Diagnosefähige Aktorik in sicherheitsgerichteten Kreisen

Ein Vergleich von Architekturkonzepten

Für Feldgeräte in sicherheitstechnischen Kreisen ist es entscheidend, zur Vermeidung systematischer Fehler den Sicherheitslebenszyklus entsprechend DIN EN 61511 und DIN EN 61508 zu implementieren. In diesen Normen finden sich klare Forderungen nach definierten Prozeduren, regelmäßigen Überprüfungen sowie einer Dokumentation der erzielten Ergebnisse bis hin zur Analyse und de daraus resultierenden Maßnahmen. Diese organisatorischen Forderungen können durch Instrumentierung entsprechend dem derzeitigen Stand der Technik wirkungsvoll unterstützt werden. Für den Bereich der Stellgeräte sind Konfigurationen mit marktgängigen Komponenten möglich. Neben einem erhöhten Automatisierungsgrad, insbesondere für die Phasen der Validierung, wiederkehrenden Prüfung und Prüfung im laufenden Betrieb, können diese sogar die Installationen vereinfachen. Aufbauend auf den Forderungen der Normen werden in diesem Beitrag entsprechende Architekturen vorgestellt und ein Ausblick auf die Einbindung in Arbeitsabläufe gegeben.

SCHLAGWÖRTER DIN EN 61511, Partial Stroke Test / Wiederkehrende Prüfung / Sicherheitslebenszyklus / Automatisierte Prüfverfahren / Stellgeräte

Control Valves with Diagnostic Functions in Safety-instrumented Systems – A Comparison of Architectures

Implementing the safety life cycle according to IEC 61511 and IEC 61508 is decisive in preventing systematic failures in field units installed in safety-instrumented systems. In these standards, clear requirements for defined procedures, regular testing, documentation of test results, failure analysis and resulting actions are stipulated. Modern instrumentation is an important means of implementing the safety life cycle. In the field of control valves the required accessories are readily available on the market. In addition to the higher degree of automation for validation, proof testing and online testing while a process is running, these control valves may even be simpler in their hook-up.

KEYWORDS IEC 61511 / partial stroke test / proof test / safety life cycle / automated testing / control valves

THOMAS KARTE, Samson
BERND SCHÄFER, Hima

Um Stellgeräte in Anlagen der Prozessindustrie im laufenden Betrieb zu testen, wird seit einigen Jahren das Verfahren des Partial Stroke Testing (PST) viel diskutiert. Dabei wird die betreffende Armatur um eine begrenzte Strecke bewegt; einerseits soll durch diese Bewegung die Funktionsfähigkeit nachgewiesen werden, andererseits wird durch eine Wegbegrenzung sichergestellt, dass der laufende Prozess nicht beeinträchtigt wird. Schon länger bekannt sind Vorgehensweisen, bei denen eine mechanische Verblockung benutzt wird. Der Test wird dann durch manuelles Abziehen des Steckers am Magnetventil ausgelöst. Inzwischen sind jedoch Feldgeräte verfügbar, die diesen Test automatisch durchführen. Insbesondere Stellungsregler verschiedener Hersteller bieten eine solche Möglichkeit. Diese Technologie gilt inzwischen als ausgereift. Ursprüngliche Sorgen, zum Beispiel bezüglich eines Überschwingens des Ventils und einer damit verbundenen Störung des laufenden Betriebs der Anlage, sind widerlegt.

Trotz dieser technischen Fortschritte und trotz des hohen potenziellen Nutzens werden die Möglichkeiten des Online-Testens noch wenig genutzt. Es hat sich gezeigt, dass nicht nur die Gerätetechnik des speziellen Feldgeräts (Stellungsregler) sondern die gesamte Einbindung in Anlagenstruktur und Arbeitsorganisation über die Machbarkeit und den Erfolg des Verfahrens entscheiden. Der Beitrag erläutert den Stand der Technik bezüglich dieser Aspekte.

1. ANWENDUNG

Eine sehr gute Übersichtsdarstellung zu den Anforderungen an Test- und Diagnoseverfahren in sicherheitsgerichteten Kreisen findet sich zum Beispiel in [1]. Eine umfassende Behandlung etwa der Auswirkungen des Partial Stroke Testing auf die Verfügbarkeit (Probability of Failure on Demand – PFD) ist in [2] nachzulesen. Eine Betrachtung zur Kategorisierung der Test- und Diagnoseverfahren wird in [3] gegeben. Insgesamt fällt auf, dass sich die Betrachtungen durchgängig mit den Auswirkungen der Testverfahren auf die Rate der zufälligen Fehler befassen. Wichtig erscheint aber, das gesamte Anforderungsprofil aus DIN EN 61511 zu verstehen und daraus entsprechende Schlussfolgerungen für den Einsatz von Testverfahren abzuleiten. Die Diskussionen und Veröffentlichungen der letzten Jahre haben die Bedeutung von systematischen Fehlern, insbesondere für Aktorik und damit Stellgeräte, in den Mittelpunkt gestellt [4, 9, 1]. Entsprechend der Norm werden systematische Fehler und zufällige Fehler unterschieden (Bild 1).

Kann die Ursache eines Fehlers – und sei es nur nach einem entsprechenden Vorfall – klar festgestellt werden und lassen sich Maßnahmen ergreifen, die einen solchen Fehler zuverlässig verhindern, so handelt es sich um einen systematischen Fehler. Hierunter fällt für Stellgeräte zum Beispiel die richtige Dimensionierung, die Auslegung für den Einsatzfall entsprechend Medienverträglichkeit, Druck- und Temperaturverhältnissen sowie die Beachtung der Umgebungsbedingungen [5]. Das entscheidende Werkzeug zur Beherrschung systematischer Fehler ist die Einführung eines Sicherheitslebenszyklus (Functional Safety Management System – FSM). Bild 2 verdeutlicht die Forderung nach einer geregelten Vorgehensweise, die Schritt für Schritt eine systematische Abarbeitung einzelner Phasen wie Sicherheitsanalyse, Definition der Anforderungen, Definition der Auslegung, geordnete Implementierung, Validierung bis hin zur definierten Vorgehensweise für Betrieb und Wartung vorsieht. Eine eingehende Erörterung dieser Aspekte findet sich in [4]. Werden alle geforderten Schritte eingehalten, so ist davon auszugehen, dass systematische Fehler auf ein Minimum reduziert sind. Das verbleibende Risiko – unerkannte systematische Fehler – wird entsprechend Bild 1 durch drei Mechanismen eingegrenzt, nämlich durch:

- Diagnose oder Tests,
- Fail-Safe-Verhalten der eingesetzten Geräte – wenn Ausfall, dann in die sichere Richtung,
- Redundanz, bevorzugt diversitäre Redundanz.

Schon diese Betrachtungsweise macht jenseits jeder Wahrscheinlichkeitsbetrachtung die Bedeutung von Diagnose und Tests, insbesondere im laufenden Betrieb, klar. Aufbauend auf der Sicherheitsanalyse werden sicherheitsgerichtete Kreise implementiert. In der überwiegenden Mehrzahl der Fälle ist es Aufgabe der in diesen Kreisen installierten Stellgeräte, im Falle einer Anforderung eine Rohrleitung abzusperren oder freizugeben. Die Überprüfung der Funktionsfähigkeit dieser Stellgeräte im laufenden Betrieb kann zur Aufdeckung bisher nicht erkannter systematischer Fehler führen. Das wird an einem einfachen Beispiel verdeutlicht: Berücksichtigt die Antriebsauslegung eines Stellgeräts nicht alle Betriebsphasen, so mag die Validierung (also der Funktionstest der Armatur) im Rahmen der sogenannten Wasserfahrt noch einwandfreie Funktionalität signalisieren. Das Festsitzen der Armatur während einer kritischen Betriebsphase, zum Beispiel wegen kritischer Medien oder falsch eingeschätzter Druckverhältnisse an der Armatur, lässt sich aber nur über den Beweglichkeitstest im laufenden Betrieb erkennen.

Einige Anforderungen, die sich im Sicherheitslebenszyklus ergeben und in den Normen explizit aufgeführt sind, seien kurz zitiert: Durchgängig wird eine strukturierte Vorgehensweise gefordert, das heißt, es müssen nach DIN EN 61511 Kapitel 15 und 16, sowie VDI 2180-3 und VDI 2180-5 [6, 7, 8]:

- definierte Prozeduren vorhanden sein, die reproduzierbar durchgeführt werden können,
- die Prozeduren dokumentiert werden,
- das Ergebnis von Prüfungen dokumentiert werden, sowohl im Falle eines Fehlers als auch im Fall einwandfreier Funktion,
- die Testergebnisse analysiert und Schlussfolgerungen für mögliche Verbesserungen gezogen werden,
- alle Betriebsphasen in den Tests berücksichtigt werden,
- Stellgeräte unter Betriebsbedingungen geprüft werden, insbesondere bei vollem Betriebsdruck.

Besonders die letzten beiden Forderungen sind durch die oft geübte Praxis – Test des Sicherheitskreises durch Funktionstest bei abgestellter Anlage – sicherlich nicht erfüllt. Insgesamt verdeutlicht die Aufzählung, dass ein automatisierter Testablauf dem geforderten Sicherheitslebenszyklus weit besser entspricht als manuelle Prüfmethoden mit Bewertung durch Beobachtung. „Einrichtungen zur automatischen Funktionsüberwachung (zum Beispiel Laufzeit- oder Stellungsüberwachung, Plausibilitätsprüfung, Schritt- und Zeitüberwachung)“ werden in VDI 2180-3, Absatz 2.2.3.2 [7] explizit verlangt. Die Anforderungen an den Sicherheitskreis müssen definiert werden. Aus diesen lassen sich auch die Anforderungen für das Stellgerät ableiten. Diese sind im Wesentlichen:

- Die Reaktionszeit: Innerhalb welchen Zeitraums nach Anforderung der Sicherheitsfunktion muss dass Stellgerät die vorgesehene Position erreichen?
- Welche Dichtheit oder welcher Öffnungsquerschnitt muss erreicht werden? Daraus lassen sich Anforderungen an die genaue Position herleiten.
- Welche Antriebskraft oder welches Drehmoment muss aufgebracht werden? Wie groß ist die erforderliche Reserve, mit der alle Betriebsbedingungen und Alterungsprozesse sicher beherrscht werden können?

Je nach spezieller Anwendung können sich zusätzliche Forderungen ergeben [5, 8]. Entsprechend den gestellten Anforderungen sind Diagnose- und Testverfahren nach dem Grad der Fehleraufdeckung (Diagnostic coverage, proof test coverage) zu bewerten. Dies kann zum Beispiel durch eine FMEDA geschehen.

Bei der Sensorik ist ein interessanter Trend zu beobachten: In dem Bemühen um einen möglichst hohen Grad an Fehleraufdeckung werden inzwischen binäre Überwachungen wie Grenzwertschalter für Füllstand, Temperatur oder Durchfluss häufig durch analoge Sensoren ersetzt. Ein analoges Signal lässt sich eben besser auf Plausibilität überprüfen; hier bieten sich zum Beispiel eine Analyse des Rauschverhaltens und eine Korrelation mit Prozesswerten anderer Messstellen an. Dem würde auf Seiten der Aktorik der Einsatz eines analogen Stellungsmelders mit kontinuierlicher Wegerfassung für den gesamten Hubbereich anstelle der bisher gebräuchlichen induktiven Endlagenschalter entsprechen. Dies ist in der betrieblichen Praxis entsprechend dem Kenntnisstand der Autoren nur selten implementiert.

Für folgende Phasen des Lebenszyklus bieten sich automatisierte Testverfahren an:

- Validierung bei Inbetriebnahme
- Wiederkehrende Prüfung
- Prüfung im laufenden Betrieb
- Prüfung bei planmäßiger oder insbesondere auch unvorhergesehener Abschaltung

Neben der Betrachtung systematischer Fehler sind auch zufällige Fehler zu berücksichtigen. Bei mechanischen Systemen ist die Ursache eines Versagens in der Regel erkennbar. Dieser Ursache kann durch entsprechende Design- oder Verfahrensänderung Rechnung getragen werden. Daher sind für mechanische Systeme zufällige Fehler weit weniger signifikant. Eine ausführliche Begründung für diesen Sachverhalt findet sich zum Beispiel in [9]. Auch im Fall zufälliger Fehler fordert die Norm [6] die Anwendung der Werkzeuge Diagnose, Fail-Safe-Verhalten und Redundanz. Zusätzlich wird der rechnerische – probabilistische – Nachweis der erreichten Zuverlässigkeit verlangt.

Zur Berechnung der Ausfallwahrscheinlichkeit wird entsprechend [6] der einfache Zusammenhang:

Formel 1: $PFD = ½ \cdot \lambda_{du} \cdot T_{PR}$

angewendet.

Wird ein Testverfahren wie zum Beispiel PST mit einer gegenüber dem Prooftestintervall häufigeren Testfrequenz eingesetzt, ändert sich die PFD zu

Formel 2:
$PFD = ½ \cdot \lambda_{du} \cdot (1\text{-}DC) \cdot T_{PR} + ½ \cdot \lambda_{du} \cdot DC \cdot T_{PST}$

Diagnose und Testverfahren gehen also direkt in das Ergebnis ein. Demzufolge kann eine verlängerte Prüfdauer über entsprechende Diagnoseverfahren angestrebt werden. Dies erscheint für viele Anwendungen realistisch, muss aber im Einzelfall analysiert werden. Näherungsweise ergibt sich, dass eine Testabdeckung von 50 % eine Verdoppelung der Laufzeit zwischen zwei vollständigen Prüfungen mit Anlagenstillstand ermöglicht. Weiterfüh-

rende Betrachtungen liefern [2, 11, 12]. Dieser rechnerisch ermittelte Wert ist jedoch nur bei konstanter Fehlerrate gültig. Steigt die Fehlerrate im betrachteten Zeitraum an, zum Beispiel durch Verschleiß oder Alterung, so ist dies der maßgebliche Mechanismus. Soll zum Beispiel eine ununterbrochene Laufzeit von fünf Jahren erreicht werden, so ist bei entsprechend geringer Ausfallrate der rechnerische Nachweis zur Erreichung dieser Laufzeit einfach möglich. Es ist zu beachten, dass die angenommene Konstanz der Fehlerrate durch Prozesseinfluss, Alterung, Verschleiß oder andere Mechanismen beeinträchtigt wird.

In diesem Zusammenhang ist jedoch Vorsicht im Umgang mit den statistischen Daten ratsam: Bei allen den Autoren bekannten Veröffentlichungen zur rechnerischen Betrachtung der Ausfallwahrscheinlichkeit (PFD) wird keine Fehlerrechnung durchgeführt, die Belastbarkeit der ermittelten Werte also nicht untersucht. Dies kann zu nicht gerechtfertigtem Vertrauen in die rechnerischen Werte führen. So wird beispielsweise in [10] angeführt, dass sich verschiedene Datenbanken für elektronische Bauteile oft in ihren Angaben um mehr als eine Zehnerpotenz unterscheiden.

2. ANFORDERUNGEN AN DEN WORKFLOW

Feldgeräte bieten eine Vielzahl von Diagnosemöglichkeiten. Über den möglichen Nutzen für den Anwender entscheiden nicht nur die Leistungsfähigkeit dieser Geräteeigenschaften sondern insbesondere die Möglichkeit, die Anwendung dieser Diagnose in den betrieblichen Alltag einzubinden.

Die Möglichkeiten für Stellgeräte werden anhand des Einsatzes von Stellungsreglern oder intelligenten Grenzsignalgebern kurz angedeutet. Eine grafische Darstellung eines automatisierten Vollhubtests findet sich in Bild 3, eine parametrisierte Auswertung in Bild 4. Messungen dieser Art können von diesen Geräten lokal durchgeführt, aufgezeichnet und ausgewertet werden [11, 12]. Bild 5 stellt zwei Aufbauvarianten dar: links eine mit Magnetventil und induktiven Endlagenschaltern automatisierte Klappe, rechts einen nach Stand der Technik mit elektronischem Grenzwertgeber ausgerüsteten Kugelhahn. Die Parameter Totzeit, Laufzeit der Armatur bis zum Erreichen der Endstellung, genaue Messung der erreichten Endlage und benötigte Antriebskraft werden durch die geräteinterne Weg- und Druckmessung erfasst. Die Resul-

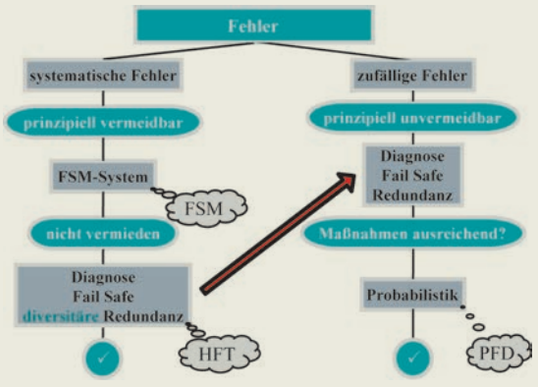

BILD 1: Versagensursachen nach [4]

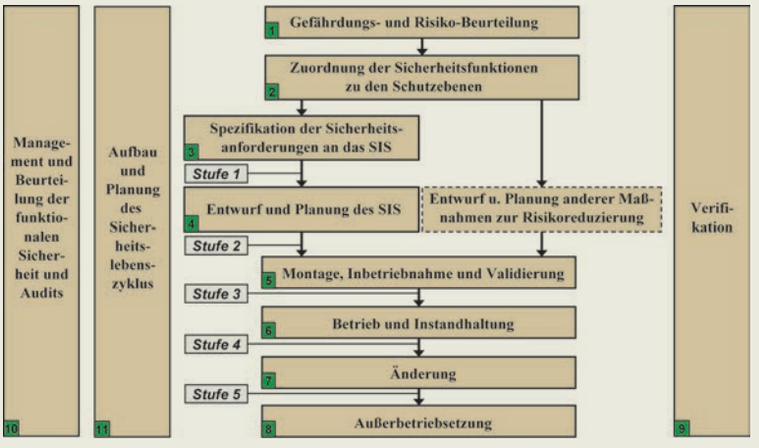

BILD 2: Sicherheitslebenszyklus nach DIN EN 61511-1 Bild 8

SYMBOLVERZEICHNIS		
BPCS	Basic process control system	Betriebs- und Überwachungseinrichtungen als ein System (Leitsystem)
DC	Diagnostic coverage	Diagnose-Deckungsgrad
FMEDA	Failure modes, effects and diagnostic coverage analysis	Fehlermöglichkeits-, Einfluss- und Diagnoseanalyse
FSM	Functional safety management system	Management der funktionalen Sicherheit
HFT	Hardware fault tolerance	Hardware-Fehlertoleranz (Redundanzgrad)
PFD	Probability of failure on demand	Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung
PST	Partial stroke testing	Teilhub-Testverfahren
SIS	Safety instrumented system	Sicherheitstechnisches System
T_{PR}	Proof test intervall	Zeitdauer zwischen den wiederkehrenden Prüfungen
T_{PST}	Partial stroke test intervall	Zeitdauer zwischen Partial-Stroke-Tests
λ_{du}	Failure rate dangerous undetected	Rate gefährlicher, unentdeckter Fehler

tate lassen sich aus dem Weg-Zeit-Diagramm ablesen, sie werden aber auch innerhalb des Stellungsreglers als charakteristische Zeiten beziehungsweise Werte ermittelt. Darüber hinaus kann noch über den Stick-Slip-Effekt auf Reibkräfte geschlossen werden. Ein Antrieb mit hoher Reibung würde im Weg-Zeit-Diagramm ein ruckhaftes Verfahren zeigen.

Ein Vergleich all dieser Messwerte mit den erwähnten aus der Norm resultierenden Anforderungen zeigt, dass die Funktionsfähigkeit des Stellgerätes im Sicherheitskreis umfassend beurteilt werden kann. Der genaue Grad der Diagnose- sowie die Testabdeckung ist im Einzelnen festzulegen, ein mögliches Vorgehen dafür ist die Gegenüberstellung der potenziellen Fehlerquellen der Gefahrenanalyse zu den Diagnosemöglichkeiten des eingesetzten Feldgerätes. Die Beweglichkeit der Armatur und das genaue Erreichen der Endlage oder Zwischenposition kann einwandfrei beurteilt werden. Lediglich bei hohen Anforderungen an die Dichtigkeit können eventuell zusätzliche Messungen erforderlich werden.

Die Einbindung dieser Methodik in den Betriebsablauf ist mit der Durchführung eines einzelnen Tests aber noch nicht gegeben. Eine Übersicht über die Abfolge aller notwendigen Schritte gibt Tabelle 1. Neben der automatisierten Durchführung eines Tests ist es insbesondere von Bedeutung, dass die Ergebnisse erfasst und abgespeichert werden können. Es muss eine Datenbank zur Verfügung stehen, die es gestattet, alle durchgeführten Testläufe festzuhalten. Hierbei ist die Archivierung von Bedeutung sowie die entsprechende Auswertung, sowohl für den Einzeltest als auch für Trends, die sich erst in der Zusammenschau mehrerer Tests oder gar in Korrelation mit anderen Prozesswerten ergeben. Entsprechend trägt Tabelle 1 in senkrechter Richtung alle notwendigen Arbeitsschritte auf, in waagrechter Richtung wird eine Aufgabenverteilung auf die Ressourcen Stellungsregler und Asset-Management-System vorgeschlagen. Die genaue Verteilung der Aufgaben ist natürlich diskussionsfähig, aber es wird doch die Notwendigkeit eines übergeordneten Systems mit gegenüber einem Feldgerät erweiterten Ressourcen evident.

3. ARCHITEKTUREN DES SICHERHEITSKREISES

Wird die Verfügbarkeit eines PST-fähigen Stellungsreglers vorausgesetzt, so ergibt sich sofort eine Anordnung der Feldgeräte wie in Bild 6 A dargestellt und in Tabelle 2 bewertet. Der Sicherheitskreis ist klassisch mit Magnetventil zur Abschaltung und Endlagenschaltern zur Positionsmeldung ausgerüstet. Ein Stellungsregler, pneumatisch dem Magnetventil vorgeschaltet, sorgt für die gewünschte PST-Funktionalität. Die Auslösung des Tests erfolgt lokal am Stellungsregler, die Datenübertragung der Messdaten und ausgewerteten Ergebnisse an das übergeordnete Asset-Management-System über digitale Kommunikation per HART-Protokoll. Eine Auskoppelung des HART-Protokolls kann zum Beispiel über geeignete Trennverstärker geschehen, wie sie am Markt verfügbar sind (Beispiele siehe [13, 14]). Diese Konfiguration wurde und wird in der Praxis eingesetzt, für den Test – insbesondere durch Bedienpersonal vor Ort – ist sie auch durchaus geeignet. Für große Anlagen mit einer Vielzahl von Armaturen und bei reduziertem Wartungspersonal fällt aber der erforderliche Testaufwand negativ ins Gewicht. Eine Vielzahl weiterer Konfigurationen ist möglich, hier wird die vorteilhafteste Lösung B beschrieben (Bild 6 B):

- Unter Verzicht auf das Magnetventil wird der Stellungsregler zur sicherheitsgerichteten Abschaltung und zum automatisierten Test eingesetzt. Voraussetzung dafür ist eine Eignung des Stellungsreglers entsprechend DIN EN 61508 beziehungsweise 61511. Entsprechende Geräte sind verfügbar. Diese Konfiguration erspart in erheblichem Umfang Verkabelungsaufwand und erhöht auch die Testtiefe, da nur eine pneumatische Einheit verwendet wird und diese auch den Testlauf durchführt.
- Der Stellungsregler ist über 4–20 mA direkt an die Sicherheits-SPS angeschlossen. Entsprechend zertifizierte Ausgangskarten sind am Markt.
- Das HART-Protokoll wird ohne zusätzliche Rangierung auf die Ebene der Trennverstärker durch die Sicherheits-SPS getunnelt. Zur Weiterleitung an das Asset-Management-System wird die in der Praxis ohnehin meist gelegte Ethernetverbindung zwischen SPS und Leitsystem (Basic Process Control System – BPCS) benutzt. Die Schematik der Verschaltung zeigt Bild 7. Die Besonderheit dieser Architektur ist die parallele, gleichzeitige Funktion der HART-Kommunikation. Dies bedeutet gegenüber der seriellen Arbeitsweise eines Multiplexers einen erheblichen Zeitvorteil. Die Kommunikationsmöglichkeiten können gezielt eingeschränkt werden. Damit ist gewährleistet, dass die ermittelten Testdaten aus den Feldgeräten ausgelesen werden können, ohne durch irrtümliche Parametrierung deren Funktionalität zu verändern.

Mit der favorisierten Lösung nach Bild 6 B ist einerseits das Auslesen von Diagnosedaten möglich, andererseits wird eine irrtümliche Konfiguration des Feldgeräts zuverlässig verhindert. Folgende Kriterien werden zur Beurteilung herangezogen:

- Der Stellungsregler wird durch Standardsignale angesteuert:
  +20 mA signalisieren Normalbetrieb – Endlage
  +12 mA signalisieren Start Testlauf
  +4 mA signalisieren sicherheitsgerichtete Abschaltung
  Stellungsregler mit entsprechendem Zertifikat für zuverlässige Abschaltung bei 4 mA (anstelle von 0 mA) gibt es.
- Auch während des Testlaufs ist die sicherheitsgerichtete Abschaltung möglich, da der Stellungsregler eine etwaige Abschaltung priorisiert behandelt.
- Der Testlauf wird nach Triggerung durch ein externes Signal lokal durch den Stellungsregler durchgeführt. Dadurch ist eine hohe Regelgüte für den vorgegebenen Verfahrweg möglich.
- Die Daten entsprechend Bild 3 werden lokal erfasst und abgespeichert. Diese Vorgehensweise ermöglicht Abtastraten beispielsweise für die Position der Armatur und den Antriebsdruck im Millisekundenbereich mit entsprechend positiver Auswirkung auf die Güte der Messwerte und damit eine hohe Diagnoseabdeckung.
- Die Bedienschnittstelle wird über die sicherheitsgerichtete Steuerung abgebildet. Damit ist es möglich,

Arbeitsschritte PST	Stellungsregler	Asset Management	Annahme
Auslösen	Manuell/Automatisch	Manuell/Automatisch	
Durchführen	Rampe/Sprungantwort		
Erfassung Ergebnisse in Echtzeit	Weg-Zeit-Diagramm, Kennzahlen		Datenübertragung in Echtzeit nicht möglich
Ergebnisse aus Feldgerät auslesen	Weg-Zeit-Diagramm, Kennzahlen	Weg-Zeit-Diagramm, Kennzahlen	
Ergebnisse abspeichern	Weg-Zeit-Diagramm, Kennzahlen	Weg-Zeit-Diagramm, Kennzahlen	
Arbeitsschritte Nachbereitung			
Auswertung eines Testlaufs	Lokale Diagnose	Diagnose, Verbindung zu Prozess-informationen	
Alarmgenerierung	Lokale Alarmgenerierung	Alarmgenerierung und Einbeziehung Prozessinformation	
Archivierung		Langzeitspeicherung in Datenbank	
Trend über mehrere Testläufe		Vergleich einzelner Messwerte über mehrere Testläufe, Diagnose, Alarmgenerierung	

TABELLE 1: Workflow Partial Stroke Test (PST)

	Lösung A	Lösung B	Lösung C	Lösung D
Sicherheitsgerichtete Ansteuerung	Magnetventil	Stellungsregler	Magnetventil	Magnetventil
Partial Stroke Testing (PST)	Stellungsregler	Stellungsregler	Magnetventil	Magnetventil
Wegrückmeldung	Endlagenschalter	Endlagenschalter, alternativ Transmitter	Endlagenschalter, alternativ Transmitter	Endschalter
Druckmessung Antrieb	Stellungsregler	Stellungsregler	Optional Transmitter	
Test der Pneumatik	nein	ja	ja	ja

TABELLE 2: Architekturvergleich der Vorschläge aus Bild 6

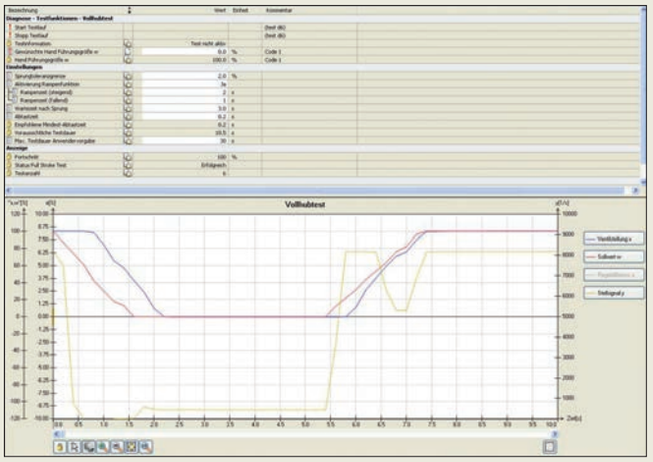

BILD 3: Vollhubtest

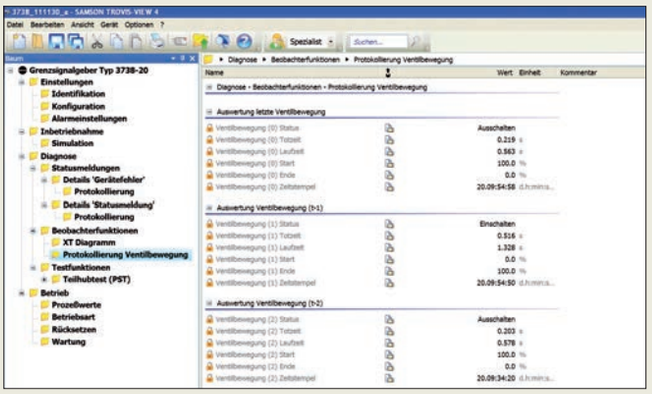

BILD 4: Protokoll Ventilbewegungen

ein entsprechendes, normkonformes Regelwerk für eine Ent- und Verriegelung des Sicherheitskreises mit einfachen Mitteln zu hinterlegen.

- Die Wegrückmeldung erfolgt analog. Dies wiederum führt gegenüber einer Signalisierung über zwei Endlagenschalter zu einem geringeren Verkabelungsaufwand und hat den Vorteil einer höheren Messgenauigkeit beziehungsweise verbesserten Diagnosemöglichkeit.
- Bei großen Armaturen mit entsprechender Anforderung an die Luftleistung der steuernden Komponenten kann ein analoger pneumatischer Booster in der Verbindungsleitung zwischen Stellungsregler und Antrieb eingesetzt werden (gestrichelte Darstellung in Bild 6 B). Auch hier sind inzwischen zertifizierte Geräte marktgängig.

Zu weiteren denkbaren Varianten sind einige Anmerkungen angebracht:

- Bild 6 C legt die Funktionalität des Tests ganz in die Sicherheits-SPS: Der pneumatische Antrieb wird nun über das Magnetventil angesteuert, der Regelkreis zur Steuerung des Testlaufs über einen analogen Stellungstransmitter geschlossen. Um eine im Vergleich zu Variante B gleichwertige Diagnosetiefe zu erhalten, ist ein Drucktransmitter zur Messung des Antriebsdrucks vorgesehen. Diese Konfiguration hat den Vorteil, dass das komplette Regelwerk für den Testablauf und die Auswertung in der SPS hinterlegt werden kann und damit zertifizierungsfähig ist. Nachteilig ist demgegenüber eine verringerte Abtastrate, die aber beim Einsatz moderner Systeme je nach Ausführung auch unter 100 Millisekunden liegen kann. Die Abtastrate ist für die erzielbare Regelgüte des Testlaufs (Überschwingen) und für die Güte der Diagnose von Bedeutung. Entsprechend kommt Konfiguration C bevorzugt für große Armaturen mit Laufzeiten größer 5 Sekunden in Betracht.
- Bild 6 B ist auch für den Sonderfall der Mitnutzung einer Regelarmatur für die sicherheitsgerichtete Abschaltung einsetzbar. Diese Mitnutzung findet sich häufig in Anlagen im deutschen und europäischen Raum. Eine entsprechende Analyse der sicherheitstechnischen Aspekte findet sich in [15]. Klassisch wird in diesem Fall ein Stellungsregler – angesteuert durch das BPCS – und ein Magnetventil – angesteuert durch die SPS – instrumentiert. Es sind zwei Leitungen ins Feld notwendig. Entsprechend der Abbildung wäre aber auch eine sehr elegante und einfache Lösung denkbar. Ein Stellungsregler wird zur Regelung, Abschaltung und für den Test eingesetzt. Die Ansteuerung erfolgt nur über die SPS. Der notwendige Regelalgorithmus müsste dann in der SIS hinterlegt werden. Beispiele für solche Anwendungen finden sich im Bereich Turbo Machinery Control bei Überströmventilen oder im Bereich Burner Management bei Brennstoffregelungen. Über Ethernet ist die SPS an das BPCS angebunden und erhält von dort Vorgaben (beispielsweise eine Lastanforderung) während des Normalbetriebs. Entsprechende Applikationen sind aufgrund der heute verfügbaren Systemtechnik ebenfalls marktgängig (zum Beispiel Himax-System mit Flexsilon-Bibliotheken).
- Bild 6 D zeigt eine Variante, die sich ganz an den klassischen Signalen (Namursignal für Endlagenschalter entsprechend IEC 60947-5-6, 24 Volt zur Ansteuerung des Magnetventils) orientiert. Hier wird ein Gerät eingesetzt, dass die Funktionalität von Endlagenschalter und Magnetventil kombiniert, durch den Einsatz von analoger Wegmessung und Mikrorechner aber diagnosefähig ist. Der Vorteil der Benutzung vorhandener Verkabelung wird allerdings mit dem Verzicht auf Kommunikation erkauft; hierfür existiert bei dieser Art von Signalübermittelung kein standardisiertes Protokoll. Allerdings kann das Ergebnis der internen Diagnose wie zum Beispiel ein nicht erfolgreicher PST über einen Statuskontakt (Namursignal) an die übergeordnete Steuerung gemeldet werden (siehe auch [16]).

Zusammenfassend findet sich eine knappe Gegenüberstellung der verschiedenen Architekturen in Tabelle 2. Allen Lösungen ist gemeinsam, dass sie marktgängige Komponenten verwenden, die auch außerhalb des Sicherheitskreises eingesetzt werden. Damit ist der Einsatz betriebsbewährter Komponenten möglich, wie von Anwendern nachdrücklich gefordert [17]. In diesem Artikel nicht behandelt sind spezielle, herstellerspezifische Instrumentierungen mit proprietärer Architektur und Verdrahtung. Anstelle des HART-Protokolls kann auch ein Feldbus-Protokoll wie Profibus oder Fieldbus Foundation eingesetzt werden. Nach heutigem Stand der Technik müssen die sicherheitsgerichteten Signale aber noch durch diskrete Verkabelung übertragen werden.

4. EINBINDUNG IN BETRIEBLICHE ARBEITSABLÄUFE

Tabelle 1 listet die zu leistenden Arbeitsschritte auf. Erfahrungen mit ersten Installationen zeigen, dass Einzeltests auf Ebene der Feldgeräte unproblematisch durchzuführen sind und aussagekräftige Ergebnisse bringen. Soll jedoch eine Vielzahl von Geräten in einer großen Anlage regelmäßig getestet werden, so treten im Wesentlichen folgende Schwierigkeiten auf:

- Die mögliche Datenrate für die Übertragung der lokal in den Feldgeräten abgespeicherten Testergebnisse entspricht nicht den Anforderungen. Es scheint nach heutigem Stand der Technik nicht möglich, aus einer großen Menge von Feldgeräten täglich oder auch nur wöchentlich einen vollständigen Datensatz auszulesen. Die Begrenzung liegt weniger im Übertragungsprotokoll (HART-Protokoll) als vielmehr in der gesamten Architektur des Leitsystems. Hier müssen die für den Prozessbetrieb notwendigen Datentransfers gegenüber Diagnosedaten natürlich priorisiert behandelt werden.
- Auswertemöglichkeiten: Mehrere Hersteller bieten Asset-Management-Systeme an. Hier können Datensätze eines Feldgeräts mit Diagnoseinformationen ausgelesen und abgespeichert werden. Die Fähigkeit, aus einem Datensatz einzelne Messwerte isoliert zu betrachten und mit anderen Messwerten nach einem freien Algorithmus zu verknüpfen, ist jedoch noch nicht in wünschenswerter Weise implementiert. Notwendig kann es beispielsweise sein, die Historie eines Messwertes, zum Beispiel der Nullpunktlage eines Ventils, über mehrere Testläufe hinweg wiederzugeben (Bild 8). Auch die Verknüpfung eines Wertes mit aus anderen Feldgeräten gewonnenen Prozesswerten, zum Beispiel die Plausibilitätsprüfung von Ventilstellung gegen Durchfluss, erscheint in der Praxis noch nicht möglich. Insgesamt gibt Tabelle 1 einen Hinweis

BILD 5: Aufbauvarianten (links: separate Montage Magnetventil und Grenzsignalgeber; rechts: Stand der Technik, Grenzsignalgeber mit integriertem Magnetventil)

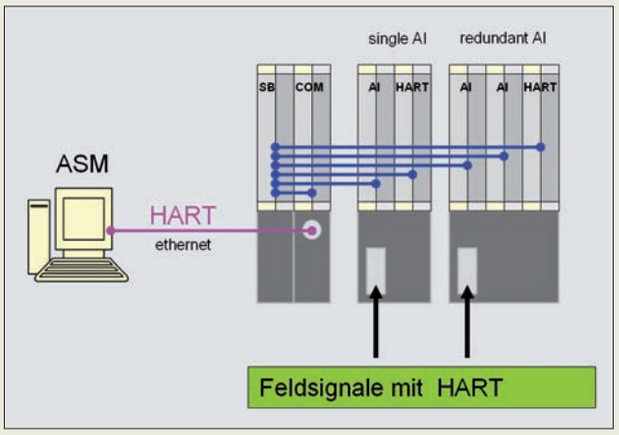

BILD 7: Tunnelung von HART-Signalen

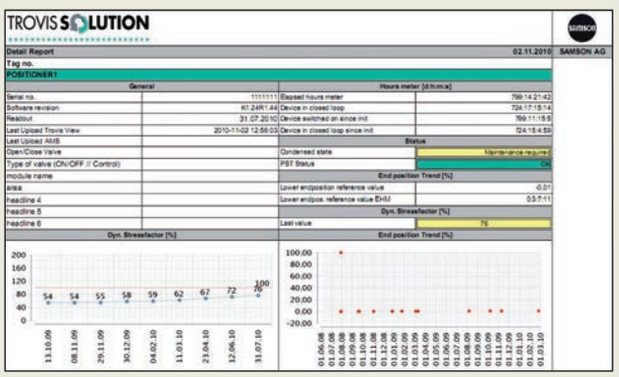

BILD 8: Nullpunkttrend

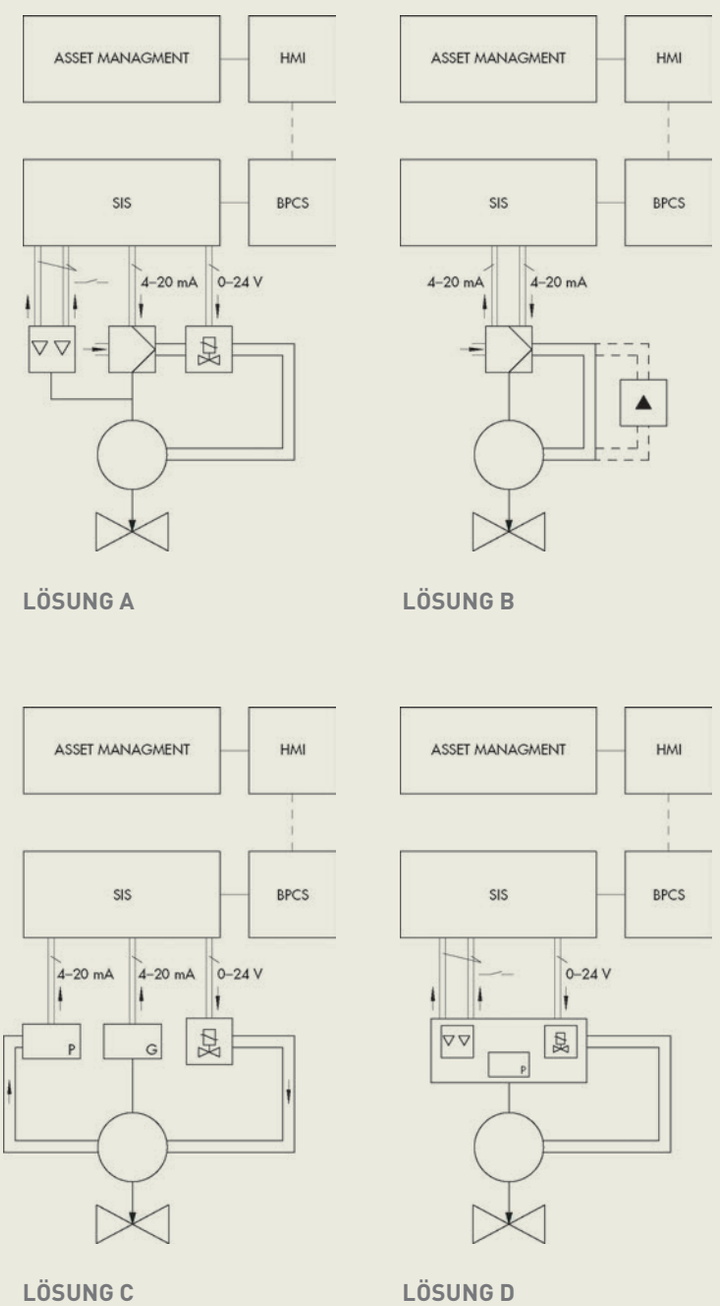

BILD 6: Mögliche Architekturen des Sicherheitskreises– Lösung A (oben links), Lösung B (oben rechts), Lösung C (unten links) und Lösung D (unten rechts)

AUTOREN

Dr. rer. nat. **THOMAS KARTE** (geb. 1955) beschäftigt sich bei der Samson AG in Frankfurt/Main mit der Anwendungstechnik elektropneumatischer Geräte.
Er ist Mitglied im FA 6.13 „Engineering von sicherheitsgerichteten Systemen“ des VDI/VDE-GMA und im DKE GK 914 „Funktionale Sicherheit“.

Samson AG,
Mess- und Regeltechnik,
Weismüllerstr. 3, D-60314 Frankfurt am Main,
Tel. +49 (0) 69 40 09 20 86,
E-Mail: tkarte@samson.de

Dipl.-Ing. (FH) **BERND SCHÄFER** (geb. 1967) arbeitet seit 1996 bei Hima, anfangs im Projekt-Management. Seit 2004 betreut er als Produktmanager den Bereich der OPC- und SCADA-Produkte. Darüber hinaus fallen in sein Aufgabengebiet spezielle Applikationen wie zum Beispiel Asset-Management-Lösungen und OTS (Operator Training Simulator)-Lösungen. Er ist Mitglied in der PLCOpen-Arbeitsgruppe zum Thema „OPC UA Informationsmodell“.

Hima Paul Hildebrandt GbmH & Co KG,
Albert-Bassermann-Str. 28, D-68782 Brühl bei Mannheim,
Tel. +49 (0) 6202 70 94 53,
E-Mail: b.schaefer@hima.com

auf die Arbeitsschritte und die mögliche Aufteilung auf das Feldgerät und das übergeordnete Asset-Management-System. Die Domäne des Feldgerätes ist die schnelle Datenerfassung und lokale Regelung. Wegen der durch den Energieverbrauch limitierten Verarbeitungsgeschwindigkeit und des dadurch auch begrenzten Speichers ist es sinnvoll, die langfristige Archivierung, Auswertung nach Trends und komplexe Alarmbildung im übergeordneten System zu leisten. Hier können auch die Informationen aus verschiedenen Feldgeräten sinnvoll zusammenfließen und nach übergeordneten Kriterien ausgewertet werden.

ZUSAMMENFASSUNG

Für Feldgeräte in sicherheitsgerichteten Kreisen, insbesondere solche mit direktem Kontakt zum Prozessmedium, ist die Behandlung der systematischen Fehler ausschlaggebend für die sicherheitstechnische Verfügbarkeit. Die notwendige Implementierung des Sicherheitslebenszyklus kann durch eine moderne Instrumentierung unterstützt werden. Der Stand der Technik bei Feldgeräten und sicherheitsgerichteten Steuerungen ermöglicht inzwischen die Implementierung wirkungsvoller und zugleich einfacher Architekturen mit marktgängigen Komponenten. Weitere Entwicklungen bezüglich Datenübertragungsrate und Funktionalität im Bereich des Asset Managements sind notwendig, damit die in den Feldgeräten verfügbaren Diagnosetools ihre volle Funktionsfähigkeit entfalten. Hierzu erscheint eine enge Zusammenarbeit zwischen Herstellern und Anwendern bei ausgewählten Pilotprojekten notwendig.

MANUSKRIPTEINGANG
14.03.2012
Im Peer-Review-Verfahren begutachtet

REFERENZEN

[1] Rogiers, I.: Using a „Smart“ Partial Stroke Test Device on SIS Loop On/Off Valves: Adding Value or Adding Cost?. P4039, Valve World 2004. KCI Publishing BV
[2] Börcsök, J., Schrörs, B. und Holub, P.: Reduzierung der Ausfallwahrscheinlichkeit und Verlängerung des Proof-Test-Intervalls durch Einsatz von Partial-Stroke-Tests am Beispiel von Stellgeräten. atp edition – Automatisierungstechnische Praxis 50(11), 2008
[3] McCrea-Steele, R.: Partial Stroke Testing The Good, the Bad and the Ugly. TUEV 7th International Symposium on Safety, 2006 .
[4] Götz, A., Hildebrandt, A., Karte, T., Schäfer, B und Ströbl, J.: Realisierung von Schutzeinrichtungen in der Prozessindustrie – SIL in der Praxis“. atp edition – Automatisierungstechnische Praxis 50(8), 2008
[5] Samson AG: Handbuch „Funktionale Sicherheit für Stellventile, Drehkegelventile, Kugelhähne und Stellklappen. WA 236
[6] DIN EN 61511-1 und DIN EN 61511-2: Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 1 und 2. Mai 2005
[7] VDI 2180-3: Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT) – Anlagenplanung, -errichtung und –betrieb. April 2007
[8] VDI 2180-5: Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT) – Empfehlungen zur Umsetzung in die Praxis. Mai 2010
[9] Hildebrandt, A.: SIL-Bewertung von Mechanik – Versagenswahrscheinlichkeit mechanischer Komponenten. atp edition– Automatisierungstechnische Praxis 53(1-2), 2011
[10] Smith, D.: Reliability, Maintainability and Risk. Elsevier Butterworth-Heinemann, Burlington, MA 01803, Sixth edition 2001
[11] Karte, T. und Kiesbauer, J.: Diagnosefähige Ventilstellungsregler und ihre Anwendung in sicherheitsgerichteten Kreisen. Industriearmaturen, Heft 3, 2008 (September)
[12] Samson AG: Handbuch Applikationshinweise für sicherheitsgerichtet Kreise. WA 239
[13] P+F Datenblatt: Ventilsteuerbaustein KFD2-RI-Ex1. Ausgabedatum 2010-04-13. Druckschrift 216568_GER.xml
[14] P+F Datenblatt: HART Loop Converter KFD2-HLC-Ex1.D. Ausgabedatum 2011-01-26. Druckschrift 198804_GER.xml
[15] Gabriel, T., Litz, L. und Schrörs, B.: Nutzung von SIS-Armaturen für Leitsystemfunktionen – Rahmenbedingungen für die Ausführung von BPCS-Funktionen. atp edition – Automatisierungstechnische Praxis 52(3), 2010.
[16] Karte, T. und Kiesbauer, J.: Intelligenter Grenzsignalgeber für Auf/Zu-Armaturen in der Prozesstechnik. atp edition – Automatisierungstechnische Praxis 51(5), 2009.
[17] Hablawetz, D., Matalla, N. und Adam, G.: IEC 61511 in der Praxis – Erfahrungen eines Anlagenbetreibers. atp edition – Automatisierungstechnische Praxis 49(10), 2007