Allein die Physik entscheidet

Zuverlässigkeit mechanischer Sicherheitseinrichtungen bewerten

Industrie Service

Mehr Wert.
Mehr Vertrauen.

Fachaufsatz

Zufällige oder systematische Fehler? Das ist die Frage, wenn es um die Bewertung der Zuverlässigkeit von mechanischen Sicherheitseinrichtungen geht. Häufig wählen Planer, Konstrukteure und Hersteller von Anlagen probabilistische Bewertungsmodelle wie die SIL-Betrachtung. Doch diese Extrapolation des Ansatzes ist nicht zulässig: Zufällige Fehler spielen beim Versagen von mechanischen Bauteilen keine Rolle.

TÜV SÜD Industrie Service GmbH

Mechanische Komponenten wie Absperreinrichtungen, Überdruckventile oder Berstscheiben werden seit jeher als Bestandteile risikoreduzierender Einrichtungen oder als Einzelmaßnahmen in Anlagen der Prozessindustrie eingesetzt. Wie bei allen sicherheitsrelevanten Bauteilen, die hier genutzt werden, ist die zuverlässige Funktion sicherzustellen.

In den Ursprüngen der funktionalen Sicherheit wurden dazu ausschließlich deterministische Fehler- und Bewertungsmodelle herangezogen. Die Einführung probabilistischer Bewertungsmodelle beschäftigt sich mit der Wahrscheinlichkeit des Auftretens zufälliger Fehler. Dieser Ansatz wird in der Praxis häufig auch auf mechanische Komponenten ausgedehnt. Aufgrund des Fehlens zufälliger Fehler in mechanischen Komponenten – wie die folgenden hypothetischen Beispiele zeigen – ist die Extrapolation dieses Ansatzes allerdings nicht zulässig:

- In einem Behälter steigt der Druck und erreicht ein sicherheitskritisches Maß. Das Überdruckventil bleibt jedoch verschlossen, obwohl der Ansprechdruck weit überschritten wurde. Die Analyse des Vorfalls zeigt: Die Einwirkung des Prozessmediums hat im Lauf der Zeit dazu geführt, dass die Dichtflächen verkleben.
- Die Zuleitung zu einem Reaktionsbehälter soll durch eine Sicherheitsabsperrarmatur verschlossen werden, um die darin ablaufende chemische Reaktion zu stoppen. Doch sie läuft weiter und wird unkontrollierbar. Die Analyse zeigt: Das Material des Schiebers war für den Kontakt mit dem Edukt nicht geeignet und stellenweise korrodiert. Er schloss deshalb nicht dicht.

Mechanik überlässt nichts dem Zufall

Die beiden Beispiele zeigen typische Ausfälle von mechanischen Sicherheitseinrichtungen wie Undichtigkeiten, Verkleben, Überlastung oder Materialfehler. Sie lassen sich auf jeden Vorfall, bei dem eine mechanische Schutzeinrichtung versagt, übertragen. Bei näherer Betrachtung stellt man fest, dass es sich ausnahmslos um Ausfälle aufgrund von systematischen Fehlern handelt. Dies verdeutlichen auch die Unterschiede der beiden Fehlermodelle und der zugrundeliegenden Ansätze (Tabelle).

Es sei zudem betont, dass die probabilistischen Bewertungsmodelle in erster Linie dazu entwickelt wurden, zufällige Fehler zu quantifizieren und damit beherrschbar zu machen, die aus den physikalischen Eigenschaften von elektrischen, elektronischen und programmierbar elektronischen Bauteilen (EIE/PE-Systemen) resultieren. Dies betrifft insbesondere Transistoren, Halbleiter, Platinen und andere Komponenten der Stromkreise, die analoge oder digitale Schaltprozesse durchführen. Fehler bzw. fehlerhafte Schaltprozesse in diesen Bauteilen treten zufällig auf, das bedeutet:

- Sie sind nicht vorhersehbar.
- Sie sind nicht reproduzierbar.
- Sie sind den EIE/PE-Systemen immanent.

Diese zufälligen Fehler sind prinzipiell unvermeidbar, müssen also antizipiert und das Versagen der Bauteile somit einkalkuliert werden. Dem gegenüber stehen die systematischen Fehler, die durch kausale Zusammenhänge gekennzeichnet sind:

- Sie treten immer dann auf, wenn bestimmte Rahmenbedingungen erfüllt sind.
- Sie haben eine nachvollziehbare und feststellbare Ursache.
- Sie führen zu einer vorhersehbaren Wirkung und sind stets auf menschliches (Fehl-) Verhalten zurückzuführen.
- Ursache und Wirkung hängen kausal zusammen.

Systematische Fehler können aufgrund dieser Eigenschaften prinzipiell vermieden werden. Das zeigen die beiden oben genannten Beispiele, bei denen die mechanischen Sicherheitseinrichtungen keineswegs zufällig nicht funktioniert haben. Vielmehr mussten die Bauteile zwangsläufig aufgrund der herrschenden Betriebsbedingungen versagen: Für sach- und fachkundige Personen war es absehbar, dass die Dichtflächen verkleben bzw. dass das aggressive Medium den Werkstoff des Schiebers angreift. Das Versagen war in beiden Fällen nur eine Frage der Zeit und hätte doch gänzlich vermieden werden können, entweder mithilfe von geeigneten Werkstoffen oder mit angepassten Wartungsintervallen, in denen die kritischen Bauteile gereinigt oder ausgetauscht werden.

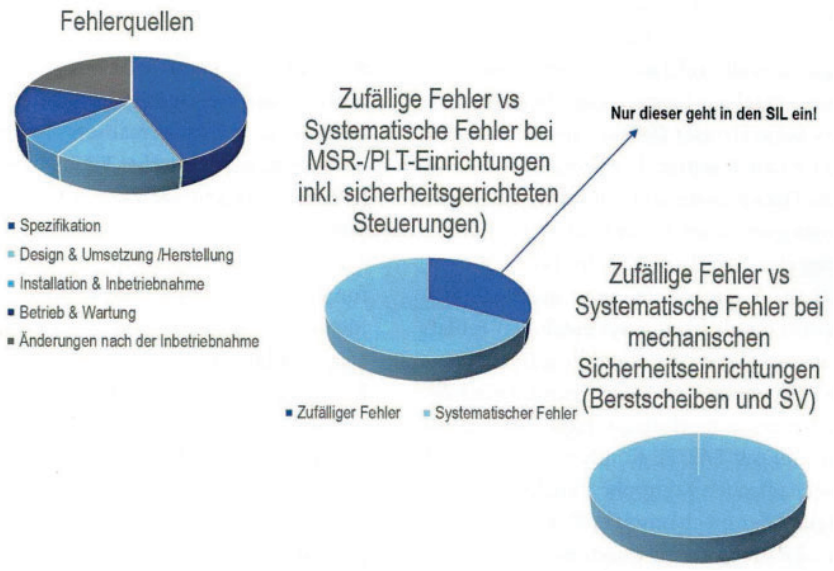
Die Erfahrung der Sachverständigen von TÜV SÜD zeigt: Die Tatsache, dass bei mechanischen Sicherheitseinrichtungen ausschließlich syste-

matische Fehler zu einem Versagen im Anforderungsfall führen, wird heutzutage immer häufiger nicht beachtet – selbst von versierten Experten mit viel Erfahrung im Bereich des Chemieanlagenbaus. Ein Grund dafür könnte in missverständlichen Formulierungen der Einführungskapitel der Regelwerke IEC 61508-1 und IEC 61511-1 liegen. Dort eröffnen die Verfasser die Möglichkeit, die Normen auch über die EIE/PE-Systeme hinaus anzuwenden. Die Anwendung bestimmter normativer Anforderungen ist somit auch für andere Technologien wie Mechanik oder Hydraulik möglich und darüber hinaus auch zielführend bei der Führung des Eignungsnachweises.

Diese Aussage trifft übrigens ausschließlich auf die rein mechanischen Teile der Sicherheitseinrichtung zu, nicht auf die möglicherweise assoziierten elektronischen Komponenten (z. B. elektronische Ansteuerungen von Absperrarmaturen). Die häufig anzutreffende, hybride Bauweise hat dazu beigetragen, den Blickwinkel auf die mechanischen Sicherheitseinrichtungen zu verändern und Missverständnisse zu verstärken.

Unterschiede der beiden Fehlermodelle

Probabilistisches Fehlermodell (Aussage aufgrund von Wahrscheinlichkeiten)		**Deterministisches Fehlermodell (Aussage aufgrund von kausalen Zusammenhängen)**
Gut prognostizierbar	**Umgebungs- und Betriebsbedingungen**	Bekannt
Unbekannt	**Häufigkeit, Frequenz bzw. zeitliche Abfolge**	Bekannt
Gut prognostizierbar	**Auswirkungen**	Bekannt
Nein, kann aber näherungsweise quantifiziert werden	**Ausschluss von möglichen Ausfallszenarien**	Ja
Zufällig aufgrund physikalischer Eigenschaften von elektronischen Bauteilen (z. B. Transistoren, Halbleiter etc.)	**Zeitpunkt für möglichen Ausfall**	Prognostizierbar aufgrund physikalischer Eigenschaften mechanischer Bauteile (z. B. zu geringe Wanddicke durch Korrosion)



Gegenüberstellung der Fehlerquellen bei MSR-/PLT-Einrichtungen und mechanischen Sicherheitseinrichtungen

Jedes Bauteil auch separat bewerten

Jedoch aus gutem Grund fordern die Verfasser im selben Absatz der IEC 61508-1 auch eine technologiespezifische Sicherheitsstrategie. Doch offenbar wird oft nicht bedacht, dass dazu die auftretenden Fehlerarten in jedem einzelnen Element oder Teilsystems eines Schutzkreises (Sensor, Steuereinheit und Aktor) auch separat betrachtet werden müssen. Darauf basierend erfolgt die Auswahl eines geeigneten Fehlermodells zur Bewertung der Zuverlässigkeit. Im Falle von EIE/PE-Komponenten wird die Eintrittswahrscheinlichkeit eines zufälligen Fehlers auf Basis des probabilistischen Fehlermodells bewertet. Die Realisierung einer MSR-Sicherheitseinrichtung erfolgt üblicherweise sowohl mit EIE/PE-Komponenten als auch mechanischen Komponenten. Die Zuverlässigkeit der mechanischen Komponenten wird dann unter Verwendung des deterministischen Fehlermodells durchgeführt.

In der Praxis stellt sich jedoch häufig die Frage, welche Zuverlässigkeitskennwerte für mechanische Komponenten im rechnerischen SIL-Nachweis der Sicherheitseinrichtung einzusetzen sind. Grundsätzlich muss jede mechanische Komponente für die jeweilige Applikation geeignet sein. Der Fokus bei der Führung des Eignungsnachweises muss daher auf die Vermeidung systematischer Fehler gerichtet sein. Bei bestimmungsgemäßer Verwendung einer mechanischen Komponente kann daher im rechnerischen Nachweise $\lambda_{DU} = 0$ eingesetzt werden. Die Eignung von mechanischen Komponenten muss aufgrund ihrer physikalischen Eigenschaften bewertet und festgestellt werden. Die Bewertung auf Basis des deterministischen Fehlermodells hat die Zielsetzung, das Auftreten systematischer Fehler gänzlich zu vermeiden. Die Eignungsprüfung einer mechanischen Komponente für die konkrete verfahrenstechnische Anwendung ist also das richtige Werkzeug. Auf dieser Basis können systematische Fehler wie Korrosion, mechanisches Versagen oder Verkleben sicher und nachweislich ausgeschlossen werden. Die Nachweisführung kann über Baumusterprüfungen, Einzelprüfungen oder über Betriebserfahrung unter identischen Rahmenbedingungen (Prior Use) erfolgen. In Verbindung mit einem Managementsystem der funktionalen Sicherheit können systematische Fehler über den gesamten Sicherheitslebenszyklus wirksam vermieden werden. Es gilt allerdings zu beachten, dass die Architekturanforderungen durch den festgelegten Safety Integrity Level auch auf Teilsysteme mit mechanischen Komponenten anzuwenden sind.

Andere Normen und Regelwerke

Konkret können beispielsweise die Druckgeräterichtlinie und die DIN EN 4126 herangezogen werden. Denn für Ausrüstungsteile mit Sicherheitsfunktion im Bereich der Absicherung gegenüber Überdruck sind dort die Anforderungen beschrieben: Konkret müssen die Komponenten gemäß der Kategorie IV mit den dafür zulässigen Modulen für das Qualitätssicherungsverfahren im Rahmen der Herstellung in Verkehr gebracht werden.

In DIN EN 161 werden Anforderungen an automatische Absperrventile für Gasbrenner und Gasgeräte beschrieben. Wird ein Absperrventil gemäß den dort genannten Anforderungen hergestellt und geprüft, kann aus Sicht der Normensetzer ein gefahrbringender Ausfall – innerhalb der festgelegten Lebensdauer und bei Beachtung der Wartungsvorgaben – ausgeschlossen werden. Zur Herstellung, Auslegung, Eignung und Auswahl von mechanischen Komponenten stehen demnach schon heute valide Vorgehensweisen und Strategien zur Verfügung. Bei deren Umsetzung werden systematisch Fehler vermieden. Das Ergebnis sind uneingeschränkt sichere mechanische Sicherheitseinrichtungen und Komponenten.

Ausblick

Hersteller von Komponenten, Baugruppen und Anlagen sowie Planer, Konstrukteure und Betreiber sollten bei der Auswahl von Bewertungs- und Berechnungsverfahren sorgfältig überprüfen, ob diese tatsächlich die realen physikalischen Gegebenheiten ausreichend exakt abbilden. Die probabilistischen Ansätze zur Berechnung von Ausfallwahrscheinlichkeiten sind bei mechanischen Komponenten sicher nicht zielführend, sondern vermitteln ein nicht belastbares Gefühl von Berechenbarkeit und Sicherheit. Aus diesem Grund sollten aus Sicht von TÜV SÜD vorhandene Lösungsansätze kritisch hinterfragt und gegebenenfalls verworfen werden, bei denen aufgrund der Nachfrage von einigen Marktteilnehmern etwa SIL-äquivalente Kenngrößen für mechanische Sicherheitseinrichtungen angestrebt werden. Stattdessen sollten die bereits am Markt vorhandenen Regelwerke und Ansätze zur Orientierung genutzt und zur Vermeidung von systematischen Fehlern künftig weiter spezifiziert werden. Die Orientierung an den oben genannten Regelwerken stellen einen bewährten Ansatz zur Vermeidung von systematischen Fehlern dar.

www.prozesstechnik-online.de
Suchwort: cav0219tuevsued

Von außen sieht dieses Sicherheitsventil gut aus. Durch falsche Werkstoffauswahl traten jedoch massive Korrosionsschäden im Bereich der beweglichen Teile auf, der Ventilteller war nicht mehr beweglich, das Ventil hätte nicht angesprochen.

Autoren

Rainer Semmler

Process Safety Management
TÜV SÜD Chemie Service GmbH
Frankfurt

Christian Eberle

Leiter Kompetenzzentrum
Funktionale Sicherheit
TÜV SÜD Industrie Service GmbH
Regensburg

TÜV SÜD Industrie Service GmbH
Kompetenzzenrum Funktionale Sicherheit
93051 Regensburg

Telefon 0941 9910-402
christian.eberle@tuev-sued.de

www.tuev-sued.de/is