahme gehuldigt, dass „sicherheitsrelevante Teile von Steuerungen voraussichtlich nur so gut sind, wie der rechnerische Systemnutzen ihrer Sicherheitsfunktion.“

Es reicht in der Folge nicht aus, eine Anlage mit lauter SIL zertifizierten Komponenten zu betreiben, in der Annahme, so auf Nummer sicher zu gehen. Entscheidend ist die Bewertung des gesamten Safety Instrumented System, kurz SIS. Also der gesamten Kette – bestehend aus Sensor, Steuerung und Aktor. Deren obligate Gefährdungs- und Risikoanalyse ermittelt verbindlich, ob und wie viel funktionale Sicherheit erforderlich ist. Im Klartext: Um den Nachweis eines sicheren Systems zu führen, benötigt der Betreiber statt einzelner SIL Zertifikate seiner sicherheitsrelevanten Komponenten vielmehr deren Kennzahlen.

Selbst wenn ein Sensor SIL zertifiziert ist, muss der Nachweis, dass er in „meinem“ speziellen System sicher ist, dennoch zusätzlich separat geführt werden.

Drei wichtige Empfehlungen für die Umsetzung eines Sicherheitsprojektes:

1. Lassen Sie sich bei der Auswahl der sicherheitstechnischen Systemkonfiguration und beim Validierungsprozess von einem kompetenten Partner unterstützen.
2. Verwenden Sie ausschließlich gemäß Anhang IV der Maschinenrichtlinie geprüfte Logiksteuerungen, oder alternativ zentrale oder dezentrale Steuerungen mit integrierten Sicherheitsfunktionen gemäß DIN EN 61800-5-2. Die für die Validierung nach DIN EN 13849 erforderlichen Werte bestimmt der Hersteller selbst.
3. Verwenden Sie nur solche Komponenten, die ihrerseits für sicherheitstechnische Anwendungen geeignet sind.

Steht ein Sicherheitsprojekt an, ist das Hinzuziehen kompetenter – auch externer – Ratgeber ebenso wichtig, wie der frühzeitige Aufbau eigener Sachkenntnis

Praxistauglichkeit und Kompetenz statt starrer Normen

Und in der Praxis: Innerhalb einer Anlage können unter Umständen sicherheits- und nicht-sicherheitsrelevante Komponenten miteinander verbunden sein. Für das SIS fließen dabei nur die sicherheitsrelevanten Komponenten in die „Wertung“ mit ein.

Jede Anlage besitzt einzigartige Anforderungen – so auch in punkto funktionaler Sicherheit. Aufgrund ihrer modularen Architektur können SIS anforderungsspezifisch gebildet werden. Hier kristallisiert sich die Bedeutung unterschiedlicher Einsatzbedingungen der jeweiligen Anlagen heraus, die optimal berücksichtigt werden wollen. Im Klartext: Der richtige Drehgeber für das eine System ist eben genau der falsche für das andere. Und nicht immer ist das am höchsten zertifizierte System auch das Beste: Es gilt den optimalen Weg – zumeist ein schmaler Grat – für das erforderliche SIL mit einem kompetenten Partner zu finden und entwickeln. Auf diese Weise gewährleistet die Anwendung der neuen Sicherheitsnormen neben optimaler Qualität auch optimale Wirtschaftlichkeit.

Drehgeber: Von der Teilmaschine zur „unvollständigen Maschine“

Inwiefern schließt das Thema Funktionale Anlagensicherheit den Produktbereich Drehgeber nun explizit mit ein? Sind Drehgeber als Einzelgeräte Sicherheitsbauteile im Sinne der neuen Maschinenrichtlinie? Und welchen Vorteil bringen SIL zertifizierte Drehgeber im Hinblick auf das Gesamtzertifikat der Anlage?

Zunächst gilt, dass Drehgeber als Ermittler sicherer Positionen und Geschwindigkeit mitten im Thema „sichere Bewegung“ verankert sind und als unvollständige Maschinen nach Art. 5, Abs. 2 der neuen MRL definiert werden.

Für unvollständige Maschinen – vormals Teilmaschinen – gelten mit der neuen Richtlinie erweiterte Herstellerpflichten. Dabei stehen die Einhaltung festgelegter Sicherheits-

und Gesundheitsschutzanforderungen inklusive Risikobeurteilung und die Erstellung und Bereithaltung spezieller technischer Unterlagen im Mittelpunkt. Im Sinne der Maschinenrichtlinie handelt es sich bei einem Gerät oder Bauteil dann um ein Sicherheitsbauteil, wenn die in Art. 2 c) genannten Anforderungen vorliegen. Dazu gehört die Intention: Dient das Gerät einer Sicherheitsfunktion? Wird es zusammen mit einer Maschine in den Verkehr gebracht?

Bottom-up versus Top-down

Noch ist offen, welche Methode sich in der Praxis bei der Bewertung von Anlagen durchsetzen wird: Bottom-up oder Top-down. Nichts ist entschieden, viel spricht jedoch dafür, dass beide ihre Berechtigung haben: Die vermeintlich theorielastige „Bottom-up“-Methode errechnet die Ausfallwahrscheinlichkeit einer Sicherheitsfunktion (SIF) auf der Basis bekannter Einzel-Ausfallstatistiken der Komponenten. Dies können beispielsweise SIL-2-konforme Geräte mit Herstellerangaben sein. Zwei Probleme wirft dieser Ansatz auf: Zum einen liegen nur selten für alle eingesetzten Komponenten die benötigten Werte vor; zum anderen unterliegen Feldgeräte den unterschiedlichsten Einsatzbedingungen, was in der Praxis für eine Sicherheitslücke sorgt.

Die pragmatischere „Top-down“-Methode greift das tradierte Prinzip der Verwendung betriebsbewährter Geräte



Für unvollständige Maschinen gelten mit der neuen Maschinenrichtlinie erweiterte Herstellerpflichten. Dazu zählen die Einhaltung festgelegter Sicherheits- und Gesundheitsschutzanforderungen inklusive Risikobeurteilung

auf. Stördaten werden statistisch ausgewertet. Eine Aufgabe, die sowohl dem Anwender, wie auch dem Hersteller zufallen kann. Doch auch hier lauert ein Problem: Die Losgröße muss schon imposant sein, um statistisch aussagekräftig zu sein. An Zahlenwerke verbindlicher Größenordnung kom- >

BERECHNUNG DES SIL BEI EINER BETRIEBSART MIT HOHER ODER KONTINUIERLICHER ANFORDERUNGSRATE (AUSFÄLLE PRO STUNDE)

| | |
|--------------|--|
| SIL 4 | >10⁻⁹ bis <10⁻⁸ |
| SIL 3 | >10⁻⁸ bis <10⁻⁷ |
| SIL 2 | >10⁻⁷ bis <10⁻⁶ |
| SIL 1 | >10⁻⁶ bis <10⁻⁵ |

men aber – gerade kleine und mittlere – Unternehmen nur mit großem Aufwand heran.

Die Diskussion ist noch immer nicht abgeschlossen. Denkbar ist, dass sich in der Praxis eine Mischform beider Verfahren etablieren wird; eine Kombination aus den Vorteilen des Bottom-up, der „Betrachtung des gesamten Safety Loops“, und des Top down, „dem Einsatz praxisbewährter Komponenten“. Vorbereitend punktet lässt sich am besten mit Informationsvorsprung, breiter Sachkenntnis und engem Dialog mit den entscheidenden Behörden.

Zusammenfassung

Um im Markt bestehen zu können, muss ein Anlagen- und Maschinenbauer aber nicht nur innovative Produkte nach aktuellen Sicherheitsbestimmungen produzieren, son-

dern muss ebenso schnell wie kostengünstig agieren. Wie rechnen sich eigens zertifizierte Kleinkomponenten in diesem Zusammenhang?

Komponentenhersteller befinden sich bei ihrer Lösungssuche auf schmalen Grat. Denn zum einen soll Anlagenbetreibern der Weg zur Zertifizierung ihres Gesamtsystems möglichst breit gebahnt werden, zum anderen soll der optimale Schutz für die Menschen, die mit der Anlage umgehen, Hauptaugenmerk und -motivation bleiben. Zum Dritten zählt die Wirtschaftlichkeit des Gesamtsystems. Bei der Evaluierung letzterer fallen vor allem drei Gesichtspunkte in die Waagschale: Zum einen: Welchen Anteil am Gesamtpreis einer Anlage hat ein Drehgeber? Wie hoch sind die Sicherheitsanforderungen an die gesamte Anlage? Und nicht zuletzt, welchen Mehrwert und damit höheren Marktpreis kann meine Anlage und Maschine aufgrund ihrer Sicherheitskonformität erzielen?

Hier ist weder ein Zuviel noch ein Zuwenig ratsam, da beides unerwartete Kosten nach sich ziehen kann. Und nicht immer ist die teuerste Lösung die sicherste: Oft erledigt das althergebrachte redundante System zweier – geringer zertifizierter – Komponenten im Vergleich zu hoch-zertifizierten Alternativen den besseren Job.

Ein Dilemma also im Spannungsfeld divergierender Trends und Forderungen nach einerseits immer sicheren

BERECHNUNG DES SIL BEI EINER BETRIEBSART MIT NIEDRIGER ANFORDERUNGSRATE (MITTLERE WAHRSCHEINLICHKEIT EINES AUSFALLS BEI ANFORDERUNG - PFD AVG)

| | |
|--------------|--|
| SIL 4 | >10⁻⁵ bis <10⁻⁴ |
| SIL 3 | >10⁻⁴ bis <10⁻³ |
| SIL 2 | >10⁻³ bis <10⁻² |
| SIL 1 | >10⁻² bis <10⁻¹ |

und andererseits immer günstigeren Anlagen. Ein Patentrezept liegt nicht vor; weder für Anlagen- noch für Komponentenhersteller.

Einen Vorsprung versprechen indes: Der frühzeitige Aufbau eigener Sachkenntnis, das Hinzuziehen kompetenter – auch externer – Ratgeber, die vertrauensvolle, flexible Zusammenarbeit von Komponenten- und Anlagenherstellern im eingespielten Team. Und der gute Draht zur zertifizierenden Behörde. □

Literatur

- [1] SIL in der Praxis, Chemie Technik, April 2006, <http://www.chemietechnik.de/ai/resources/243f1b9eb1f.pdf> (Stand 13.5.2009)
- [2] BGIA Report 2/2008, Funktionale Sicherheit in der Praxis. Deutsche Gesetzliche Unfallversicherung (Hrsg.), http://www.dguv.de/bgia/de/pub/rep/pdf/rep07/biar0208/rep2_08_textteil.pdf (Stand 13.5.2009)
- [3] Hans-J. Ostermann, Paradigmenwechsel für die neue Maschinenrichtlinie vorgeschlagen, <http://www.maschinenbautage.eu/maschinenrichtlinie1/mrl-98-37-eg0.html> (Stand 13.5.2009)
- [4] Peter Wratil, Michael Kieviet, Sicherheitstechnik für Komponenten und Systeme, Hüthig-Verlag, 2005, ISBN 3-7785-2984-6

> MORE@CLICK ADK90061