Sicher ist sicher

SIL-qualifizierte Messgeräte sorgen für funktionale Sicherheit im Anlagenbetrieb

Zunehmende Anforderungen an die Sicherheit und weiter steigende Rohstoffpreise – es wird immer wichtiger, Ausfälle in der Produktion zu vermeiden. Eine Schlüsselrolle für die Anlagensicherheit spielt die eingesetzte Messtechnik: Je zuverlässiger ein Messgerät in jeder Situation ist, desto sicherer ist die gesamte Anlage. Messgeräte für Druck- und Temperaturmessung mit SIL-Qualifikation erfüllen die hohen Ansprüche an die Anlagenverfügbarkeit.

Keywords
- *Anlagensicherheit*
- *funktionale Sicherheit, SIL*
- *Messumformer*
- *Druck-, Temperaturmesstechnik*

Bilder © Labom

Druckmessumformer Pascal CI4 mit hoher Messpräzision.

Um Ausfälle bei der Produktion zu vermeiden und den Anlagenbetrieb möglichst sicher für Mensch und Umwelt zu gestalten, empfiehlt sich der Einsatz SIL-qualifizierter Messgeräte. Die Abkürzung SIL steht für Safety Integrity Level, die entsprechenden Geräte werden nach den Anforderungen für die Qualifizierung von Messgeräten, dem SIL-Regelwerk DIN EN 61508, eingestuft. Diese Anforderungen erstrecken sich über den kompletten Lebenszyklus eines Gerätes – von der Entwicklung über die Produktion bis zur sorgfältigen Prüfung bei jeder Produktänderung. Dabei müssen sowohl zahlreiche organisatorische Maßnahmen als auch Kontrollmechanismen und Anforderungen an die gegebenenfalls vorhandene Software erfüllt werden. Hard- und Software müssen besonders robust gegen Ausfälle sein; die Software enthält zudem zahlreiche Überwachungsroutinen. So wird unter anderem laufend überprüft, ob alle Programmteile aktiv sind und der Datenspeicher wird gespiegelt oder mit Checksummen versehen, um fehlerhafte Speicherstellen zu entdecken.

Ausfallsicherheit für jede Anlage

Mit der SIL-Qualifizierung kann sich der Betreiber einer Anlage also auf eine hohe Ausfallsicherheit verlassen und hat alle für seine Sicherheitsbetrachtung notwendigen Werte zur Hand. Und die SIL-Anleitungen zu Messgeräten beinhalten auch Informationen zur Reaktionszeit im Anforderungsfall: Jedes Messgerät und jeder Aktor braucht Zeit, um seine jeweilige Aufgabe zu erfüllen – manchmal nur Millisekunden, manchmal einige Sekunden. Der Betreiber einer Anlage muss sich dabei die Frage stellen, wieviel Zeit nach dem Ausfall eines wichtigen Systems für die Sicherheitskette bleibt, um zu reagieren sowie eine Gegenmaßnahme einzuleiten und umzusetzen.

Ein Beispiel: Die Temperaturmessung misst, dass die Heizung eines Tanks zu heiß wird. Die Steuerungseinheit erkennt die Temperaturüberschreitung und schaltet die Heizung ab. Dieser Mechanismus muss greifen, bevor eine für den Tankinhalt kritische Temperatur erreicht ist. Die Messtechnik hat in der Regel kurze Reaktionszeiten und mit dem Wert für die Reaktionszeit gemäß der SIL-Anleitung hat der Betreiber die notwendige Information zur optimalen Auslegung der Anlage.

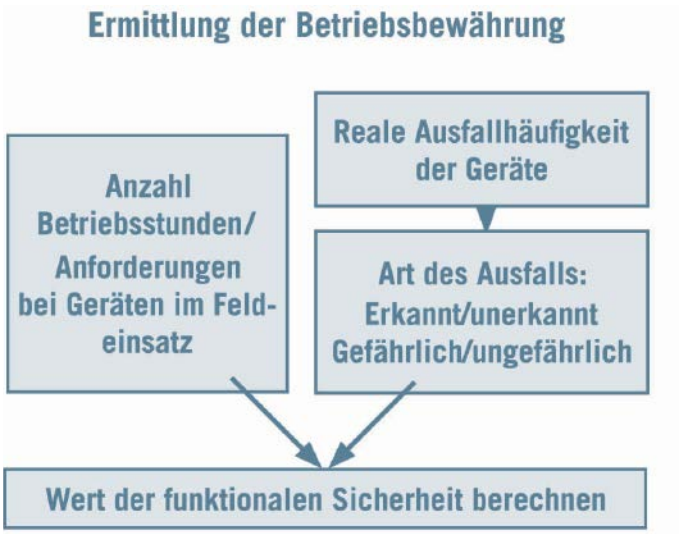
Eine der Überwachungsroutinen ist der sogenannte Watchdog, der „Wachhund im Messgerät“ – ein spezielles Werkzeug zur Ausfallerkennung. Der Watchdog in SIL2-Messgeräten überwacht einzelne Softwareeinheiten und zählt dabei zum Beispiel kontinuierlich von 100 auf null. Er springt im Anschluss nur dann wieder auf 100 zurück, wenn alle überwachten Teile ein „Okay“ melden. Läuft der Zähler auf null, so meldet das Messgerät den Fehler der Steuerungseinheit – so kann etwa geprüft werden, ob alle Komponenten noch aktiv sind.

Qualifizierung von SIL-Messgeräten

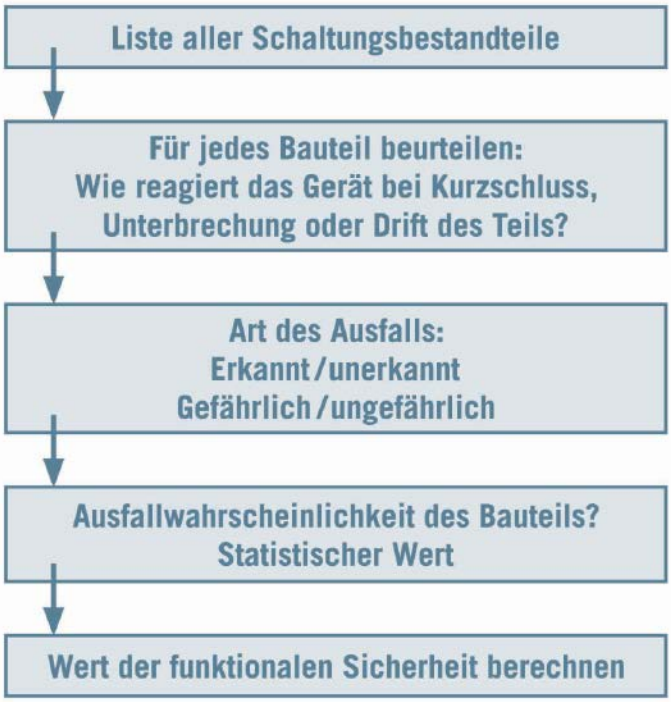
Es gibt zwei Möglichkeiten bei der Qualifizierung eines SIL-Geräts: Zum einen die Betriebsbewährung aufgrund langjähriger Erfahrung mit einer hohen Anzahl von Geräten im Feld oder zum anderen das sogenannte „SIL by Design“ über eine Failure Modes, Effects and Diagnostics Analysis (FMEDA) mit bestimmten Anforderungen bei der Entwicklung der Geräte.

Die Qualifizierung per Betriebsbewährung beruht auf einer hohen Anzahl von Geräten im Einsatz und deren konkreten Ausfällen. In der DIN EN 1508 ist festgelegt, wie viele Betriebsstunden oder Anforderungen der Sicherheitsfunktion mindestens erreicht sein müssen, um die Voraussetzungen für Betriebsbewährung zu erfüllen. Beobachtete Fehler werden in sicher und unsicher, erkannt und unerkannt unterteilt. Diese Daten sind dann die Basis für die Berechnung der Werte der funktionalen Sicherheit.

Bei der Methode „SIL by Design“ werden per FMEDA alle für die sichere Funktion relevanten Bauteile erfasst und einzeln auf ihre Auswirkung bei einem Ausfall geprüft. Zur Beurteilung der Wahrscheinlichkeit eines Ausfalls eines Bauteils kann auf entsprechend veröffentlichte Erfahrungswerte oder auf Angaben



Die Qualifizierung per Betriebsbewährung.



Die FMEDA (Failure Modes Effects and Diagnostic Analysis) ist das Verfahren zur detaillierten Ermittlung von Fehlerursachen und deren Auswirkung auf ein System.

der Hersteller zurückgegriffen werden. So werden dann die Werte der funktionalen Sicherheit gemäß DIN EN 61508 berechnet – z.B. der Raten der gefährlichen Ausfälle, die Wahrscheinlichkeit eines Ausfalls bei Anforderung oder der Anteil der sicheren Fehler.

SIL-Geräte regelmäßig prüfen

Auch im laufenden Betrieb sollten SIL-Geräte in regelmäßigen Abständen Prüfungen unterzogen werden. Die SIL-Anleitungen enthalten Vorschläge, welche Aspekte zu prüfen sind und der PTC-Wert (Proof Test Coverage-Wert) sagt dabei aus, wieviel Prozent der möglichen Fehler bei diesem Test erkannt werden. Bei einem PTC-Wert von 100 % wäre das Gerät nach dem Test in Bezug auf die Ausfallraten „wie neu". Bei niedrigeren PTC-Werten steigt die Ausfallrate. Weitere Informationen können bei Bedarf in Namur NA106 nachgelesen werden. Abhängig davon, welche Ausfallrate der Anlagenbetreiber einhalten muss, beeinfluss der PTC-Wert also den Zeitpunkt, zu dem ein Gerät ausgetauscht werden muss.

Druckmessumformer Pascal CV3 mit Funktionsmodulen zum Anzeigen, Schalten und Kommunizieren.

SIL3 mit SIL2-qualifizierten Messgeräten

SIL-Qualifizierungen sind unterteilt in SIL1 bis SIL3, wobei SIL3 die größten Anforderungen an die Ausfallsicherheit erfüllt. Auch mit SIL2-geeigneten Messgeräten kann jedoch eine SIL3-Qualifizierung erfolgen. Um die entsprechenden Anforderungen zu erfüllen, muss eine Kette – also Messgerät, Übertragungsschicht, SPS und Prozessleitung – normalerweise aus SIL3-Geräten aufgebaut sein. Eine andere Möglichkeit ist, SIL2-Messgeräte redundant einzusetzen. Grundsätzlich betrachtet dabei der Anlagenbetreiber das Gesamtsystem und berechnet für dieses eine Ausfallwahrscheinlichkeit. Dafür notwendig sind zwei SIL2-Geräte ohne Software, z.B. ein Manometer oder ein analoges Druckmessgerät, zwei SIL2-Geräte mit SIL3-geeigneter Software oder für diverse Redundanz zwei unterschiedliche SIL2-Geräte wie etwa die Labom-Geräte Pascal CI4 und Pascal CV3.

Der Pascal CV3 ist ein Druckmessumformer mit smarten Funktionsmodulen zum Anzeigen, Schalten und Kommunizieren. Die Module können vor Ort durch einfache Plug-and-measure-Technologie – ohne Neuabgleich und ohne das Gerät aus dem Prozess zu nehmen – ausgetauscht oder ergänzt werden. Bei einer Kombination mit dem Schaltkontaktmodul kann dadurch auf eine weitere Steuerungseinheit verzichtet werden, da der Druckmessumformer direkt das Schaltsignal an den Aktor z.B. die zu stoppende Pumpe weitergeben kann. Dies ist ein Vorteil für den Anwender, denn neben den zusätzlichen Kosten unterliegen Steuerungseinheiten relativ hohen Ausfallwahrscheinlichkeiten und sind ein weiteres zu betrachtendes Glied in der Sicherheitskette. Neben dem Pascal CV3 hat der Anbieter noch eine ganze Reihe weiterer SIL-geeigneter Druck- und Temperaturmessgeräte im Portfolio – und entwickelt bei Bedarf auch individuelle Lösungen.

Dr. Christine Schweder,
Entwicklung,
Labom Mess- und Regeltechnik

Wiley Online Library

Labom Mess- und Regeltechnik GmbH, Hude
Tel.: +49 4408 804 - 228
c.schweder@labom.com · www.labom.com