Realisierung von Schutzeinrichtungen in der Prozessindustrie – SIL in der Praxis

Arno Götz, Endress+Hauser GmbH+Co. KG; Andreas Hildebrandt, Pepperl+Fuchs GmbH;
Thomas Karte, SAMSON AG; Bernd Schäfer, HIMA Paul Hildebrandt GmbH + Co KG;
Johann Ströbl, TÜV SÜD Industrie Service GmbH

DIN EN 61508 und DIN EN 61511 sind mittlerweile akzeptiertes Handwerkszeug für den Umgang mit Sicherheitskreisen. Im deutschen Sprachraum werden sie durch die abgeleitete VDI/VDE 2180 konkretisiert. Grundlegende Begriffe wie SIL, Ausfallrate, Anteil gefährlicher Fehler und andere sind im Bewusstsein verankert. Unsicherheiten bestehen dagegen häufig über eine Vorgehensweise zur praktischen Umsetzung im betrieblichen Alltag. Es gilt, das erforderliche Maß an Betriebssicherheit der Anlage mit gerichtsfesten Nachweismöglichkeiten und praktikablen Lösungswegen zu verbinden, die dabei auch ökonomische Aspekte einbeziehen. Im Nachfolgenden wird vorausgesetzt, dass aufbauend auf einer Gefährdungs- und Risikoanalyse die Anforderungen an eine PLT-Schutzeinrichtung (SIF, Safety Instrumented Function) definiert sind. Im Rahmen dieses Artikels wird dargestellt, was bei der Implementierung dieser Schutzeinrichtung zu beachten ist. Es werden Hinweise zum praktischen Einsatz der einzelnen Geräte gegeben. Hierbei werden nicht nur technische Aspekte berücksichtigt, sondern es wird auch die Einbindung in ein übergeordnetes Sicherheitsmanagement diskutiert.

Sicherheitstechnik / PLT-Schutzeinrichtungen / DIN EN 61511

Implementation of safety equipment in the process industry – SIL in practice

The IEC 61508 and IEC 61511 standards have become widely accepted as the basis for handling safety instrumented systems. In German-speaking countries, the VDI/VDE 2180 standard supplements these international standards. Users have become familiar with the basic terms, such as SIL, failure rate, safe failure fraction etc. However, many users are often uncertain when it comes to the practical implementation of these concepts in everyday operation. The decisive point is to combine the required degree of operational plant safety with legally compliant documentation and practical solutions, while taking into account the economic aspects as well. It is assumed in this article that the demands placed on a Safety Instrumented Function (SIF) are based on a hazard and risk analysis. This article explains which points need to be observed when implementing safety equipment and includes tips on how to use the instruments in practice. Besides the technical aspects, integration into a higher level safety management system is dealt with.

Safety in the process industry / Safety Instrumented Systems / DIN EN 61511

1. Einleitung

Umfang, aber auch theoretischer Hintergrund und nicht zuletzt Begriffswahl und Diktion der DIN EN 61511 geben immer noch Anlass für zahlreiche Fragen, seien diese nun bezogen auf das Verständnis der Zusammenhänge oder mehr auf ein „Kochbuchrezept" für einfache Umsetzung zielend. Zahlreiche Veröffentlichungen vertiefen Spezialthemen. Demgegenüber wird nachfolgend eine Schutzeinrichtung, deren Komponenten von unterschiedlichen Herstellern stammen, unter einheitlichen Gesichtspunkten beschrieben. Ziel ist es, die Kerngedanken der DIN EN 61511 und deren praktische Umsetzung herauszuarbeiten. Der Natur der Sache entsprechend kann das Ergebnis keine einfache Handlungsanweisung sein, wohl aber erweist sich klassisches ingenieurmäßiges Vorgehen als Dreh- und Angelpunkt sicherer Instrumentierung.

2. Normative Basis zur Risikoreduzierung an Prozessanlagen

Schon die Anwendbarkeit der Normen wirft viele Fragen auf:

- Muss ich die Anforderungen zwingend einhalten?
- Haben die Normen nur Empfehlungscharakter?
- Womit muss ich bei Nichteinhalten der Empfehlungen rechnen?

sind nur einige Beispiele aus der täglichen Praxis.

Klarheit bringt hier ein Blick auf die „Normungspyramide" (Bild 1). Diese Pyramide verdeutlicht einen zunehmenden Entscheidungsfreiraum, die Möglichkeit weg von starren gesetzlichen Regelungen hin zum individuellen Lösungsansatz zu gehen, wobei das zu erreichende Schutzziel aber stets im Mittelpunkt der Überlegungen stehen muss. Allerdings muss klar sein, dass bei steigender Individualität der

gewählten Lösung auch die individuelle Verantwortung und Haftung steigt. Im Falle eines Störfalles und einer Schuldzuweisung liegt die Beweislast für das Einhalten der Regeln der Technik beim Anwender. Der Verantwortliche steht im Falle eines Schadens in persönlicher Haftung. Im Umkehrschluss bietet der Weg, weg von den Unsicherheiten der technischen Regeln und deren Auslegung zur klaren Vorgabe durch Verordnungen und Gesetze, natürlich Sicherheit und weniger Eigenverantwortung durch den Betreiber. Dies geht jedoch mit dem Verlust flexibler Lösungen einher.

Zuerst muss geklärt werden, ob die betreffende Anlage der Norm, einem entsprechenden Gesetz oder einer Verordnung entsprechen muss. Viele Anlagen der chemischen oder petrochemischen Industrie sowie Prozessöfen unterliegen in Deutschland der Störfallverordnung.

In der Störfallverordnung (12. BImSchV 2000) ist im § 3 „Allgemeine Betreiberpflichten" Folgendes zu Normen und Regeln vermerkt:

„(1) …
(2) …
(3) …
(4) Die Beschaffenheit und der Betrieb der Anlagen des Betriebsbereichs müssen dem Stand der Sicherheitstechnik entsprechen."

D. h. der Betreiber ist verpflichtet, die Anlagen auf dem Stand der Sicherheitstechnik zu halten. Der Stand der Sicherheitstechnik ist laut Störfallverordnung „der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zur Verhinderung von Störfällen oder zur Begrenzung ihrer Auswirkungen gesichert erscheinen lässt. Bei der Bestimmung des Standes der Sicherheitstechnik sind insbesondere vergleichbare Verfahren, Einrichtungen oder Betriebsweisen heranzuziehen, die mit Erfolg im Betrieb erprobt worden sind."

Grundlage der Sicherheitsbetrachtung sind die anerkannten Regeln der Technik. Da der Stand der Sicherheitstechnik den anerkannten Regeln der Technik vorauseilt, sind die Abweichungen im Einzelfall zu diskutieren.

Normen sind immer nur richtungweisend. Andere Wege zur Erreichung des Schutzziels sind ebenfalls zulässig. Im Schadensfall muss jedoch deren Gleichwertigkeit nachgewiesen werden. Bei Lösungsansätzen außerhalb von Normen ist in jedem Fall der Planer bzw. das Planungsteam persönlich haftbar für eventuelle Schäden.

Werden Normen angewendet, so haben anwendungsspezifische Normen Vorrang vor Grundnormen. So muss zum Beispiel bei der Beurteilung

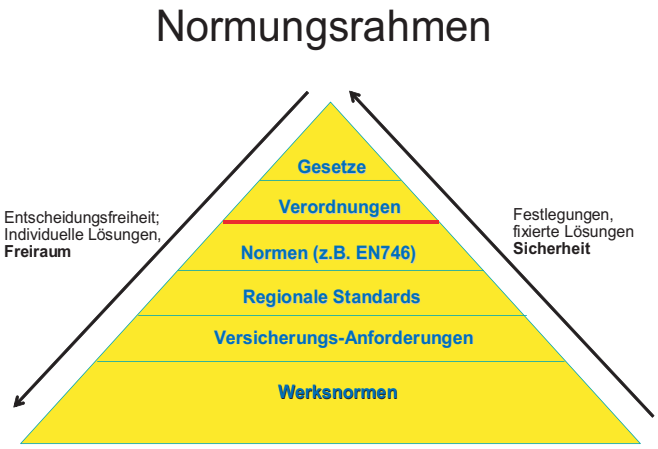

Bild 1: Normungsrahmen.

von Schutzeinrichtungen an Prozessöfen der petrochemischen Industrie die Norm EN 746-2 in Verbindung mit der Norm DIN EN 50156 „Elektrische Ausrüstung von Feuerungsanlagen" beachtet werden. Aus dem nachfolgenden Bild 2 „Normenaufbau" ist dies ersichtlich. Weiterhin zeigt Bild 3 die Zuordnung anwendungsspezifischer Normen zu den einzelnen Funktionseinheiten am Beispiel einer Raffinerie.

Bild 2: Normenaufbau.

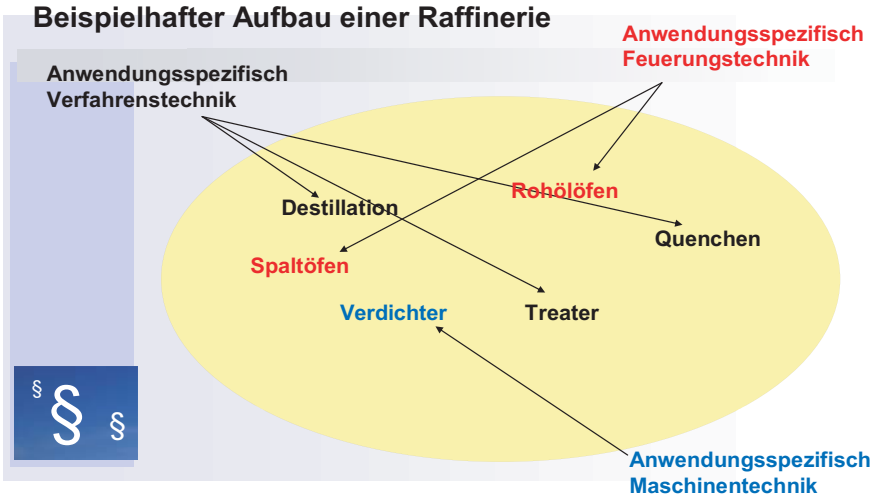

Bild 3: Zuordnung anwendungsspefizischer Normen.

Grundsätzlich beruht Anlagensicherheit auf drei Säulen:
- dem Sicherheitsmanagement
- den technischen Anforderungen
- der Qualifikation der Mitarbeiter.

Im Folgenden werden zunächst die technischen Anforderungen an eine Schutzeinrichtung behandelt.

3. Allgemeine Grundsätze

Unterteilt man eine Schutzeinrichtung in die Teileinheiten Sensor – Steuerung – Aktor so gelten neben den gerätespezifischen Besonderheiten folgende allgemeine Zusammenhänge (eine sehr gute, praxisnahe Beschreibung findet sich in [1]:

Nach einer vielzitierten Untersuchung der HSE (Health and Safety Executive, UK) sind die häufigsten Ursachen für das Versagen von Schutzeinrichtungen im organisatorischen Bereich zu finden. So werden zum Beispiel Planungsfehler, falsche Wartung oder Fehler nach Änderungen an wichtiger Stelle genannt. Aus diesem Grund stellt die DIN EN 61511 den sogenannten„Sicherheitslebenszyklus" (Safety Lifecycle) (Bild 4) in den Mittelpunkt.

Die Implementierung einer Schutzeinrichtung erfordert als ersten Schritt eine klare Spezifikation, die sowohl die geforderte Funktionalität beschreibt als auch deren Qualität (SIL). Beispiel: „ Bei einem Druck von über ... bar in Behälter … schließt Ventil … innerhalb von … Sekunden mit einer höchstzulässigen Restleckagemenge von … Rohrleitung … ab, Risikoabdeckung SIL 2". Ergänzend zu diesem Schutzziel ergeben Maßnahmen zur ordnungsgemäßen Planung und Auslegung, Implementierung, Inbetriebnahme, Verhalten während des Betriebes sowie Anforderungen an die Wartung und das Vorgehen bei Änderungen eine umfassende Handlungsanweisung für die Schutzeinrichtung.

Die Norm stellt drei grundsätzliche Forderungen:
- Systematische Fehler vermeiden
- Rate zufälliger Fehler bestimmen
- Architekturanforderung erfüllen

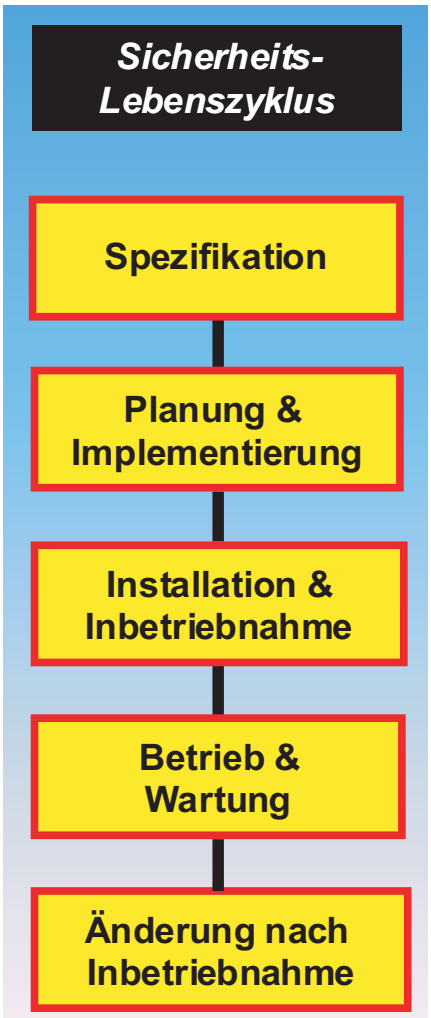

Bild 4: Vereinfachter Sicherheitslebenszyklus.

Zum Verständnis der aus diesen drei Punkten abzuleitenden Anforderungen an die Teilsysteme der Schutzeinrichtung ist es notwendig, die Einsatzbedingungen zu betrachten. Per Definition werden in DIN EN 61511 „elektrische, elektronische und programmierbare elektronische Systeme betrachtet". Sind diese Systeme, wie zum Beispiel im Falle der Steuerung meistens gegeben, in definierter Umgebung (bezogen auf Temperatur, Feuchte, Vibration, korrosive Atmosphäre, verschmutzte Atmosphäre) untergebracht, greift ein sehr schematisches und detailliert beschriebenes Vorgehen, um zufällige und systematische Fehler zu beherrschen. Die Gewichte der einzelnen Maßnahmen verschieben sich jedoch entscheidend, wenn
- Komponenten betrachtet werden, die den Prozessmedien und/oder aggressiven Umgebungsbedingungen ausgesetzt sind
- es sich um mechanische Systeme handelt, da deren Ausfallmechanismen und deren Diagnosefähigkeit grundsätzlich verschieden sind von elektronischen Systemen.

Der Anwender ist verantwortlich für den bestimmungsgemäßen Gebrauch. Bei Medienberührung ist es wichtig, sich nicht alleine auf eine generelle Fehleranalyse oder eine Datenbank zu verlassen, sondern zusätzlich die Eignung gezielt für den jeweiligen Prozess festzustellen. Deshalb ist gerade für diesen Fall der Betriebsbewährung eine große Bedeutung beizumessen. In [1] wird ausgeführt: „Von einem „blinden" Einsatz neuer, auch zertifizierter Geräte ohne Betriebsbewährung ist abzuraten!"

Wesentliche Elemente einer konformen Implementierung einer Schutzeinrichtung sind:
- Genaue Spezifikation der notwendigen Funktionalität: So lässt zum Beispiel die Beschreibung „Ventil muss schließen" noch die Leckagerate offen. Einige Prozent Leckage sind für das Abschalten eines Wärmetauschers völlig unproblematisch, die Sicherheit der Anlage wäre gegeben. Soll der Austritt eines toxischen Gases gegen Atmosphäre verhindert werden, so ist aber eine Leckage im ppm-Bereich zu fordern.
- Wiederholungsprüfungen: Zur Aufdeckung gefährlicher unerkannter Fehler sind sie unabdingbarer Bestandteil des Gesamtsicherheitskonzeptes. Hier sind Prüfintervall und -verfahren festzulegen. Der Fehleraufdeckungsgrad

ist durch eine entsprechende Analyse festzustellen, ein hoher Automatisierungsgrad ist wünschenswert.

- Diagnose: Ergänzend zur wiederkehrenden Prüfung ist ein hoher Grad an Diagnose wünschenswert. Diagnose bedeutet die automatisierte Aufdeckung von Fehlern im laufenden Prozess. Im Gegensatz dazu verlangt die wiederkehrende Prüfung in der Regel ein Abschalten der Anlage, oft sind auch aufwändige Architekturmaßnahmen wie zum Beispiel ein Bypass einer Armatur notwendig. Ein gutes Beispiel für Diagnose ist die Diskrepanzüberwachung bei Drucktransmittern.
- Betriebsbewährung: Um systematische Fehler auszuschließen sind entsprechend DIN EN 61511 zwei Möglichkeiten gegeben: Entweder wird die Entwicklung des fraglichen Gerätes entsprechend den Vorgaben der DIN EN 61508 durchgeführt oder es wird dessen Betriebsbewährung nachgewiesen. Die Anforderungen für „Betriebsbewährung" sind allerdings nicht detailliert formuliert, hier wird eine für Mitte 2008 geplante NAMUR Empfehlung klare Hinweise geben. In jedem Fall beinhaltet Betriebsbewährung den Einsatz der Geräte im Prozess, es werden also alle Einflüsse von Umgebung und Prozess mit aufgenommen. Ausdrücklich ist es auch gestattet, die Erfahrungen des Einsatzes in nicht sicherheitsgerichteten Kreisen mit zu berücksichtigen, vorausgesetzt die betrieblichen Bedingungen sind gleich. Geräte, die betriebsbewährt sind, werden in Tabelle 6 der DIN EN 61511-1 mit einer um eins verbesserten HFT bewertet. Damit kann eine SIL 2 Schutzeinrichtung mit betriebsbewährten Geräten einkanalig aufgebaut werden, alternativ ist eine Bescheinigung entsprechend DIN EN 61508 erforderlich.
- Dokumentation: Alle Schritte des Safety Lifecycle sind zu dokumentieren. Dies gilt insbesondere auch für die Wiederholungsprüfung. Die Dokumentation dieses Schrittes sollte auch den Zustand der Schutzeinrichtung vor der Wiederholungsprüfung beschreiben. Aus diesen Daten kann jeder Betreiber eine für seinen individuellen Prozess gültige Störstatistik aufbauen. Bei Verwendung externer Datenbanken ist auf Vergleichbarkeit der Betriebsbedingungen zu achten.
- Fehlerbetrachtung: Die Forderung nach zusätzlicher Erfüllung einer bestimmten HFT wird in DIN EN 61511-1 (11.4.1, Anmerkung 2) mit der begrenzten Genauigkeit sicherheitstechnischer Kenngrößen begründet. Fehlerrechnung ist grundlegendes Instrument der mathematischen Betrachtung eines naturwissenschaftlichen oder technischen Zusammenhanges, diese Methodik wird aber bei der Berechnung zufälliger Fehler nach DIN EN 61511 bisher nicht angewendet. Literaturhinweise, dass die verwendeten Zahlen mehr als eine Zehnerpotenz Ungenauigkeit aufweisen können [2], erscheinen dem in Instrumentierungspraxis Erfahrenen durchaus plausibel. Bisher weist leider keines der im Markt befindlichen „SIL" Berechnungstools eine Möglichkeit zur Fehlerbetrachtung auf.
- Verfügbarkeit und Quellen sicherheitstechnischer Kenngrößen: Es empfiehlt sich, schon bei der Geräteauswahl die Verfügbarkeit der sicherheitstechnischen Kenngrößen zu überprüfen. Einige Hersteller stellen diese Daten im Internet zur Verfügung.

Bild 5: Beispiele für Sensoranschlüsse unter Prozesseinfluss.

3. Aktorik/Sensorik

3.1 Unterschiede Feldgeräte/ Schaltschrankgeräte

DIN EN 61511 unterscheidet an vielen Stellen zwischen Logiksystemen (Schaltschrankgeräten) und Sensoren bzw. Aktoren (Feldgeräten). Letztere sind im Feld montiert und dadurch sowohl den Umgebungsbedingungen als auch den Prozessmedien ausgesetzt. Hieraus ergeben sich chemische und physikalische Belastungen, zum Beispiel durch Druck, Temperatur, Vibration und Feuchte. Prozessmedien wirken durch Korrosion, Kristallisation, Polymerisation, Abrasion, Ansatzbildung und andere Effekte auf die Feldgeräte ein (Bild 5). Beim Einsatz von Aktoren spielen zudem Strömungsgeschwindigkeiten und das Auftreten von Kavitation und Flashing eine bedeutende Rolle [3]. Da es sich bei den oben genannten Mechanismen um systematische Einflüsse handelt, müssen diese bereits bei der Anlagenplanung entsprechend berücksichtigt werden. Im Falle neuer Prozesse kann die Bewertung dieser Effekte schwierig sein. Dem kann durch besondere Maßnahmen, wie zum Beispiel verkürzte Prüfintervalle, Rechnung getragen werden.

3.2 Unterschiede Mechanik – Elektronik

Mechanische Komponenten sind bei Sensoren und noch stärker bei Aktoren wesentlicher Teil der Funktionskette. Scope und gedanklicher Hintergrund der DIN EN 61511 ist jedoch stark durch die Betrachtung elektronischer Systeme geprägt. Unterschiede zwischen mechanischen und elektronischen Systemen sind tabellarisch in Bild 6 dargestellt. Makroskopische Dimensionen, wie sie zum Beispiel bei Aktoren vorherrschend sind, ergeben eine bessere Prüfbarkeit. Dieser Sachverhalt und die geringe Teilezahl legen die Folgerung nahe, dass statistische Fehler im Rahmen der geforderten Genauigkeit wenig oder gar nicht relevant sind, entsprechend ist in vielen Fällen ein Fehlerausschluss zulässig, der

Elektronisches System	Mechanisches System
• Vielzahl von Bauteilen	• Begrenzte Anzahl von Bauteilen
• Funktionalität der Halbleiter in mikroskopischen Dimensionen	• Makroskopische Dimensionen
• Alterungsmechanismus über Diffusionsprozesse - Arrheniusgleichung	• Keine statistischen Ausfälle, aber Verschleiß
• Begrenzte Prüftiefe gehäuster Bauteile	• Hohe Prüftiefe in Fertigung und im Einsatz
	• Das Ventil muss auf den Einsatzfall ausgelegt werden

Bild 6: Unterschiede zwischen mechanischen und elektronischen Systemen.

allerdings begründet sein muss. Dagegen sind systematische Fehler von großer Bedeutung, sie sind durch systematisches, ingenieurmäßiges Vorgehen auszuschließen. Neben einem ordnungsgemäßen Entwurf und kontrollierter, spezifikationsgerechter Fertigung spielt die Berücksichtigung der Einsatzbedingungen eine entscheidende Rolle.

3.3 Verantwortung Hersteller – Anwender

Entsprechend können die vom Hersteller zur Verfügung gestellten sicherheitstechnischen Kenngrößen nicht alleine die Grundlage der Sicherheitsbetrachtung sein. Trotz aller Sorgfalt bei der sicherheitstechnischen Bewertung der Sensoren oder Aktoren durch die Hersteller, bleibt diese letztendlich auf die Gerätetechnik begrenzt. Bei einem Drucktransmitter wird die Bewertung beispielsweise von der Prozessmembran bis zum Klemmenblock durchgeführt (Elektronik und Mechanik). Die Ergebnisse dieser Betrachtung stellen die Gerätehersteller zur Verfügung. Dies ist aber insbesondere bei kritischen Prozessen bei weitem nicht ausreichend.

Eine Schutzeinrichtung kann nur dann bestimmungsgemäß arbeiten, wenn die Herstellervorschriften zur Installation, Inbetriebnahme, Bedienung, Wartung usw. beachtet werden und insbesondere die Einflüsse des spezifischen Prozesses und der jeweiligen Umgebung berücksichtigt werden. Auch hier also wieder der Hinweis, dass sich Anlagensicherheit nur mit begründetem ingenieurmäßigem Vorgehen und in Zusammenarbeit von Anwender mit dem Gerätehersteller erreichen lässt.

3.4 Ausschluss systematischer Fehler

Es ist empfehlenswert, den Ausschluss systematischer Fehler durch die Anfertigung eines PLT- Stellenblattes für jeden eingesetzten Sensor oder Aktor zu verifizieren. Weiterhin sind neben den Einzelkomponenten auch die Schnittstellen zu betrachten, also mechanischer Anbau, Kraftübertragung, elektrischer Anschluss mit Kabel und Klemmen, pneumatischer Anschluss mit Rohrleitungen und Fittings, auch wenn diese Elemente in der DIN EN 61511 nicht oder nur knapp beschrieben sind. Insgesamt erfordert eine vollständige Analyse aller möglichen Betriebszustände eine umfangreiche Betrachtung, hier sei auf die für 2008 geplante Veröffentlichung des Blattes 5 zur VDI 2180 verwiesen.

3.5 Safety Manual

Der Hersteller stellt alle sicherheitsrelevanten Informationen in Form eines Safety-Manuals zur Verfügung. Der Anwender muss diese Hinweise vollständig berücksichtigen. Dieses Manual enthält Informationen für den sicheren Geräteeinsatz, wie zum Beispiel:

- Anwendungsbereich in Schutzeinrichtungen
- Zulässige Geräteausführungen und Versionen (Hardware, Software/ Firmware)
- Einschränkungen für den sicheren Betrieb
- Sicherheitstechnische Kenngrößen
- Hinweise zur Parametrierung und Konfiguration
- Geräteverhalten im Betrieb und bei Störung
- Vorgehensweise bei der Wiederholungsprüfung

3.6 Redundanz

In der Praxis kann es etwa aus Gründen der sicherheitstechnischen Verfügbarkeit vorteilhaft sein, Sensoren oder Aktoren in Schutzeinrichtungen redundant einzusetzen.

Aufbaumöglichkeiten für redundante Teilsysteme von Sicherheitsfunktionen sind:

- Homogen redundanter Aufbau (identische Sensoren): Vorteil ist eine höhere Verfügbarkeit der Schutzeinrichtung (zum Beispiel bei Auswahlschaltung 1oo2), sowie vereinfachte Lagerhaltung und vereinfachte Inbetriebnahme und Wartung. Grenzen bestehen in möglichen Einschränkungen bei der Beherrschung systematischer Fehler während des Betriebes.
- Diversitär redundanter Aufbau (verschiedene Messverfahren oder gleiches Messverfahren mit unterschiedlichen Geräten): Neben der höheren Verfügbarkeit der Schutzeinrichtung (zum Beispiel bei Auswahlschaltung 1oo2) ist hier die Beherrschung systematischer Fehler besser realisierbar. Damit wird die Wahrscheinlichkeit des gleichzeitigen Ausfalls mehrerer Kanäle reduziert.

Beispiele für diversitär redundante Teilsysteme:

- Zwei Drucktransmitter unterschiedlicher Baureihen oder unterschiedlicher Hersteller.
- Zwei unterschiedliche Geräte mit unterschiedlichen Messprinzipien für die gleiche physikalische Größe, zum Beispiel Differenzdrucktransmitter und frei abstrahlendes Radarmessgerät für Füllstandsmessung
- Zwei unterschiedliche Geräte für verschiedene physikalische Größen, zum Beispiel Drucktransmitter und Temperaturtransmitter. Voraussetzung: Druck und Temperatur sind Prozesssicherungsgrößen.
- redundantes Absperren einer Rohrleitung durch Hubventil und Kugelhahn

3.7 Sichere Parametrierung

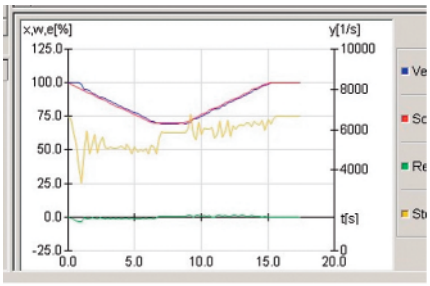

Bild 7: Diagnosefähiger Stellungsregler, Aufzeichnung Teilhubtest.

Werden die Geräte eines Sicherheitskreises falsch parametriert, kann die Schutzeinrichtung gegebenenfalls ihre Aufgabe nicht erfüllen. Hier setzt die sichere Geräteparametrierung an. Sensoren mit dieser Funktion verhindern Bedienungs- und Eingabefehler. Durch Validierung der Eingaben im Gerät ist die sichere Parametrierung unabhängig vom verwendeten Parametriertool. Das Konzept beruht auf der Auswahl sinnvoller Grundeinstellwerte und Bereichsüberprüfungen für festgelegte Geräteparameter. Die Zahl der frei editierbaren Parameter wird auf ein Mindestmaß reduziert. Nach Validierung der Parameteranzeige werden diese Eingaben nochmals verifiziert. Die Aktivierung der sicheren Parametrierung erfolgt in einer menügeführten Prozedur über ein Passwort. Den Abschluss bildet die Geräteverriegelung. So ist sicher gestellt, dass die Konfiguration und Parametrierung nicht versehentlich geändert werden.

3.8 Wiederholungsprüfung

Schutzeinrichtungen müssen regelmäßig geprüft werden. Das Zeitintervall dieser Wiederholungsprüfungen ergibt sich aus der SIL-Verifikation (rechnerischer Nachweis). Die Prüfung dient zur Aufdeckung gefährlicher unerkannter Fehler. Sie stellt unter Beweis, dass die Komponenten noch den Anforderungen entsprechen.

Grundlage der Wiederholungsprüfung ist die genaue Spezifikation der Anforderungen. Darauf aufbauend sind in der Prüfanweisung quantitativ die zu erfassenden Parameter mit Sollwerten und Fehlerbandbreiten festzulegen. Ferner ist der Anteil der aufdeckbaren Ausfälle zu ermitteln (Proof Test Coverage), ein zu niedriger Wert der Proof Test Coverage kann die Einhaltung des geforderten SIL gefährden. So kann zum Beispiel im Bereich der Aktorik das bisher übliche, rein visuelle Beobachten des Schließvorganges der Armatur vorteilhaft durch genaue Messung von Schließzeit, Endlage, Dichtigkeit etc. ergänzt werden. Diese Messung wie auch die notwendige Dokumentation kann durch moderne Instrumentierung geleistet und eventuell auch automatisiert werden [4, 5]. Das Ergebnis der Wiederholungsprüfung (insbesondere der vorgefundene Zustand) ist zu dokumentieren. Ergänzende Inspektionen im laufenden Betrieb sind zu empfehlen. Damit können zum Beispiel Korrosion, Vibrationen, Geräuschentwicklung, erkennbare Leckagen gegen Atmosphäre und Ähnliches frühzeitig erkannt werden.

Das derzeit in der Aktorik Anwendung findende Verfahren des Teilhubtestes (Partial Stroke Test) im laufenden Betrieb lässt sich entsprechend obigen Ausführungen als Teil eines Gesamtkonzeptes für die Wiederholungsprüfungen und Diagnoseverfahren interpretieren. Eine detaillierte Darstellung findet sich in [4; 5]. Dieses Verfahren kann inzwischen als Stand der Technik angesehen werden. Es verringert den Anteil der gefährlichen, unerkannten Fehler des eingesetzten Aktors. Der Gewinn an Sicherheitsmarge kann zu einer Verlängerung des Intervalls der Wiederholungsprüfung führen, bei günstigen Parametern ist etwa ein Faktor zwei realistisch. Wie stets ist hier aber der Einzelfall zu überprüfen. Wie jede Diagnose wirkt dieses Verfahren in erster Linie in Richtung eines verbesserten PFD-Wertes. Eine Veränderung der Anforderung an den Redundanzgrad (HFT – Hardware fault tolerance) ist gemäß DIN EN 61511 nicht möglich. Bild 7 zeigt beispielhaft einen modernen, diagnosefähigen Stellungsregler und die Aufzeichnung eines Teilhubtestes.

4. Steuerung

Üblicherweise werden in Schutzeinrichtungen Logiksysteme mit Zertifizierung entsprechend DIN EN 61508 eingesetzt.

Bei der Systemauswahl sind folgende Punkte zu berücksichtigen:

- Benötigte E/A-Arten (zum Beispiel Intitiatoreingänge, Leitungsüberwachung, Anforderungen an Explosionsschutz)
- Online-Erweiterbarkeiten (Software, Hardware).
- SIL-konforme Kommunikation zwischen verteilten Systemen.
- Benötigte Sicherheits-/Reaktions-Zeiten (kann das System den Prozess schnell genug in den sicheren Zustand bringen).

Beim Vergleich der sicherheitstechnischen Kenngrößen ist darauf zu achten, ob die Zahlen nach DIN EN 61508 oder nach ANSI/ISA TR84.0.02 ermittelt wurden, da sich unterschiedliche Werte ergeben.

Mindestanforderungen an das Programmiertool sind:

1. Exakte, eindeutige und nicht-manipulierbare Kennung der Version des Programmes und der verwendeten Bausteine
2. Änderungsmanagement durch zertifizierten Revisionsvergleicher.

Mindestanforderungen an das Anwenderprogramm sind:

1. Vorschriften für die Erstellung
2. Konsequenter Einsatz von vorab validierten und/oder zertifizierten Standardbausteinen

Die Beachtung dieser Punkte führt zu übersichtlicher Programmierung und erleichtert die Inbetriebnahme, Pflege und Wartung der Anlage, insbesondere wenn mehrere Lieferanten an der Erstellung beteiligt sind.

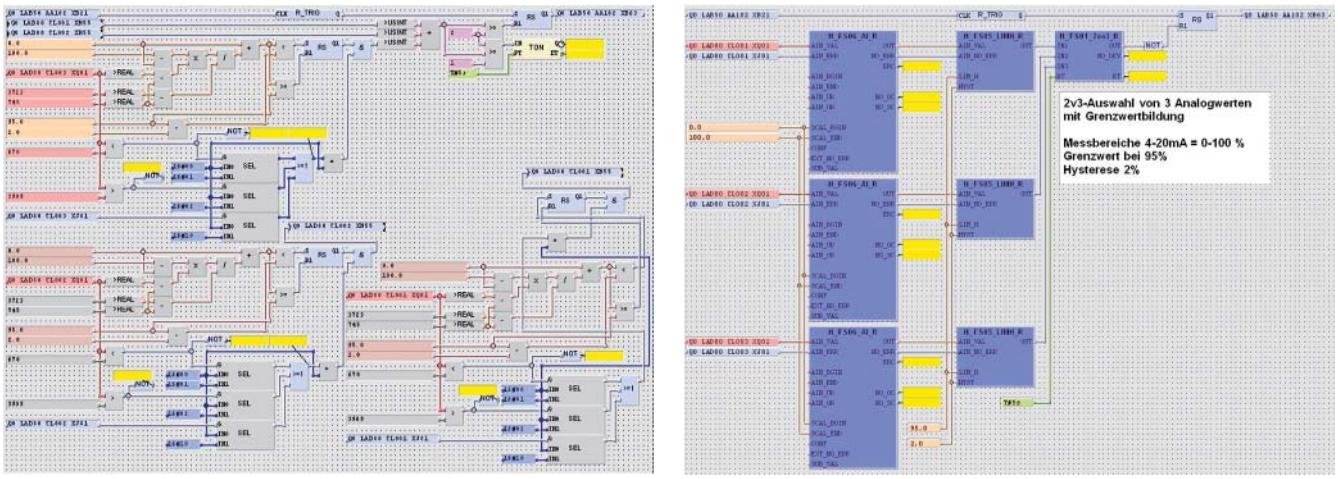

Bild 8: Programmbeispiel, rechts: Konventionelle Codierung; links: Verwendung von Standardblöcken.

Die Vorschrift zur Erstellung des Anwenderprogramms sollte Folgendes berücksichtigen:

a) Projektstruktur (zum Beispiel: Bibliotheken, Steuerungen)
b) Namenskonventionen sowohl für Variablen als auch für Bausteine
c) Vollständige Definition der einzustellenden Programm-/Sicherheitsparameter
d) Logik-Typicals: Standardisierung und Definition gleicher logischer Abläufe
e) Dokumentation: Wie ist das Projekt zu dokumentieren

Das Anwenderprogramm soll modular mit immer wieder verwendeten Funktionen und Funktionsbausteinen aufgebaut sein ([7], Blatt 3). Dies dient zur Minimierung des Wartungs- und Prüfaufwandes. Bild 8 zeigt anhand eines Beispiels eine „diskret" aufgebaute Logik und zum Vergleich dieselbe Logik zusammengeschaltet aus Standardbausteinen.

Standardbausteine werden üblicherweise für folgende Funktionen eingesetzt:

- E/A-Aufbereitung, zum Beispiel Voting bei 1oo2, 2oo3, 2oo2-Architekturen, Analogeingangsüberwachung, Skalierungs-/Korrekturbausteine
- Diagnosefunktionen, zum Beispiel Online-Driftdiagnosen, Diskrepanzüberwachungen und Bereichsüberwachungen
- Wartungsschalter für Aktor/Sensortests
- Partial Stroke Test

Bei der Erstellung von Standardbausteinen ist die Verwendung zumindest eines vereinfachten V-Modells gemäß DIN EN 61511 empfehlenswert. Es beschreibt den kompletten Software-Entwicklungsprozess von der Spezifikation bis zur abschließenden Validierung. Die einzelnen Prozessschritte sind in Bild 9 dargestellt.

Die Validierung kann durch die erstellende Firma oder durch eine externe Organisation erfolgen.

Durchgängig ist zu beachten:

1. Lückenlose Dokumentation aller im V-Modell erwähnten Schritte (Anforderungs- und Testspezifikation, Testberichte, Bausteindokumentation etc.)
2. 4-Augen-Prinzip als organisatorische Anforderung, zum Beispiel unterschiedliche Personen für Testspezifikation und Testdurchführung

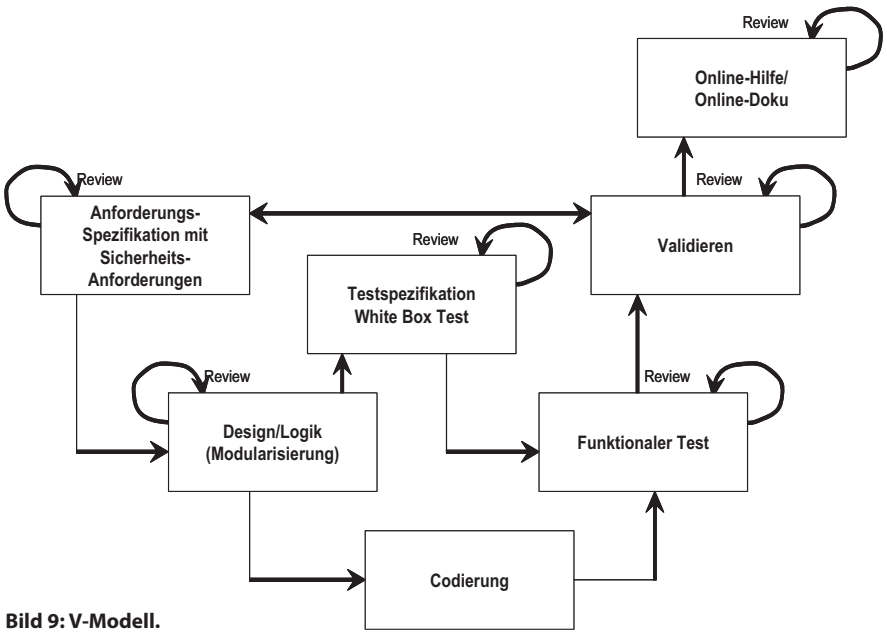

Bild 9: V-Modell.

5. Bewertung von Sicherheitskreisen

Aus DIN EN 61511 folgt, dass Maßnahmen zur

- Fehlervermeidung,
- Fehlerbeherrschung und
- Fehlererkennung

in Abhängigkeit des zu erreichenden SIL implementiert werden müssen. Für jede Sicherheitsfunktion ist somit eine Bewertung bezüglich der Architektur (HFT) und der Ausfallwahrscheinlichkeit (PFD) durchzuführen.

6. Architekturforderung

Entsprechend DIN EN 61511-1, Tabelle 6 (siehe Bild 10), kann bei Feldgeräten bis SIL 2 einkanalig instrumentiert werden, SIL 3 erfordert redundanten Aufbau.

Mindest-Hardware-Fehlertoleranz von Sensoren, Aktoren und nichtprogrammierbaren Logiksysstemen.	
SIL	**Mindest-Hardware-Fehlertoleranz (siehe 11.4.3 und 11.4.4)**
1	0
2	1
3	2
4	Es gelten besondere Anforderungen. Siehe IEC 61508

Bild 10: DIN EN 61511-1, Tabelle 6, Architekturforderung.

6.1 Ausfallwahrscheinlichkeit

Die Ausfallwahrscheinlichkeit (PFD) muss berechnet werden und dem geforderten SIL entsprechend DIN EN 61511-1, Tabelle 3, genügen. Die Berechnung der PFD kann mit Hilfe von Formeln erfolgen, welche in DIN EN 61508-6 und in Blatt 4 der VDI 2180 [7] zu finden sind. Bei den Formeln der VDI/VDE 2180 handelt es sich um Näherungsformeln, die nur unter den dort aufgeführten Randbedingungen angewendet werden dürfen. Die Grundstrukturen sind damit einfach zu berechnen. Bei gemischten Strukturen (zum Beispiel Sensorkreis redundant, Aktorkreis einkanalig) müssen die Systeme Schritt für Schritt auf bekannte Grundstrukturen zurückgeführt werden.

6.2 PFD – Berechnungsbeispiel

Die in Bild 11 gezeigte Struktur wird schrittweise vereinfacht. Hierzu werden zunächst alle in Reihe liegenden Blöcke durch Addition der PFD- bzw. Lambda-Werte zusammengefasst. Man erhält dann die im Bild 12 gezeigte, vereinfachte Struktur. Anschließend wird das diversitär redundante Sensorteilsystem zu einem Block zusammengefasst, indem die PFD dieses Teilsystems mit Hilfe der Formel für ein 1oo2-System berechnet wird. Hierbei ist zu beachten, dass die Formeln aus den o. g. Quellen nur für homogene Systeme gelten. Für diversitäre Systeme empfiehlt sich eine Worst-Case Abschätzung unter Verwendung der Daten des Kanals mit den höheren Ausfallraten. Hat man das System so weit vereinfacht, muss abschließend lediglich die Summe der PFD – Werte gebildet werden (Bild 13). Das Endergebnis wird dann mit Hilfe der DIN EN 61511-1, Tabelle 3, einem SIL zugeordnet.

6.3 SIL-Nachweis im Überblick

Die technischen Anforderungen zur Bewertung einer sicherheitstechnischen Einrichtung können wie folgt zusammengefasst werden:

1. Prüfen, ob alle eingesetzten Geräte für den geforderten SIL geeignet sind (Herstellererklärung).
2. Wenn „Ja", PFD - Berechnung durchführen und das Ergebnis mit Hilfe der DIN EN 61511-1, Tabelle 3, bewerten.
3. Falls Punkt 1 nicht erfüllt wird, Redundanz vorsehen. In Bezug auf die Strukturanforderung gilt, dass durch Vergrößern der Hardware Fehlertoleranz der nächsthöhere SIL erreicht werden kann. Es ist jedoch zu beachten, dass bei Einsatz gleicher Geräte, die Software enthalten, diese für den höheren SIL geeignet sein muss.
4. Falls Punkt 2 nicht erfüllt wird, kann entweder durch Verkürzen des Intervalls der Wiederholungsprüfung oder durch Redundanz eine kleinere PFD erreicht werden. Liegt bereits eine redundante Struktur vor, so kann evtl. auch eine Reduzierung der „Fehler mit gemeinsamer Ursache" eine Verbesserung der PFD bewirken.
5. Alle Betrachtungen bzw. Berechnungen gemäß den Punkten 1 bis 4 sind entsprechend den Forderungen des QM-Systems nach DIN EN 61511 zu verifizieren (4-Augenprinzip) und zu dokumentieren. Eine Auditierung muss jederzeit möglich sein.

Der Einsatz von Softwarewerkzeugen kann das beschriebene Vorgehen unterstützen und die Dokumentation erleichtern.

7. Grenzen der SIL-Betrachtung

7.1 Managementsystem der funktionalen Sicherheit

Durch DIN EN 61511 ist jeder Betreiber von Prozessanlagen aufgefordert, ein Managementsystem der funktionalen Sicherheit einzuführen. Im einfachsten Fall orientiert sich der Betreiber an dieser Anforderung der Norm, die im Detail durch den Sicherheitslebenszyklus beschrieben sind.

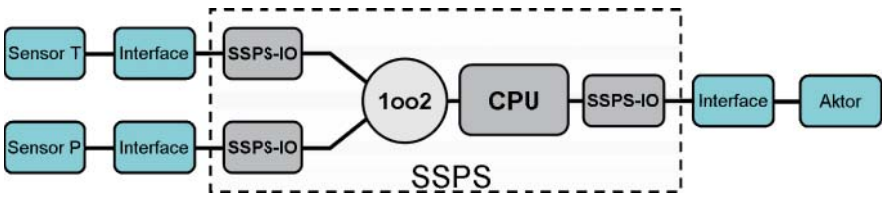

Bild 11: Sicherheitstechnisches System mit diversitär redundantem Sensorteil.

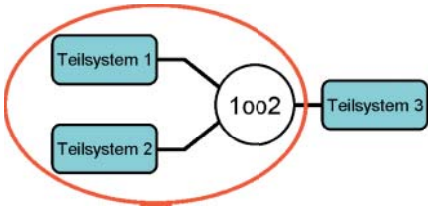

Bild 12: Vereinfachte Struktur. Die seriellen Zweige wurden zusammengefasst.

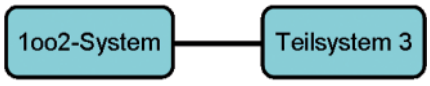

Bild 13: Vorletzter Schritt der Vereinfachung. Jetzt müssen nur noch die beiden PDF-Werte des 1oo2-Systems und des Teilsystems addiert werden.

1 Ziel / Zweck
2 Begriffe und Abkürzungen
3 Geltungsbereich
4 Organisation im Sicherheitslebenszyklus
- **4.1 Sicherheitsplan (Safety Lifecycle)**
- **4.2 Delegation der Verantwortung**
  - **4.2.1 Planungsteam**
  - **4.2.2 Beurteilungsteam**
- **4.3 Risikobetrachtung**
  - **4.3.1 Betrachtung der Risiken im Rahmen der HAZOP**
  - **4.3.2 Zuordnung des Geltungsbereiches der jeweiligen Norm**
  - **4.3.3 Einstufung der Sicherheitstechnischen Systeme (SIS)**
- **4.4 Erstellung des Lastenheftes**
- **4.5 Erstellung des Pflichtenheftes**
- **4.6 Implementierung der Software**
- **4.7 Verifizierung der Software**
- **4.8 Montage und Inbetriebnahme**
- **4.9 Validierung**
- **4.10 Betrieb und Instandhaltung**
- **4.11 Außerbetriebnahme**

5 Änderungsmanagement
6 Prüfungen im Sicherheitslebenszyklus
- **6.1 Zweck**
- **6.2 Durchzuführende Prüfungen**
  - **6.2.1 Prüfung des Lastenheftes**
  - **6.2.2 Prüfung des Pflichtenheftes**
  - **6.2.3 Verifizierung der Software**
  - **6.2.4 Überprüfung der ordnungsgemäßen Durchführung von Montage und Inbetriebnahme**
  - **6.2.5 Validierung**

Bild 14: Elemente eines Managementsystems.

In jedem Fall ist es erforderlich, ein Planungs- und ein getrenntes Beurteilungsteam zu benennen. Hierbei ist zu berücksichtigen:

Planungsteam
- Technisches Wissen bezogen auf
  - Verfahrenstechnik
  - verwendete Technologien
  - verwendete Technik
- Sicherheitstechnisches Wissen bezogen auf
  - Kenntnis der Gesetze, Normen und Richtlinien
  - Stand der Sicherheitstechnik

Beurteilungsteam
- Festlegung, welche anderen Sicherheits-Fachgruppen bei der Beurteilung mitwirken sollen;
- Festlegung, welche Mittel erforderlich sind, um die Beurteilung vollständig durchführen zu können
- Unabhängigkeit vom Planungsteam

Planungs- und Beurteilungsteam müssen aus voneinander unabhängigen Personen bestehen, das sogenannte 4-Augen-Prinzip muss durchgängig eingehalten werden.

Bild 14 zeigt beispielhaft eine mögliche Gliederung für ein Managementsystem.

7.2 Qualifikation von Mitarbeitern

Zwingend erforderlich im Hinblick auf einen hohen kontinuierlichen Qualitätsstandard ist die Weiterbildung der Mitarbeiter sowie ein regelmäßiger Erfahrungsaustausch. Der Einsatz gleicher Mitarbeiter für vergleichbare Aufgaben ist sinnvoll, um von vorhandenen Erfahrungen zu profitieren.

Nicht zu vernachlässigen sind jedoch auch die so genannten „weichen Faktoren". Wesentlich ist:
- Wie fördere ich die Qualität von Mitarbeitern?
- Werden regelmäßig Weiterbildungsmaßnahmen initiiert?
- Wie hoch ist die Mitarbeiterzufriedenheit?
- Wie ist es um das Betriebsklima bestellt?
- Gibt es Probleme bei der Personalbeschaffung?

Nur unter Berücksichtigung der drei Säulen Managementsystem, technische Anforderungen und Qualifikation des Personals kann die optimale Risikoreduzierung mit Hilfe von PLT-Schutzeinrichtungen erreicht werden. Jedoch sind selbst bei Beachtung dieser Kriterien Grenzen in der Auslegung von Schutzkreisen vorhanden.

7.3 Berechnung von Schutzkreisen

Bei der PFD-Berechnung von Schutzkreisen sind insbesondere folgende Punkte zu beachten:
- Welche Datenbasis liegt der Berechnung zugrunde?
- Wie wurden die Daten gewonnen?
- Sind generische Werte aus einer gegebenen Quelle wirklich übertragbar?
- Welche Auflagen sind mit dem Einsatz verbunden?

Was nützen generische Werte, die im Reinraum gewonnen wurden, für eine Schutzkreisberechnung im rauen Raffinerieeinsatz?

Was nützen Schutzkreise, die täglich getestet werden müssen, um zum Beispiel ein SIL 3 Risiko absichern zu können?

7.4 Nachweis der erforderlichen Qualifikation

Geräte können nach [7]wie folgt zum Einsatz in Schutzeinrichtungen qualifiziert werden:
SIL-Nachweis nach DIN EN 61508 (IEC 61508)
- Nachweis der Betriebsbewährung (Proven in use) durch Hersteller oder Betreiber
- Eignungsnachweis durch Baumusterprüfung [8] oder
- Einzelprüfung [8]

7.5 Aufbautechnik

Zusätzlich zu Eignungsnachweisen der Geräte sind zum Beispiel noch folgende Punkte zu bedenken:

- Sind die Prozessanschlüsse ausreichend groß, gegen Verlegen durch Produkt gesichert?
- Wurde in der Verdrahtung das Ruhestromprinzip eingehalten?
- Werden Kurzschluss und Unterbrechung in den Signalleitungen erkannt?

Für diese Punkte gibt es keine Rechenwerte, hier ist der Sachverstand des Planungsteams gefragt. Entsprechende Überlegungen und Entscheidungen sollten dokumentiert werden.

Zusammenfassung

Zusammenfassend lässt sich feststellen, dass sich Anlagensicherheit durch die – im Wesentlichen vertrauten – Elemente erreichen lässt:

- Management: Erstellung eines Sicherheitsmanagement-Systems
- Technologie: Beachtung der einschlägigen Regeln der Technik bei Auswahl und Einsatz der notwendigen Geräte und Systeme sind wichtige Grundlagen der Anlagensicherheit
- Bevorzugte Verwendung zertifizierter oder betriebsbewährter Komponenten für Schutzeinrichtungen
- Standardisierung: möglichst weitgehende Standardisierung bei Hardware und Software
- Mitarbeiter: Einsatz qualifizierter Mitarbeiter

Literatur

[1] *Hablawetz, Dirk; Matalla, Norbert; Adam, Gerhard,* BASF AG: IEC 61511 in der Praxis – Erfahrungen eines Anlagenbetreibers, atp – Automatisierungstechnische Praxis 10.2007 S. 34 ff.

[2] *Smith, David J.:* Reliability, Maintainability and Risk, Elsevier Butterworth-Heinemann, Burlington, 2003.

[3] *Karte, Thomas; Nebel, Eugen; Dietz, Manfred; Essig, Helge:* Kennwerte und Einsatz von Ventilen in der Prozessindustrie entsprechend IEC 61508/61511, atp – Automatisierungstechnische Praxis 2.2005.

[4] *Karte, Thomas; Kiesbauer, Jörg:* Partial Stroke Testing For Final Elements, Proceedings of „Petroleum and Chemical Industry Conference (PCIC) Europe 2005", Basle, Switzerland.

[5] *Karte, Thomas; Schärtner, Karl-Bernd:* Partial Stroke Testing an Stellgeräten zur Verlängerung der Anlagenlaufzeit, atp – Automatisierungstechnische Praxis 4.2005.

[6] DIN EN 61511, Teil 1–3, Berlin 2005.

[7] VDI/VDE 2180, Blatt 1–4, Berlin 2007.

[8] Interne Mitteilung des VDI/VDE GMA 6.13 „Funktionale Sicherheit".

Manuskripteingang: 2.5.2008

Dr. *Arno Götz* (46) leitet die Abteilung Produktsicherheit und das Testcenter der Endress+Hauser GmbH+Co. KG, Maulburg. Seine Hauptarbeitsgebiete sind die funktionale Sicherheit und der Explosionsschutz. Daneben ist er Mitarbeiter im DKE GK 914.

Adresse: Endress+Hauser GmbH+Co. KG, Hauptstr. 1, D-79689 Maulburg, Tel. +49 7622 28-1645, E-Mail: arno.goetz@pcm.endress.com

Dr. *Andreas Hildebrandt* (48) ist seit 2006 Leiter der Gruppe „Schulung und Gremienarbeit" der Pepperl+Fuchs GmbH, Mannheim. Arbeitsschwerpunkte bilden unter anderem der Explosionsschutz und die funktionale Sicherheit. Daneben leitet er die ZVEI – Arbeitsgruppe „EMV" und ist Mitglied im DKE UK 921.3, im DKE K 767.0.4 und im FA 6.13 der Gesellschaft Mess- und Automatisierungstechnik (GMA) des VDI/VDE.

Adresse: Pepperl+Fuchs GmbH, Königsberger Allee 87, D-68307 Mannheim, Tel. +49 621 776 1454, E-Mail: ahildebrandt@de.pepperl-fuchs.com

Dr. T*homas Karte* (52) beschäftigt sich bei der SAMSON AG in Frankfurt mit der Anwendungstechnik elektropneumatischer Geräte. Er ist Mitglied im FA 6.13 der GMA - VDI/VDE und im DKE GK 914.

Adresse: SAMSON AG, Weismüllerstr. 3, D-60314 Frankfurt, Tel. +49 69 4009 2086, E-Mail: tkarte@samson.de

Dipl.-Ing. (FH) *Bernd Schäfer* (41) ist seit 1996 Mitarbeiter des Unternehmens HIMA. Zuerst im Engineering als Projektleiter tätig, kümmert er sich seit 2004 als Produktmanager um den Bereich OPC und SCADA, sowie um das Thema Asset Management und Sonderapplikationen wie Trainingssimulation.

Adresse: HIMA Paul Hildebrandt GmbH & Co KG, Abt. PM, Albert-Bassermann-Str. 28, D-68782 Brühl bei Mannheim, Tel. +49 6202 709-453, E-Mail: b.schaefer@hima.com

Dipl.Ing.(FH) *Johann Ströbl* (54) ist seit 1980 bei TÜV SÜD Industrie Service tätig. Er leitet derzeit die Abteilung Elektro- und Gebäudetechnik sowie die Außenstelle Feuerungs- und Wärmetechnik in der Niederlassung Regensburg. Hauptarbeitsgebiet: Bewertung von Schutzeinrichtungen in verfahrenstechnischen Anlagen, Bewertung von komplexen industriellen Thermoprozessanlagen.

Adresse: TÜV SÜD Industrie Service GmbH, Friedenstraße 6, D-93051 Regensburg, Tel. +49 941 9910-402, Fax: -470, Mobil: +49 160 3601202, E-Mail: johann.stroebl@tuev-sued.de