Funktionale Sicherheit in der Sensorik

Risiken reduzieren

Für die Messgröße „Druck“ gibt es auf dem Markt eine nahezu unüberschaubare Zahl von Sensoren. Je nach Anwendungsbereich sind die Anforderungen an diese Sensoren sehr unterschiedlich. Gerade im Bereich der funktionalen Sicherheit führten in den letzten Jahren Änderungen der Gesetze und der relevanten Normen zu einer differenzierten Betrachtung der Gefährdungen eines Gesamtsystems und dessen Komponenten.

Von Dipl.-Ing. Michael Sieber

Was bedeutet funktionale Sicherheit? Und was bedeutet dies für die Auslegung von Sensoren oder Sensorsystemen? Prinzipiell darf nach der EU-Maschinenrichtlinie von keiner Maschine eine Gefahr ausgehen. Hierzu ist eine Risikoanalyse nach EN 1050 oder EN ISO 12100 durchzuführen. Kann man eine Maschine/Anlage so konstruieren und auslegen, dass definitiv keine Gefahr von ihr ausgeht? Es wäre zwar wünschenswert, in der Praxis ist dies jedoch unmöglich zu realisieren. Ein Nullrisiko ist in der Technik nicht möglich. Daher gilt es, das Gesamtrisiko zu reduzieren, indem Fehler erkannt oder vermieden werden und ein akzeptables Restrisiko erreicht wird. Das kann durch Festlegung einer Sicherheitsfunktion geschehen. Anhand dieser Funktion werden Maßnahmen definiert, die das System bei Auftreten von kritischen Fehlern in einen sicheren Zustand versetzen. Je nach Gefährdungseinstufung darf ein Fehler nicht zum Verlust der Sicherheitsfunktion führen. Um dies sicherzustellen, muss die Wahrscheinlichkeit für einen Fehler bestimmt werden. Dies stellt zwar einen erheblichen Mehraufwand bei der Entwicklung dar, ermöglicht aber eine Reduzierung des Gefährdungspotenzials. Oberste Priorität sollte bleiben, die Konstruktion so auszulegen, dass die Wahrscheinlichkeit von Funktionsfehlern hinreichend gering ist. Dies kann durch verschiedene Möglichkeiten realisiert werden, auf die in der Folge näher eingegangen wird.

Nicht jeder Fehler kritisch

Dabei ist nicht jeder Fehler im Sensor ein kritischer Fehler. Betrachtet man zum Beispiel die Offset-Drift eines Drucktransmitters in einer Lastmomentbegrenzung, sind zwei Fehler zu unterscheiden: eine negative Offsetdrift und eine positive Offsetdrift. Bei einer positiven Drift wird die Lastmomentbegrenzung zu früh anschlagen und damit die Verfügbarkeit der Maschine herabsetzen. Eine Gefährdung geht von diesem Fehler jedoch nicht aus. Anders sieht es bei einer negativen Drift aus: Die Lastmomentbegrenzung ermittelt eine zu geringe Last, das heißt, es geht eine Gefahr von einer zu hohen Belastung aus. Eine genaue anwendungsspezifische Gefährdungsanalyse ist wichtig, da es auch Anwendungen gibt, in denen eine positive Offsetdrift zu einer Gefährdung führen kann.

Als Kennzahl für die potenzielle Gefährdung dient gemäß EN ISO 13849-1 die Kennzahl „Performance Level (PL)“. Die genaue Zuordnung des PL ist die „durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde [1/h]“. Diese Wahrscheinlichkeit ist ein rechnerischer Wert, der sich für das fertige Produkt ermitteln lässt. Der PL wird in Kleinbuchstaben a bis e angegeben. Dabei stellt a die geringste und e die größte Gefährdungseinstufung dar. Für eine erste Abschätzung, welcher PL für die Transmitter oder das System notwendig ist, bietet das Diagramm in Bild 1 ein gutes Hilfsmittel. Mit nur drei Entscheidungen lässt sich der benötigte PL ermitteln. An erster Stelle steht die Frage nach der Schwere einer potenziellen Verletzung. Alle irreversiblen Verletzungen (und dazu gehört schon ein gebrochener Arm oder ähnliches) sind in die Kategorie 2 einzustufen, so dass sich für die meisten Anwendungen in mobilen Arbeitsmaschinen per se ein PL von c bis e ergibt. Die zweite Frage stellt sich nach der Häufigkeit oder Dauer der Gefährdungsexposition. Bleibt man bei dem zuvor genannten Beispiel der Lastmomentbegrenzung, so ist davon auszugehen, dass diese Gefährdung sehr häufig vorliegt. Bei der dritten Frage geht es darum, die Gefährdung zu vermeiden. Misst man also bei der Lastmomentbegrenzung zuverlässig, besteht eine große Möglichkeit, die Gefährdung zu vermeiden. Eine erste Abschätzung dieser Einstufung für die Lastmomentbegrenzung kommt also zu dem Ergebnis, dass für das Gesamtsystem PL d ausreichend ist. In einem solchen System kommen mehrere Sensoren/Transmitter zum Einsatz. Da sich der PL des Gesamtsystems bei Verwendung mehrerer Sicherheitskomponenten reduziert, bietet es sich an, die einzelnen Sensoren/Transmitter in PL e auszuführen.

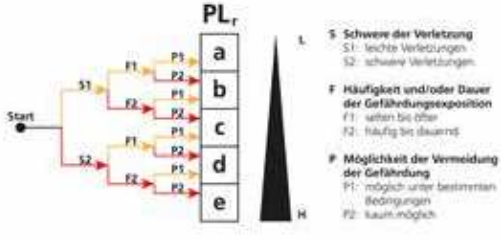

Bild 1: Ermittlung des benötigten Performance-Levels.

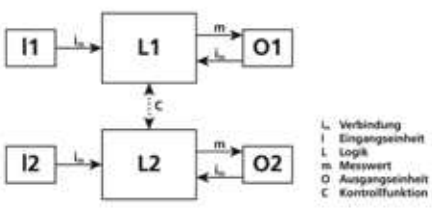

Bild 2: Blockschaltbild Kategorie 3.

Anforderungen

Ein weiteres Beispiel ist ein CO-Warngerät, wie es in Heizungsanlagen eingesetzt wird. Auch hier besteht die

Gefahr einer schweren Verletzung (Tod durch Ersticken); dafür ist die Häufigkeit dieser Gefährdung eher gering und die Möglichkeit einer Vermeidung sehr gut. Als Resultat der Abschätzung ergibt sich in diesem Fall PL c. Selbstverständlich bietet diese Abschätzung nur eine erste Information, die genauer hinterfragt werden muss.

Nachdem der benötigte PL abgeschätzt wurde, kommen weitere Kenngrößen ins Spiel, die die Anforderungen an den Transmitter beziehungsweise das System genauer beschreiben. Zunächst muss die Architektur definiert werden. Hierzu werden verschiedene Kategorien bereitgestellt. In Bild 2 ist ein Blockschaltbild für ein Gerät der Kategorie 3 dargestellt. Hier reicht es nicht mehr, nur ein Messelement vorzusehen. Die Messung selbst sowie die Auswertung müssen zweikanalig erfolgen. Eine weitere Kenngröße ist der MTTFd-Wert, die mittlere Zeit bis zu einem gefährlichen Ausfall. Im Worst-Case-Fall kann hier auch der MTBF-Wert eingesetzt werden, wenn man davon ausgeht, dass alle Fehler kritisch sind. Eine grobe Näherung erlaubt es, 50 Prozent der Fehler als kritisch einzustufen. Daraus ergibt sich ein MTTFd-Wert, der dem zweifachen MTBF-Wert entspricht. Daneben spielt der Diagnosedeckungsgrad eine wichtige Rolle, um sicherzustellen, dass ein potenzieller Fehler vom System erkannt wird. Es gibt noch weitere normative Kenngrößen, auf die hier nicht näher eingegangen wird.

Betrachtet man die Architektur der Kategorie 3, kann man grundsätzlich drei Bereiche erkennen: Eingangseinheiten (zum Beispiel Sensorelemente), Logikblock (Elektronik) und Ausgangseinheiten (zum Beispiel analoge Signale). Im Falle eines Drucktransmitters werden in diesem Fall zwei Druckmesszellen benötigt, die von der Elektronik redundant ausgewertet werden. Idealerweise setzt man Messzellen mit unterschiedlichen Druckbereichen ein,

Bild 3: Safety-Drucktransmitter.

Bild 4: Applikationsbeispiel.

um eine Drift des Messzellensignals oder Überdruckschäden erkennen zu können. Die Elektronik kann die Ausgänge abschalten, wenn bei der internen Überprüfung des Sensors ein Fehler erkannt wird und der Drucktransmitter in einen sicheren Zustand schalten muss. Die Ausgänge werden doppelt ausgeführt und deren Signale idealerweise invertiert, um Fehler auf dem Übertragungsweg vom Transmitter zur Steuerung erkennen zu können. Fehler können etwa als Parallelwiderstand zum Analogsignal wegen Feuchtigkeit im Stecker auftreten. Der Vorteil eines solchen Safety-Drucktransmitters (Bild 3) liegt darin, dass die Sicherheitsfunktionalität an der Messstelle implementiert wird und somit die Steuerung entlastet. Zudem ist nur eine Bohrung im Hydraulikzylinder zum Anschluss des Drucktransmitters notwendig, was die Wahrscheinlichkeit einer Leckage gegenüber einer Lösung mit zwei Drucktransmittern herabsetzt.

Balance zwischen Sicherheit und Verfügbarkeit

Wie wichtig eine solche Sicherheitsfunktionalität für den Anwender ist, wird in Bild 4 dargestellt. Nicht auszudenken, wenn die Lastmomentbegrenzung im entscheidenden Moment einen falschen Wert errechnen würde und es hier zu einem Unfall käme.

Die Entwicklung und Produktion von Produkten mit funktionaler Sicherheit stellt sicher höhere Anforderungen an alle Beteiligten. Bei der Umsetzung ist eine umfangreiche Betrachtung der Fehlermöglichkeiten und der Fehlererkennung notwendig. Auch ist eine Balance zwischen der Sicherheit und der Verfügbarkeit der Anlage zu finden. Durch die Vielzahl von Produkten, die bei STW bereits für die funktionale Sicherheit entwickelt und auch gefertigt wurden, steht dem Anwender eine breite Know-how-Basis für diesen Produktbereich bereit. (*anm*)