Diesmal im Fokus:

Weiterfahren – aber sicher

Carsten Gregorius, Senior Specialist Safety

Wer schon einmal eine Autoreifenpanne durchlebt hat, weiß wie unangenehm es sein kann. Vor allem auf dem Weg in den Urlaub, zu einem wichtigen Termin oder nachts auf einer einsamen Landstraße. Um in solchen Fällen eine begrenzte Zeit weiterfahren zu können, hat die Reifenindustrie sogenannte „Runflat-Reifen" entwickelt, mit denen sich – unter Beachtung einer reduzierten Geschwindigkeit – die nächste Werkstatt am Zielort anfahren lässt.

Inwieweit kann man dieses Konzept auf automatisierte Fertigungskonzepte, insbesondere im Bereich der Sicherheitstechnik, übertragen?

Wenn bei heutigen Sicherheitskonzepten ein sicherheitsrelevanter Fehler eintritt, wird in der Regel der sichere Zustand so schnell wie möglich herbeigeführt, obwohl die meisten Sicherheitsfunktionen für höhere Sicherheitsintegritätslevel (SIL) oder Performance Level (PL) redundant ausgelegt sind. Deshalb hat sich eine Arbeitsgruppe beim ZVEI unter Mitwirkung verschiedener Mitgliedsfirmen und einem Institut der Frage gestellt, inwieweit ein zeitlich begrenzter Weiterbetrieb eines Automatisierungssystems mit einem sicherheitskritischen Fehler aus normativer Sicht zulässig ist.

Bei verfahrenstechnischen Anlagen könnten bestimmte Fertigungsschritte mit kritischen Prozessparametern zu Ende gefahren werden, abhängig von der Anzeige beim Auftreten eines Fehlers und des angezeigten Status des „degradierten Betriebs". Spätestens bei Erreichen der maximal zulässigen Betriebsdauer im „degradierten Zustand" muss durch einen „Entscheider" der sichere Zustand herbeigeführt werden. Im Rahmen einer Fehlerarten- und Auswirkungsanalyse unterscheidet man zwischen zwei Fehler-Arten. Bei nicht-tolerierbaren Fehlern kann ein sicherer Weiterbetrieb nicht gewährleistet werden und der unmittelbare Stillstand muss eintreten. Tolerierbare Fehler ermöglichen einen zeitlich begrenzten Weiterbetrieb, sofern zum Beispiel ein zweiter unabhängiger Abschaltpfad die Sicherheitsfunktion korrekt ausführen kann.

Die relevanten Normen EN ISO 13849 bzw. IEC 62061 beinhalten keine Anforderungen im Hinblick auf eine sofortigen oder unmittelbaren Fehlerreaktionen beim Auftreten eines Fehlers. Darüber hinaus lassen auch die Modelle zur Berechnung der Ausfallwahrscheinlichkeit (PFHD) den notwendigen Gestaltungsspielraum zu, da diese bei redundanten Architekturen anfangs auf niedrigem Niveau verbleibt und erst nach einiger Zeit ansteigt. Je nach Risikobeurteilung und Qualität der eingesetzten Maßnahmen zur Fehlerbeherrschung lässt sich der Zeitraum bis zum Abschalten durch den „Entscheider" auf maximal eine Woche ansetzen. Einen anderen Ansatz verspricht die Idee, dass ein „Entscheider" im Fehlerfall eine alternative bzw. ergänzende Sicherheitsmechanismen aktiviert. So könnte bei der Überwachung von sicherbegrenzten Geschwindigkeiten in einem Antriebssystem (SLS gemäß EN 61800-5-2) nur noch der Betrieb mit reduzierter Geschwindigkeit zulässig sein. Konkrete Anwendungsbereiche ergeben sich auch bei führerlosen Transportsystemen (FTS), bei denen die Fahrwegkontrolle durch die geschwindigkeitsabhängige Dimensionierung des Schutzfeldes eines Laserscanners realisiert ist.

Entscheidend für die Akzeptanz wird es sein, ob sich der Nutzen durch die Möglichkeit des „degradierten Betriebs" messbar greifen lässt. Vor allem im Hinblick auf die zunehmende Vernetzung kommt der Diagnosefähigkeit einzelner Komponenten in Bezug auf die Anlagenverfügbarkeit eine besondere Bedeutung zu.

phoenixcontact.com/fehlertoleranz-safety

Autor
Dipl.-Ing. (FH) C. Gregorius,
Senior Specialist Safety,
Phoenix Contact Electronics GmbH, Bad Pyrmont

Kontakt

Phoenix Contact GmbH & Co.KG
Blomberg
cgregorius@phoenixcontact.com
www.phoenixcontact.com