IEC 61511 in der Praxis

Erfahrungen eines Anlagenbetreibers

Dirk Hablawetz, Norbert Matalla und Gerhard Adam,
BASF Aktiengesellschaft, Ludwigshafen

Das Thema „Anlagensicherung mit Mitteln der Prozessleittechnik" ist für den Bereich der Prozessindustrie im deutschen Sprachraum innerhalb der letzten zwanzig Jahre in Normen (VDI/VDE 2180, DIN V 19250/19251) und Empfehlungen der NAMUR (beispielsweise die NE 31) geregelt worden. In allen größeren Firmen existieren auf dieser Basis bewährte Konzepte zur gerichtsfesten Umsetzung in die Praxis.
Auf internationaler Ebene wurde auf Basis der für die gesamte Industrie als Sicherheitsgrundnorm vorliegende und primär für die Geräteentwicklung geltenden IEC 61508 „Funktionale Sicherheit elektrischer/elektronischer/programmierbarer elektronischer sicherheits-bezogener Systeme" die IEC 61511 „Funktionale Sicherheit: Sicherheitstechnische Systeme für die Prozessindustrie" erarbeitet. Der Standard wurde international 2004 und national 2005 als DIN IEC 61511 (VDE 0810) verabschiedet. Seit ca. 3 Jahren stellt die IEC 61511 weltweit die „best-practice" für PLT-Schutzeinrichtungen dar. Grund genug, die Erfahrungen bei der Implementierung der Anforderungen des Standards in den betrieblichen Alltag aufzuzeigen.

Sicherheitstechnik / PLT-Schutzeinrichtungen / Sicherheitsintegrität / IEC 61511 / Risikoanalyse

Application of IEC 61511 – Experiences of an operational company
The topic „plant safety with means of the process instrumentation" was regulated for the process industry in Germany within the last twenty years in standards (e.g. VDI/VDE 2180, DIN V 19250/19251) and recommendations of the NAMUR (e.g. the NE 31). In all larger companies concepts exist for court-firm implamentation to the practice on this basis.
On international level based on the industry independent generic standard IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety related systems" (mainly used as a standard for the equipment development) the IEC 61511 „Safety-relevant systems for the process industry" was developed as sector specific approach. This standard was adopted internationally 2004 and national 2005 as DIN IEC 61511 (VDE 0810). For approx. 3 years the IEC 61511 represents world-wide the best-practice for Safety Insturmented Systems. Reason enough to point out the experiences with the implementation of the requirements of the standard into the operational everyday life.

Safety / Safety instrumented systems / Safety integrity / IEC 61511 / Risk analysis

Einleitung

Nachdem anfänglich vielerorts die Frage aufgeworfen wurde, wofür man eigentlich einen neuen Standard zum Thema Anlagensicherung braucht, hat sich die Akzeptanz dieses Standards inzwischen sehr positiv entwickelt. Obwohl es an der einen oder anderen Stelle in der IEC 61511 [1] noch Optimierungspotenzial gibt, hat es sich gezeigt, dass der ganzheitliche Ansatz und die Kombination von qualitativen und quantitativen Anforderungen zu einer optimalen Ausführung von PLT-Schutzeinrichtungen führt. Weiterhin hat die Beschäftigung mit der quantitativen Analyse von Schutzkreisen in manchen, insbesondere komplexeren Fällen, schon zu „Aha-Erlebnissen" geführt. Speziell für global agierende Unternehmen bietet auch die internationale Gültigkeit dieser Norm klare Vorteile beim Bau und Betrieb von Anlagen.

Die BASF begann bereits im Jahr 2001 ihre bestehende und bewährte Sicherheitsphilosophie RPI 10 [2] den Anforderungen der IEC 61511 anzupassen. Die Festlegung des Safety Integrity Level (SIL) sowie der quantitative Nachweis der sicherheitstechnisch notwendigen Verfügbarkeit einer PLT-Schutzeinrichtung standen dabei im Mittelpunkt. Eine weitere Herausforderung stellte die Überführung einer bisher nur in Europa verbindlichen BASF-Richtlinie in einen globalen, konzernweiten Standard für PLT-Schutzeinrichtungen dar [3].

Anforderungen an das Sicherheitsmanagement

Obwohl die rein technischen Anforderungen bei prozessleittechnischen Einrichtungen oftmals im Vordergrund stehen, stellen diese jedoch nur einen Aspekt der Sicherheit dar. Der

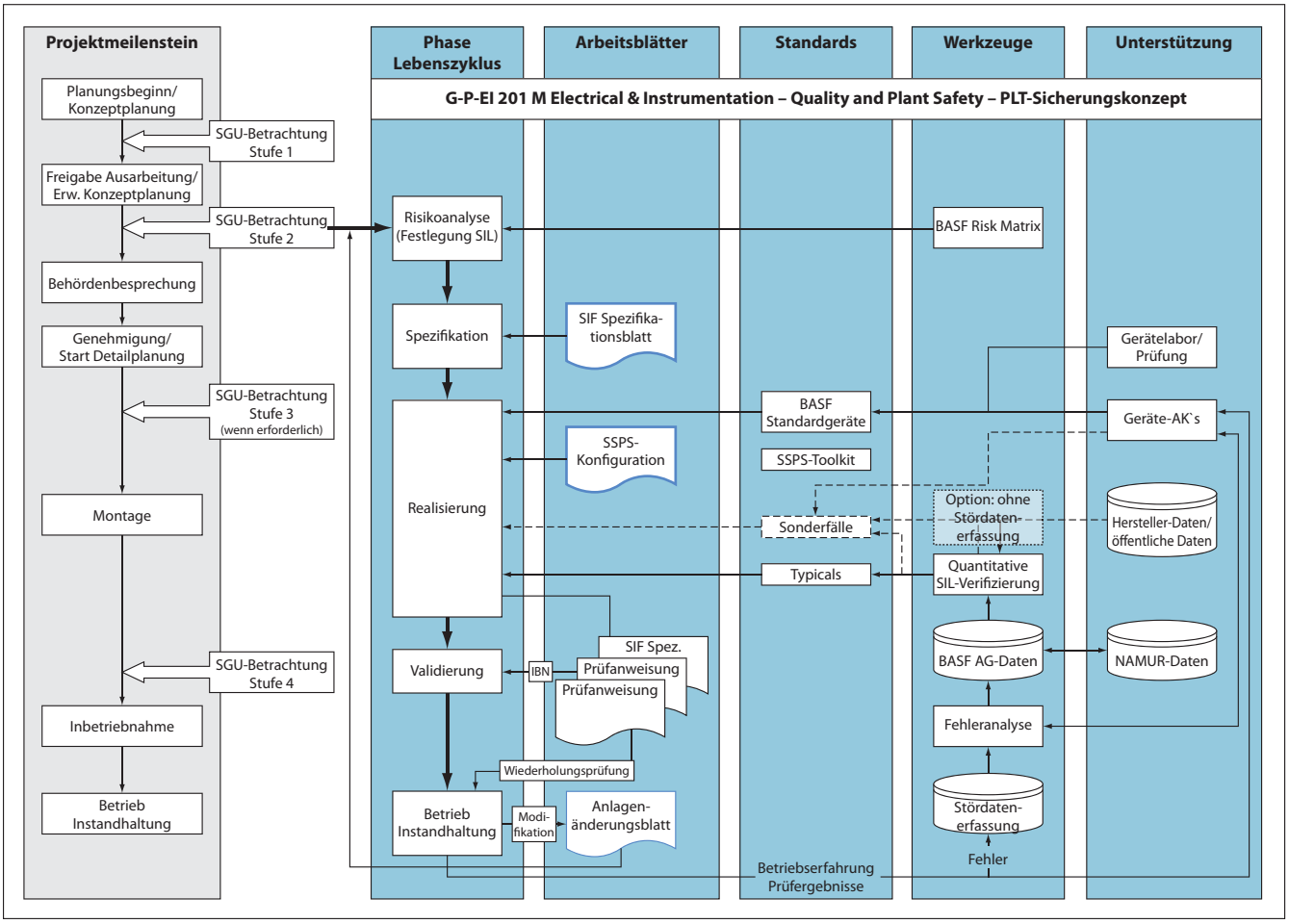

Bild 1: Überblick BASF PLT-Sicherheitskonzept.

Faktor Mensch spielt beim Erreichen der notwendigen Sicherheit eine ebenso wichtige Rolle.

Aus diesem Grund unterliegen sämtliche Aktivitäten in allen Phasen des Lebenszyklus von PLT-Schutzeinrichtungen einem gemeinsamen Sicherheitsmanagement. Dies beinhaltet beispielsweise notwendige Vorgehensweisen (z. B. im Rahmen von Entwicklungs-, Instandhaltungs- oder Änderungstätigkeiten), Verantwortlichkeiten von Mitarbeitern, organisatorischen Einheiten oder anderen beteiligten Unternehmen sowie notwendige Audits und Prüfungen.

Besonders erwähnenswert sind in diesem Zusammenhang die Anforderungen an die Kompetenz der handelnden Personen. Dazu gehören beispielsweise allgemeine, prozessunabhängige Kompetenzen wie eine adäquate Ausbildung, anzuwendende Engineering-Methoden, Erfahrung in den Bereichen Sicherheitstechnik und Risikoanalyse, normative Anforderungen und Kenntnisse der rechtlichen Aspekte. Darüber hinaus sind Kenntnisse über den abzusichernden Prozess, die eingesetzten Geräte (Feldgeräte, Steuerungen, Hard- und Software) und nicht zuletzt der möglichen Konsequenzen bei Versagen einer PLT-Schutzeinrichtung unabdingbar.

Generell muss über den gesamten Lebenszyklus das „Vier-Augen-Prinzip" (Verifikation von Arbeitsergebnissen durch eine zweite Person, die nicht direkt in diesen Arbeitsschritt eingebunden war) angewandt werden.

Permanente Leistungsbewertungen von PLT-Schutzeinrichtungen im Betrieb oder während der Instandhaltung sowie der Rückfluss der dabei gewonnenen Erkenntnisse tragen zur Optimierung sowohl der technischen Realisierung als auch der Arbeitsabläufe bei.

Die IEC 61511 beschreibt damit erstmals international eine Reihe von Anforderungen, die jedoch bei Betreibern, die sich bisher an der nationalen Normung in den Bereichen Anlagensicherung und Qualitätssicherung orientierten, inhaltlich nicht neu sind.

Aufbauend auf der bisherigen firmeninternen Richtlinie RPI10 wurden alle Anforderungen der IEC 61511 überprüft und Maßnahmen und Prozesse bei Bedarf angepasst oder

BASF	Risk Matrix			
	Severity			
Probability	S 1	S 2	S 3	S 4
P 0	A	B	D	E
P 1	A/B	B	E	E
P 2	B	C	E	F
P 3	C	D	F	F
P 4	E	F	F	F

Bild 2: BASF Risk Matrix.

Risikoklasse	Risikovermindernde Maßnahme
A	Verfahrens- oder Designänderung bevorzugt
B	Verfahrens- oder Designänderung, oder eine Schutzeinrichtung SIL 3 (SV, PLT)
C	Verfahrens- oder Designänderung, oder eine Schutzeinrichtung SIL 2 (SV, PLT)
D	Eine Überwachungseinrichtung guter Qualität mit dokumentierter Prüfung oder organisatorische Maßnahme von guter Qualität
E	Eine Überwachungseinrichtung oder organisatorische Maßnahme
F	Keine

Bild 3: Risikomindernde Maßnahmen.

implementiert. So wurden zum Beispiel Verantwortlichkeiten eindeutiger im Lebenszyklus festgelegt und so genannte „Verantwortliche Personen" für PLT-Schutzeinrichtungen schriftlich benannt. Zur besseren praktischen Unterstützung und vor allem einfacheren Umsetzung wurden weitere Werkzeuge, Standards oder Arbeitsblätter eingeführt, so z. B. einheitliche Spezifikationsunterlagen, SSPS-Konfigurationsunterlagen, eine SSPS-Baustein- und Funktionsbibliothek (Toolkit) oder eine IT-gestützte Stördatenerfassung.

Das aktuelle PLT-Sicherheitskonzept (Bild 1) ist ein geschlossenes, konsistentes Gesamtsystem. Durch permanentes Feedback aus Produktion und Engineering wird das Konzept kontinuierlich optimiert und bei Bedarf angepasst. Bild 1 gibt einen Überblick über das aktuelle PLT-Sicherheitskonzept der BASF über den Lebenszyklus einer PLT-Schutzeinrichtung.

BASF Risk-Matrix

Primäres Ziel eines verantwortlich handelnden Unternehmens muss der Einsatz inhärent sicherer Verfahren und die Verwendung von verfahrenstechnischen Komponenten sein, die keine weiteren technischen Sicherheitsmaßnahmen benötigen. Die Umsetzung dieses Ziels stößt in der Praxis jedoch oft an technische oder wirtschaftliche Grenzen. In diesen Fällen müssen Maßnahmen zur Risikoreduzierung ergriffen werden, vorzugsweise durch mechanische Schutzeinrichtungen oder bauliche Maßnahmen und erst, wenn dies nicht möglich ist, durch PLT-Schutzeinrichtungen.

Der erste und wichtigste Schritt zu einer sicheren und kostenoptimalen Auslegung von PLT-Schutzeinrichtungen ist die Identifikation der möglichen Gefährdungen. Nur für Gefährdungen, die eindeutig identifiziert worden sind, können wirksame Maßnahmen zur Risikominderung ergriffen werden. Um zu eindeutigen Ergebnissen zu kommen ist ein systematisches Vorgehen unabdingbar.

Die BASF nutzt für die Klassifizierung von Risiken ein von ihr entwickeltes Werkzeug – die Risk-Matrix. Die Risk-Matrix stellt eine semi-quantitative Methode dar, die auf langjährigen Erfahrungswerten beruht und entwickelt wurde um BASF-weit einheitlich bei der Bewertung von Risiken vorzugehen. Die BASF Risk-Matrix (Bild 2) ist eine 4x5-Matrix mit 4 Klassen für Schadensausmaß (S_1 bis S_4) und 5 Klassen für die Eintrittshäufigkeit (P_0 bis P_4).

Um ein denkbares Ereignis möglichst einfach beschreiben zu können, werden praxisnahe Beschreibungen benutzt, so für die Eintrittswahrscheinlichkeit

- P_0 – schon mehrmals passiert („einmal pro Jahr"),
- P_1 – schon einmal passiert („einmal pro 10 Jahre"),
- P_2 – ein Beinaheunfall ist bereits passiert („einmal pro 100 Jahre"),
- P_3 – kann nicht ausgeschlossen werden obwohl kein Fall bekannt ist („einmal pro 1000 Jahre"),
- P_4 – vernünftigerweise nicht zu erwarten („einmal pro 10 000 Jahre"),

bzw. das Schadensausmaß

- S_1 – Todesfälle,
- S_2 – Schwerverletzte (irreversible Effekte),
- S_3 – Verletzte (reversible Effekte),
- S_4 – geringfügige Verletzungen (keine Ausfallzeit).

20 potenzielle Risikofelder sind in sechs Risikoklassen (A–F) zusammengefasst und liefern damit die Anforderungen für eine notwendige Risikoreduzierung basierend auf einem von der BASF festgelegten maximal akzeptierbarem Risiko. Wenn das Risiko als nicht akzeptabel identifiziert wird (Risikoklasse A, B, oder C), sind risikomindernde Maßnahmen notwendig (Bild 3).

Festlegung des Sicherheits-Integritätslevel (SIL)

In der Zeit vor der IEC 61511 war in der Chemischen Industrie in Deutschland die Basis für die Klassifizierung von PLT-Schutzeinrichtungen die VDI/VDE Richtlinie 2180 „Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik" [4] sowie die NE 31 „Anlagensicherung mit Mitteln der Prozessleittechnik" [5]. Die Anforderungen an PLT-Schutzeinrichtungen wurden entsprechend dem vorliegenden Prozessrisiko in die Klassen AI (niedriges Risiko) bzw. AII (höheres Risiko) eingestuft. Die Einstufung wurde in interdisziplinären Teams in einer Sicherheitsbetrachtung vorgenommen.

Analog dazu definiert die IEC 61511 vier Sicherheits-Integritätslevel (SIL). Jeder SIL korrespondiert als Kernanforderung mit einer mittleren Ausfallwahrscheinlichkeit bei Anforderung für einen Funktionskreis vom Sensor über die Steuerung bis zum Aktor (PFD – Probability of Failure on Demand). Zusätzlich werden technische und organisatorische Anfor-

Tabelle 1: Anforderungsstufen in verschiedenen Standards.

BASF „neu"		IEC 61511 VDI/VDE 2180	DIN V 19250	BASF „alt"
SIL	**Risikobereich**	**SIL**	**AK**	**Risikobereich**
in der BASF nicht genutzt	D	1	1	A I
			2	
2	C	2	3	
			4	
3	B	3	5	A II
			6	
in der BASF nicht genutzt	A (extremes Risiko)	4	7	in der BASF nicht genutzt

derungen definiert (zu den Themen Sicherheitsmanagement, Entwicklung, Konstruktion, Bau, Prüfung, Montage, Instandhaltung und Wiederholungsprüfungen). Eine PLT-Schutzeinrichtung muss die durch den für sie festgelegten SIL repräsentierten Anforderungen qualitativ und quantitativ erfüllen.

Zwischen den SILs der IEC 61511, den bisherigen nationalen Normen (Anforderungsklassen der DIN V 19250 [6]) und den Risikoklassen der BASF besteht folgender Zusammenhang (Tabelle 1).

Tabelle 1 macht ebenfalls deutlich, dass in der BASF die Sicherheits-Integritätsstufen 4 und 1 nicht benutzt werden. SIL 4 ist in der IEC 61511-1 als der größtmögliche Wert festgelegt, der mit Mitteln der Prozessleittechnik realisiert werden kann. Gleichzeitig wird jedoch darauf hingewiesen, dass bei einem derartig hohen Wert vor dem Einsatz von PLT-Einrichtungen das entsprechende Verfahren überprüft und/oder mechanische Schutzeinrichtungen eingesetzt werden sollten. SIL 4 korrespondiert in der BASF Risk-Matrix mit der Risikostufe A und führt zu der Forderung, das Verfahren bzw. die Anlagenauslegung zu ändern. Die Risikoklasse D fordert als risikomindernde Maßnahme Überwachungseinrichtungen guter Qualität mit einer dokumentierten regelmäßigen Prüfung bzw. zusätzlichen organisatorischen Maßnahmen. Bei Einsatz von betriebsbewährten BASF-Standardgeräten wird in Kombination mit den festgelegten organisatorischen Maßnahmen eine Qualität der risikomindernden Maßnahme erreicht, die typischerweise vergleichbar SIL 1 ist, jedoch bei BASF nicht als Schutzeinrichtung eingestuft wird.

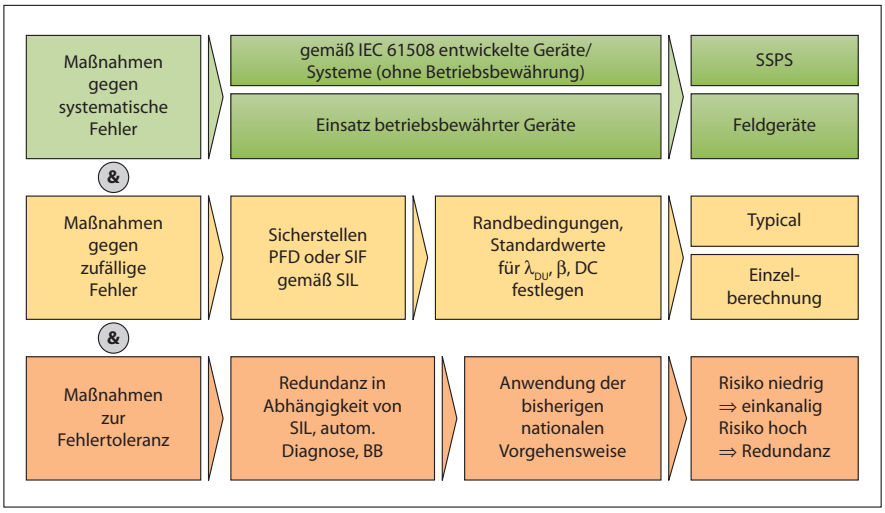

Bild 4: Maßnahmen beim Einsatz von Geräten in Schutzeinrichtungen gemäß IEC 61511.

Layer of Protection Analysis (LOPA)

Immer wieder taucht auch die Frage auf: "Warum nicht LOPA?" LOPA ist ebenfalls eine von der IEC 61511 empfohlene Methode zur SIL-Klassifizierung, die insbesondere im angelsächsischen Raum sehr populär ist. Sie eröffnet unter anderem die Möglichkeit, von separaten Schutzebenen „Kredit" zu nehmen. Richtig angewendet, bringt LOPA ähnliche Ergebnisse wie die BASF Risk-Matrix. Bei nicht vollständig voneinander unabhängigen Schutzebenen, was ja in der Praxis oftmals der Fall ist, kann unter Umständen Kredit in Form von vermeintlich bestehender Risikoreduzierung an die PLT-Schutzeinrichtung „weitergegeben" werden. Dies führt als Ergebnis zu einem falschen Sicherheitsgefühl und einer zu geringen Risikoreduzierung. Aus diesem Grund hat sich die BASF entschlossen, LOPA als Analysemethode nicht zu nutzen.

Geräteauswahl für PLT-Schutzeinrichtungen

Schutzeinrichtungen müssen robust gegenüber Fehlern sein. In der IEC 61511 wird deshalb gefordert, bei Schutzeinrichtungen Maßnahmen

- gegen systematische Fehler,
- gegen zufällige Fehler sowie
- zur Fehlertoleranz

zu treffen.

Für jede Schutzeinrichtung/sicherheitstechnische Funktion müssen immer *alle drei* Maßnahmen gleichzeitig ergriffen werden. Es genügt nicht, eine sehr geringe Ausfallwahrscheinlichkeit der sicherheitstechnischen Funktion aufgrund zufälliger Fehler nachzuweisen. Es müssen gleichzeitig auch Maßnahmen gegen systematische Fehler und Maßnahmen zur Fehlertoleranz ergriffen werden (Bild 4).

Maßnahmen gegen systematische Fehler

Bei den Maßnahmen gegen systematische Fehler einer Schutzeinrichtung muss unterschieden werden zwischen systematischen Fehlern des eingesetzten Geräts selbst und systematischen Fehlern, die sich durch den Einbau dieses Gerätes in eine bestimmte Anlage ergeben.

Systematische Fehler in Geräten

Typische systematische Fehler im Gerät selbst können die Verwendung falsch dimensionierter Bauteile, die Verwendung ungeeigneten Materials für den Prozessanschluss oder aber beim Einsatz mikroprozessorgestützter Geräte Softwarefehler sein. Die Wahrscheinlichkeit solcher systematischer Fehler im Gerät selbst hängt in entscheidender Weise vom Entwicklungs- und Herstellprozess des betreffenden Gerätes sowie des dafür eingesetzten Personals ab. Hält sich der Gerätehersteller an die in der IEC 61508 festgelegten Anforderungen, dann kann davon ausgegangen werden, dass das betreffende Gerät hinreichend frei von systematischen Fehlern ist.

Aus diesem Grund sollten künftige Gerätegenerationen, unabhängig davon, ob sie als Betriebs- oder als Schutzeinrichtung eingesetzt werden, gewisse Mindestanforderungen aus der IEC 61508 [7], die sich mit vertretbarem Aufwand umsetzen lassen, erfüllen. Im Rahmen einer Herstellererklärung (SIL 2) sollte ersichtlich sein, inwieweit die Forderungen der Norm erfüllt sind und welche sicherheitstechnischen

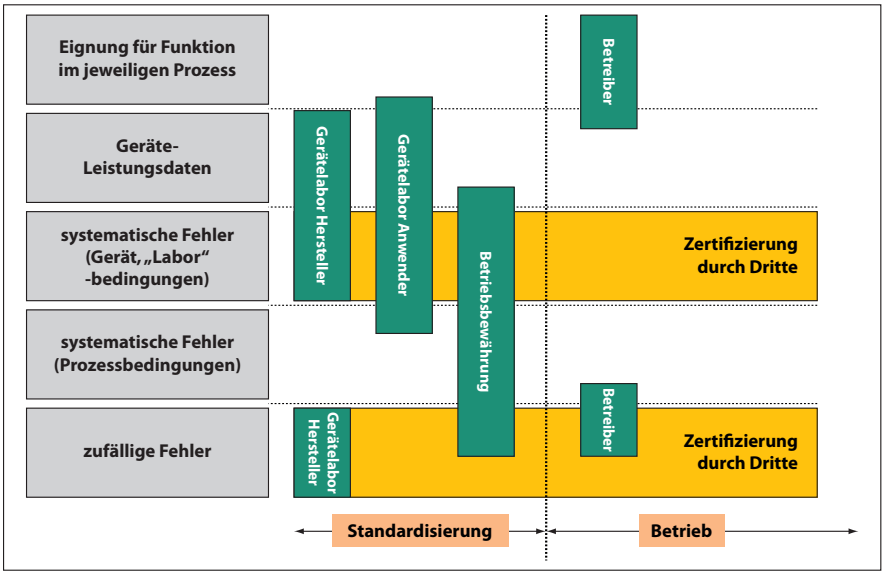

Bild 5: Rollen und Aufgaben im Rahmen der Zertifizierung/Standardisierung von Feldgeräten.

Kenngrößen für das Gerät unter definierten Einsatzbedingungen gelten. Eine Zertifizierung durch Dritte ist aus Sicht der BASF grundsätzlich nicht erforderlich.

Neben der besseren Gerätequalität haben diese Geräte den Vorteil, dass der Standardisierungsprozess in den Betreiberfirmen auf ein Minimum reduziert werden kann. Bei Geräten *ohne* Herstellererklärung für SIL 2 muss davon ausgegangen werden, dass diese Geräte systematische Fehler beinhalten, die erst im Rahmen des Betriebsbewährungsprozesses aufgedeckt werden können. Der Aufwand dafür, insbesondere Anzahl der Geräte, Anzahl der unterschiedlichen Anwendungen und Dauer der Betriebsbewährung ist ungleich höher, als bei einem Gerät, bei dem laut Herstellererklärung keine systematischen Fehler mehr vorliegen. Zudem muss in diesem Fall der Prozess der Betriebsbewährung bei allen wesentlichen Änderungen von neuem gestartet werden, während bei Geräten mit Herstellererklärung durch die Änderung keine systematischen Fehler in das Gerät eingebracht werden.

Eine Herstellererklärung für SIL 2 eines Geräts kann jedoch keine Aussage über die Eigenschaften der Gesamtfunktion machen, in der das Gerät eingesetzt ist. Sie kann sich nur auf die systematischen Fehler dieses Gerätes beziehen. Die SIL-Eignung der sicherheitstechnischen Funktion (SIF) muss zusätzlich nachgewiesen werden.

Systematische Fehler beim Einsatz von Geräten in der Anlage

Während der Hersteller des Gerätes nur eine Aussage hinsichtlich systematischer Fehler bis zur Schnittstelle zum Prozess machen kann, liefert die Betriebsbewährung des Gerätes beim Betreiber auch Aussagen über die Eignung bzw. mögliche systematische Fehler in Verbindung mit einem bestimmten verfahrenstechnischen Prozess. Deshalb sollte auch ein Gerät mit Herstellererklärung oder TÜV-Zertifikat immer noch einer anschließenden, üblicherweise verkürzten Betriebsbewährungsphase unterzogen werden. Der Anwender, der ein solches Gerät einsetzt, kann somit sicher sein, dass das Gerät als solches frei von systematischen Fehlern ist und für die in seinem Unternehmen vorliegenden üblichen Randbedingungen einsetzbar ist. Stimmen diese Randbedingungen mit den Randbedingungen seiner konkreten Anlage überein, kann er das Gerät in seinem Prozess einsetzen. Gibt es Abweichungen, muss er diese entsprechend bewerten und entsprechende Gegenmaßnahmen ergreifen oder im Extremfall ein anderes Gerät auswählen.

Eine in der BASF bewährte Methode ist der Einsatz von Standardgeräten in Betriebs- und Überwachungsfunktionen einer Anlage, bevor ein Einsatz innerhalb einer Schutzeinrichtung erfolgt. Vom einem „blinden" Einsatz neuer, auch zertifizierter Geräte ohne Betriebsbewährung ist abzuraten!

Maßnahmen gegen zufällige Fehler

Als Maßnahme gegen zufällige Fehler fordert die IEC 61511 eine Ausfallwahrscheinlichkeit einer Schutzeinrichtung unterhalb eines vorgegebenen Werts. Die Tabellen in der IEC 61511, in denen den einzelnen SIL-Stufen mittlere Ausfallwahrscheinlichkeiten (PFDs) zugewiesen werden, beziehen sich dabei einzig und allein auf zufällige Fehler. Dies ist deshalb nachvollziehbar, da ein vorhandener systematischer Fehler immer vorliegt und damit die Eintrittswahrscheinlichkeit 1 hat.

Beim Berechnen der PFD des gesamten Schutzkreises kann üblicherweise dann auf die Herstellerwerte zurückgegriffen werden, wenn der Hersteller auch den Prozessanschluss seines Gerätes unter vorgegebenen (Standard)-Randbedingungen in die Kalkulation einbezogen hat. Voraussetzung für die Anwendung der Herstellerwerte ist, dass das Gerät spezifikationsgerecht betrieben wird.

Maßnahmen zur Fehlertoleranz

Die dritte Anforderung in der IEC 61511 entstand aus der Kenntnis heraus, dass die vom Hersteller ermittelten λ_{DU}-Werte in vielen Fällen relativ unsicher sind. Es sollte vermieden werden, dass insbesondere bei höheren Risiken einkanalige Schutzkreise auf Basis solcher unsicherer λ_{DU}-Werte geplant und realisiert werden. Diese Anforderung stimmt im Wesentlichen mit der bisherigen nationalen Vorgehensweise überein, Schutzfunktionen mit niedrigem Risiko (≤ SIL2) einkanalig und Schutzfunktionen mit höherem Risiko (SIL 3) mehrkanalig auszurüsten.

BASF-Standardgeräte

Steuerungen

Die IEC 61511 lässt für Steuerungen grundsätzlich auch eine Verwendung von betriebsbewährten Geräten zu. Allerdings

ist die Verwendung an eine Reihe von Voraussetzungen geknüpft, die sich in der Praxis als fast unüberwindliche Hürde erweisen. Da sich die Verwendung von zertifizierten sicherheitsgerichteten Steuerungen bewährt hat und der Markt mittlerweile auch Lösungen für kleinere Mengengerüste bereit hält, nutzt die BASF ausschließlich nach IEC 61508 entwickelte und zertifizierte Steuerungen.

Feldgeräte

In der BASF kommen in PLT-Schutzeinrichtungen weitestgehend so genannte BASF-Standardgeräte zum Einsatz. Dabei handelt es sich um Geräte, die in einem NAMUR-Prüflabor getestet wurden und über eine ausreichende Betriebsbewährung (mehr als zehn Geräte bei einer Einsatzdauer von größer einem Jahr) verfügen. Gleichzeitig muss durch die Gerätehersteller der Nachweis erbracht werden, dass eine ausreichend niedrige Geräteausfallwahrscheinlichkeit (λ_{DU}, DC, SFF) sowie eine Entwicklung entsprechend den Qualitätsanforderungen nach SIL 2 der IEC 61508 vorliegt (Herstellererklärung). Zusätzlich erfolgt ein regelmäßiger Informationsaustausch zwischen den Standardlieferanten und den BASF-Arbeitskreisen.

Bild 5 beschreibt die Rollen und Aufgaben im Rahmen eines solchen Standardisierungsprozesses.

Der Bedarf an Feldgeräten für den Einsatz in Schutzkreisen ist angesichts des geringen Anteils von ca. 1–2 % aller PLT-Funktionen gering. Somit dürfte sich die Entwicklung spezieller Geräte gemäß IEC 61508 für den Einsatz in Schutzeinrichtungen allenfalls für Sonderanwendungen lohnen. Für die BASF sind solche Sondergeräte beispielsweise wegen der fehlenden Betriebserfahrung in Nicht-Sicherheitsanwendungen, der zusätzlichen Lagerhaltung von Reservegeräten und nicht zuletzt wegen des zwangsläufig höheren Preises nicht das Mittel der Wahl. Interessant können solche Geräte jedoch dann sein, wenn durch ihren Einsatz Redundanzen vermieden werden können; allerdings ist dann ein besonderes Augenmerk auf systematische Fehler im Bereich des Prozessanschlusses zu richten.

Betrieb von PLT-Schutzeinrichtungen

Jeder Anlagenbetreiber muss sicherstellen, dass die geforderte Risikoreduzierung jeder sicherheitstechnischen Funktion während des Betriebs und der Instandhaltung aufrecht erhalten wird. Dazu gehören neben den regelmäßigen Funktionsprüfungen und deren Dokumentation auch die Dokumentation und Analyse von Systemausfällen und Anforderungsraten einer PLT-Schutzeinrichtung. Die dabei gewonnenen Erfahrungen sind notwendig um die Wirksamkeit des Sicherheitskonzepts bzw. der PLT-Schutzeinrichtungen permanent zu überprüfen und bei Bedarf zu optimieren.

Erfassung und Analyse von Fehlern

Mit der kontinuierlichen Dokumentation und Analyse von Fehlern in PLT-Schutzeinrichtungen über einen längeren Zeitraum und einer statistisch aussagekräftigen Anzahl von Geräten in PLT-Schutzeinrichtungen kann gleichzeitig der Nachweis der Betriebsbewährung für die eingesetzten Geräte unterstützt werden.

Die BASF erfasst seit 2001 systematisch und IT-gestützt Fehler in PLT-Schutzeinrichtungen und stellt die Ergebnisse der NAMUR zur Verfügung. Gleichzeitig entsteht firmenintern eine aussagekräftige Datenbasis für die Abschätzung von sicherheitstechnisch bedeutsamen Kennwerten für die quantitative Bewertung von PLT-Schutzeinrichtungen. Nach einer Pilotierungsphase in Ludwigshafen wurde dieses Konzept auf die großen europäischen Standorte der BASF ausgeweitet und wird gegenwärtig im NAFTA-Raum und Asien schrittweise eingeführt. Neben einer größeren und damit auch statistisch aussagekräftigeren Datenbasis können so auch regionale Besonderheiten identifiziert werden.

Geräteausfälle oder andere Störungen werden jährlich von BASF-internen Gerätearbeitskreisen oder Expertengruppen analysiert und bewertet. Bei der Erfassung und Auswertung ist die Abgrenzung der systematischen und der zufälligen Fehler voneinander in der Praxis oftmals schwierig: Fällt ein Magnetventil beispielsweise häufig aus, dann kann das einerseits daran liegen, dass der Hersteller Bauteile mit niedriger Standzeit verwendet hat und somit der berechnete Wert für λ_{DU} als Summe der λ der Einzelbauteile schlecht ist. Andererseits kann der Hersteller hervorragende Bauteile verwendet haben. Es ergibt sich ein sehr gutes λ_{DU}. Der Ausfall des Magnetventils ist auf Rost in der Zuluftleitung zurückzuführen. In diesem Fall liegt ein systematischer Fehler vor, nämlich die Verwendung ungeeigneten, nämlich nicht rostgeschützten Leitungsmaterials für die Zuluftleitung.

Wegen dieser Abgrenzungsproblematik gehen in vielen Fällen systematische Fehler mit in die Störstatistik ein, ver-

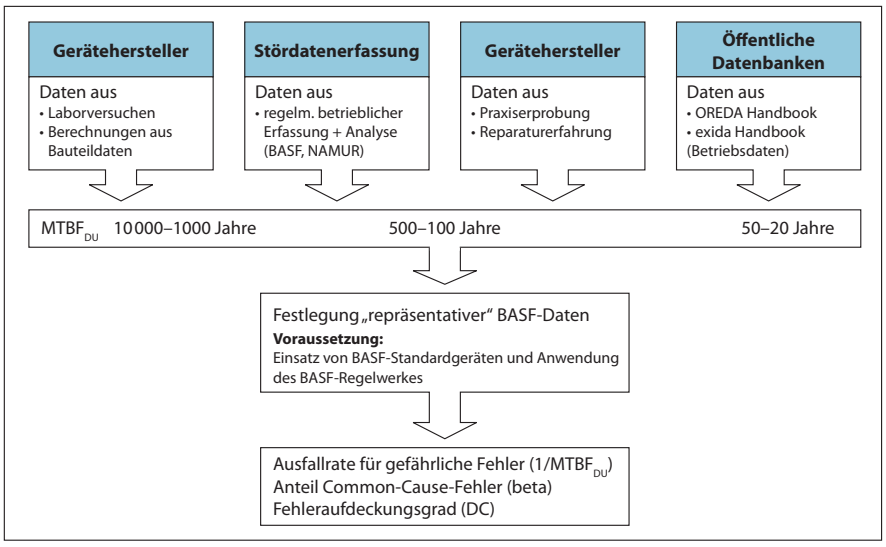

Bild 6: Varianz von Gerätedaten vs. pragmatischer Ansatz.

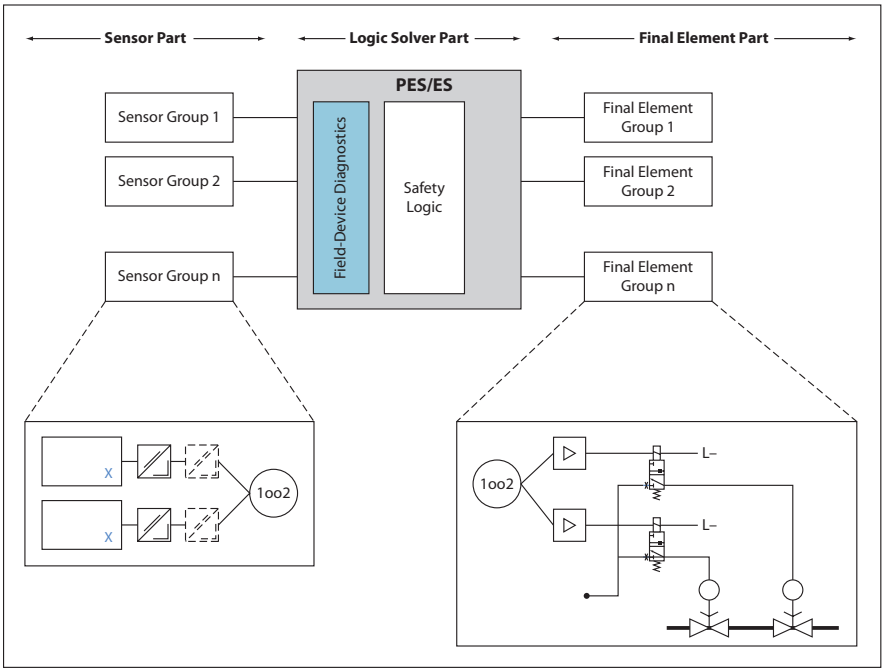

Bild 7: Beispiel für SIL 3-Typical mit Sensor- und Aktorgruppen mit interner 1oo2-Verschaltung.

schlechtern also den Wert für λ_{DU} im Vergleich zu dem vom Hersteller errechneten Wert.

In verschiedenen Projekten und während der internationalen Abstimmung der BASF-Richtlinie wurde ebenfalls deutlich, dass es auch regionale Unterschiede in der Einordnung von zufälligen und systematischen Fehlern und damit auch common-cause-Fehlern gibt. Insbesondere bei global operierenden Unternehmen entsteht an dieser Stelle ein nicht zu unterschätzender Abstimmungs- und Verständigungsaufwand. Hier sollte im Rahmen des Maintenance-Prozesses der IEC 61511 für eine erhöhte Klarheit gesorgt werden.

Neben der Gewinnung von Datenmaterial für die eingesetzten Geräte werden aus den gewonnenen Erfahrungen z.B. Maßnahmen für Geräteauswahl/-einsatz oder Optimierungsansätze für Prozessabläufe abgeleitet.

Nachweis der notwendigen Sicherheitsintegrität

Die bisher übliche rein qualitative Vorgehensweise reicht zukünftig nicht mehr aus, da die IEC 61511 explizit einen quantitativen Nachweis der Zuverlässigkeit einer PLT-Schutzfunktion fordert.

Für den rein mathematischen Teil des Nachweises stehen heute verschiedene geeignete Tools am Markt zur Verfügung. Jedoch machen zwei Besonderheiten einen quantitativen Nachweis in der Praxis nicht ganz so einfach – erstens die Abgrenzung der zu untersuchenden PLT-Schutzeinrichtung und zweitens das für die Berechung notwendige Datenmaterial.

„Gehört dieses oder jenes Ventil noch zur PLT-Schutzfunktion? Müssen wir es bei der PFD-Analyse mit berücksichtigen?“ Um Fragen wie diese zu vermeiden und die Abgrenzung der eigentlichen Schutzfunktion gegenüber den in der Anlage installierten Geräten für Betriebs- oder Überwachungsfunktionen sicher zu stellen, ist eine akkurate Risikoanalyse und eine eindeutige Spezifikation zu Beginn des Lebenszyklus unabdingbar. [8]

Ein größeres Problem stellen die für die Berechnung notwendigen Gerätedaten dar. Was im Bereich der Steuerungen kein Problem ist – hier liegen umfangreiche Daten für genau definierte Betriebsbedingungen vor – erweist sich bei Feldgeräten als umso problematischer.

Im Gegensatz zu Industriezweigen mit vergleichbaren Einsatzbedingungen, wie z.B. dem Off-Shore-Bereich, der Petrochemie oder der Kerntechnik ist ein rechnerischer Nachweis für jeden einzelnen Funktionskreis in den verfahrenstechnischen Anlagen der chemischen und pharmazeutischen Industrie sehr schwierig, da aufgrund der äußerst unterschiedlichen Einsatzbedingungen keine gesicherten Daten über individuelle Ausfallraten von Feldgeräten vorliegen. Vergleicht man Gerätedaten aus öffentlich zugänglichen Datenbanken mit Daten von Geräteherstellern oder auch Herstellerwerte bei technologisch vergleichbaren Geräten untereinander, werden teilweise gravierende Abweichungen sichtbar [9]. Die Ursachen dafür sind vielfältig, einmal werden Daten als reine Laborwerte angegeben, bei anderen Herstellern sind bereits Einflüsse des Prozesses oder spezielle Umgebungsbedingungen enthalten, die Vorgehensweise zur Bestimmung der sicherheitstechnischen Gerätekenndaten sind unterschiedlich oder es werden unterschiedliche Datenbanken für Elektronikbauteile verwendet usw. (Bild 6).

Für den Anwender ist dies keine zufrieden stellende Situation, da Berechnungen je nach verwendetem Datenmaterial stark streuende Ergebnisse liefern können und man sich einerseits in einer trügerischen Sicherheit wähnen kann oder andererseits vielleicht einen viel zu konservativen Ansatz wählt.

Eine mögliche Lösung dieses Dilemmas ist die Definition von Typicals und der pauschale Nachweis ihrer Zuverlässigkeit. Diese Definition kann dabei unternehmensspezifisch vorgenommen werden oder wie in der NAMUR Empfehlung NE 93 [10] beschrieben alle PLT-Schutzeinrichtungen, die in Übereinstimmung mit der bisherigen VDI/VDE 2180 und DIN V 19250/51 [6, 11] errichtet und betrieben werden, umfassen.

BASF-Standardstrukturen (Typicals) für PLT-Schutzeinrichtungen

Einzelnachweise von PLT-Schutzeinrichtungen sind teilweise aufwändig und wie bereits erwähnt [9] mit Unsicherheiten behaftet. Aus diesem Grund verfolgt die BASF den Ansatz,

PLT-Schutzeinrichtungen auf der Basis von Standardschaltungen zu implementieren und zu validieren.

Standardstrukturen (Typicals) dienen der Vereinfachung von Planung und Nachweis der Sicherheitsintegrität von PLT-Schutzeinrichtungen. Sie decken die überwiegende Zahl (> 90 %) von PLT-Schutzeinrichtungen in der BASF-Praxis ab.

Bei der Verwendung von BASF-Standardgeräten (Feldgeräte und SSPSen) und unter Einhaltung sämtlicher Vorgaben der Hersteller sowie relevanter BASF-Richtlinien sind zum Nachweis der geforderten Sicherheitsintegrität durch den Anwender keine Berechnungen erforderlich. Die zugrunde liegenden Berechnungen wurden auf der Basis von BASF-Standardgeräten durchgeführt. Die dabei notwendigen sicherheitstechnischen Kenngrößen (λ_{DU}, β, DC, SFF) basieren auf der jährlichen Stördatenerfassung der BASF und wurden als worst-case-Werte für Teilsysteme (Sensor- und Aktorgruppen) festgelegt. Die BASF-Typicals sind unabhängig vom Messprinzip (beispielsweise Druck, Differenzdruck, Temperatur, Füllstand) mit Ausnahme von Analysegeräten und bis zu festgelegten Obergrenzen variabel in Anzahl und Art der Sensor- bzw. Aktorgruppen.

Allen Typicals liegt ein Prüfintervall von ≤ 1 Jahr sowie normale Prozessbedingungen („sauberer Betrieb") zugrunde. Besondere Prozessbedingungen können die Zuverlässigkeit negativ beeinflussen und deshalb kürzere Prüfintervalle erforderlich machen.

PLT-Schutzeinrichtungen können in Einzelfällen von den Standardstrukturen abweichen, so z. B.

- bei einem notwendigen ununterbrochenen Anlagenbetrieb von mehr als einem Jahr,
- wenn eine größere Anzahl von Prozessgrößen in der Schutzfunktion verarbeitet werden muss,
- wenn eine größere Zahl von Abschaltungen (z. B. Schließen/Öffnen von Produktleitungen, Abschalten von Motoren) notwendig sind oder
- wenn eine besondere Mess- oder Stellaufgabe vorliegt, die nicht mit BASF-Standardgeräten gelöst werden kann. Analysengeräte fallen grundsätzlich unter diesen Punkt.

In diesen oder ähnlichen Fällen erfolgt eine individuelle Analyse der Schutzeinrichtung durch ein Expertenteam, welches z. B. zusätzliche technische und organisatorische Maßnahmen zur Steigerung der sicherheitstechnischen Zuverlässigkeit festlegt [12]. Parallel dazu erfolgt ein flankierender individueller quantitativer Nachweis bzw. Abschätzung der sicherheitstechnischen Integrität.

Gegenwärtig wird dieses Vorgehen für die europäischen Standorte der BASF angewendet. Wenn von den außereuropäischen Standorten ausreichend Datenmaterial aus der regionalen Stördatenerfassung zur Verfügung steht, können auch in diesen Regionen die vereinfachten Nachweismethoden angewendet werden.

Zusammenfassung

Das vorgestellte PLT-Sicherheitskonzept ist Teil des Gesamtsicherheitskonzepts der BASF. Es sorgt für eine dem jeweiligen

Risiko angepasste Risikoreduzierung und sowohl für sichere aber auch wirtschaftliche Lösungen. Das Konzept und hat sich in den letzten Jahren insbesondere in den großen Verbundstandorten Ludwigshafen und Antwerpen bewährt.

Die Anwendung von Standardstrukturen erlaubt einerseits die Implementierung von PLT-Schutzeinrichtungen mit vermindertem Planungs- und Nachweisaufwand, andererseits lässt es genügend Freiraum, eine Schutzeinrichtung funktions- und kostenoptimal aufzubauen, um so die Vorteile einer quantitativen Herangehensweise der IEC 61511 ausnutzen zu können.

Die IEC 61511 hat sich als gutes, weitestgehend praktikables Werkzeug erwiesen. Die neuen Anforderungen können bei einem bisherigen, auf der VDI/VDE-Richtlinie 2180 basierenden Konzept mit geringem Aufwand implementiert werden.

Ein wesentlicher Vorteil, insbesondere für global tätige Unternehmen, liegt in der weltweiten Anwendbarkeit und den damit verbunden einheitlichen Bewertungsmaßstäben für PLT-Schutzeinrichtungen.

Das PLT-Sicherungskonzept der BASF setzt die Anforderungen der IEC 61511 möglichst pragmatisch um, so dass der Planungs- oder Instandhaltungsingenieur mit vorgefertigten Standardfunktionen arbeiten kann, ohne sich zu sehr in Details einarbeiten zu müssen. Zusätzlich wird das Konzept durch permanentes Feedback aller Beteiligten kontinuierlich optimiert.

Seit 2005 die Bayer Material Science AG ebenfalls das BASF PLT-Sicherheitskonzept. Aufgrund der guten Modularität waren die erforderlichen BMS-spezifischen Anpassungen problemlos zu implementieren.

Literatur

[1] IEC 61511: Functional safety: Safety Instrumented Systems for the process industry sector, Teile 1 bis 3, Genf (2003/2004).

[2] Fachrichtlinien für Planung und Instandhaltung Prozessleittechnik – PLT-Sicherungskonzept, RPI 10, BASF Aktiengesellschaft, Ludwigshafen (2003).

[3] Technical Community – Global Procedure Electrical & Instrumentation – Quality Control and Plant Safety (PLT-Sicherungskonzept), G-P-EI 201 M, BASF Aktiengesellschaft, Ludwigshafen (2006).

[4] VDI/VDE 2180, Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT), Teile 1 bis 5 (2007).

[5] NE31, Anlagensicherung mit Mitteln der Prozessleittechnik (1993).

[6] DIN V 19250, Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen (1994).

[7] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety related systems, Teile 1–7, Genf (1998/2000).

[8] *Hablawetz, D.*: Softwarebasierte Anlagenabsicherung in Chemieanlagen, atp – Automatisierungstechnik 45 (2003), H. 7, S.77–82.

[9] *Düpont, D., Litz, L., Netter, P.*: Sources of Mistakes in PFD Calculations for Safety-related Loop Typicals. Proceedings of the 4th Petroleum and Chemical Industry Conference Europe – Electrical and Instrumentation Applications, pp. 139-146, Paris (Frankreich), Juni 2007.

[10] NE93, Nachweis der sicherheitstechnischen Zuverlässigkeit von PLT-Schutzeinrichtungen (2003).

[11] DIN V 19251, Leittechnik – MSR-Schutzeinrichtungen – Anforderungen und Maßnahmen zur gesicherten Funktion (1995).

[12] *Kuhn, U.*: Sicherstellung der Qualität von umfangreichen PLT-Schutzeinrichtungen, atp – Automatisierungstechnische Praxis 47 (2005), H. 5, S. 32–39.

außerdem

Matalla, N.: Überarbeitung der VDI/VDE 2180, atp – Automatisierungstechnische Praxis 47 (2005), H. 1, S. 10–12.

Manuskripteingang: 5. Juli 2007.

Dipl.-Ing. *Dirk Hablawetz* (43) leitet in der BASF AG das Servicecenter Durchflussmesstechnik sowie das BASF Testcenter für PLT-Geräte und ist Mitglied im Europäischen Center of Expertise PLT-Anlagensicherung sowie im globalen Kompetenzteam der BASF-Gruppe für PLT-Sicherheitskonzepte.

Adresse: BASF AG, WLE/EC – L440, 67056 Ludwigshafen, Deutschland, Tel. +49 621 60-47132, E-Mail: dirk.hablawetz@basf.com

Dipl-Ing. *Norbert Matalla* (52) leitet in der BASF AG die Gruppe Zentrale Instandhaltung und ist darüber hinaus in BASF internen, in nationalen und in internationalen Arbeitskreisen auf dem Gebiet der Anlagensicherheit mit Mitteln der PLT tätig.

Adresse: BASF AG, WLM/IA – H515, 67056 Ludwigshafen, Deutschland, Tel. +49 621 60-40213, E-Mail: norbert.matalla@basf.com

Dr. *Gerhard Adam* (60) leitet in der BASF AG die Gruppe Zentrale Planung beim Site Engineering Ludwigshafen und ist darüber hinaus Leiter des Europäischen Center of Expertise PLT-Anlagensicherung der BASF und dem globalen Kompetenzteam der BASF-Gruppe für PLT-Sicherheitskonzepte.

Adresse: BASF AG, WLM/PA – B014, 67056 Ludwigshafen, Deutschland, Tel. +49 621 60-45801, E-Mail: gerhard.adam@basf.com