1-2/2011
53. Jahrgang B3654
Oldenbourg Industrieverlag

atp edition

Automatisierungstechnische Praxis

Safety First – funktionale Sicherheit ist unverzichtbar

Dr. Norbert Kuschnerus,
Vorsitzender des Namur-Vorstands Bayer Technology Services GmbH

Sicherheit von Chemieanlagen ist nach dem Jahr 2010 aktueller als zuvor, ja geradezu in den Brennpunkt vieler Diskussionen geraten. Als die Namur sich das Thema „funktionale Sicherheit" – also Sicherheit mit Mitteln der Prozessleittechnik – als Thema für die Hauptsitzung 2010 auswählte, schrieben wir das Jahr 2008 mit den aufrüttelnden Ereignissen in Texas und bei London, in dem vollen Bewusstsein, dass wir dieses Thema wieder stärker in den Fokus unserer Ingenieure rücken müssen. Umso wichtiger ist es uns, dass wir gemäß des vor Jahren verabredeten Brauchs über die atp edition in der ersten Ausgabe des Jahres dieses überaus wichtige Thema nun einem noch größeren Kreis nahe bringen können.

Der sichere Betrieb von verfahrenstechnischen Anlagen ist das oberste Ziel in der Prozessindustrie. Vor dem Ausschöpfen von Optimierungspotenzial bei der Prozessführung oder der Minimierung von Kosten bei der Errichtung der Anlagen ist zunächst die Sicherheit zu gewährleisten. Es gibt also buchstäblich kein wichtigeres Thema in der Namur als den Beitrag, den die Automatisierungstechnik für die Anlagensicherheit leistet.

Voraussetzung für die praktische Umsetzung von innovativen Produktideen in der funktionalen Sicherheit ist die absolute Verlässlichkeit der eingesetzten Technologie. Dies führt dazu, dass neue Technologien erst nach eingehender Prüfung für Schutzaufgaben eingesetzt werden, was mancher Laie als „altmodisch" oder „rückständig" empfinden mag, aber auch wir Automatisierungsingenieure müssen den Slogan „Safety First!" wirklich ernst nehmen.

Die Wirklichkeit sieht so aus: Die heute verfügbare Sicherheitstechnik hat einen beeindruckenden Stand. Dies betrifft nicht nur ihre außergewöhnliche Zuverlässigkeit, sondern auch ihre Funktionalität. Perfekte Technik ist allerdings auch in diesem Fall nicht ausreichend: Ein sicherer Betrieb ist erst möglich, wenn der Betreiber der Anlage das Know-how hat, diese Technik richtig einzusetzen. Dazu ist neben tiefgehendem technischem Verständnis auch erhebliches organisatorisches Know-how und Umsetzungskompetenz notwendig.

Die Sicherheitstechnik entwickelt sich nicht nur selbst weiter, ihr stehen auch sich ändernde Anforderungen gegenüber. Eine optimierte Führung von Prozessen bedeutet eben, näher an ihre Grenzen zu gehen und damit den Abstand zu potenziell gefahrbringenden Zuständen zu verringern, ohne Sicherheit selbst zu reduzieren oder gar aufzugeben. Dies wird in Zukunft neue Lösungen in der funktionalen Sicherheit erfordern, denn solche Anforderungen sind häufig nur mit Mitteln der Leittechnik zu lösen. Wie solche neue Anforderungen aussehen können, erkennt man beispielsweise daran, dass heute durchaus stoffbezogene, das heißt PAT-Messungen, in Schutzfunktionen eine entscheidende Rolle spielen: vor einigen Jahren noch undenkbar.

Die verbindungsprogrammierte, „verdrahtete" Sicherheitssteuerung hat längst ausgedient. Heute werden Sicherheits-SPSen mit Engineering-Systemen auf Standard-Plattformen eingesetzt, Feldgeräte sind ohne leistungsfähige Prozessoren heute nicht mehr denkbar. Damit wird zum Beispiel „IT-Security" ein Thema auch in der funktionalen Sicherheit. Man wird Antworten auf die damit verbundenen Fragestellungen finden müssen. „Zurück zur verbindungsprogrammierten Steuerung" wird sicher kein erfolgversprechender Ansatz sein.

Funktionale Sicherheit ist ein sehr wichtiges, technisch faszinierendes und organisatorisch herausforderndes Thema. Es hat damit alles, was ein gutes Motto für eine Namur-Hauptsitzung ausmacht. Das haben im vergangenen November 550 Besucher hautnah und eindrucksvoll erlebt.

Liebe Leser, ich wünsche Ihnen viel Spaß und Nutzen bei der Lektüre dieser Ausgabe der atp edition.

FORSCHUNG

VERBAND

BRANCHE

BRANCHE | NAMUR-HAUPTSITZUNG

PRAXIS

HAUPTBEITRÄGE | NAMUR-HAUPTSITZUNG

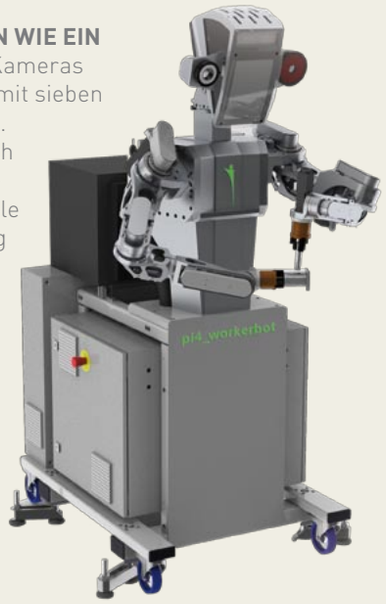
HAUPTBEITRAG

RUBRIKEN

Automatisiert und doch flexibel montieren – „Workerbot“ besitzt hoch entwickelte Motorik

Automatisierung und Flexibilität schließen sich oft aus. Nicht so bei einem Roboter für Montageaufgaben, der am Fraunhofer-Institut für Produktionsanlagen und Konstruktionstechnik im Rahmen eines Forschungsprojekts entwickelt wurde. Zwei Arme, drei Kameras, Fingerspitzengefühl und Mimik – das zeichnet den pi4-Workerbot aus.

Vorsichtig nimmt der Roboter das Zahnrad in die eine und das Gehäuse in die andere Hand. Dann steckt er die beiden Teile zusammen. Da sie nicht gleich einrasten, unterbricht er seine Bewegung. Langsam dreht er das Zahnrad ein kleines Stück zurück. Jetzt lässt es sich ohne Widerstand in der Halterung bewegen. „Lächelnd“ legt er die erfolgreich zusammengesteckte Verbindung auf das Laufband. Dem pi4-Workerbot gelingt motorisch vieles, was normale Roboter nicht können. Er gilt als Glanzstück des mit europäischen Mitteln geförderten PISA-Projekts. Ziel des Forschungsvorhabens ist es, mit Hilfe von Robotern bei Montageaufgaben einer industriellen Massenfertigung flexibler zu sein.



PROPORTIONEN WIE EIN MENSCH, drei Kameras und zwei Arme mit sieben Freiheitsgraden. Damit eignet sich der pi4-Workerbot für die flexible Automatisierung von Montage- und Messaufgaben. Bild: Fraunhofer-IPK

„Wir haben den Workerbot so entwickelt, dass er ähnliche Proportionen wie ein Mensch hat“, sagt Dr.-Ing. Dragoljub Surdilovic, Arbeitsgruppenleiter am Fraunhofer-Institut für Produktionsanlagen und Konstruktionstechnik IPK in Berlin. So lässt sich der Hightech-Helfer an jedem modernen Stehsitzarbeitsplatz der industriellen Fertigung einsetzen.

Die Umgebung erfasst er mit einer hochmodernen 3D-Kamera in der Stirn. Zu Inspektionszwecken dienen zwei weitere Kameras. Die Bandbreite seiner Fähigkeiten ist groß: „Er kann Gegenstände vermessen oder unterschiedliche Oberflächen inspizieren“, sagt Matthias Krinke, Geschäftsführer von pi4-Robotics, dem Unternehmen, das den Workerbot vermarktet. Über die Reflektion des Lichts auf dem Material erkennt der Roboter, ob etwa die Chromschicht auf einem Werkstück makellos aufgetragen wurde. „Wenn man zwei unterschiedliche Kameras einsetzt, kann er mit dem linken Auge einen anderen Aspekt prüfen als mit dem rechten“, sagt Krinke.

Eine weitere Besonderheit des pi4-Workerbot: Er verfügt über zwei Arme. „Das erlaubt neue Arten von Bewegungsabläufen“, sagt Surdilovic. Die Roboter können ein Werkstück von einer Hand in die andere reichen. Etwa, um kompliziert gebaute Teile aus allen Winkeln zu betrachten. Konventionelle Roboterarme verfügen nur über sechs Freiheitsgrade und nicht über sieben wie der menschliche Arm. Der Workerbot hat neben dem Drehgelenk in der Schulter eine zusätzliche Drehmöglichkeit, die dem Handgelenk beim Menschen entspricht. Die Arbeitsgruppe von Surdilovic arbeitete die Steuerung aus.

Zudem haben die Forscher ihn mit Fingerspitzengefühl versehen. „Wenn man die Greifkräfte richtig einstellt, nimmt er ein Ei, ohne es zu zerquetschen“, hebt Surdilovic hervor. Der Roboter kann sich sogar mit Mimik ausdrücken. Läuft die Arbeit reibungslos, „lächelt“ er zufrieden. Sieht er gelangweilt aus, wartet er auf Arbeit, und der Produktionsleiter weiß, dass der Produktionsprozess beschleunigt werden kann.

FRAUNHOFER-INSTITUT FÜR PRODUKTIONSANLAGEN UND KONSTRUKTIONSTECHNIK,
Pascalstraße 8–9, D-10587 Berlin,
Tel. +49 (0) 30 39 00 61 72,
Internet: www.ipk.fraunhofer.de

GMA fordert wissenschaftliche Zentren

Deutschland braucht wissenschaftliche Zentren für Automatisierungstechnik, um seine internationale Führungsposition zu sichern und weiter auszubauen. Zu diesem Schluss kommt die VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) in ihren Thesen „Automation 2020“. „Automatisierungstechnik ist ein wesentlicher und wachsender Wirtschaftsfaktor für die Bundesrepublik. Weltweit ist Deutschland in einer führenden Position“, sagt der GMA-Vorsitzende Dr. Kurt D. Bettenhausen. „Um diese Position auch in Zukunft zu halten, brauchen wir gemeinsame Anstrengungen von Forschung und Industrie für die Entwicklung neuer Methoden und Anwendungen.“

Ein Anfang sind laut Bettenhausen Pläne für eine erste Bewerbung um einen Spitzencluster Automation im Rahmen der Hightech-Strategie des Bundesministeriums für Bildung und Forschung. Die GMA unterstütze diese Initiative zur Förderung der Automation ausdrücklich, so ihr Vorsitzender.

VDI/VDE-GESELLSCHAFT MESS- UND AUTOMATISIERUNGSTECHNIK,
VDI-Platz 1, D-40468 Düsseldorf,
Tel. +49 (0) 211 621 42 26,
Internet: www.vdi.de

Ein Mitarbeiter geht nach 33 Jahren in Rente.
Mit ihm gehen 33 Jahre Berufserfahrung.
Und jetzt muss jemand mit gerade mal 3 Jahren Praxis den Job erledigen.

EIGENTLICH UNMÖGLICH

Mit den neuen Human Centered Design Technologien von Emerson geht die Erfahrung nicht in Pension. Wir haben genau analysiert, wie Mitarbeiter ihre Aufgaben verrichten, und alle neuen Produkte auf der Basis von Human Centered Design gestaltet. Dies versetzt uns in die Lage, Erfahrungen und Wissen aus Ihrer Anlage in unsere Kontroll- und Überwachungstechnologien zu integrieren. Eine bisher unerreichte intuitive Benutzerfreundlichkeit ist das Resultat. Aufgaben werden schneller und zuverlässiger erledigt, selbst wenn Sie dabei auf weniger Erfahrung und Fachwissen zurückgreifen können. Sie haben die Gewissheit, dass alle Arbeiten korrekt ausgeführt werden – egal von wem. Finden Sie verloren geglaubte Erfahrung wieder unter: **www.EmersonProcess.com/Experience**
E-mail: **info.de@emerson.com**

EMERSON™
Process Management

EMERSON. CONSIDER IT SOLVED.™

Namur-Konferenz in China zog mehr Besucher an

Zum zweiten Mal veranstaltete die Namur China ihre Hauptkonferenz ganz nach dem Muster der Namur in Deutschland. Wenn auch die Teilnehmerzahl der Tagung in Shanghai mit etwa 130 Zuhörern noch ein gutes Stück von der Rekordzahl der diesjährigen Namur-Konferenz in Deutschland entfernt blieb, so ist sie doch eine Plattform, auf der sich gerade ein Hauptsponsor seinen Geschäftspartnern in China präsentieren kann. Im Vorjahr hatte die Tagung in China knapp 90 Teilnehmer. „Die hochkarätigen Berichte und Vorträge aus den Arbeitskreisen der Namur in China – ergänzt durch Beiträge, die in ähnlicher Form eine Woche zuvor bei der deutschen Namur-Hauptsitzung in Bad Neuenahr präsentiert wurden – ergaben ein insgesamt rundes Bild“, betont Dr.-Ing. Gunther Kegel, Vorsitzender der Geschäftsführung der Pepperl+Fuchs GmbH, des Hauptsponsors der chinesischen Hauptkonferenz.

DR.-ING. GUNTHER KEGEL, Vorsitzender der Geschäftsführung der Pepperl+Fuchs GmbH, referierte bei der chinesischen Namur-Hauptkonferenz über innovative Explosionsschutz-Technologie.
Bild: Pepperl+Fuchs

Im Unterschied zum deutschen Vorbild teilt die Namur in China ihr Publikum nach dem Hauptvortrag (noch) nicht in einzelne Vortragssäle auf – alle Beiträge werden dem gesamten Plenum präsentiert. So hatte die Firma die Gelegenheit, neben dem Hauptvortrag noch zwei weitere Fachvorträge zu präsentieren. Auf intensives Interesse traf auch der mit den neuesten Pepperl+Fuchs-Exponaten bestückte Ausstellungsraum. Eindeutiges Highlight waren hier die Präsentationen und Exponate rund um das Thema DART.

Die Namur China hatte ihre Hausaufgaben gemacht und nach der ersten Hauptkonferenz im vorigen Jahr die Teilnehmer nach einem favorisierten Hauptthema befragt. Der Themenschwerpunkt „Explosionsschutz“ stand damals ganz oben auf der Liste, und so erfüllte das innovative Explosionsschutz-Konzept DART die Wünsche und Erwartungen der Besucher.

Die Qualität der Veranstaltung lässt erwarten, dass die Teilnehmerzahl in den kommenden Jahren deutlich wachsen wird – vor allem, wenn es der Namur China gelingt, Mitglieder auf dem chinesischen Markt zu werben, die nicht ohnehin schon Mitglied der Namur in Deutschland sind.

PEPPERL+FUCHS GMBH,
Geschäftsbereich Prozessautomation,
Lilienthalstraße 200,
D-68307 Mannheim,
Tel. +49 (0) 627 776 22 22,
Internet: www.pepperl-fuchs.com

Wolfgang Hofheinz neuer Vorsitzender der DKE

Dipl.-Ing. Wolfgang Hofheinz (63), Geschäftsführer der Bender GmbH in Grünberg, ist neuer Vorsitzenden der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE. Am 1. Januar 2011 trat er die Nachfolge von Dr.-Ing. E.h. Dietmar Harting an, der nach zwölf Jahren aus seinem Amt als DKE-Vorsitzender ausscheidet. Erster Stellvertreter von Hofheinz ist Dr. Klaus Mittelbach, Vorsitzender der Geschäftsführung des ZVEI, zweiter Stellvertreter ist Prof. Dr. Hartwig Steusloff.

DIPL.-ING. WOLFGANG HOFHEINZ führt seit 1. Januar die DKE

Hofheinz ist seit 1975 bei der Bender GmbH & Co. KG tätig, seit 1995 als Geschäftsführer. „Bei Bender betrachten wir die Mitarbeit in der nationalen und internationalen Normung als strategisches Erfolgskonzept. Die Normung hat wesentlich zum Erfolg unseres Unternehmens beigetragen“, so Wolfgang Hofheinz. Die Bender GmbH entwickelt Mess-, Schutz- und Überwachungssysteme zur elektrischen Sicherheit von Maschinen und Anlagen. Seit fast 30 Jahren ist Hofheinz in vielen Gremien der DKE vertreten, 2008 erhielt er die DKE-Nadel für seine Verdienste in der elektrotechnischen Normung, 2006 wurde er mit dem IEC 1906 Award ausgezeichnet.

DKE DEUTSCHE KOMMISSION ELEKTROTECHNIK ELEKTRONIK,
Informationstechnik im DIN und VDE,
D-60596 Frankfurt am Main,
Tel. +49 (0) 69 630 80,
Internet: www.dke.de

Druck sicher überwachen.

Optimale Sensoren für optimale Ergebnisse
Cerabar M | Deltabar M | Deltapilot M | Waterpilot

Das modulare Design der neuen kompakten Druck- und Differenzdrucktransmitter der M-Linie sowie eine Vielzahl an betriebsbewährten Sensoren ermöglichen eine perfekte Anpassung an jede Applikation:

- Hochvakuum mit ölfreien Keramiksensoren bis +150 °C Mediumstemperatur
- außerordentlicher Kondensatanfall gemessen mit patentierter hermetisch dichter CONTITE™-Messzelle
- extreme Temperaturen von -70… +400 °C mit vollverschweißten Druckmittlern.

Die einheitlichen Komponenten der Gerätefamilie, wie Elektronik und Anzeige, reduzieren die Ersatzteil- und Lagerhaltung. Mit einer komfortablen und intuitiven Vor-Ort-Bedienung ausgestattet, geht auch die Inbetriebnahme schnell von der Hand – das spart Zeit und minimiert den notwendigen Schulungsaufwand.

www.de.endress.com/m-plattform

Endress+Hauser
Messtechnik GmbH+Co. KG
Colmarer Straße 6
79576 Weil am Rhein

Telefon 0 800 EHVERTRIEB
oder 0 800 348 37 87
Telefax 0 800 EHFAXEN
oder 0 800 343 29 36

Endress+Hauser
People for Process Automation

Export-Rekord: Elektroindustrie erhöht Ausfuhren zum Jahresende um 26 Prozent

Neues Jahr, neue Prognosen: „Die Elektro-Produktion dürfte im Jahr 2011 um sieben Prozent zulegen“, so Dr. Klaus Mittelbach, Vorsitzender der Geschäftsführung des ZVEI. „Der Branchenumsatz steuert damit 2011 auf die Marke von 175 Mrd. Euro zu.“ 2012 könnte der Branchenumsatz damit bereits eine neue Höchstmarke erreichen.

Im gesamten Jahr 2010 ist die Produktion Schätzungen des ZVEI zufolge um zwölf Prozent gestiegen. Der Umsatz dürfte mehr als 162 Mrd. Euro erreichen – nach 145 Mrd. Euro im Jahr 2009 und 182 Mrd. Euro im Jahr 2008. Damit wird die ZVEI-Prognose, die zuletzt im August nach oben angepasst wurde, noch etwas übertroffen. „Dies darf aber nicht darüber hinweg täuschen, dass die Verluste von 2009 noch nicht vollständig aufgeholt sind“, so Dr. Mittelbach.

Bei Produktion, Umsatz und Auftragseingängen befindet sich die Elektroindustrie immer noch zwischen 13 und 15 Prozent unterhalb des Niveaus des Vor-Krisen-Jahres 2008. Die Elektroexporte erreichten Ende des vergangenen Jahres allerdings bereits eine Rekordmarke. Mit einem Ausfuhrvolumen von 14 Mrd. Euro exportierte die deutsche Elektroindustrie im November 2010 rund 26 Prozent mehr als im Jahr zuvor. „Noch nie zuvor wurden in einem November höhere Exporterlöse erzielt“, so Dr. Andreas Gontermann, ZVEI-Chefvolkswirt. Dabei machen sich die Branchenexporte nach China mittlerweile mit sieben Prozent der gesamten Elektroexporte bemerkbar. Damit ist China nach Frankreich und USA das drittwichtigste Abnehmerland. 2011 dürfte das Reich der Mitte nach Gontermann die Spitzenposition der Elektroimporteure deutscher Waren einnehmen.

Der Aufschwung wirkt sich auch auf die Beschäftigung aus: In der Krise war die Zahl der Mitarbeiter um 17 000 auf 810 000 gesunken. Zwischenzeitlich sind es bereits wieder 815 000.

ZVEI – ZENTRALVERBAND ELEKTROTECHNIK- UND ELEKTRONIKINDUSTRIE E.V.,
Lyoner Straße 9, D-60528 Frankfurt,
Tel. +49 (0) 69 630 20,
Internet: www.zvei.org

Kolloquium zu Schutzeinrichtungen und funktionaler Sicherheit nach IEC 61508

Zum „Kolloquium Schutzeinrichtungen der Elektrotechnik und funktionale Sicherheit nach IEC 61508“ laden VDE und DKE am 29. März. Die Veranstaltung in Fulda richtet sich an Elektrotechniker und Experten für funktionale Sicherheit.

Bei der Auslegung von Schutzeinrichtungen in der Elektrotechnik wird anders vorgegangen als bei sicherheitsgerichteten Steuerungen („funktionale Sicherheit“). Das Kolloquium legt den Schwerpunkt zum einen auf die Erläuterung dieser unterschiedlichen Vorgehensweisen. Zum anderen beschreibt es die Anwendungskriterien und Abgrenzungen dieser Methoden. Diese sollen in den Workshops herausgearbeitet werden. Beispielsweise wird Ingo Rolle von der DKE zur „Einführung und dem Vergleich der Vorgehensweisen nach IEC Guide 104 und IEC 61508 (VDE 0803)“ sprechen. Die Workshops mit Impulsvorträgen zur Herausarbeitung von Anwendungskriterien und Grenzen der Vorgehensweisen schließen sich um etwa 14 Uhr, nach dem Mittagsimbiss, an.

Die Veranstaltung findet am 29. März von 10 bis 16 Uhr im Hotel Esperanto in Fulda statt. Aktuelle Informationen zur Veranstaltung finden sich unter www.vde.com/kolloquium.

VDE VERBAND DER ELEKTROTECHNIK ELEKTRONIK INFORMATIONSTECHNIK E.V.,
Konferenz Service,
Stresemannallee 15,
D-60596 Frankfurt,
Tel. +49 (0) 69 630 80,
Internet: www.vde.de

VDE-Präsidium stellt sich neu auf

Das VDE Präsidium ist neu gewählt. Dr.-Ing. Joachim Schneider, Mitglied des Vorstands RWE Rheinland Westfalen Netz AG, und Reinhard Clemens, Mitglied des Vorstands Deutsche Telekom AG, sind neue Mitglieder des VDE-Präsidiums. Am 1. Januar 2011 hatte Dipl.-Ing. Alf Henryk Wulf (48) das VDE-Präsidentenamt übernommen. Der Vorstandsvorsitzende der Alcatel-Lucent Deutschland AG ist im Rahmen des VDE-Kongresses „E-Mobility“ in Leipzig für zwei Jahre in das Spitzenamt gewählt worden. Wulf tritt damit die Nachfolge von Dr.-Ing. Joachim Schneider an, der dem ABB-Vorstand angehört.

Schneider ist ab 2011 Stellvertretender VDE-Präsident, ebenso wie sein bereits erwähnter Namensvetter Dr.-Ing. Joachim Schneider (RWE). Wulf begann seine berufliche Laufbahn 1991 bei Alcatel SEL in Stuttgart. Seit 2009 ist Wulf Vorstandsvorsitzender der Alcatel-Lucent Deutschland AG.

VDE VERBAND DER ELEKTROTECHNIK ELEKTRONIK INFORMATIONSTECHNIK E.V.,
Stresemannallee 15, D-60596 Frankfurt,
Tel. +49 (0) 69 630 80, Internet: www.vde.de

… mehr als 1600 Signalkombinationen

Einfach planen, schneller Service – passt sicherlich auch in Ihre Anlage

Der universelle Analogtrennwandler deckt über 1600 Signalkombinationen im Bereich der MSR-Technik ab, somit ist der Anwender für alle Aufgaben im Bereich der analogen Signaltrennung und -wandlung gerüstet.
Das umfangreiche Zulassungspaket sowie Weitbereichsversorgung und schnelle Reaktionszeit prädestinieren ihn für Anwendungen, die mit herkömmlichen Standardtrennern nicht realisierbar sind.

Mehr Informationen unter
Telefon (0 52 35) 3-1 20 00 oder
phoenixcontact.de

PHOENIX CONTACT
INSPIRING INNOVATIONS

Kosten senken mit dem Namur-Standardgerät

Neue Empfehlung definiert Anforderungen, die 80 Prozent der üblichen Anwendungen abdecken

Mit der Namur-Empfehlung NE 131 wird bei den Herstellern die Entwicklung einer Gerätebaureihe „Namur-Standardgerät“ angestoßen, bei der die Geräteeigenschaften auf das notwendige Maß beschränkt und trotzdem 80 Prozent der üblichen Anwendungsfälle abgedeckt sind. Das schafft ein großes Potenzial für Kosteneinsparungen.

Der Kostendruck wächst auch in der chemischen Industrie. Gleichzeitig sollen Prozesssicherheit und Anlagenverfügbarkeit weiter steigen. Darüber hinaus nimmt die Komplexität bei der Planung und dem Betrieb von Anlagen und der darin enthaltenen Messtechnik für die Betreiber, bedingt durch die Vielzahl von Messaufgaben und der dafür verfügbaren Gerätefamilien unterschiedlicher Hersteller, stetig zu. Deswegen sind Konzepte gefragt, die heute und in Zukunft die Komplexität reduzieren und die Anlagenplanung und den Betrieb nachhaltig vereinfachen.

Dafür hat die Namur mit ihrer Empfehlung NE 131 „Standardgerät“ eine wesentliche Voraussetzung geschaffen. Die folgenden drei Auszüge aus dem Text der Empfehlung zeigen die Zielrichtung:

„In der vorliegenden NE wird eine Feldgeräteausstattung vorgestellt, die für rund 80 Prozent der Einsatzfälle geeignet ist. Mit dieser Geräteserie für den normalen oder „Standard“-Anwendungsfall ist der Anspruch der Anwender verbunden, für die üblichen Einsatzfälle nur die tatsächlich benötigte Gerätefunktionalität zu erhalten.“

„Mit der Konzentration auf die wesentlichen Gerätemerkmale für das „Massengeschäft“ und der hierfür geschaffenen Namur-Standardgerätereihe profitieren Hersteller und Anwender. Durch den höheren Standardisierungsgrad wird die Typenvielfalt reduziert und können höhere Stückzahlen erreicht werden. Daraus ergeben sich zusätzliche Potenziale für eine Kostenreduzierung.“

„Die Vorgaben fokussieren auf die Messaufgaben Durchfluss und Stand, da hier die größten wirtschaftlichen Potenziale und auch der größte Handlungsbedarf gesehen werden.“

Die wichtigsten, generellen Vorgaben an die heutige und zukünftige Standard-Feldgerätetechnik lauten: Die Berücksichtigung aller gültigen DIN-Normen, Namur- und VDE/VDI-Empfehlungen sowie die Kosten zu senken und die Sicherheit zu erhöhen mit reduzierter Komplexität durch Einheitlichkeit der Gerätekonzepte. Vor allem die kostensenkende und sichere Zweileiter-Instrumentierung wird für die Zukunft bevorzugt.

Die einfache Wartung durch Komponententausch ohne Datenverlust, mittels modularem Aufbau und einfache Austauschbarkeit von Komponenten durch eine dauerhafte Interoperabilität und eine zuverlässige Geräte- und Prozessdiagnose steht dabei im Fokus.

FELDGERÄTE FÜR STANDARDANWENDUNGEN

Zur Ermittlung der Anforderungen hat die Namur vornehmlich drei Datenquellen genutzt, um die Spezifikation für den Standard-Anwendungsfall ausreichend sicher zu beschreiben: Die Analyse der aktuellen Geräte-Installationen in der Prozessindustrie, Expertenmeinungen von Anwendern und Herstellern sowie Marktstudien.

Bei der Analyse der aktuellen Geräte-Installationen wurde beispielsweise stichprobenartig eine Datenbasis von etwa 800 000 Messstellen-Planungsdaten analysiert. Bei der Marktbefragung unterstützte Endress+Hauser die Namur hinsichtlich der Systematik. Insgesamt ergaben sich bei allen drei Methoden eine gute Überdeckung und vergleichbare Ergebnisse. Damit ist eine sehr hohe Sicherheit für die Spezifikation des Standard-Einsatzfalls

DIE ANFORDERUNGEN DER NE 131 IM ÜBERBLICK

- Deckt 80 Prozent der Anwendungen ab mit reduziertem Leistungsumfang für Standardanwendungen und reduzierten Kosten
- Nach DIN EN 61508 entwickelt, Lambda du 1/200 Jahre
- Ex-Zulassung (Zone 1 Gruppe C Temperaturklasse T4, möglichst Zone 22, Feldbusse nach FISCO-Modell)
- Messunsicherheit unter Referenzbedingungen für gesamten spezifischen Messbereich (Spezifikation gilt für den Ausgang)
- Einfluss Prozessdruck, Prozesstemperatur, Umgebungstemperatur spezifiziert
- Langzeitstabil (max. 2x Messabweichung/5 Jahre)
- Zweileitergerät bevorzugt
- Ausgang: Strom Ex-i passiv HART, Binarausgang Namur IEC 60947-5-6 [5]
- Keine geschirmten Kabel für Analoggeräte, Erdungsmöglichkeit mit externer Erde, Geräteerdung über Potenzialanschluss sichergestellt
- Ausgänge und Versorgung sind galvanisch getrennt
- Kabeleinführung entspricht der Ex-Klassifizierung (kein Ex-d wegen erhöhtem Prüfaufwand)
- Medienberührte Teile sind aus Edelstahl. Europäisch zugelassene Werkstoffe (PAS 1085 [6]) DIN EN 1503-1,3,4), Auskleidungen und Beschichtungen Stand der Technik
- Keine regelmäßigen Wartungen laut BA, die über gesetzliche Auflagen hinausgehen
- Teurere Geräte sind reparierbar und modular aufgebaut
- Beim Austausch von Teilen gehen keine gespeicherten Daten verloren und können einfach übertragen werden
- Zuverlässige Diagnose (Diagnose-Funktionalitäten), ausgeführt nach NE 107
- Daten werden vor Ort anzeigt und sind dort parametrierbar
- Einheitliche Bedienung innerhalb der Gerätefamilien eines Herstellers
- Dauerhafte Interoperabilität mit dem PLS nach NE 105
- Spezifikation des Gerätes nach NE 100, genormte Gerätebeschreibung

Durchflussspezifische Spezifikationen

- Kompaktgerät in Standardausführung
- Einheitliche Einbaulängen nach DVGW oder NE70/132 oder VDI/VDE 3512
- Nennweite DN15...80, Auslegungstemperatur 150 °C, Umgebungstemperatur -25...+60 °C

Messgenauigkeit:

- Coriolis 0,5 Prozent, Magn-Indukt. 0,8 Prozent, Wirbelzähler 1 Prozent, Ultraschall 1 Prozent Inline bzw. 3 Prozent Clamp On
- Wiederholbarkeit 1/2 x Messabweichung

FÜR ERHEBLICHES SPARPOTENZIAL sorgt die Namur-Empfehlung 131 mit der generellen Umsetzung der Zweileitertechnik auch im Bereich der Durchflussmessung, im Bild ein Praxisbeispiel. Pro Messstelle lassen sich so rund 1000 Euro sparen. Bild: Endress+Hauser

Nenngröße	Einbaulänge (mm)	Flanschanschluss (PN)
15	510	40
25	600	40
50	715	40
80	915	40
100	1000/1400	16
150	1200/1700	16
200	1400/2100	16
250	1400/2100	10

DURCH DIE FESTLEGUNG einheitlicher Einbaulängen für Coriolis-Durchflussmessgeräte schafft die NE 131 Planungssicherheit im Rohrleitungsbau und vereinfacht die Reparatur und Ersatzgeräte-Bereitstellung im Anlagenbetrieb. Quelle: NE 132

gegeben. Verwiesen wird in der NE 131 auch auf zahlreiche mitgeltende Namur-Empfehlungen.

Viele der Spezifikationen (siehe Kasten „Die Anforderungen der NE 131 im Überblick“) stellen Grundanforderungen dar, die dem heutigen Stand der Technik entsprechen. Die NE 131 formuliert jedoch in mancher Hinsicht innovative Anforderungen, für die es bisher noch keine technisch hinreichende Umsetzung gab. Beispielsweise die Forderung nach:

- Genereller Umsetzung der Zweileitertechnik auch im Bereich der Durchflussmessung
- Implementierung der NE 107 Gerätediagnose
- Entwicklung der Geräte nach DIN EN 61508
- Sicherstellung einer zukünftigen Interoperabilität von Gerätetreiber und Gerät nach NE 105

Eine weitere wesentliche Neuheit in der NE 132 ist die Definition von einheitlichen Einbaulängen für Coriolis-Massedurchflussmessgeräte, wie sie schon viele Jahre nach DVGW (NE 70) bereits in der Betriebspraxis für magnetisch-induktive und Vortex-Durchflussmessgeräte etabliert sind. Die einheitlichen Einbaulängen schaffen zukünftig Planungssicherheit im Rohrleitungsbau bei Neuanlagen und vereinfachen die Reparatur und Ersatzgeräte-Bereitstellung im Anlagenbetrieb (siehe Tabelle).

Maßstäbe setzt Endress+Hauser bei der Umsetzung der NE 131 mit dem neuen Zweileiterkonzept für Durchfluss und Füllstand. Das Konzept stellt die erste konsequente Umsetzung der genannten Anforderungen in einer einheitlichen Gerätelinie dar. Dabei wurden viele innovative Neuerungen, dem Bedarf der Namur-Chemie entsprechend, umgesetzt. Hierzu zählen:

- Die konsequente Umsetzung der Industriestandards
- Die exakte Geräte- und Prozessdiagnose nach NE 107
- SIL (Safety Integrity Level) – entwickelt nach DIN EN 61508
- Erstes Coriolis-Massedurchflussmessgerät in Zweileitertechnik
- Umsetzung der Namur-Einbaulängen
- Erstes Multiparameter Füllstandmessgerät zur sicheren Trennschichtmessung
- Erstes einheitliches Gerätekonzept für Durchfluss und Füllstand
- Perfekte Einheitlichkeit bei Bedienung, Software, Gehäusekomponenten, Elektronikmodulen, Schnittstellen, Datenmanagement, Systemintegration, Bestellstrukturen und Dokumentation

1000 EURO SPARPOTENZIAL PRO MESSSTELLE

Den Anwendern bieten sich nun neue Möglichkeiten. Mit einer geeigneten Segmentierung von „Standardanwendungen“ sowie speziellen Anforderungen und dem flächendeckenden Einsatz des neuen Gerätekonzepts sind weitreichende Einsparpotenziale umsetzbar. Allein die mögliche Kostensenkung durch die Verwendung von Zweileiter- statt der heutigen Vierleiter-Durchflussmessgeräte wird pro Messstelle mit etwa 1000 Euro beziffert. Einer flächendeckenden Kostensenkungswelle in der Planung und Umsetzung von zukünftiger Feldinstrumentierung steht somit nichts mehr im Wege.

AUTOR

Dipl.-Wirtsch.-Ing. (FH) **CHRISTIAN RÜTZEL** leitet bei Endress+Hauser die Abteilung Marketing Durchflussmesstechnik in Weil am Rhein.

Endress+Hauser Messtechnik GmbH+Co.KG,
Colmarer Str. 6, D-79576 Weil am Rhein,
Tel. +49 (0) 7621 97 59 49,
E-Mail: Christian.Ruetzel@de.endress.com,

Field Device Integration: Der einheitliche Standard rückt in greifbare Nähe

FDI bringt sowohl Endanwendern als auch System- und Geräteherstellern Vereinfachungen

Mit FDI („Field Device Integration“) entsteht der von Endanwendern lange geforderte einheitliche Standard zur Geräteintegration für die Prozessindustrie. Aber auch System- und Gerätehersteller profitieren von FDI. Systemhersteller, die aktuell FDT implementieren, können durch die Nutzung eines FDI-DTMs zu FDI migrieren.

Für Gerätehersteller bietet FDI die Möglichkeit, tatsächlich nur einen einzigen Gerätepräsentanten zu erstellen – nämlich das FDI Device Package. Dieses FDI Package lässt sich dann in „nativen“ FDI-Systemen nutzen aber mittels FDI-DTM eben auch in FDT-basierten Umgebungen. Das bedeutet deutlich weniger Aufwand in Entwicklung, Test und Pflege. Damit erübrigt sich auch die Entwicklung von DTMs seitens der Gerätehersteller.

Geräteintegration stellt für Anwender seit langem eine große Hürde für die umfassende Nutzung der Vorteile und Potenziale intelligenter Feldgeräte dar. Auch neue Kommunikationstechnologien wie etwa wireless HART eröffnen ihre Kundennutzen nur im Rahmen einer reibungslosen Geräteintegration. Um die aktuellen Herausforderungen bei der Geräteintegration zu beheben, wurde im April 2007 die Entwicklung des zukünftigen Standards für die Integration von Feldgeräten „Field Device Integration“ (FDI) gestartet. Um sicherzustellen, dass die Anforderungen der Endanwender in FDI einfließen, wurden Namur und WIB (International Instrument Users‘ Association) in den Prozess mit einbezogen.

DIE FDI-TECHNOLOGIE

Das FDI-Basiskonzept definiert die Komponenten FDI Package, FDI Server und FDI Client (siehe Bild 1). Die Client-Server-Architektur basiert auf OPC UA und nutzt die Vorteile dieser Technologie wie beispielsweise Plattformunabhängigkeit. Gerätehersteller liefern FDI Packages. Sie enthalten alle Informationen, die für eine Geräteintegration notwendig sind. Der FDI Server importiert FDI Device Packages in seinen internen Gerätekatalog. Dies vereinfacht das Versionsmanagement von FDI Packages enorm, da die Verwaltung zentral im FDI Server erfolgt.

Da FDI Packages keine Registrierung im Sinne einer Software-Installation benötigen, gibt es auch keine unangenehmen Nebeneffekte. Die Repräsentation von Geräteinstanzen im FDI Server erfolgt im Informationsmodell. Hier finden sich die Daten, Funktionen und Bedienoberflächen der Geräte. Möchte ein FDI Client mit einem Gerät arbeiten, greift er auf das

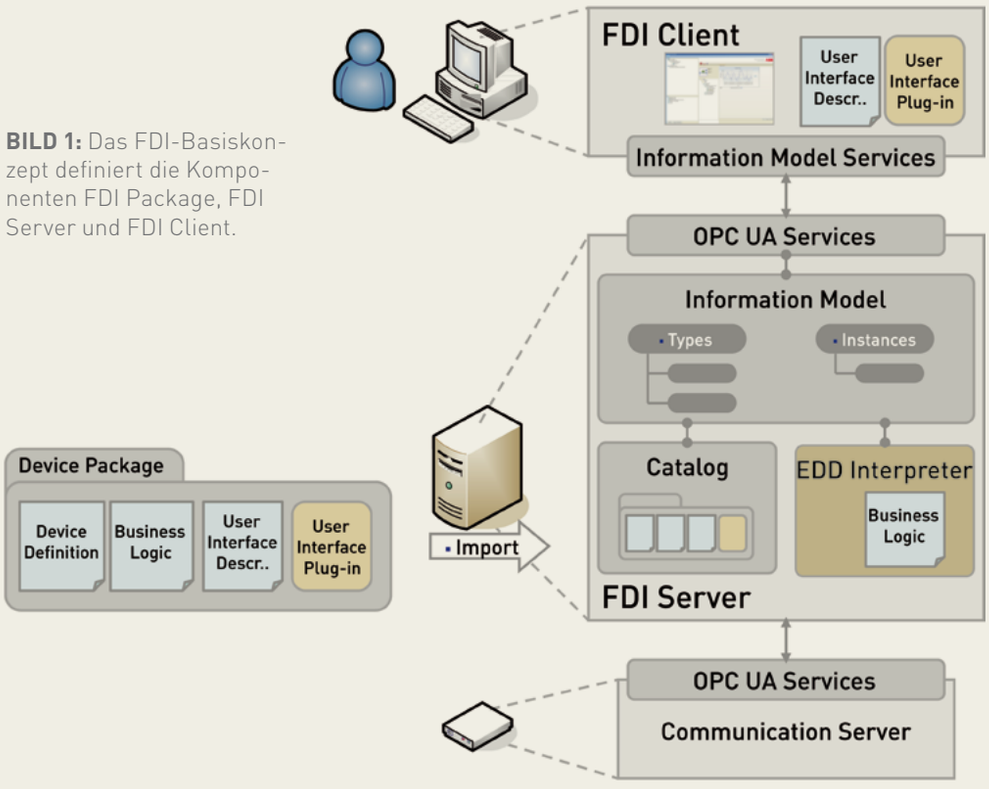


BILD 1: Das FDI-Basiskonzept definiert die Komponenten FDI Package, FDI Server und FDI Client.

Informationsmodell zu und lädt beispielsweise die Bedienoberfläche des Gerätes, um sie vergleichbar mit einem Webbrowser Client-seitig anzuzeigen. Der FDI Server stellt dabei immer sicher, dass der Datenhaushalt des Gerätes konsistent bleibt. Natürlich greifen die Authentifizierungs- und Verschlüsselungsmechanismen von OPC UA, die unerlaubte Zugriffe verhindern.

FDI-FDT-KOMPATIBILITÄT

Durch ein übergreifendes Team aus FDT- und FDI-Experten wurde dafür gesorgt, dass die Interfaces eines FDI UIP (User Interface Plug-in) und eines DTM UI (User Interface Komponente eines DTM) gleich sind. Es finden im Wesentlichen FDT 2.0 Interfaces Wiederverwendung. Damit ist die Voraussetzung dafür geschaffen, dass FDI Packages in zwei Systemarchitekturen verarbeitet werden können: Einem reinen FDI Host (Bild 1) und einem FDT-basierten FDI Host (Bild 2).

In der Architektur „System Y“ verhält sich der FDI-DTM aus Sicht des FDI Packages wie ein FDI Host, zur FDT Rahmenapplikation wie ein DTM. Damit eröffnet sich für viele FDT-Frame-Hersteller ein einfacher und wirtschaftlich attraktiver Migrationsweg nach FDI. Der FDT 2.0 Frame wird unverändert beibehalten und lediglich um einen FDI-DTM ergänzt. FDT wird so zu einem Applikations-Framework für Systemkomponenten wie etwa einen FDI-DTM anstatt eines Framework für eine große Anzahl von unterschiedlichen Geräte-DTMs – Eine Situation, die auch das Handling sehr vereinfacht.

Dabei ist die Erwartung, dass FDI-DTMs wie bereits heute existierende EDD-DTMs auf dem Markt angeboten werden, und somit nicht jeder FDT-Frame-Hersteller die Komponente selbst entwickeln muss.

Die beschriebene Lösung trägt wesentlich zur Verbesserung der Interoperabilität von Host-Systemen und FDI Packages bei:

- Durch den vielfachen Einsatz desselben FDI-DTMs in verschiedenen Host Systemen wird die Anzahl der FDI-Host-Varianten verringert
- Die vom FDI-Projekt bereitgestellte „Standard“-EDD-Engine wird auch im FDI-DTM zum Einsatz kommen

Der aufgezeigte Weg der FDI-FDT-Kompatibilität ermöglicht allen System- und Tool-Herstellern, FDI zu unterstützen, das heißt FDI Packages verarbeiten zu können. Davon werden vor allen Dingen Gerätehersteller profitie-

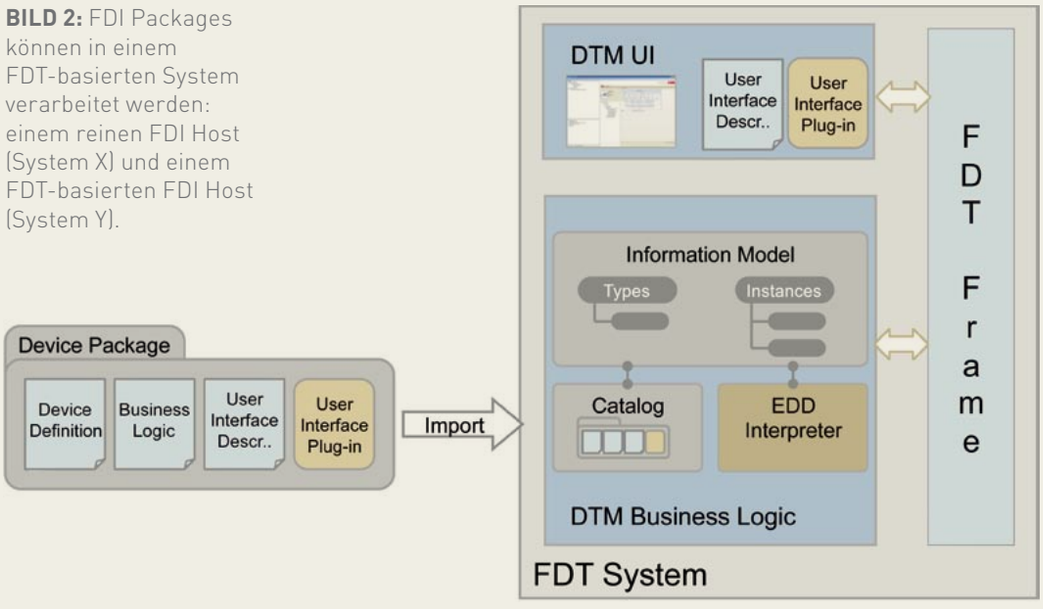


BILD 2: FDI Packages können in einem FDT-basierten System verarbeitet werden: einem reinen FDI Host (System X) und einem FDT-basierten FDI Host (System Y).

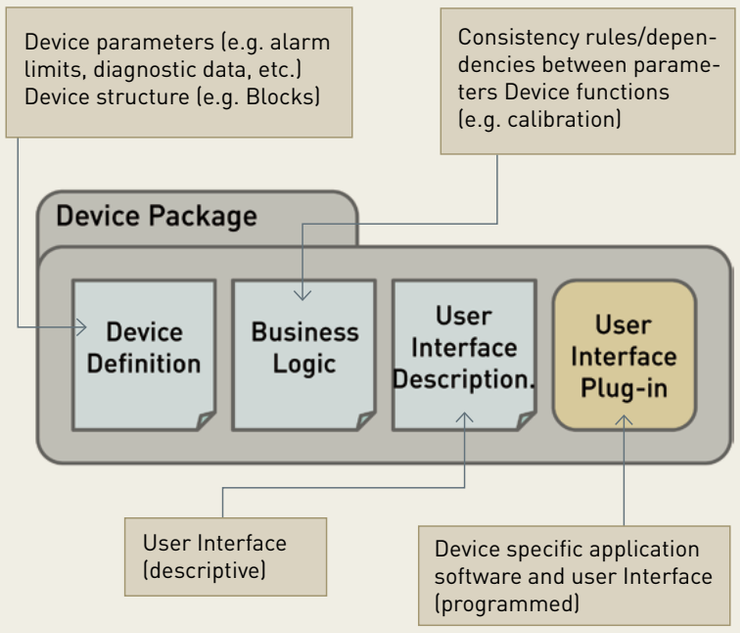


BILD 3: Die Komponenten des FDI Device Packages.

ren, die heute für ein Gerät einen DTM und verschiedene EDD-Varianten bereithalten müssen.

Im Ergebnis werden auch in FDT-2.0-basierten Systemen keine gerätespezifischen DTMs mehr gebraucht. Es genügt, wenn Gerätehersteller FDI Packages liefern. Das führt längerfristig zur Verringerung der Anzahl der Gerätetreiber pro Gerätetyp und damit zu erheblichen Einsparungen in der Produktentwicklung und -pflege.

Nutznießer der verbesserten Interoperabilität und geringen Variantenvielfalt werden letztendlich die Endanwender sein.

FDI PACKAGE – REPRÄSENTANT EINES GERÄTES

In FDI wird ein Gerät mittels eines so genannten FDI Packages repräsentiert. Es ersetzt die vorher verwendeten EDDs und DTMs. Das FDI Package besteht aus mehreren standardisierten Komponenten mit unterschiedlichen Funktionen und stellt sich dem Benutzer lediglich als eine Datei dar. Das vereinfacht den Umgang mit dem FDI Package erheblich.

Neben dem den Paketinhalt beschreibenden Katalog und den so genannten Attachments zur Bereitstellung von Gerätedokumentation oder Integrationsdateien (wie GSD, CFF) besteht das FDI Device Package aus den im Folgenden beschriebenen Komponenten (Bild 3).

Die EDD beschreibt drei logische Bestandteile des FDI Packages. In der Gerätedefinition (DEF) werden die Parameter des Gerätes, deren Abhängigkeiten voneinander, sowie die hierarchische Struktur der Geräteparameter dargestellt. Die User Interface Description (UID) erlaubt eine Beschreibung einer Bedienoberfläche, ähnlich der HTML-Technologie in der Internet-Welt. Die Business Logic (BL) stellt die Datenintegrität der Gerätedaten sicher und reagiert aktiv auf Parameteränderungen. Auch die so genannte „Nested Communication“, die „Übersetzung“ von Kommunikationsanfragen in verschiedene Protokolle wird von der Business Logic umgesetzt.

Das User Interface Plug-in (UIP) findet seine Anwendung für komplexe Berechnungen von Parameterwerten oder aufwendige Benutzeroberflächen zur Evaluierung von Eingabedaten, die sich nicht mit Mitteln der EDDL umsetzen lassen. Ein FDI Package kann mehrere UIPs enthalten.

Das Gerät kann also mit deskriptiven (EDDL) oder programmatischen Mitteln (User Interface Plug-in) beschrieben werden. Dieser Ansatz ermöglicht volle Skalierbarkeit der Geräteintegration und Gerätemanagement-Lösung sowie die Möglichkeit, alle Gerätefunktionen bedienen zu können. Für einfachste Geräte enthält das FDI Device Package lediglich die EDD. Sehr komplexe Geräte hingegen enthalten darüber hinaus noch mehrere User Interface Plug-ins.

VORHANDENE LÖSUNGEN SIND WIEDERVERWENDBAR

Die Tatsache, dass sowohl die EDDL, als auch FDT in FDI ein neues zu Hause gefunden haben, gestaltet die Migration existierender EDD- und DTM-Lösungen für den Gerätehersteller denkbar einfach. Gerätehersteller haben in der Majorität ohnehin bislang beide Geräteintegrationstechnologien in verschiedenen Varianten

für jeden Gerätetyp implementieren müssen, um dem Endbenutzer eine Verwendung des Gerätes in allen Systemen zu ermöglichen. Insofern können die existierende EDD und Algorithmen, sowie grafische Controls als Basis für ein FDI Package wiederverwendet werden. Das ermöglicht eine kostengünstige Entwicklung und zeitnahe Verfügbarkeit von FDI Packages auch für bereits am Markt eingeführte Gerätetypen ohne aufwendige, vollständige Neuentwicklung.

Darüber hinaus werden FDI Packages – wie oben beschrieben – in zukünftigen FDT-2.0-Systemen verwendbar sein. Diese Eigenschaften und Leistungsmerkmale von FDI lassen in eine klar strukturierte und für den Endanwender einfacher zu verstehende Geräteintegrationszukunft blicken.

AUTOREN

DANIEL GROSSMANN,
Research Area Coordinator

ABB AG, FORSCHUNGSZENTRUM,
Wallstadter Str. 59 ,
D-68526 Ladenburg,
Tel. +49 (0) 6203 71 62 41
E-Mail:
daniel.grossmann@de.abb.com

ALEXANDER KAISER,
Global Product Manager
Fieldbus&Tools

ABB Automation Products GmbH,
Schillerstraße 72,
D-32425 Minden,
Tel. +49 (0) 571 830 15 11
E-Mail:
alexander.kaiser@de.abb.com

ACHIM LAUBENSTEIN,
Manager Fieldbus
Standardization

ABB Automation GmbH,
Schillerstraße 72,
D-32425 Minden,
Tel. +49 (0) 571 830 84 71
E-Mail:
achim.laubenstein@de.abb.com

Dynamische Simulation optimiert Erdgasverflüssigung

Verbesserungen von der Prozessauslegung bis zur täglichen Optimierung des Anlagenbetriebs

Die dynamische Simulation kann über den gesamten Lebenszyklus von Anlagen zur Herstellung von Flüssigerdgas (LNG, Liquefied Natural Gas) beträchtlichen Mehrwert generieren. Sie hilft, die Auslegung zu prüfen und zu verfeinern, das Leitsystem vor dem Anfahren virtuell in Betrieb zu nehmen, das Betriebspersonal vor und nach der Inbetriebnahme zu schulen, Betriebsprobleme zu beheben und vorgeschlagene Änderungen im Anlagenbetrieb vor der Umsetzung zu validieren.

LNG-Betriebe mit Kältemittelgemischen können besonders vom Einsatz des UniSim Design-Moduls zum spiralförmig gewickelten Rohrbündel profitieren. Dieses Modul wurde als integraler Funktionsbestandteil der dynamischen Simulation von UniSim Design entwickelt. Das Modell berechnet die Axialtemperatur, Dampffraktion und Druckprofile für jeden Rohrstrang, den Mantelstrang sowie die Axial- und Radialtemperatur-Profile für die Rohrwände, die Mantelwand und die Isolierung. Die Technologie hat sich bereits in zahlreichen dynamischen Simulationsstudien und Operator-Schulungssystemen bewährt. Eingesetzt wurde sie beispielsweise bei der Straße 3 der Ras Laffan LNG-Anlage in Katar.

HAUPTWÄRMETAUSCHER BILDET DAS KERNSTÜCK

Der Hauptwärmeaustauscher (MHE, Main Heat Exchanger), ein spiralförmig gewickelter kryogener Wärmeaustauscher mit mehreren Rohren, ist das Kernstück der Wärmeübertragungseinrichtung in Verflüssigungszyklen mit Kältemittelgemischen für die Erzeugung von Flüssigerdgas (Crawford and Eschenbrenner, 1972). Wie in Bild 1 dargestellt werden mehrere Schichten Rohre auf die Spindel gewickelt und mit Abstandshaltern (wie Stäbe oder Draht) versehen.

Für große, in Flüssigerdgas-Anlagen eingesetzte Wärmeaustauscher liegen die Rohrdurchmesser zwischen $^3/_8$ bis $^3/_4$ Zoll (etwa 1-2 cm), und die Rohre werden mit einem Wicklungswinkel von etwa 10 Grad auf die Spindel gewickelt. Die Rohre werden an jedem Ende des Wärmeaustauschers mit Rohrblechen verbunden, und jede Schicht enthält Rohre aus allen Strängen, so dass die Mantelseite gleichmäßig ausgelastet ist. Der Wärmeaustauscher arbeitet im vollständigen Gegenstrom, wobei die entlang der Mantelseite nach unten fließende Flüssigkeit verdampft und die unter Hochdruck stehende, kondensierende Flüssigkeit entlang der Rohrseite nach oben fließt.

Für die Mehrfachbündel-Austauscher, die während des Erdgas-Verflüssigungsprozesses eingesetzt werden, sind die Bündel in einem einzigen Gehäuse untergebracht. Zusätzlich gibt es für jedes Bündel innerhalb dieser Spindel einen Behälter, um die Flüssigphase des Kältemittels über die Ringe im Gehäuse des Rohrbündels zu sammeln und weiter zu verteilen.

VEREINFACHUNG WIRD DER DYNAMIK NICHT GERECHT

Aus der Prozessbeschreibung ist klar ersichtlich, dass das Grundelement für die Modellierung des Hauptwärmeaustauschers ein spiralförmig gewickeltes Wärmeaustauscher-Bündel aus Rohren und Gehäusen mit mehreren Strängen und einem einzigen Mantelstrang ist. Obwohl in zahlreichen Veröffentlichungen und Vorträgen die Modellierung von Erdgas-Verflüssigungsprozessen auf qualitativer Basis diskutiert wurde, gibt es nur wenige, die die Modellierung dieser Prozesse, vor allem die Modellierung des Hauptwärmeaustauschers, nach quantitativen Gesichtspunkten behandeln.

Ein vereinfachtes Modell eines spiralförmig gewickelten Rohrbündels wird nicht das erwartete dynamische Verhalten des Prozesses über alle Betriebsbereiche vorberechnen können. Hierfür ist eine umfassende dynamische Simulation erforderlich. Beispielsweise wird ein vereinfachtes Modell die Dynamik beim Anfahren nicht genau vorhersagen, wenn beim ersten Anfahren die volumetrische Kapazität den Ladevorgang des Kältemittels beeinflusst und die Kompressoransaugbedingungen durch die Versorgung mit dem Kältemittel als eine Funktion der Wärmeaustauscher-Aufgaben beeinflusst werden. Ebenso führt eine vereinfachte Modellierung von Wärmeaustauschern zu irrationalen Temperaturprofilen mit Überschneidungen an Segmentgrenzen und zwischen einzelnen Rohr- und Mantelsträngen.

DYNAMISCHES MODELL BIETET FUNDIERTE AUSSAGEN

Daher wurde in UniSim Design als dynamisches Modell der Einrichtung ein mathematisches Basismodell

BILD 1: Der Hauptwärmeaustauscher, ein spiralförmig gewickelter kryogener Wärmeaustauscher mit mehreren Rohren, ist das Kernstück der Wärmeübertragungseinrichtung in Verflüssigungszyklen mit Kältemittelgemischen für die Erzeugung von Flüssigerdgas. Skizze nach Fredheim und Fuchs, 1990

mit genauen Berechnungen der physikalischen Eigenschaften und thermodynamischen Entspannungspunkte für das Rohrbündel eines spiralförmig gewickelten Wärmeaustauschers erstellt. Dieses Grundelement, das so genannte spiralförmig gewickelte Rohrbündelmodul, wurde in einem Fließbild zusammen mit den Standardmodellen von UniSim Design eingesetzt und spiegelte das Verhalten in Erdgas-Verflüssigungsprozessen mit der Genauigkeit, Zuverlässigkeit und Robustheit wider, die erforderlich sind, um aussagekräftige Ergebnisse für die Prozessvorgänge zu erzielen, wie sie für dynamische Simulationsstudien und eine simulationsgestützte Schulung von Anlagenbedienern typisch sind.

Das spiralförmig gewickelte Rohrbündelmodul errechnet die folgenden Parameter in Relation zur Zeit und in Bezug auf Änderungen des Durchflusses, der Temperatur, des Drucks und der Zusammensetzung der eingehenden Stränge sowie der Umgebungstemperatur.

- Austrittsmenge, Temperatur, Druck, Dampffraktion und Zusammensetzung für jeden Ausgangsstrang
- Phasenveränderungen in jedem einzelnen Rohrstrang und im Mantelstrang
- Temperaturen der Rohr- und Mantelwände
- Zwischentemperaturen entlang des Wärmeaustauschers und
- die Wärmeprofile in der Mantelwand und der Isolierung

Bild 2 zeigt einen Bildschirmausschnitt mit den Standardsichten des spiralförmig gewickelten Rohrbündelmoduls bei UniSim Design und vermittelt einen Eindruck der detaillierten Auslegung des Modells.

ABWÄGEN ZWISCHEN GENAUIGKEIT UND TEMPO

Bei dynamischen Simulationen mit großem Umfang, in Echtzeit oder schneller, die typisch für dynamische Studien und simulationsgestützte Schulungen für Anlagenfahrer sind, sind Genauigkeit und Berechnungsgeschwindigkeit stets konkurrierende Ziele. Um ein Gleichgewicht zwischen diesen Zielen zu erreichen, wurden bei der Formulierung des mathematischen Modells vereinfachende Hypothesen wie die Verwendung einer repräsentativen Rohrwicklung für jeden Rohrstrang und die Zusammenführung der Außenringe auf der Mantelseite in einen einzigen Mantelstrang aufgestellt.

Die Modellformulierung beinhaltet ein axial verteiltes Modell für die Materialströme in den verschiedenen Rohrsträngen und dem Mantelstrang sowie ein axial und radial verteiltes Modell für den Wärmefluss durch die Rohrwände, die Mantelwand und die Isolierung. Um Phasenveränderungen in den Rohrsträngen und im Mantelstrang vorauszusagen, umfasst das Modell für die Materialströme einen isobarisch-isenthalpischen (PH) Entspannungspunkt an jedem Rasterpunkt.

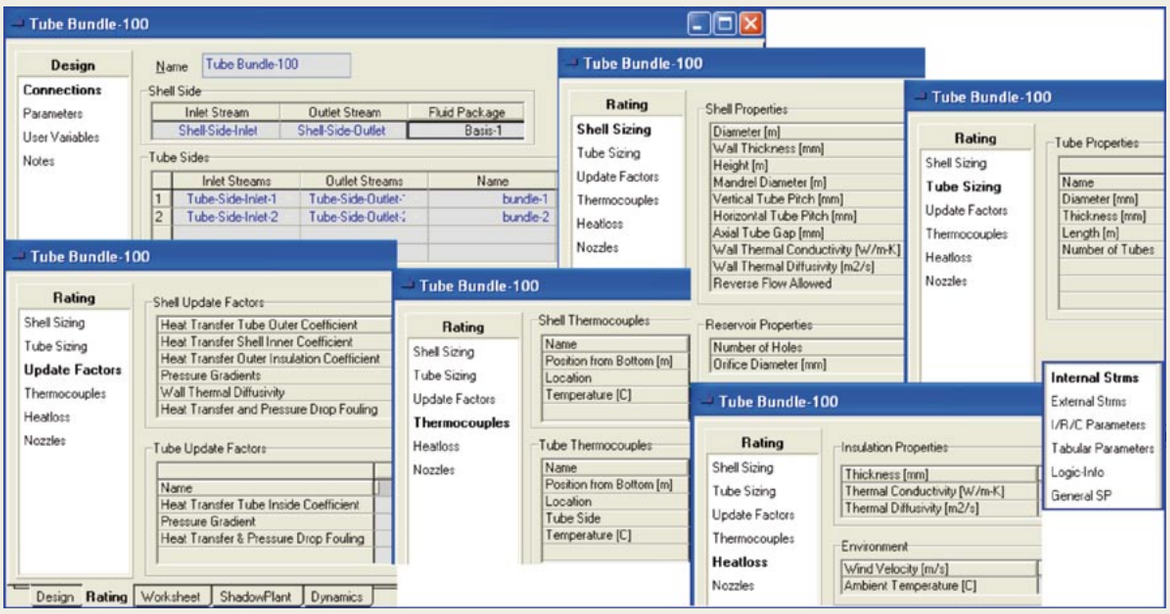


BILD 2: Der Bildschirmausschnitt mit den Standardsichten des spiralförmig gewickelten Rohrbündelmoduls bei UniSim Design vermittelt einen Eindruck der detaillierten Auslegung des Modells. Bild: Honeywell

Die Lösung eines räumlich verteilten Modells mit Entspannungspunkt-Berechnungen für eine Gegenstrom-Durchfluss-Konfiguration bei Mehrfachrohrsträngen ist aus rechnerischer Perspektive eine Herausforderung, was Stabilität, Robustheit und Geschwindigkeit anbelangt. Die Stabilität der Lösung wird durch die Anwendung der gleichungsorientierten Lösungsarchitektur erreicht, die alle Modellierungsgleichungen für die Grundoperation gleichzeitig löst.

ROBUST UND SCHNELL

Robustheit und Rechengeschwindigkeit werden berücksichtigt, indem man die stark nicht-linearen PH-Entspannungsgleichungen durch die Erweiterungen der Taylor-Reihen erster Ordnung ersetzt. Deren Koeffizienten werden ausnahmsweise aktualisiert, während sich die Lösung durch den Betriebsraum bewegt. Zusätzlich errechnet ein Mehrschichtenraster für diese Prozessströme einige Mengen auf einem groben Raster und projiziert diese Werte anschließend auf ein feineres Lösungsraster.

Die für das spiralförmig gewickelte Rohrbündel verwendete Modellformulierung und Lösungsmethodik wurde bereits erfolgreich in dynamischen Simulationsmodellen in mehr als zehn Erdgas-Verflüssigungsanlagen eingesetzt (Henderson et al., 2004).

VORTEILE BEREITS IN DER AUSLEGUNGSPHASE

In der Auslegungsphase können dynamische Simulationsmodelle dazu beitragen, Handhabungs- und Regelungsprobleme zu erkennen und die Auslegung zu optimieren. Sie sind wertvolle Instrumente für die Auslegung, Prüfung und Feinabstimmung der Regelungsstrategien vor der Inbetriebnahme. Sie können außerdem dafür eingesetzt werden, um Diskrepanzen auszugleichen zwischen einer optimalen statischen Auslegung, die auf minimale Investitionsausgaben und Betriebskosten ausgerichtet ist, und dem dynamischen Prozessbetrieb. Des Weiteren helfen derartige Modelle häufig bei der Entwicklung von Betriebsabläufen. Jedoch ist der Einsatz von dynamischen Modellen für die Schulung von Anlagenfahrern vor der Inbetriebnahme die weitaus bekannteste Anwendung einer dynamischen Simulation (Tang and Stephenson, 1997).

Sobald eine Anlage in Betrieb genommen ist, können dynamische Simulationsmodelle dazu beitragen, den Betrieb täglich zu verbessern. Die dynamischen Modelle erlauben es den Prozessingenieuren und Anlagenfahrern, Fallstudien durchzuführen, die Auswirkungen von möglichen Änderungen des Ausgangsmaterials, der Betriebsbedingungen, Regelungsstrategien oder Betriebsabläufen zu überprüfen und Schwierigkeiten, die während des Anlagenbetriebs auftreten, zu beheben.

MODELLE FÜR DIE STÄNDIGE AUSBILDUNG

Parallel dazu können dynamische Modelle, die vor der Inbetriebnahme einer Anlage für die Schulung des Bedienpersonals eingesetzt werden, zu „As-built"-Modellen aktualisiert und für die ständige Ausbildung verwendet werden (Stephenson et al., 2009). Auswertungen haben gezeigt, dass etwa 90 Prozent aller Störfälle in Anlagen vermeidbar sind und die Mehrheit der Störfälle – nach einigen Schätzungen die große Mehrheit – auf menschliche Fehlbedienung zurückgehen. Daher trägt eine kontinuierliche Schulung des Anlagenpersonals dazu bei, einen sicheren, zuverlässigen und effizienten Anlagenbetrieb zu gewährleisten.

AUTOREN

WGRANT STEPHENSON,
ist Engineering Fellow und Global Simulation Architect bei Honeywell Process Solutions Canada.

Honeywell Process Solutions
Suite 300 Wellington Square, 250 York Street
London, ON, Canada, N6A 6K2
Tel. +519 640 66 18
E-Mail: grant.stephenson@honeywell.com

LITERATURHINWEISE

Crawford, D.B., and G.P. Eschenbrenner, „Heat Transfer Equipment for LNG Projects", Chem. Eng. Prog., 68(9), 62 (1972).
Fredheim, A., and P. Fuchs, „Thermal Design of LNG Heat Exchangers", in Proc. European Applied Research Conference on Natural Gas (Eurogas '90), Trondheim, Norway, 567 (1990).
Henderson, P., H. Schindler and A. Pekediz, „Dynamic Simulation Studies Help Ensure Safety by Conforming Operational Readiness of LNG Plant Assets", AIChE Spring Conference, New Orleans (2004).
Stephenson, G., P. Henderson and H. Schindler, „Profit More from Process Simulation," Chemical Processing, August (2009).
Tang, A.K.C. and G. Stephenson, „LNG Plant Operator Training," Petroleum Technology Quarterly, Autumn (1997).

NEU-ERSCHEINUNG

ISO 26000 in der Praxis

DER RATGEBER ZUM LEITFADEN FÜR SOZIALE VERANTWORTUNG UND NACHHALTIGKEIT

Eine Norm zur Verbesserung der Welt?
Nein, die ISO 26000 ist ein Leitfaden – nicht mehr aber auch nicht weniger!

Auch wenn die ISO 26000 keine zertifizierbare Managementsystem-Norm und die Anwendung freiwillig ist, wird ihre Tragweite für Unternehmen beträchtlich sein. Denn sie ist ein Leitfaden, der anhand von beispielhaften Verhaltensregeln (Best Practices) Orientierung gibt, wie sich Organisationen verhalten sollten, damit sie nach internationalem Verständnis als gesellschaftlich verantwortungsvoll angesehen werden. Er stimmt sowohl mit den Richtlinien der Vereinten Nationen UN als auch mit den Richtlinien der internationalen Arbeitsorganisation ILO überein. Im besonderen Fokus dieses höchst aktuellen Ratgebers steht das Wirtschaftsleben im Zeitalter der Globalisierung.

Hrsg.: K.-C. Bay
1. Auflage 2010, ca. 200 Seiten, Hardcover

Oldenbourg Industrieverlag München
www.oldenbourg-industrieverlag.de

SOFORTANFORDERUNG PER FAX: +49 (0)201 / 82002-34 oder im Fensterumschlag einsenden

Ja, ich bestelle ☐ gegen Rechnung ☐ 3 Wochen zur Ansicht

___Ex. ISO 26000 in der Praxis
1. Auflage 2010 – ISBN: 978-3-8356-3222-6
für € 49,90 (zzgl. Versand)

Die bequeme und sichere Bezahlung per Bankabbuchung wird mit einer Gutschrift von € 3,- auf die erste Rechnung belohnt.

Antwort
Vulkan Verlag GmbH
Versandbuchhandlung
Postfach 10 39 62
45039 Essen

Firma/Institution

Vorname, Name des Empfängers

Straße/Postfach, Nr.

PLZ, Ort

Telefon Telefax

E-Mail

Branche/Wirtschaftszweig

Bevorzugte Zahlungsweise ☐ Bankabbuchung ☐ Rechnung

Bank, Ort

Bankleitzahl Kontonummer

✘
Datum, Unterschrift PAISO12010

Widerrufsrecht: Sie können Ihre Vertragserklärung innerhalb von zwei Wochen ohne Angabe von Gründen in Textform (z.B. Brief, Fax, E-Mail) oder durch Rücksendung der Sache widerrufen. Die Frist beginnt nach Erhalt dieser Belehrung in Textform. Zur Wahrung der Widerrufsfrist genügt die rechtzeitige Absendung des Widerrufs oder der Sache an die Vulkan-Verlag GmbH, Versandbuchhandlung, Huyssenallee 52-56, 45128 Essen.

Nutzung personenbezogener Daten: Für die Auftragsabwicklung und zur Pflege der laufenden Kommunikation werden personenbezogene Daten erfasst und gespeichert. Mit dieser Anforderung erkläre ich mich damit einverstanden, dass ich vom Oldenbourg Industrieverlag oder vom Vulkan-Verlag ☐per Post, ☐per Telefon, ☐per Telefax, ☐per E-Mail, ☐nicht über interessante, fachspezifische Medienund Informationsangebote informiert und beworben werde. Diese Erklärung kann ich mit Wirkung für die Zukunft jederzeit widerrufen.

Optimale Sicherheit und maximale Anlagenverfügbarkeit

Funktionale Sicherheit ohne Kompromisse muss den gesamten Safety-Lifecycle einbeziehen

Bei funktionaler Sicherheit ist weitaus mehr als der Einsatz zertifizierter Komponenten zu berücksichtigen. Das stellten Steffen Philipp und Thomas Hinzmann bei der Namur-Hauptsitzung in ihrem Eröffnungsreferat „Funktionale Sicherheit ohne Kompromisse“ heraus. Philipp ist geschäftsführender Gesellschafter, Hinzmann Bereichsleiter Vertrieb Prozessautomation und Service bei Hima, dem Hauptsponsor der Veranstaltung. Sie sind auch Autoren dieses Beitrags.

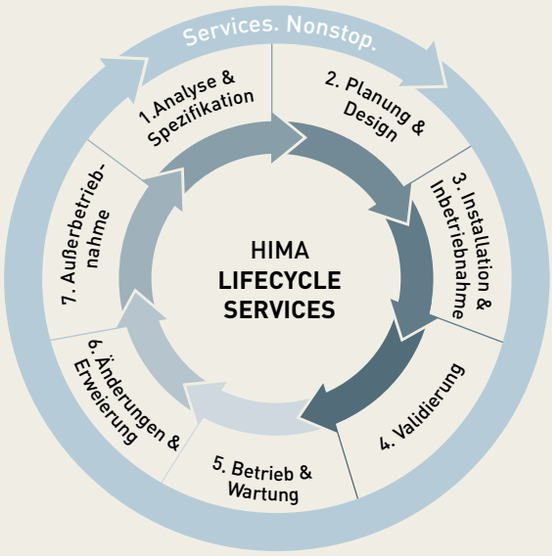
Vielmehr, so unterstrichen Philipp und Hinzmann, ist der gesamte Safety-Lifecycle, der Faktor Mensch als größte Fehlerquelle und eine intelligente Integration der Sicherheitslösung in die Automatisierungsumgebung zu betrachten. Und dies alles ohne Kompromisse hinsichtlich der Anlagenverfügbarkeit und Wirtschaftlichkeit.

Die beste Technik nutzt nichts, wenn der Faktor Mensch nicht „funktioniert“. In einer Analyse der Europäischen Kommission wurden alle seit 1982 gemeldeten Störfälle in der chemischen Industrie auf ihre Ursachen untersucht. Bei über 90 Prozent der Störfälle sind organisatorische Fehler die Hauptfehlerquelle. Mit anderen Worten: Sie sind auf den Faktor Mensch zurückzuführen.

HERAUSFORDERUNGEN BEI DER IMPLEMENTIERUNG

Anwender sind bei der Implementierung von funktionaler Sicherheit mit verschiedenen Herausforderungen konfrontiert:

1 | Die Anlagensicherheit muss zu jedem Zeitpunkt sichergestellt sein.
2 | Die Sicherheitstechnik verdient als kritischste Prozesstechnik besondere Aufmerksamkeit, obwohl sie im täglichen Einsatz am wenigsten vom Bedienpersonal verwendet wird.
3 | Für einen wirtschaftlichen Betrieb muss eine maximale Verfügbarkeit der Anlagen sichergestellt sein.
4 | Sicherheits-Expertenwissen ist auf Prozessanlagen- und Lieferantenseite erforderlich.
5 | Die steigende Komplexität verfahrenstechnischer Prozesse, auch durch die zunehmende Mikrosegmentierung, betrifft auch die Sicherheitstechnik.
6 | Im Hinblick auf einen optimierten CAPEX sollen Unter- oder Überdimensionierungen vermieden werden.



DER EINSATZ ZERTIFIZIERTER KOMPONENTEN allein garantiert noch keine Sicherheit. Es gilt vielmehr, den gesamten Safety-Lifecycle zu betrachten und auch den Faktor Mensch ausreichend zu berücksichtigen. Quelle: Hima

Die internationalen Normen IEC 61508 und IEC 61511 definieren Standards zur Realisierung von funktionaler Sicherheit. Dabei dient die IEC 61508 als Vorlage für die Sektornormen aller Industrien, während die IEC 61511 als Sektornorm die Umsetzung der funktionalen Sicherheit für die Prozessindustrie beschreibt. Warum fällt es trotz dieser Normen vielen Unternehmen schwer, Sicherheit in ihren Anlagen zu implementieren? Die Antwort ist eindeutig: Weil es oft keine Systemfrage ist, sondern eine Frage der Sicherheitskultur in den Unternehmen.

SAFETY-LIFECYCLE-ANSATZ

Die IEC 61511 beinhaltet als wesentlichen Bestandteil den Safety-Lifecycle, der sich in die drei Bereiche Analyse, Realisierung und Betrieb aufteilen lässt. Die Tätigkeiten im Rahmen des Safety-Lifecycle werden flankiert von zwei weiteren wichtigen Bereichen: dem Aufbau und der Planung des Safety-Lifecycles sowie von der Verifikation, für die stellvertretend das Vier-Augen-Prinzip steht. Ein Managementsystem zur funktionalen Sicherheit bildet den Gesamtrahmen. Die Seveso-II-Richtlinie der EU schreibt vor, dass in Prozessanlagen ein Functional Safety Management System (FSM) zu implementieren ist. In Deutschland beschreibt die Störfallverordnung (12. BImSchV), wie dies umzusetzen ist.

FSM-Systeme werden in Unternehmen eingeführt, um klare Prozesse zu beschreiben und Verantwortlichkeiten zu definieren. Die Umsetzung eines solchen Systems ist ein komplexer Vorgang und erfordert umfangreiche Erfahrung. Sie beginnt mit einem minutiösen Vergleich vorhandener Qualitätsmanagement-Maßnahmen mit den Anforderungen aus den IEC-Normen. Anschließend wird im Rahmen einer Gap-Analyse der Erfüllungsgrad der definierten Anforderungen ermittelt und Abweichungen werden aufgezeigt. Durch Anpassung wird die Konformität zu den geforderten Regelwerken schließlich erreicht.

Zertifizierungen nach IEC 61508 und IEC 61511 mögen Sicherheit vermitteln, in den letzten Jahren gab es aber Negativbeispiele, die an den Zertifikaten zweifeln ließen. Das „Spiel mit den Zahlen“ war offenbar für einige Hersteller so verlockend, dass sie im Zusammenhang mit der Safe Failure Fraction (SFF) ihre Geräte in die nächsthöhere SIL-Kategorie gehoben haben, indem sie die Zahl

der sicheren Fehler „unnötigerweise“ erhöhen. Solchen „Zahlenspielereien“ hat die Normierung einen Riegel vorgeschoben, doch Geräte mit solchen Zertifikaten sind auf dem Markt. Ein Zertifikat allein macht also nicht sicher. Genaues Hinschauen hilft hier – und auch bei weiteren Themen der Zertifizierung wie Haftungsausschlüsse der zertifizierenden Stelle, Verwendung unterschiedlicher Tabellen für die Ausfallraten, Auflagen im Sicherheitshandbuch, die die Verantwortung für die sichere Funktion des Systems auf den Anwender übertragen.

Anlagenverfügbarkeit wird nicht allein durch einfach oder mehrfach redundante Systemtechniken erzielt. Sicherheitslösungen sollten ohne Einschränkung der Sicherheit einen unterbrechungsfreien Anlagenbetrieb, auch bei Modifikationen und Wartungsarbeiten, gewährleisten. Da die Sicherheitstechnik nicht täglich im Gebrauch ist, trägt ein intelligentes Design zur Fehlervermeidung entscheidend bei. Die Technik muss für die Anwender intuitiv und selbsterklärend sein. Das beginnt mit einem minimierten Planungsaufwand und setzt sich fort über eine einfache Verschaltung der Systemarchitektur, eine minimierte Redundanzverwaltung bis hin zu einfachster Handhabung und einer graduierten Diagnostik.

INTEGRATION DURCH ÜBERGREIFENDE STANDARDS

Bei der Integration der Schutzeinrichtung in die Betriebseinrichtung sollte darauf geachtet werden, dass die Einkaufsstrategie keine negativen Auswirkungen auf die Sicherheitsstrategie hat. Werden MAC/MIV-Konzepte (Main Automation Contractor/Main Instrument Vendor) vom Einkauf favorisiert und Betriebs- und Schutzeinrichtung von dem selben Lieferanten bezogen, sind folgende Aspekte zu berücksichtigen.

Der Betreiber hat über Jahre Prozesse etabliert, die zur Vermeidung systematischer Fehler beitragen. Die resultierende Qualität ist Garant für störungsfreien und risikoarmen Anlagenbetrieb. Wird bei der Planung einer neuen Anlage das gesamte Projekt an einen MAC übertragen, besteht die Gefahr, dass aus Kostengründen die Neuanlage zwar normkonform (hier ist jedoch ein Interpretationsspielraum der Norm zu berücksichtigen) aber dennoch mit anderer Qualität vom MAC umgesetzt wird.

Schutzeinrichtungen (sicherheitsrelevante Aufgaben) und Betriebseinrichtungen (nicht sicherheitsrelevante Aufgaben) werden im Rahmen der Gesamtautomatisierung als Schutzebenen betrachtet. DIN EN 61511 fordert hinreichende Unabhängigkeit dieser Einrichtungen. Die Störfallverordnung geht noch weiter und fordert, dass der Betreiber die Anlagen des Betriebsbereichs mit zuverlässigen Messeinrichtungen und Steuer- oder Regeleinrichtungen auszustatten hat, die voneinander unabhängig sind. Diese Unabhängigkeit von Betriebs- und Schutzeinrichtung reduziert das Risiko systematischer Fehler und sogenannter Human-Common-Cause-Fehler. Des Weiteren haben die häufig notwendigen Modifikationen der Betriebseinrichtung keinen Einfluss auf die Sicherheitseinrichtungen.

Derselbe Ansatz „Unabhängigkeit der Schutzebenen“ findet sich auch beim aktuellen Thema Security. Die „Last Line of Defense“ wird am besten durch ein mehrstufiges, unabhängiges Abwehrsystem sichergestellt. Der jüngste Virenangriff machte deutlich, dass Unabhängigkeit zwischen Betriebs- und Schutzeinrichtung wichtig ist, um größere Schäden zu vermeiden. Am klarsten ist diese Unabhängigkeit darzustellen, wenn Betriebs- und Schutzeinrichtung auf unterschiedlichen Plattformen, Entwicklungsgrundlagen und Philosophien basieren. Optimale Voraussetzung: Sie kommen von verschiedenen Herstellern.

FAZIT

Funktionale Sicherheit ist „missionskritisch“, erfordert ausgewiesenes Expertenwissen und muss nach dem aktuellsten Stand der Technik instrumentiert werden. Neueste Lösungen maximieren die Anlagenverfügbarkeit ohne Kompromisse bei der Sicherheit. Um die Sicherheitsstrategien der Anlagenbetreiber darstellen zu können, sollten die Sicherheitslösungen unabhängig von der Wahl des Prozessleitsystems spezifiziert und ausgewählt werden. Eine Integration auf Basis offener, herstellerübergreifender Kommunikationsstandards ist eine Lösung ohne Kompromisse hinsichtlich funktionaler Sicherheit und Security und schafft dabei eine hohe Investitionssicherheit.

AUTOREN

STEFFEN PHILIPP, ist geschäftsführender Gesellschafter der Hima Paul Hildebrandt GmbH + Co KG

HIMA Paul Hildebrandt GmbH + Co KG,
Albert-Bassermann-Strasse 28,
D- 68782 Brühl,
Tel. +49 (0) 6202 70 90,
E-Mail: info@hima.com

THOMAS HINZMANN ist Bereichsleiter Vertrieb Prozessautomation und Service der Hima Paul Hildebrandt GmbH + Co KG

HIMA Paul Hildebrandt GmbH + Co KG,
Albert-Bassermann-Strasse 28,
D- 68782 Brühl,
Tel. +49 (0) 6202 70 90,
E-Mail: info@hima.com

Funktionale Sicherheit elektrotechnischer Komponenten

Ein Leitfaden für Anwender

Die wichtigste Aufgabe für die Elektrotechnik bezüglich funktionaler Sicherheit ist die sicherheitsgerichtete Abschaltung eines Verbrauchers. Der Beitrag stellt Kriterien für den Einsatz elektrotechnischer Komponenten in Sicherheitseinrichtungen vor und gibt anhand von Beispielen Empfehlungen für deren Umsetzung im Bereich Nieder- und Mittelspannung.

Die sicherheitsgerichtete Trennung der Schaltkontakte eines Verbrauchers muss auch unter ungünstigsten Bedingungen den zu erwartenden Anforderungen genügen. Das Versagen des Schaltgerätes muss mit hoher Wahrscheinlichkeit ausgeschlossen werden können.

Um solche Anforderungen zu erfüllen, müssen zunächst einfache Regeln für diese komplexen Zusammenhänge aufgestellt werden. Ziel ist es, möglichst Standardschaltungen auch für Sicherheitseinrichtungen SIL1 bis SIL3 einsetzen zu können, deren Einsatzbedingungen unter Beachtung gültiger, internationaler Normen im Folgenden definiert werden.

SIL-Level	Mindest-Hardware-Fehlertoleranz nach IEC 61511-1. 11.4.3.und 11.4.4.
1	0
1	1
3	2
4	besondere Anforderungen, siehe IEC 61508

TABELLE 1: Mindest-Hardware-Fehlertoleranzen nach IEC 61511

Safe Failure Fraction (SFF)	Hardware Failure Tolerance (HFT), hier für einfache Komponenten Typ A, wie Schütze, LS		
	HFT 0	HFT 1	HFT 3
< 60%	SIL 1	SIL 2	SIL 3
60% - < 90%	SIL 2	SIL 3	SIL 4
90% - < 99%	SIL 3	SIL 4	SIL 4
≤ 99%	SIL 3	SIL 4	SIL 4

TABELLE 2: Zusammenhang Hardware Failure Tolerance (HFT) und Safe Failure Fraction (Quelle: IEC 61508-2, Tabelle 2)

1. KRITERIEN FÜR DEN EINSATZ

Die IEC 61508 ist die Grundnorm und damit die Basis für die Sicherheitsnormierung. Daneben gibt es noch sektorspezifische Normen auf Basis der IEC 61508, die besonders für Planer und Betreiber wichtig sind. Für die Prozessindustrie gilt die IEC 61511. Mögliche Anwendungen und Validierungen für sicherheitsrelevante Schutzfunktionen sowie Regeln für (betriebs-)bewährte Technik werden durch europäische und internationale Normen (zum Beispiel DIN EN 50116 oder DIN ISO 13849-2) definiert.

Der SIL-Einsatzbereich einer Sicherheitsfunktion, deren Vorgabe im Sicherheitsgespräch festgelegt wird, ist begrenzt durch:

- PFD (Probability of Failure on Demand, Wahrscheinlichkeit des Auftretens eines Fehlers bei Anforderung – zumeist Anwendungen in der Prozessindustrie, Low Demand Mode)
- PFH (Probability of Failure per Hour, Wahrscheinlichkeit des Auftretens eines Fehlers pro Stunde – zumeist Anwendung im Maschinenbau, High Demand Mode)
- HFT (Hardware Failure Tolerance, gibt an, ob das Auftreten eines oder mehrerer Fehler zum Verlust der Sicherheitseinrichtung führt)
- SFF (Safe Failure Fraction, Anteil ungefährlicher Ausfälle)

Die IEC 61508 unterscheidet zwischen einer Betriebsart mit niedriger Anforderungsrate (Low Demand Mode) und einer Betriebsart mit hoher oder kontinuierlicher Anforderungsrate (High Demand oder Continuous Mode). Low Demand Mode liegt nur dann vor, wenn die Anforderungsrate an das sicherheitsbezogene System nicht mehr als einmal pro Jahr beträgt und nicht größer als die doppelte Frequenz der Wiederholungsprüfung ist.

Unter Hardware Failure Tolerance (HFT) versteht man die Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen. Eine HFT=0 (typisch für alle einkanaligen Schütze und Leistungsschalter) bedeutet, dass bereits ein Fehler zum Verlust der Sicherheitsfunktion führen kann. Deshalb definiert die IEC 61511 eine Mindest-Hardware-Fehler-Toleranz, die für Sensoren, Aktoren und nichtprogrammierbare Logiksysteme gilt (Tabelle 1).

Bei Verwendung von (betriebs-)bewährten Geräten darf nach IEC 61511 die Hardware Failure Tolerance, die in der Tabelle 1 genannt wird, um 1 reduziert werden (gilt nur für Anforderungen nach SIL ≤ 3).

In der IEC 61511 wird „betriebsbewährt“ definiert, jedoch kann nur der Betreiber eine Betriebsbewährung aussprechen, der Hersteller nicht. Betriebsbewährte Geräte werden zumeist durch die Anwender in Standardgerätelisten festgehalten. Betriebsbewährungen müssen lückenlos dokumentiert werden und in hinreichendem Maße die Einsatzerfahrungen über einen längeren Zeitraum wiedergeben.

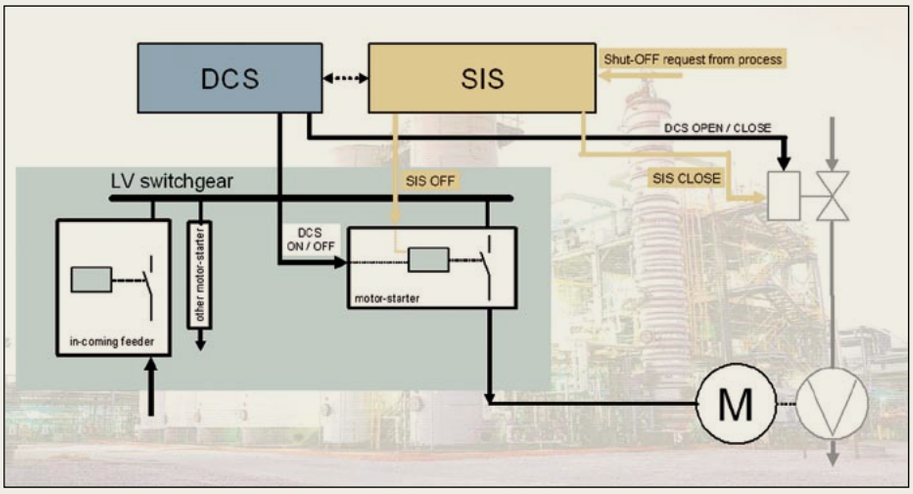


BILD 1: Beispiel A – Niederspannung, zweikanalige Abschaltung, Nutzung der Diversität

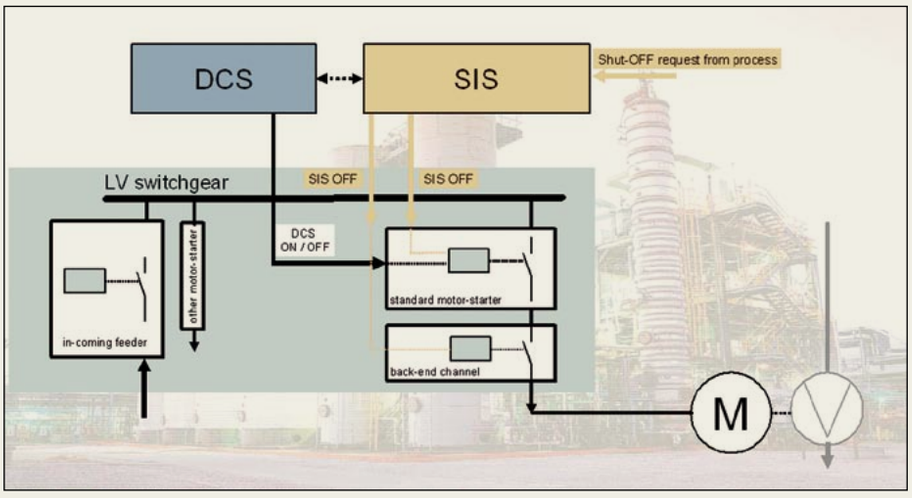


BILD 2: Beispiel B – Niederspannung, zweikanalige Abschaltung, Nutzung der Reihenschaltung

Alternativ kann man die Anforderungen an die Fehlertoleranz nach IEC 61511-1, 11.4.5. ermitteln, wenn man eine Beurteilung der Anforderungen nach IEC 61508-2, Tabellen 2 und 3 durchgeführt hat. Diese Tabellen definieren einen erreichbaren SIL-Level auf Basis der Hardware Failure Tolerance und des Safe Failure Fraction.

Unter Safe Failure Fraction versteht man nach IEC 61508 den Anteil ungefährlicher Ausfälle bezogen auf die Gesamtzahl potenzieller Ausfälle. Dieser lässt sich wie folgt berechnen:

$$SFF = 1 - \frac{\lambda^{DU}(gefahrbringende\ Ausfälle)}{\lambda^{Total}(Ausfälle\ gesamt)}$$

Annahme: Alle gefahrbringenden Ausfälle bleiben unerkannt.

Das folgende Beispiel eines Schützes zeigt die Berechnung des SFF-Wertes aus den Daten eines Herstellers:

- Low Demand: Standardausfallrate: 100 FIT, Anteil gefahrbringender Ausfälle $\lambda^D = \lambda^{DU} \leq 40\,\%$
- High Demand: B10-Wert: 1 000 000 Schaltspiele, Anteil gefahrbringender Ausfälle $\lambda^D = \lambda^{DU} = 75\,\%$

Aus diesen Vorgaben berechnet sich nach obiger Formel der SFF(low demand) = 60 % und der SFF(high demand) = 25 %.

Aus der Tabelle 2 können dann die realisierbaren SIL-Level als Funktion der Hardware-Fehlertoleranz entnommen werden. Im Beispiel würde eine zweikanalige Ausführung für Low Demand einen SIL-Level 3 erfüllen, während die gleiche Konfiguration als High Demand nur SIL 2 erreicht. Erfahrungsgemäß genügen die berechneten PFD-Werte den Anforderungen für SIL 3.

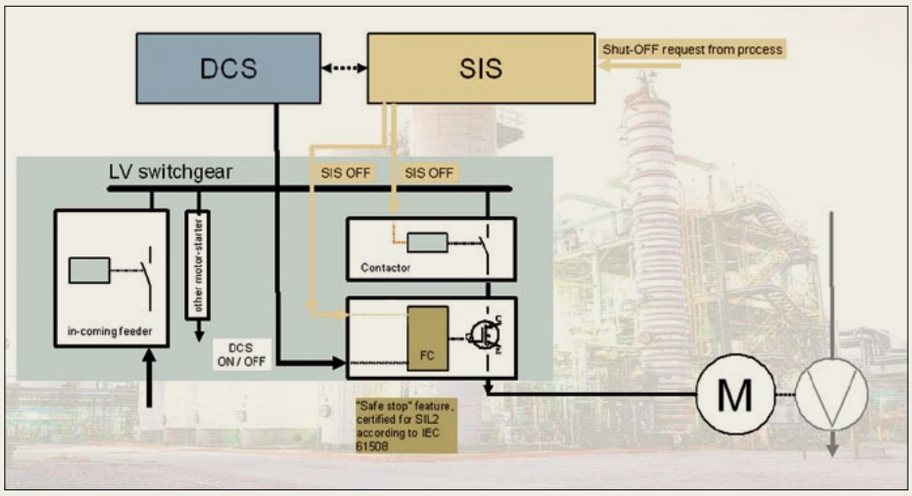


BILD 3: Beispiel C – Niederspannung, Frequenzumrichter, zweikanalige Abschaltung, „Sicherer Stopp"

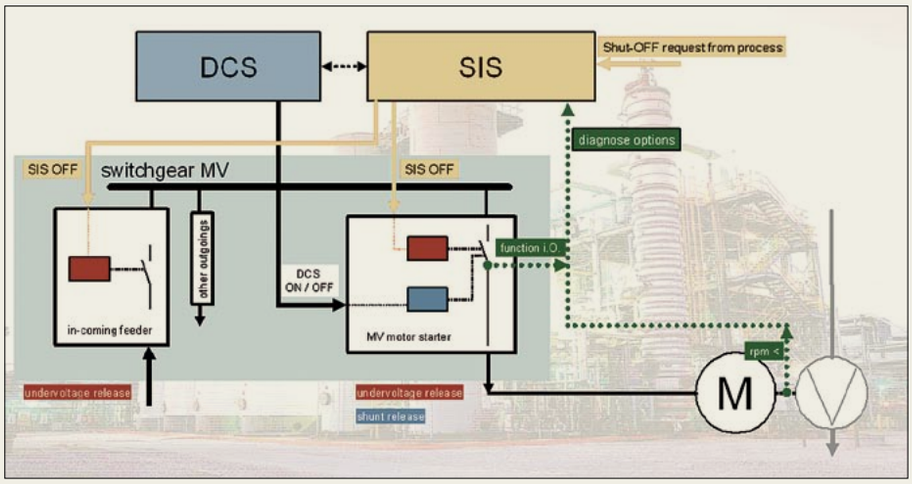


BILD 4: Beispiel D – Mittelspannung, zweikanalige Abschaltung, Nutzung des vorgelagerten Netzes

2. EINSATZEMPFEHLUNGEN

Planer und Betreiber müssen sich stets klar machen, dass die in den Normen genannten Forderungen für Sicherheitseinrichtungen Minimalanforderungen an die funktionale Sicherheit darstellen.

Die DIN ISO 13489-2 definiert grundlegende Sicherheitsprinzipien, wie zum Beispiel die Anwendung des Prinzips der Energietrennung (Ruhestromprinzip), sowie weitergehende, bewährte Sicherheitsprinzipien wie die Überdimensionierung. Für die Überdimensionierung von Bauteilen in Schutzschaltkreisen werden in dieser Norm konkrete Werte genannt, wie die Halbierung des Stromwertes der Schaltkontakte, die Verringerung der maximal zulässigen Schaltungen auf ein Zehntel des Nennwertes und die Reduzierung der Schaltfrequenz auf weniger als die Hälfte des Nennwertes. Auch die IEC 61508-7 definiert Überdimensionierung als eine Möglichkeit zur Erhöhung der Zuverlässigkeit.

Bezüglich der wesentlichen Aufgabe des Ausschaltens für die funktionale Sicherheit in der Elektrotechnik kommt demzufolge der Überdimensionierung und der durchgängigen Anwendung des Ruhestromprinzips eine entscheidende Bedeutung zu.

Unter Berücksichtigung der gezeigten Kriterien der IEC 61511 sowie der DIN ISO 13489-2 lassen sich folgende Einsatzempfehlungen für Teilsysteme „Aktor Elektrotechnik" in der Prozessindustrie ableiten:

- SIL 1: einkanalige Ausführung
- SIL 2: einkanalige Ausführung unter Berücksichtigung der Kriterien für bewährte Geräte/ Sicherheitsprinzipien (auch überdimensioniert)
- SIL 3: zweikanalige Ausführung, aber auch hier unter Berücksichtigung der Kriterien für bewährte Geräte/Sicherheitsprinzipien (auch überdimensioniert) Für mehrkanalige Anwendungen sind vorzugsweise diversitäre Lösungen zu nutzen, um gleichartige Fehler weitgehend auszuschließen. Ist eine Reihenschaltung zweier Schaltelemente unumgänglich, sollten diese ebenfalls verschiedenartig gewählt werden (verschiedene Bauart, Baugröße, Hersteller).

Die zuvor beschriebenen Einsatzempfehlungen für SIL 1 und SIL 2 lassen sich auch für Mittelspannungsaktoren (Nennspannung >1000 V) umsetzen. SIL 3-Anforderungen in der Mittelspannung erfordern dagegen oft besondere Betrachtungen: Dabei sollten auch die zugelassenen Überwachungsstellen (ZÜS) einbezogen werden. Planer und Betreiber sind hier besonders aufgefordert, mittels Risikoanalyse die wichtigen Kriterien Sicherheit, Verfügbarkeit und Kosten gegeneinander abzuwägen und zu entscheiden.

Die Bilder 1 bis 4 zeigen einige typische Beispiele für Realisierungen in der Praxis.

ZUSAMMENFASSUNG

Der Einsatz bewährter elektrotechnischer Komponenten in Sicherheitseinrichtungen ist eine praxiserprobte Methode zur Umsetzung der Anforderungen. Der hier vom VIK-/Namur-AK 3.14 „Niederspannungstechnik“ vorgestellte Weg soll helfen, den Einsatz von elektrotechnischen Komponenten in Sicherheitseinrichtungen, besonders in der Prozessindustrie und gestützt auf international gültigen Normen, zu standardisieren und zu vereinfachen. Die prozessbedingte Forderung nach einer rein elektrotechnischen SIL 3-Abschaltung sollte bezüglich möglicher anderer Maßnahmen zur Minimierung des Risikos überdacht werden.

REFERENZEN

[1] IEC 61508 (DIN EN 61508) – Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme,
[2] IEC 61511 (DIN EN61511) – Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie
[3] DIN EN 13849-2 - Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen

AUTOR

Dipl.-Ing. **TORSTEN KNITTEL** (geb. 1968) arbeitet als Senior Project Engineer im Engineering der Evonik Degussa GmbH und ist Obmann des VIK-/Namur-Arbeitskreises 3.14 „Niederspannungstechnik“.

Evonik Degussa GmbH, DG-TE Engineering,
Rodenbacher Chaussee 4,
D-63457 Hanau-Wolfgang,
Tel. +49 (0) 3863 55 93 24,
E-Mail: torsten.knittel@evonik.com

Vom Risiko zum Sicherheitskonzept

Bewährte Methoden und Werkzeuge

Risiko ist als das Produkt aus Eintrittshäufigkeit und Schadensausmaß definiert. Dabei werden drei Bereiche unterschieden: ein nicht akzeptabler Bereich, ein tolerierbarer Bereich und ein allgemein akzeptabler Bereich. Vom Risiko kommt man zum Sicherheitskonzept, indem man Schadensszenarien identifiziert und bewertet. Zur Bewertung der Szenarien stehen verschiedene Werkzeuge zur Verfügung. Dies sind deterministische Methoden ohne Risikobezug, der Risikograph, die Layers-of-Protection-Analyse (LOPA), die Risikomatrix und die quantitative Risikoanalyse. In diesem Beitrag wird der Weg vom identifizierten Risiko zum Sicherheitskonzept vorgestellt.

SCHLAGWÖRTER Risiko / Sicherheitskonzept

From Risk to Safety Concept – Best Practice Methods and Tools

Risk is defined as the product of frequency of occurrence and severity. Three areas are distinguished: an area being not acceptable, a tolerable area, and a commonly acceptable area. One gets from risk to the safety concept by identifying and assessing hazard scenarios. Several tools are available for the assessment of the scenarios. These include deterministic methodologies without risk consideration, the risk graph, layers of protection analysis (LOPA), risk matrix as well as quantitative risk analysis. In this paper, the way from the identified risk to a safety concept is demonstrated.

KEYWORDS Risk / Safety Concept

VOLKER ARNDT, BASF SE

Wie sieht Risiko praktisch aus? Im Bereich Sicherheit wird es als Anzahl Tote pro Jahr ausgedrückt. Um zu entscheiden, ob ein Risiko zu hoch ist, braucht man Akzeptanzkriterien. Hierzu gibt es international verschiedene Ansätze, die aber meist in einem ähnlichen Bereich liegen. Bild 1 zeigt als Beispiel die Akzeptanzkriterien von Großbritannien [1]. Dabei werden drei Bereiche unterschieden. Ein Risiko, das kleiner als 10^{-6} Tote pro Jahr ist, wird als allgemein akzeptabel angesehen (grün). Bei der Frage, was nicht akzeptabel ist, unterscheidet die britische Regierung zwischen dem Risiko am Arbeitsplatz und dem Risiko für die Öffentlichkeit. Die Werte liegen bei 10^{-3} beziehungsweise 10^{-4} Toten pro Jahr und stellen das Grenzrisiko dar. Ein Risiko, das größer ist, wird nicht akzeptiert (rot). Zwischen diesen beiden Bereichen liegt ein Sektor, in dem das Risiko als tolerierbar gilt (gelb). Die Bilder 2 und 3 veranschaulichen diese Zahlen.

In Bild 2 ist die Entwicklung für das Risiko in verschiedenen Branchen der deutschen Industrie über 50 Jahre dargestellt. Die Zahlen stammen aus Veröffentlichungen der Berufsgenossenschaften [2,3]. Drei Aspekte zeichnen sich ab:

1 | In den 60er-Jahren lagen viele Branchen selbst als Durchschnitt an der oberen Grenze der aufgezeigten Akzeptanzwerte.
2 | Alle Branchen haben sich über die letzten 50 Jahre ständig verbessert.
3 | Die chemische Industrie (die schwarzen Punkte) gehört zu den sichersten Branchen.

Bild 3 enthält einige Beispiele aus dem Alltag [1, 2, 3]. Für Risiken, bei denen das Risiko per Einzeltätigkeit angegeben war, wurde zur besseren Vergleichbarkeit eine typische Anzahl der Tätigkeit pro Jahr angenommen (Zahl in Klammer angegeben) und das entstehende Risiko pro Jahr eingetragen.

- Beispiele verschiedener Hobbys
- Häuslicher Gasanschluss (in UK)
- Teilnahme am Verkehr (Straße in Deutschland, Bahn in UK, Urlaubsreise mit dem Flugzeug)
- Blitzschlag bei Gewitter
- Erkrankung an Krebs
- Branche Chemie in Deutschland

Wenn man sieht, dass einige hohe Risiken im Alltag leicht akzeptiert werden, während manche niedrige Risiken Befürchtungen auslösen, stellt sich die Frage, ob Risiko überhaupt objektiv ist. Die Antwort ist eindeutig Nein. Hierfür gibt es drei Gründe:

Zum Einen kann ein positives Feedback die Risikowahrnehmung zurückdrängen. So wird das objektiv hohe und bekannte Krebsrisiko beim Rauchen durch den Genussgewinn kompensiert und verdrängt.

Außerdem werden freiwillig eingegangene Risiken eher akzeptiert als aufgezwungene Risiken, wie an vielen Freizeitaktivitäten erkennbar.

Schließlich werden seltene Großereignisse stärker wahrgenommen und prägen daher die Risikowahrnehmung intensiver als häufige kleine Ereignisse. Mathematisch ist 1 mal 100 gleich 100 mal 1, aber ein Bahnunglück oder Flugzeugabsturz wird anders aufgenommen als viele Autounfälle.

1. ENTWICKLUNG DES SICHERHEITSKONZEPTS

Der erste Schritt auf dem Weg zum Sicherheitskonzept ist die Identifikation von Szenarien. Die Grafik in Bild 4 ist dem EU-Projekt ARAMIS [4] entnommen und stellt die Elemente eines Szenarios dar. Im Zentrum eines Szenarios liegt immer eine Stoff- oder Energiefreisetzung – kritisches Ereignis genannt. Auf der linken Seite sieht man alle Gründe, die zu dem Ereignis führen können. Die Darstellung der „Und"- und „Oder"-Verknüpfungen wird als Fehlerbaum bezeichnet. Auf der rechten Seite zeigt der Ereignisbaum die Varianten, in denen eine Freisetzung Schaden anrichtet. Man kann nun einzelne Wege durch Barrieren unterbrechen. Auf der linken Seite sind sie eintrittsverhindernd und auf der rechten Seite schadensbe-

grenzend. Die Barrieren senken das Risiko, indem sie entweder die Eintrittshäufigkeit senken oder die Auswirkung verringern. Das Maß dieser Risikosenkung hängt dabei direkt von der Zuverlässigkeit der Barriere ab. Schutzmaßnahmen sind Barrieren mit besonders hoher Zuverlässigkeit. Meist ist es sinnvoll, mehrere Barrieren nach dem Zwiebelschalenprinzip zu kombinieren.

Ein Schwerpunkt im Sicherheitskonzept sind die Schutzmaßnahmen. Hier gibt es meist verschiedene Alternativen. In der Regel wird in dieser Prioritätsreihenfolge vorgegangen:

1 | Inhärente Sicherheit
2 | Eigensicheres Design
3 | Mechanische Schutzeinrichtungen
4 | PLT-Schutzeinrichtungen
5 | Organisatorische Schutzmaßnahmen

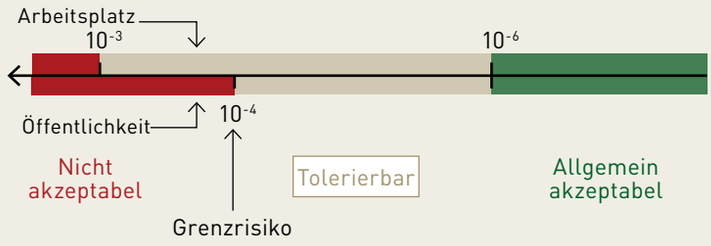


BILD 1: Risikogrenzwerte in Großbritannien

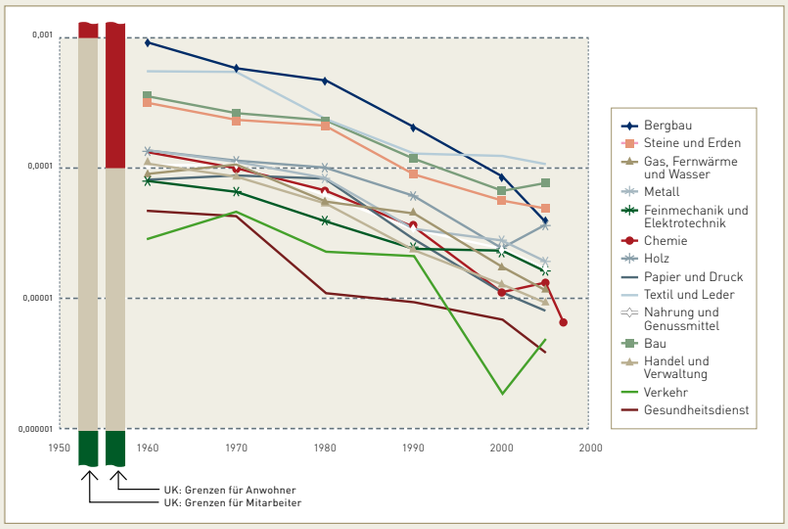


BILD 2: Entwicklung des Arbeitsplatzrisikos in Deutschland

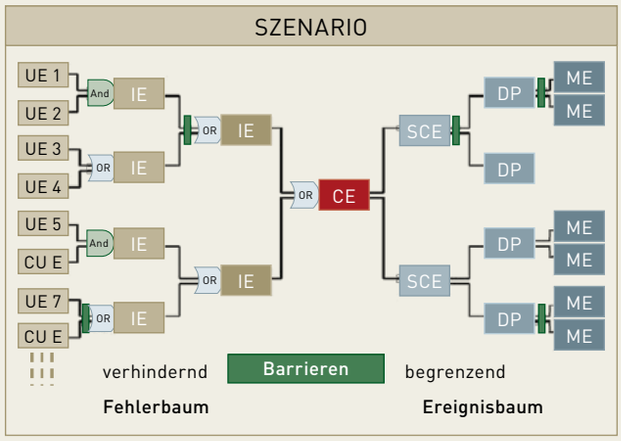


BILD 4: Darstellung eines Szenarios

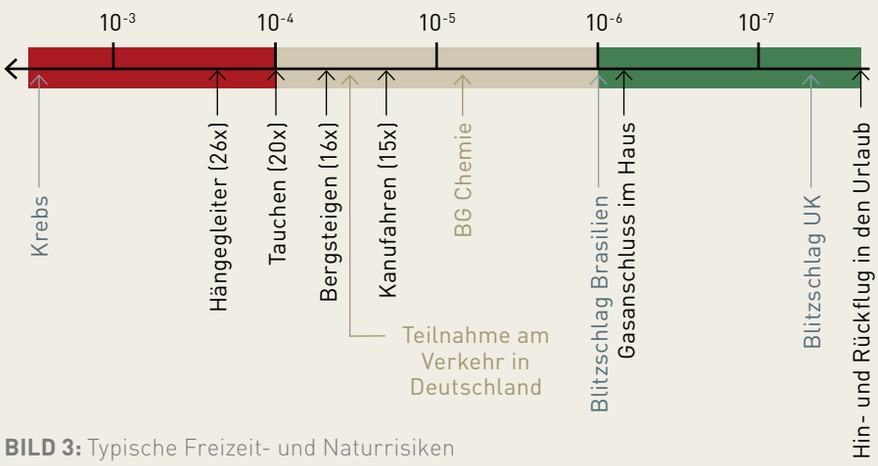


BILD 3: Typische Freizeit- und Naturrisiken

BILD 5: Risikoreduktion

Wie schon erwähnt, werden nach dem Zwiebelschalenprinzip zusätzlich schadensbegrenzende Maßnahmen vorgesehen. Wie stellt sich die Risikoreduktion bildlich dar? Dies verdeutlicht Bild 5. Das prozessspezifische Rohrisiko ist das Risiko ohne Gegenmaßnahmen. Vom Rohrisiko muss mit Hilfe der Schutzmaßnahmen mindestens der tolerierbare Bereich erreicht werden. Mit weiteren Maßnahmen nach dem Zwiebelschalenprinzip wird das Risiko dann in den akzeptablen Bereich zum verbleibenden Risiko gebracht.

2. WERKZEUGE

Um zu entscheiden, ob Schutzmaßnahmen notwendig sind und welche Qualität sie brauchen, gibt es verschiedene Werkzeuge.

Das erste sind deterministische Methoden ohne Risikobezug. Diese können aus Regelwerken kommen (zum Beispiel Mindestanforderungen an Überfüllschutz bei wassergefährdenden Stoffen) oder per Konvention festgelegt sein. Sie sind einfach anzuwenden und meist etwas konservativ, da die Mehrzahl aller Fälle abgedeckt werden muss. Situationen mit sehr hohem inhärenten Potenzial werden dabei allerdings oft unterschätzt.

Das zweite Werkzeug ist der altbekannte Risikograph. Auch er ist einfach anzuwenden. Allerdings sind die Begriffe unbestimmt und müssen kalibriert werden. Auch hier gibt es Situationen, für die er nicht geeignet ist.

Etwas neuer ist das dritte Werkzeug, die Layers-of-Protection-Analyse (LOPA). Sie scheint einfach anzuwenden zu sein, birgt aber einige Fallstricke. Zuerst muss das inhärente Potenzial bestimmt werden, um die Anzahl der notwendigen „Layers“ festlegen zu können. Dann ist es unbedingt notwendig, dass die Unabhängigkeit einzelner Layers gewährleistet sein muss. Hier ist nach Literaturangaben ein Großteil der LOPAs fehlerhaft, denn LOPA verführt dazu, abhängige Dinge mehrfach zu zählen. Bei richtiger Anwendung, die dann viel aufwändiger ist, sind die Ergebnisse jedoch korrekt.

Das vierte Werkzeug ist die Risikomatrix. Sie ist einfach anzuwenden. Es ist aber eine firmenspezifische, an die jeweiligen Rahmenbedingungen und die Vorgehensweise angepasste Kalibrierung notwendig. Dann liefert sie robuste Ergebnisse.

Das letzte Werkzeug ist die quantitative Risikoanalyse – QRA. Sie ist sehr aufwendig, da sehr viele Szenarien gerechnet werden müssen. Man erhält eine auf mehrere Stellen hinter dem Komma scheinbar sehr präzise Zahl. Auf Grund der notwendigen Vereinfachungen und Annahmen ist dies allerdings ein Trugschluss. So sind die Verteilungsfunktionen für die Häufigkeiten meist nicht bekannt, und aus der unendlichen Vielfalt an Szenarien muss ein repräsentativer Satz ausgewählt werden. Notwendige bedingte Wahrscheinlichkeiten (beispielsweise Zündung ja oder nein) werden auch bei der QRA per Konvention festgelegt.

3. DOKUMENTATION

Nachdem mit einem dieser Werkzeuge festgestellt wurde, dass eine Schutzmaßnahme nötig ist, muss für diese eine Spezifikation geschrieben werden. Die Spezifikation muss nicht nur die offensichtlichen Anforderungen enthalten – Was löst aus? Welche Aktion soll erfolgen? Notwendiger SIL? – sondern alle Angaben, die für die Erfüllung der Aufgabenstellung notwendig sind (zum Beispiel Schließzeiten, Leckageanforderungen, angestrebter Prüfmodus, und so weiter).

Die Spezifikation ist nur ein Teil der Dokumentation. Es sollte auch das Sicherheitskonzept als Positivdokumentation beschrieben werden. Ebenso wichtig ist die Dokumentation der Abnahmen, der Prüfvorschrift und der Prüf- und Wartungshistorie zur Aufrechterhaltung der Zuverlässigkeit über den Lebenszyklus.

FAZIT

Das Risiko ist die Kombination aus Eintrittshäufigkeit und Schadensausmaß. Barrieren senken die Eintrittshäufigkeit oder das Schadensausmaß. Das Sicherheitskonzept erhält man durch die Beschreibung aller Barrieren. Das Sicherheitskonzept muss vollständig dokumentiert werden. Spezifikation und Lebenszyklus müssen bei PLT-Schutzeinrichtungen dokumentiert werden.

MANUSKRIPTEINGANG
14.12.2010
Im Peer-Review-Verfahren begutachtet

REFERENZEN

[1] Reducing risks, protecting people, HSE's decision-making process, Health & Safety Executive, 2001
[2] BG Statistiken für die Praxis 2006, Deutsche Gesetzliche Unfallversicherung e.V. (DGUV)
[3] Jahresbericht der BG Chemie 2007, BG Chemie
[4] ARAMIS, Accidental Risk Assessment Methodology for Industries in the context of the Seveso II Directive – WP 1 Methodology for the Identification of Major Accident Hazards, Draft report version 1, September 2002

AUTOREN

DR. VOLKER ARNDT (geb. 1956) ist Diplom-Chemiker. Nach Tätigkeiten bei BASF in der Forschung, in der Betriebsleitung verschiedener Betriebe und mehrjähriger Leitung der Anlagensicherheit in Nordamerika führt er seit 2000 die Gruppe Anlagensicherheit B der BASF.

BASF SE,
GUS/AB – M 940, Carl-Bosch-Straße 38, D-67056 Ludwigshafen,
Tel. +49 (0) 621 607 91 13, E-Mail: volker.arndt@basf.com

IT-Sicherheit und Automation

Anwendung der VDI/VDE 2182 in der Prozessindustrie

Akutelle Ereignisse haben das Thema „IT-Sicherheit für Automatisierungssysteme“ in den Fokus gerückt und dabei Fragen nach dem richtigen Vorgehen aufgeworfen. Die VDI/VDE 2182 beschreibt hierfür mit ihrem Managementmodell einen ganzheitlichen Lösungsansatz. Der Beitrag betrachtet die wesentlichen Inhalte der Richtline aus Sicht des Betreibers in der Prozessindustrie und gibt Hinweise zu deren praktischer Umsetzung.

SCHLAGWÖRTER Kommunikation / IT-Sicherheit / Managementsystem

IT-Security and Automation –
Application of VDI/VDE 2182 in the Process Industry

Some recent events made the topic „IT Security” the focal point and raised a lot of questions for the appropriate approach. The VDI/VDE 2182 and its corresponding management model describe a holistic solution. This article considers the significant contents of the guideline from the perspective of an operator in the process industry and provides information on putting them into practice.

KEYWORDS Communication / IT Security / Management System

MICHAEL KUSCHMITZ, Bayer Technology Service

Die IT-Sicherheit der in Unternehmen eingesetzten Systeme, inklusive des speziellen Bereichs der industriellen Automation, ist verschiedenen Bedrohungen ausgesetzt. Dies kann ein nennenswertes Sicherheits- und Geschäftsrisiko darstellen. Um diese Risiken zu beherrschen, müssen finanzielle Mittel aufgewendet werden, die dadurch für Investitionen in das eigentliche Geschäft des Unternehmens nicht mehr zur Verfügung stehen. Die optimale Balance zwischen der Höhe dieser Aufwendungen und der Größe des verbleibenden Restrisikos wird erreicht, indem man sich in der Praxis der Methoden des Risikomanagements bedient.

Als Grundlage für den Aufbau eines Managementsystems für die IT-Sicherheit in der Automation wurde die Richtlinie VDI/VDE 2182 „Informationssicherheit in der industriellen Automatisierung“ erarbeitet. Daran war auch der Namur-Arbeitskreis 2.8 „Internettechnologien“ beteiligt, der sich diesem wichtigen Thema schon seit mehreren Jahren widmet. Die Ergebnisse dieser Arbeit sind in das Namur-Arbeitsblatt NA115 eingeflossen [3].

Die Richtlinie beinhaltet das eigentliche Managementsystem, das in Form eines Vorgehensmodells abgebildet wird. Darüber hinaus beschreibt sie Best Practices aus dem Bereich der IT-Sicherheit, die an die speziellen Gegebenheiten und Anforderungen im Bereich der industriellen Automation angepasst wurden. Sie umfasst ebenso ein Rollenmodell, das die unterschiedlichen Blickwinkel der Zielgruppen Systemhersteller, Integratoren/Anlagenbauer und Betreiber auf dieses Thema abbildet. Diese Aspekte wurden getrennt für Systeme in der Fertigungsautomation (FA) und Prozessautomation (PA) betrachtet.

Die Richtlinie gliedert sich in das Hauptdokument „Grundlagen und allgemeines Vorgehensmodell“ und je ein Dokument für jede Zielgruppe. Anfang 2011 sollen das endgültige Hauptdokument (Weißdruck) und die übrigen als Entwurf (Gründruck) veröffentlicht werden.

1. VORGEHENSMODELL AUS BETREIBERSICHT

In der VDI/VDE 2182 wird ein Vorgehensmodell verwendet, das so allgemein gehalten ist, dass sich die Anforderungen aller Zielgruppen der Richtlinie darauf abbilden lassen. Deshalb soll das Modell an dieser Stelle zunächst auf die konkrete Sicht des Betreibers angepasst werden.

Das PLT-Security-Konzept bildet die Grundlage aller Aktivitäten des Betreibers und damit seines Sicherheitszyklus, der sich für ihn in drei wesentliche Segmente gliedern lässt (siehe Bild 1):

- Risikoanalyse und Gegenmaßnahmen – hauptsächlich Systemdesign
- Betreiben – Notfallprävention und Notfallbeherrschung
- Überprüfen – ständige Überwachung und Audits

Der Neustart des Zyklus erfolgt entweder turnusmäßig, bei Systemänderungen, beim Eintritt bestimmter Ereignisse oder bei festgestellten Abweichungen im Rahmen der Überprüfungen.

2. PLT-SECURITY-KONZEPT

Das PLT-Security-Konzept beschreibt die generell anzuwendenden Grundsätze und Basis-Konzepte. Dabei spannt sich der Bogen von Aspekten der Organisation und Verantwortlichkeiten über Werkzeuge und Vorgehensweisen – bezogen auf die einzelnen Abschnitte des Sicherheitszyklus – bis hin zu Schnittstellen und Anforderungen an die Systeme beziehungsweise die damit im Zusammenhang stehenden Dienstleister.

Die Grundlage des Konzeptes sollte die IT-Sicherheitsrichtlinie des Unternehmens bilden. Um die Kompatibilität sicherzustellen, wird in der Praxis das PLT-Security-Konzept oft als Subdokument zur IT-Sicherheitsrichtlinie eingeordnet und in Zusammenarbeit oder in Abstimmung mit der Unternehmens-IT erarbeitet.

Der Geltungsbereich des PLT-Security-Konzeptes kann das gesamte Unternehmen oder auch nur Unternehmensbereiche, bis hinunter auf die Ebene einzelner Betriebe, umfassen. Es ist also zu prüfen, ob das ganze Unternehmen mit einem einzigen Vorgabedokument abgedeckt werden kann, besonders dann, wenn es sich um international verteilte Niederlassungen mit unterschiedlichen Gegebenheiten und Anforderungen handelt. Bei dieser Konstellation würden sich daraus eher generelle Konzepte mit einem geringen Detaillierungsgrad ergeben. Eine praktische Lösung kann beispielsweise eine hierarchische Struktur von mehreren Konzeptpapieren sein, deren obere Ebene übergeordnete und deren untere Ebene angepasste Detailvorgaben für die verschiedenen Niederlassungen beziehungsweise Betriebe beinhalten.

3. RISIKOANALYSE UND GEGENMASSNAHMEN

Dieser Abschnitt ist der Eintrittspunkt in den Sicherheitszyklus und bezieht sich hauptsächlich auf das Systemdesign.

3.1 Strukturanalyse

Die Grundlage der Analyseaktivitäten bildet die Strukturanalyse. Diese muss nicht bei jedem Neustart des Sicherheitszyklus durchlaufen werden, wenn frühere Ergebnisse weiter Gültigkeit besitzen.

Die Hauptfragen der Strukturanalyse sind: „Was soll betrachtet werden?“ und „Welche Rand-/Umgebungsbedingungen bestehen, und wie sind die Schnittstellen gestaltet?“ Es erfolgt daraufhin eine gedankliche Zerlegung des Gesamtsystems in Betrachtungsgegenstand und Einsatzumgebung, die Schnittstellen und Übergänge dazwischen beziehungsweise die jeweiligen Einflüsse aufeinander. Dabei werden nicht nur die Bestandteile des eigentlichen Systems betrachtet, sondern auch das relevante Umfeld (wie Räume, Energieversorgung, Gebäude-Infrastruktur.).

In der Praxis zeigt sich, dass die wichtigste Grundlage eine vollständige Dokumentation darstellt. Das betrifft auch die Altsysteme, die häufig zur Einsatzumgebung gehören. Eine einheitliche Art und Weise der Dokumentation hat sich als große Hilfe bei der Arbeit der Experten erwiesen, die meist mehrere Systeme bearbeiten und sich somit nicht in jedem Fall wieder neu orientieren müssen.

Durch eine gründliche Strukturanalyse ergibt sich darüber hinaus die Chance, Typicals („Standard“-Bausteine von Systemen/Systemteilen) zu identifizieren. Dadurch müssen die folgenden Analysen und Festlegungen von Gegenmaßnahmen nicht für jedes System wieder von Grund auf neu erstellt werden. Und bei Änderung der Sicherheitslage oder anderer Gegebenheiten lassen sich alle betroffenen Systeme schnell und einfach identifizieren.

Beachtet werden muss auch die Ausführung der Übergänge zwischen Betrachtungsgegenstand und Einsatzumgebung. Deren Gestaltung sollte so erfolgen, dass die Einflüsse der beiden Teile aufeinander möglichst gering sind und sich dadurch die Betrachtungen bei der Analyse auf den jeweiligen Teil beschränken lassen. Ein Beispiel für eine solche Strukturierung beziehungs-

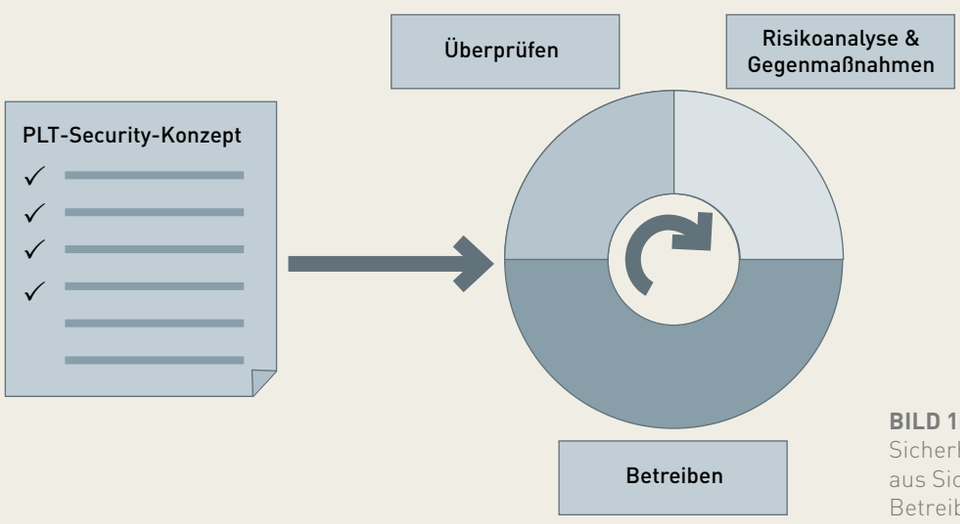


BILD 1: Sicherheitszyklus aus Sicht des Betreibers

weise Clusterung ist die in der Praxis häufig eingesetzte Barriere zwischen PLT- und Office-Netzwerken, die so beschaffen ist, dass beide Netze möglichst rückwirkungsfrei betrieben werden können.

3.2 Implementierung

Vor Beginn des Analysevorganges sieht die VDI/VDE 2182 die Bildung eines Analyseteams mit der Besetzung von bestimmten Rollen vor, die den Know-how-Bedarf für diese Aufgabe widerspiegeln (technische und Anwendungs-Experten, Entscheider, Koordinatoren und so weiter). In der Praxis kann eine Person auch mehrere Rollen repräsentieren, jedoch sollten der gleichen Person nicht Aufgaben mit potenziell gegensätzlichen Interessen übertragen werden. Eine zentrale Fachstelle kann durch die Bereitstellung von Experten und Bündelung von Know-how für die Teambesetzung vorteilhaft sein.

Für den Analysevorgang gibt die Richtlinie einen strukturierten Ablauf vor:

- Identifikation der materiellen und immateriellen Assets
- Identifikation der Schutzziele und möglicher Bedrohungen mit Auslösern und Folgen
- Ermittlung des bestehenden Risikos aus Schadensausmaß und Eintrittswahrscheinlichkeit und Definition des akzeptablen Restrisikos
- Falls das bestehende Risiko das akzeptable Restrisiko übersteigt, erfolgt die Festlegung und Umsetzung von Gegenmaßnahmen und deren Überprüfung auf Wirksamkeit

In der Praxis wird gerade dem Test der Maßnahmen oft noch nicht die notwendige Aufmerksamkeit geschenkt.

Bei der Analyse ordnet die Richtlinie dem Betreiber naturgemäß eine funktionale Sicht („Lastenheft-Niveau“) und die Festlegung des akzeptablen Restrisikos zu. Der Integrator besitzt eine Sicht auf Details beziehungsweise konkrete Geräte („Pflichtenheft-Niveau“) und ermittelt daraus das Istrisiko. Deshalb wird die Erstellung der Analyse von beiden Rollen gemeinsam vorgenommen, wobei in der Praxis die PLT des Betreibers oft auch gleichzeitig die Integratorrolle repräsentiert, da sie nicht nur für die Beauftragung eines Anlagenbauers verantwortlich ist, sondern selbst auch die Auslegung von Systemen vornimmt. Systemhersteller können ebenfalls gleichzeitig auch Integrator im Sinne der Richtlinie sein, wenn sie, statt nur einzelne Komponenten, komplette Systeme liefern oder die Applikationssoftware erstellen.

Für die Analyse schlägt die Richtlinie Werkzeuge vor, beispielsweise eine Risikomatrix, die Schadensausmaß und Eintrittswahrscheinlichkeit auf das Istrisiko abbildet und dieses wichtet, sowie eine Analysetabelle zur Dokumentation der Ergebnisse der einzelnen Analyseschritte. Deren Aufbau folgt idealerweise dem Analyseablauf. Die konkrete Festlegung der Werkzeuge, deren Umsetzung als Liste, Datenbank oder ähnlich und die Risikowichtung in der Risikomatrix sind Inhalt des PLT-Security-Konzepts.

In der Praxis erleichtern dieser formalisierte Ablauf und die dazu passende Dokumentation wesentlich Reviews und Analyse-Updates bei veränderten Rahmenbedingungen. Alle betrachteten Systemteile und Szenarios sind eindeutig beschrieben und bilden dadurch auch die Grundlage für die detaillierte Überprüfung der Wirksamkeit der Gegenmaßnahmen, da sich die entsprechenden Testfälle aus den dokumentierten Szenarios einfach herleiten lassen.

Um aus einer potenziellen eine akute Bedrohung werden zu lassen, müssen drei Bedingungen erfüllt sein:

- Es gibt eine Schwachstelle
- Es gibt einen Angriffspfad zur Ausnutzung dieser Schwachstelle
- Es ist eine ausreichend hohe Motivation beziehungsweise ein Auslöser vorhanden, die Schwachstelle über diesen Angriffspfad auszunutzen

Wirksame Gegenmaßnahmen zu ergreifen, bedeutet also die Einflussnahme auf eine oder mehrere dieser Bedingungen.

Da die Eintrittswahrscheinlichkeit im Bereich der IT- und PLT-Security in hohem Maße von Menschen und deren Motivation abhängt, sind die Analyseergebnisse nur qualitativ beschreibbar und die Bestimmung der Eintrittswahrscheinlichkeiten relativ schwierig. Zumal darüber hinaus die menschliche Motivation vielfach nicht als bewusst (zum Beispiel Hacking), sondern als fahrlässig (beispielsweise Fehlkonfiguration) einzustufen ist.

Im Bereich der Anlagensicherheit wirken dagegen immer vorhandene Naturgesetze, sodass in diesem Fall eine quantitative Ermittlung von Wahrscheinlichkeiten mittels statischer Methoden möglich ist.

Die vorgestellte formalisierte Art der Risikoanalyse wird heute schon genau so oder ähnlich in vielen anderen Bereichen genutzt, die zwar einen anderen Fokus haben, aber die gleichen Systeme betrachten wie die PLT-Security. Es zeigt sich in der Praxis, dass Teile dieser Analysen auch für die PLT-Security genutzt werden können und sich damit der Analyseaufwand reduzieren lässt. Beispielhaft seien GMP-Risikoanalysen (Fokus: Patientensicherheit) und Risikoanalysen der Anlagensicherheit genannt.

Das heute meist übliche Vorgehen, einen Basisschutz über die Umsetzung von Standardmaßnahmen zu schaffen, wird derzeit schon von einzelnen Unternehmen durch die vollständige und formalisierte Analyse gemäß VDI/VDE 2182 ergänzt, um die bisherigen Lösungen zu optimieren oder kritische Systeme detaillierter zu betrachten. Es ist zu beachten, dass die Wirkung der Gegenmaßnahmen von der vollständigen Betrachtung und der konsistenten Umsetzung abhängt. Teillösungen bieten meist keine Teilsicherheit, sondern gar keine. Nicht jede (Standard-)Maßnahme passt auch zu

jedem System. Sie kann sich an einigen Stellen sogar als kontraproduktiv erweisen. Eine tiefergehende Analyse ist also unabdingbar.

Das Vorgehen und die Ansätze für die Analyse und die Gegenmaßnahmen sind von der Art des Betrachtungsgegenstandes abhängig. Im IT- beziehungsweise MES-Bereich ist oft eine strikte Standardisierung möglich. Hier kommen meist viele gleichartige Systeme zum Einsatz. Prozessleitsysteme sind dagegen im Detail häufig Unikate. Auch bei gleicher Systemversion können unterschiedliche Softwarestände bezogen auf Servicepacks, Patches und so weiter und auch verschiedene Ausstattungen an Optionspaketen ein differenziertes Herangehen bedingen.

4. BETREIBEN

Der längste und damit bedeutendste Abschnitt im Lifecycle der Systeme ist deren Betrieb. Das Thema PLT-Security wird mit der Analyse und der Umsetzung von Gegenmaßnahmen im Systemdesign nicht abgeschlossen, sondern damit werden nur die Grundlagen geschaffen. PLT-Security ist als ein Prozess zu verstehen, der auch das Betreiben der Systeme ständig begleitet.

Der Dokumentation kommt auch hier, wie in allen anderen Teilen des Sicherheitszyklus, eine zentrale Bedeutung zu. Neben der Vollständigkeit und möglichst einheitlichen Art und Weise ist eine zentrale Ablage und damit ein schneller Zugriff verschiedener Abteilungen in der Praxis von Vorteil.

Die Richtlinie gliedert Schutzmaßnahmen beim Betreiben der Systeme in zwei Teile: Notfallprävention und Notfallbeherrschung.

4.1 Notfallprävention

Unter die Notfallprävention fallen folgende Maßnahmen:

- Verhindern von Ereignissen/Notfällen
- Erkennung von Ereignissen und Zuständen, die den Normalbetrieb der Systeme beeinträchtigen
- Vorsorgliches Begrenzen des Schadensausmaßes im Fall eines Ereignisses

Neben technischen Maßnahmen spielen dabei vor allem organisatorische Aspekte eine große Rolle. Der klaren Zuordnung von Tätigkeiten und Verantwortlichkeiten innerhalb der Organisationsstruktur kommt eine große Bedeutung zu. Dabei hat sich in der Praxis die klassische Aufgabenteilung innerhalb der PLT auch für diesen Bereich bewährt. Die PLT-Betriebsbetreuung ist für betriebsspezifische Aufgaben zuständig; die zentralen Fachstellen dagegen für Aufgaben, für die gebündeltes beziehungsweise betriebsübergreifendes Know-how notwendig ist.

In Teilbereichen zeigt sich dabei ein Trend, klassische Aufgaben der Betriebsbetreuung zu zentralisieren. Das betrifft zum Beispiel die Datensicherung der Systeme. Daraus kann sich der Vorteil ergeben, dass sich zum einen der Vorgang weiter automatisieren lässt und damit das Personal entlastet wird. Zum anderen lässt sich damit sicherstellen, dass diese Vorgänge für alle betreffenden Systeme gleichartig ablaufen und mit höherer Wahrscheinlichkeit richtig ausgeführt werden als von vielen verschiedenen Personen, denen das Vorgehen nur per Anweisung vorgegeben wird.

Eine große Bedeutung kommt auch dem Konzept zum Einbringen von Software beziehungsweise Datenträgern in die Systeme zu. Da die Systeme dafür nach außen geöffnet werden müssen, haben sich eine Reihe von Best-Practice-Lösungen zur Risikoreduzierung herauskristallisiert. Beispielsweise werden Datenträger vorab auf einem Quarantänesystem auf Schadsoftware überprüft und die Live-Systeme durch das Sperren von Laufwerken, der Autostart-Funktionen und so weiter zusätzlich geschützt.

Neben dem Einbringen von Änderungen zur Korrektur oder Anpassung von Funktionalitäten handelt es sich hierbei auch um Softwareveränderungen wie Patches und aktuelle Pattern für Virenscanner, die der Verbesserung der PLT-Security dienen sollen. Trotzdem ist für diese sehr sorgfältig zu betrachten, ob deren Vorteile nicht durch Nachteile, die sich durch das Einbringen in die Systeme ergeben können, wieder zunichte gemacht werden. Beispielhaft seien hierfür genannt: das Herabsetzen der Verfügbarkeit durch Systemstillstand während der Installation von Patches und die Kommunikationskanäle zu Pattern-Servern, die zusätzliche offene Verbindungen in den Netztrenn-Barrieren erfordern können.

Zur frühzeitigen Erkennung von Fehlern und anderen unerwünschten Zuständen dient das Monitoring. „Frühzeitig“ bedeutet, dass die Erkennung möglichst zu einem Zeitpunkt erfolgen sollte, zu dem noch Handlungsspielraum zur Behebung besteht, bevor ein nennenswerter Schaden eintritt. Dabei werden sowohl die Aspekte, die sich auf die korrekte Funktion der einzelnen Systembestandteile beziehen (Systemgesundheit), als auch die der PLT-Security (zum Beispiel Logs der verschiedenen Sicherheitskomponenten) überwacht. Eine große Bedeutung kommt dabei der Festlegung von sinnvollen Grenzwerten zu, bei deren Verletzung vom Eintritt eines Ereignisses ausgegangen werden muss. Da diese Festlegungen eine vollständige Dokumentation der Systembestandteile und ein hohes Maß an Expertenwissen erfordern, sind sie in der Praxis meist nur in Zusammenarbeit mit Herstellern und Integratoren zu treffen. Die manuelle Auswertung der laufend anfallenden Monitoringdaten ist durch deren Menge und komplexen Zusammenhänge untereinander meist nicht zu leisten. Hierzu sind zentrale Tools als Informationsdrehscheibe sehr nützlich. Diese setzen idealerweise die Daten aller relevanten Systembestandteile in Bezie-

hung und treffen möglichst automatisiert einfach zu erfassende Diagnoseaussagen.

Die komplexen technischen Zusammenhänge und die Notwendigkeit, ein hohes Bewusstsein für ein angemessenes Handeln in Bezug auf die PLT-Security (Awareness) zu pflegen, erfordern ein Konzept zur Schulung der Mitarbeiter. Diese Schulungen sollten regelmäßig erfolgen und nicht nur bei Änderungen oder Vorfällen. Da der betreffende Personenkreis die Spezialisten der PLT beziehungsweise PLT-Security bis hin zu den Anwendern der Systeme umfasst, haben sich in der Praxis Schulungen mit rollenspezifischen Inhalten und Wiederholungszyklen bewährt.

4.2 Notfallbeherrschung

Die Notfallbeherrschung umfasst alle Aktivitäten zur Aufrechterhaltung oder zur schnellen Wiederherstellung des Geschäftsbetriebes im Ereignisfall, das Einleiten und Durchführen eines Notbetriebs sowie die Störungssuche/-beseitigung.

Im Fall eines Ereignisses kommt es vor allem auf schnelles, effizientes und richtiges Handeln an, um das Schadensausmaß so gering wie möglich zu halten. Die vorab getroffene, klare Festlegung und vor allem auch Erprobung der Melde- und Eskalationswege ist deshalb von entscheidender Bedeutung. Hilfreich kann eine Kategorisierung nach Störungsarten sein, da je nach zu erwartenden Folgen des Ereignisses gegebenenfalls andere Eskalationswege gelten. Darüber hinaus ist auch die umfassende und zeitnahe Verfügbarkeit von Informationen für alle Betroffenen bedeutsam. Hier hat sich zum Beispiel deren Publizierung über die vielerorts bestehenden Intranetseiten der PLT-Communities bewährt.

Den zweiten großen Themenkreis der Notfallbeherrschung bilden die Tools zur Problemanalyse und -beseitigung. Auch hier sollte vorab klar definiert sein, welche Arten von Fehlern oder Störungen mit welchen Tools bearbeitet, welche Versionen dabei verwendet werden und welche Personen die Arbeiten ausführen sollen. Die entsprechenden Werkzeuge sind verfügbar und der Personenkreis auf dem erforderlichen Wissens- und vor allem auch praktischen Trainingsstand zu halten, um diese zielgerichtet und effizient einsetzen zu können. Darüber hinaus sind die Vorgaben und Freigaben der Systemhersteller für den Einsatz der verschiedenen Werkzeuge zu beachten. Da in vielen Fällen auf Tools zurückgegriffen wird, die auch im Office-Bereich eingesetzt werden, kann eine Zusammenarbeit mit der Unternehmens-IT aufgrund möglicher Synergieeffekte ein vorteilhafter Weg sein.

5. ÜBERPRÜFEN

Der dritte und letzte Abschnitt im Vorgehensmodell des Betreibers ist das Überprüfen. Hierbei unterscheidet die VDI/VDE 2182 zwischen laufenden Überwachungen und Audits.

Die laufenden Überwachungen lassen sich wiederum in das Monitoring, das im Rahmen der Notfallprävention durchgeführt wird, und die ständige Beobachtung der Sicherheitslage gliedern. Da in der IT- beziehungsweise PLT-Security die Höhe des Risikos von einer sich in ständiger Bewegung befindlichen Sicherheitslage bestimmt wird, ist sowohl deren lückenlose Beobachtung wie auch die damit verbundene Überprüfung der bisher getroffenen Einschätzungen entscheidend. Hierbei zeigt sich dann auch der Wert einer Analysedokumentation, die für diese Aufgaben praktisch und aufwandsarm nutzbar ist. Sollten sich Diskrepanzen zwischen vorhandener und neuer Einschätzung der Risiken ergeben, ist der Sicherheitszyklus neu zu starten. Um den Aufwand für eine möglichst lückenlose Beobachtung der Sicherheitslage zu reduzieren, ist auch hier die Kooperation mit den Herstellern und der Unternehmens-IT ein oft beschrittener Weg.

Demgegenüber dienen Audits der formalen oder qualitativen Überprüfung der Einhaltung der Vorgaben, die im Rahmen des PLT-Security-Konzeptes oder der einzelnen Schritte des Sicherheitszyklus definiert wurden. Da die Wirksamkeit des Managementsystems wesentlich von seiner vollständigen Umsetzung abhängt, stellen Audits einen nicht zu unterschätzenden Erfolgsfaktor dar. Sie sollten jedoch nicht nur als Überwachungsaktivität gesehen werden, sondern sie dienen auch dem Erfahrungsaustausch und spielen deshalb im kontinuierlichen Verbesserungsprozess eine große Rolle.

In der Praxis zeigt sich, dass regelmäßige Audits für Unternehmen mit vielen, dazu noch international verteilten, Niederlassungen eine personelle Herausforderung darstellen können. Praktikable Lösungen hierfür sind zum Beispiel die Integration der PLT-Security-Aspekte in allgemeine PLT-Audits oder die Kooperation mit anderen Abteilungen oder externen Spezialisten vor Ort.

6. ZUSAMMENARBEIT MIT HERSTELLERN UND INTEGRATOREN

Die wichtigste Forderung aus Sicht des Betreibers ist es, dass sich der Aufwand in Bezug auf die PLT-Security auf ein Minimum reduzieren muss. Das bezieht sich sowohl auf den Aufwand, der dem Betreiber direkt entsteht wie auch auf die Mehrkosten, die über die Preisbildung von Herstellern und Integratoren an ihn weitergegeben werden. Der Durchsetzung dieses Anliegens widmet sich auch die Namur schon seit etlichen Jahren. Um diesem Anspruch gerecht zu werden, müssen alle Aspekte der PLT-Security möglichst früh im Lebenszyklus der Systeme verankert werden [3].

Dadurch ergeben sich aus Sicht des Betreibers eine Reihe von Anforderungen an die anderen beiden Rollen „Hersteller“ und „Integrator“, deren Beitrag die notwendigen Grundlagen für eine erfolgreiche Umset-

zung schaffen muss. Beispielhaft seien hier folgende genannt:

- Die PLT-Security muss ein Designziel der Systeme sein.
- Alle Eigenschaften und Funktionen der Systeme müssen vollständig dokumentiert sein.
- Die von den Herstellern und Integratoren vorgeschlagenen Lösungen müssen spezifisch für den Bereich der industriellen Automation anwendbar sein.
- Hersteller und Integratoren müssen Know-how-Führer sein, PLT-Security muss zu ihrer Kernkompetenz gehören.
- Der Betreiber muss bei veränderter Sicherheitslage sofort die notwendigen Informationen und in Notfällen die benötigte Experten-Hilfe erhalten können.

Aus heutiger Sicht zeigt sich hierzu in der Praxis allerdings leider noch ein spürbarer Nachholbedarf was das Problembewusstsein und die Lösungskompetenz betrifft.

7. FAZIT

Die Richtlinie VDI/VDE 2182 beschreibt eine Möglichkeit zum Umgang mit dem Thema der PLT-Security. Sie „erfindet“ dabei nicht grundlegend Neues, sondern verbindet über ihr Vorgehensmodell bewährte Bausteine des Risikomanagements zu einem effizienten und vollständigen Prozess. Da es sich um ein noch relativ junges Themenfeld handelt, muss zukünftig noch ein erhebliches Maß an weiteren praktischen Erfahrungen gewonnen werden, bis sich optimale Werkzeuge, Risiko-Bewertungsmaßstäbe und so weiter eindeutig herauskristallisieren. Ebenso muss auch die Richtlinie parallel zu diesen Erfahrungen weiterentwickelt werden.

Aus heutiger Sicht lässt sich feststellen, dass viele der beschriebenen Teilaspekte schon angewandt werden und sich auch erste vollständige Umsetzungen in Namur-Unternehmen im Teststadium befinden. Insbesondere mit technischen Best-Practice-Lösungen ist man an vielen Stellen schon gut vertraut. Bei der Umsetzung der analytischen und organisatorischen Aspekte zeigt sich jedoch noch deutliches Verbesserungspotenzial.

MANUSKRIPTEINGANG
13.12.2010
Im Peer-Review-Verfahren begutachtet

DANKSAGUNG

Mein besonderer Dank gilt den Kollegen des Namur-Arbeitskreises 2.8 „Internettechnologien“ für die sehr konstruktive Unterstützung bei der Erarbeitung dieses Beitrages.

REFERENZEN

[1] VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung
[2] Schmidt, K.: Der IT-Security Manager. Carl Hanser Verlag München 2006
[3] NA115: IT-Sicherheit für Systeme der Automatisierungstechnik: Randbedingungen für Maßnahmen beim Einsatz in der Prozessindustrie. Juni 2006

AUTOR

Dipl.-Ing. (FH) **MICHAEL KUSCHMITZ** (geb. 1971) ist seit 1999 Mitarbeiter der Bayer AG und in unterschiedlichen Funktionen der PLT-Betriebsbetreuung und Projektabwicklung tätig. Seit 2006 ist er bei der Bayer Technology Services GmbH beschäftigt und dort als Lead Engineer für die Prozessleittechnik in Investitionsprojekten verantwortlich. Darüber hinaus beschäftigt er sich mit den Themen „funktionale Sicherheit“ und „IT-Security in der Automation“. Innerhalb der Namur ist er im Arbeitskreises 2.8 „Internettechnologien“ und in der GMA im Fachausschuss 5.22 „IT-Security in der Automatisierungstechnik“ tätig.

Bayer Technology Services GmbH,
Geb. 118, D-42096 Wuppertal, Tel. +49 (0) 202 36 28 19,
E-Mail: michael.kuschmitz@bayer.com

E20001-F218-P280

Ist Ihr Prozessleitsystem bereit für die Zukunft?

Mit SIMATIC PCS 7 überwinden Sie bestehende Grenzen.

Wo herkömmliche Prozessleitsysteme oft an ihre Grenzen stoßen, bietet SIMATIC PCS 7 eine Fülle faszinierender Möglichkeiten. Nur unser wegweisendes DCS ermöglicht die volle Integration aller Automatisierungskomponenten in Ihrer Anlage – mit gemeinsamen Tools für Projektierung und Visualisierung. Weitere Highlights: die einzigartige skalierbare Architektur von SIMATIC PCS 7, flexible Möglichkeiten zur Modernisierung vorhandener Systeme und integrierte Prozesssicherheit.
Weitere Informationen: www.siemens.de/simatic-pcs7

Answers for industry.

SIEMENS

SIL-Bewertung von Mechanik

Versagenswahrscheinlichkeit mechanischer Komponenten

Die SIL-Bewertung von Schutzeinrichtungen mit nichtelektrischen Komponenten ist oft schwierig, da die EN 61508 nur elektrische Komponenten betrachtet.
Der naheliegende Lösungsansatz, mechanische Komponenten genauso oder sinngemäß so zu behandeln wie elektrische, gelingt nur teilweise. In diesem Beitrag wird gezeigt, dass Mechanik in vielerlei Hinsicht wie Elektronik behandelt werden kann, wobei jedoch die Berechnung der Ausfallwahrscheinlichkeit hier eine Ausnahme darstellt. Verschleißbedingte Ausfälle können als Zufallsereignis betrachtet werden. Eine Beschreibung mit Hilfe der Weibull-Verteilung und die Bestimmung einer fiktiven konstanten Ausfallrate auf Basis des B10-Werts ist möglich. Wird Mechanik dagegen mit niedriger Anforderungsrate betrieben, kann meist keine aussagekräftige Ausfallrate angegeben werden. Hier muss mit deterministischen Methoden für die nötige Sicherheit gesorgt werden.

SCHLAGWÖRTER EN 61508 / systematische Fehler / zufällige Fehler / B_{10}-Wert / Ausfallrate / Weibull-Verteilung

SIL Assessment of Mechanics–
Failure probability of mechanical components

How to treat nonelectrical components is always a tricky question when safety equipment has to be assessed according SIL. As the scope of EN 61508 is limited to electrical components, the answer is still open. An obvious approach is to deal with mechanical components in the same manner as already done with electronical equipment. And, if difficulties occur it is reasonable to apply the requirements of the standard analogously. This approach shows that in most cases no "special treatment" of mechanics is necessary. Only when the failure probability has to be calculated mechanical parts need to be considered separately. A further complication is that in mechanical components, the failure behaviour depends to a very great extent on the mode of operation. When frequently used the main reason for a failure is wear out. Such failures can be considered as random events. Thus, it is possible to describe these events with the Weibull distribution. Based on the B_{10} value a fictitious constant failure rate λ_{10} can be determined as an approximation. If mechanics that is operated in the low demand mode no meaningful failure rate can be specified. Therefore, deterministic methods are necessary to achieve the safety target.

KEYWORDS SIL assessment / EN 61508 / mechanical equipment / E/E/PE systems / systematic failures / random failures / B_{10} value / fictitious constant failure rate / Weibull distribution

ANDREAS HILDEBRANDT, Pepperl+Fuchs

Wie behandelt man nichtelektrische Komponenten bei der SIL-Bewertung? Diese Frage kommt bei jedem SIL-Seminar „so sicher wie das Amen in der Kirche“. Aber was ist der Grund für diese immer wieder gestellte Frage? Ein Blick in die EN 61508 [1] gibt die Antwort: Der Anwendungsbereich besagter Norm ist beschränkt auf „elektrische, elektronische und programmierbare elektronische Systeme“ (E/E/PE-Systeme) (Bild 1). Im Teil 1, Kapitel 7.12.2 heißt es dazu: „Die Spezifikation, um die Anforderungen an die Sicherheitsfunktionen und die Anforderungen an die Sicherheitsintegrität für andere risikomindernde Maßnahmen zu erfüllen, ist nicht Gegenstand dieser Norm“. Ist diese Einschränkung wirklich zwingend notwendig oder können nichtelektrische Komponenten und Systeme genauso behandelt werden wie elektrische? Wenn Ja (das heißt, Mechanik kann wie Elektronik behandelt werden), wozu dann diese Einschränkung im Anwendungsbereich der EN 61508? Wenn Nein, wo liegt das Problem?

Zur Beantwortung dieser Fragen muss zunächst geklärt werden, wie bei der SIL-Bewertung von E/E/PE-Systemen vorgegangen wird. Anschließend kann dieses Vorgehen daraufhin untersucht werden, ob – und wenn Ja, wie – eine Anwendung auf mechanische Komponenten in vergleichbarer Weise möglich ist.

1. DREI ELEMENTE ZUR SIL-ERREICHUNG

Grundsätzlich müssen im Rahmen der SIL-Bewertung von Schutzeinrichtungen drei unterschiedliche Aspekte betrachtet werden [2]:

- Maßnahmen gegen systematische Fehler
- Maßnahmen gegen zufällige Fehler
- Maßnahmen zur Fehlertoleranz

Eine Erklärung für die Relevanz der drei genannten Punkte bei der SIL-Bewertung liefert eine genauere Betrachtung der Versagensursachen von Schutzeinrichtungen. Hier unterscheidet die Norm zwei Fehlerarten. Dies sind systematische Fehler und zufällige Fehler (Bild 2). Diese Unterscheidung ist in zweierlei Hinsicht wichtig: Erstens stellt sich die Frage, in wieweit die jeweiligen Fehler zu vermeiden sind, und zweitens, ob diese quantifiziert werden können. Bezüglich der Vermeidbarkeit ist leicht einzusehen, dass nur systematische Fehler vermieden werden können. Das „Werkzeug“ hierzu ist ein spezielles Qualitätsmanagement-System, das Functional Safety Management System (FSM-System).

Was die Quantifizierung der Fehler angeht, muss festgestellt werden, dass dies nur bei den zufälligen Fehlern über eine Wahrscheinlichkeitsaussage möglich ist. Die EN 61508 schreibt hierzu in Teil 4, Kapitel 3.6.5, Anmerkung 2: „… dass Systemausfallraten, die aus zufälligen Hardwareausfällen herrühren, mit vernünftiger Genauigkeit quantifiziert werden können, aber jene, die durch systematische Ausfälle entstehen, statistisch nicht genau quantifiziert werden können, …“ Insgesamt betrachtet führen diese Erkenntnisse zu den drei genannten Elementen der SIL-Erreichung. Der erste Punkt (Maßnahmen gegen systematische Fehler, mit anderen Worten: das FSM-System) entspricht dem linken Zweig in Bild 2, der zweite Punkt (Maßnahmen gegen zufällige Fehler, sprich: PFD-Berechnung) dem rechten Zweig und der dritte Punkt (Maßnahmen zur Fehlertoleranz, bekannt als Hardware-Fehlertoleranz HFT) dem mittleren Zweig.

Alle drei Elemente werden in nahezu identischer Weise von der EN 61511 thematisiert (Bild 3). Kapitel 5 der EN 61511, Teil 1, beschreibt das FSM-System, in Kapitel 9.2.4. Tabelle 3 und 4, sind Grenzwerte für die Ausfallwahrscheinlichkeit einer Sicherheitsfunktion definiert, und in Kapitel 11, Tabelle 5 und 6, sind Forderungen zur Hardware-Fehlertoleranz zu finden.

2. MECHANIK VERSUS ELEKTRONIK

Die Ausgangsfrage „Kann Mechanik bei der SIL-Bewertung genauso behandelt werden wie Elektronik?“ lässt sich anhand des genannten Schemas wenigstens

zum Teil leicht beantworten. Die Vermeidung systematischer Fehler mittels FSM-System ist sowohl bei Elektronik wie auch bei Mechanik in gleicher Weise möglich. Auch hinsichtlich Hardware-Fehlertoleranz können die Forderungen der EN 61511 entsprechend erfüllt werden. Eine Unterscheidung zwischen Elektronik und Mechanik ist in Bezug auf die beiden genannten Aspekte also nicht zwingend notwendig. Einzig bei der Berechnung der Versagenswahrscheinlichkeit sind prinzipielle Unterschiede auszumachen, sodass hier die von der Elektronik bekannte Vorgehensweise nicht direkt auf die Mechanik übertragen werden kann.

3. BEDEUTUNG DER AUSFALLRATE

Wie bereits erwähnt, lässt sich die Versagenswahrscheinlichkeit einer Komponente aufgrund zufälliger Fehler mit Hilfe einer Wahrscheinlichkeitsaussage quantifizieren. Üblicherweise geschieht dies durch Angabe der Ausfallrate λ. Für elektronische Geräte kann in der Regel unterstellt werden, dass die Ausfallrate λ während eines längeren Zeitraums (Gebrauchsdauer) konstant und deutlich von Null verschieden ist (Badewannenkurve).

Für mechanische Komponenten stellt sich die Situation anders dar. Hier ist zunächst zu klären, ob als Versagensursache zufällige Fehler in Betracht kommen oder ob ausschließlich systematische Fehler als Ursache ausgemacht werden können. Ist letzteres der Fall, so kann für eine mechanische Komponente keine Ausfallrate angegeben werden. Es ist demnach grundsätzlich zu hinterfragen, ob Ausfälle mechanischer Komponenten als Zufallsereignis betrachtet werden können. In Anlehnung an die Definitionen 3.6.5 und 3.6.6 der EN 61508, Teil 4, kann folgende Fragestellung bei der Klassifizierung von Ausfällen hilfreich sein: „War der Fehler zum Zeitpunkt der Inbetriebnahme bereits vorhanden? Kann der Ausfall prinzipiell reproduziert werden?“ Muss wenigstens eine der beiden Fragen bejaht werden, so wurde der Ausfall durch einen systematischen Fehler verursacht. Derartige Fehler können dann nicht mit Hilfe einer Ausfallrate quantifiziert werden (siehe oben). Anderenfalls handelt es sich um einen zufälligen Fehler.

4. AUSFALLVERHALTEN MECHANISCHER KOMPONENTEN

Die Normen zur funktionalen Sicherheit unterscheiden bei sicherheitstechnischen Einrichtungen zwei Betriebsarten: Die Betriebsart mit niedriger Anforderungsrate (engl. Low Demand Mode, kurz LDM) und mit hoher Anforderungsrate (engl. High Demand Mode, kurz HDM). Wird eine Schutzeinrichtung seltener als einmal pro Jahr benötigt, so wird diese mit niedriger Anforderungsrate betrieben, anderenfalls mit hoher Anforderungsrate. Diese Unterscheidung ist bei mechanischen Komponenten von großer Bedeutung, da sich die Art und Weise des Versagens in beiden Fällen völlig unterschiedlich darstellt. Während eine mit hoher Anforderungsrate betriebene Mechanik vorwiegend verschleißbedingt ausfällt, kann bei niedriger Anforderungsrate ein Versagen nahezu immer auf Alterungseffekte zurückgeführt werden.

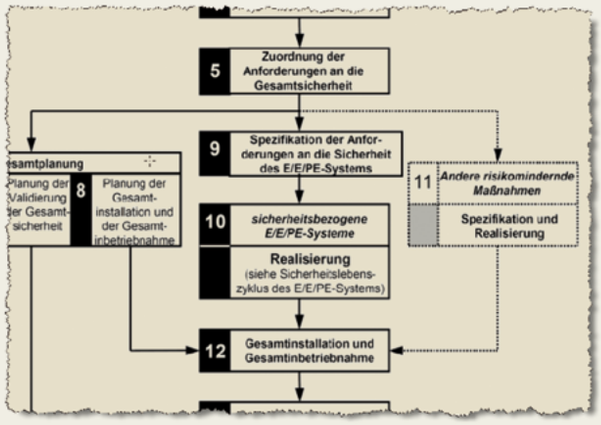


BILD 1: Im Sicherheitslebenszyklus ist die Phase „Spezifikation und Realisierung anderer risikomindernder Maßnahmen“ gestrichelt dargestellt, da sie nicht Gegenstand dieser Norm ist.

Entscheidend für die Berechnung der Ausfallwahrscheinlichkeit ist die Frage, ob es sich bei den genannten Versagensarten um Zufallsereignisse handelt. Ist dies der Fall, so kann eine Versagenswahrscheinlichkeit angegeben werden. Handelt es sich bei dem betreffenden Ausfall jedoch nicht um ein Zufallsereignis, so ist die Angabe einer entsprechenden Wahrscheinlichkeit unmöglich.

Ausfälle die durch Verschleiß zustande kommen, können meist als Zufallsereignis betrachtet werden, da zum Zeitpunkt der Inbetriebnahme der Fehler noch nicht vorlag (es gab noch keinen Verschleiß) und eine Reproduzierbarkeit in der Regel ebenfalls nicht gegeben ist.

Anmerkung: Bezüglich der Reproduzierbarkeit ist es von entscheidender Bedeutung, wie deutlich der Verscheiß ausgeprägt ist und welche Genauigkeit bei den Wiederholversuchen gefordert wird. Üblicherweise ist die Streuung der Lebensdauern verschleißbehafteter Komponenten jedoch so groß, dass Ausfälle als Zufallsereignisse betrachtet werden können. Die mathematische Modellierung von verschleißbedingten (zu-

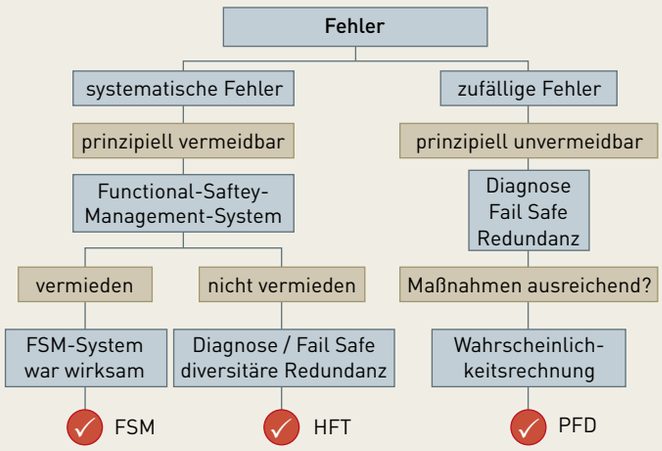
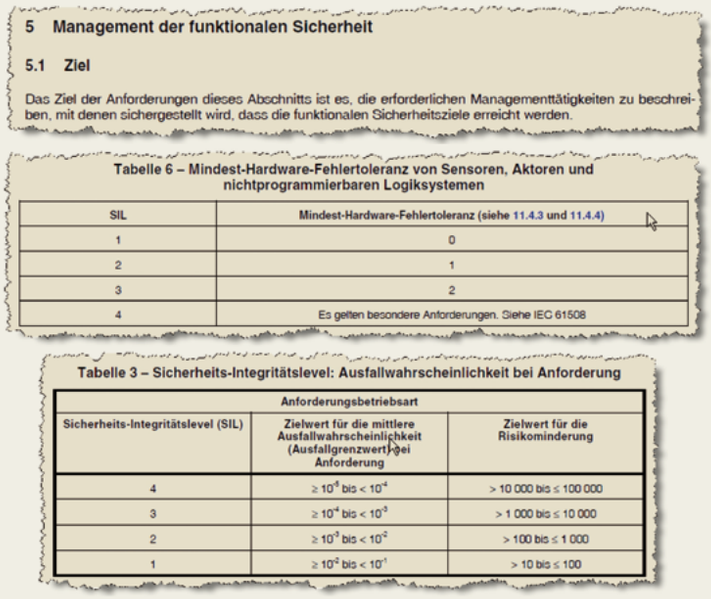


BILD 2: Fehlerarten und deren Behandlung.



5 Management der funktionalen Sicherheit

5.1 Ziel

Das Ziel der Anforderungen dieses Abschnitts ist es, die erforderlichen Managementtätigkeiten zu beschreiben, mit denen sichergestellt wird, dass die funktionalen Sicherheitsziele erreicht werden.

Tabelle 6 – Mindest-Hardware-Fehlertoleranz von Sensoren, Aktoren und nichtprogrammierbaren Logiksystemen

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

Tabelle 3 – Sicherheits-Integritätslevel: Ausfallwahrscheinlichkeit bei Anforderung

Anforderungsbetriebsart		
Sicherheits-Integritätslevel (SIL)	Zielwert für die mittlere Ausfallwahrscheinlichkeit (Ausfallgrenzwert) bei Anforderung	Zielwert für die Risikominderung
4	$\geq 10^{-5}$ bis $< 10^{-4}$	> 10 000 bis ≤ 100 000
3	$\geq 10^{-4}$ bis $< 10^{-3}$	> 1 000 bis ≤ 10 000
2	$\geq 10^{-3}$ bis $< 10^{-2}$	> 100 bis ≤ 1 000
1	$\geq 10^{-2}$ bis $< 10^{-1}$	> 10 bis ≤ 100

BILD 3: Die EN 61511 fordert ein FSM-System zur Fehlervermeidung, eine vom jeweiligen SIL abhängige HFT zur Fehlerbeherrschung und die Einhaltung SIL-abhängiger Grenzwerte bezüglich der Versagenswahrscheinlichkeit.

fälligen) Ausfällen kann dann mit Hilfe der Weibull-Verteilung erfolgen.

5. MECHANIK MIT NIEDRIGER ANFORDERUNGSRATE

Wird Mechanik mit niedriger Anforderungsrate betrieben, ist eine entsprechende mathematische Modellierung nicht möglich, da die Parameter der Weibull-Verteilung praktisch nicht bestimmbar sind. Auch ist es fraglich, ob Ausfälle aufgrund von Alterungsprozessen überhaupt als zufällig betrachtet werden können. Aus heutiger Sicht scheint es nicht möglich zu sein, für mechanische Komponenten die mit niedriger Anforderungsrate betrieben werden, eine Ausfallrate λ anzugeben, welche das reale Verhalten der jeweiligen Komponente mit ausreichender Genauigkeit beschreibt. Dies bedeutet jedoch nicht, dass in diesem Fall ein Versagen der Komponente ausgeschlossen werden kann. Vielmehr sind hier der technische Sachverstand und das Know-how erfahrener Fachleute gefragt, um durch geeignete Maßnahmen (wie Diagnose, regelmäßige Prüfung, Wartung, Redundanz) die erforderliche Sicherheit zu erreichen. Eine Berechnung der Ausfallwahrscheinlichkeit auf Basis fragwürdiger Zahlen wäre hier eher kontraproduktiv, da gegebenenfalls ein befriedigendes Berechnungsergebnis eine vermeintliche Sicherheit vorgaukeln könnte, welche in Wirklichkeit so nicht gegeben ist.

6. WEIBULL-VERTEILUNG UND B_{10}-WERT

Für verschleißbedingte Ausfälle ist – wie oben bereits erwähnt – eine Modellierung mit Hilfe der Weibull-Verteilung möglich. In diesem Fall kann eine mechanische Komponente bei der Berechnung der Versagenswahrscheinlichkeit einer Schutzeinrichtung berücksichtigt werden. Dabei ist jedoch zu beachten, dass die Ausfallrate hier nicht – wie bei elektronischen Komponenten üblich – konstant ist, sondern mit der Zeit ansteigt. Dies stellt in gewisser Weise ein Problem dar, da die Berechnung der Versagenswahrscheinlichkeit in der Regel mit Hilfe von Formeln geschieht, welche nur für konstante Ausfallraten gültig sind. Dieses Problem kann umgangen werden, indem die Weibull-Verteilung in einem begrenzten Zeitintervall durch eine konstante Ausfallrate angenähert wird (Bild 4).

Die Bestimmung dieser fiktiven konstanten Ausfallrate kann auf Basis des B_{10}-Wertes erfolgen. Der B_{10}-Wert dient häufig als Angabe der zu erwartenden Lebensdauer einer mechanischen Komponente. Hierbei handelt es sich um einen Zahlenwert, welcher angibt, nach welcher Belastung 10 % der Individuen einer Grundgesamtheit ausgefallen sind. Hierbei kann je nach Gegebenheit beziehungsweise Komponentenart die Belastung als reine Zeit, als Anzahl Schaltspiele, als gefahrene Kilometer oder ähnli-

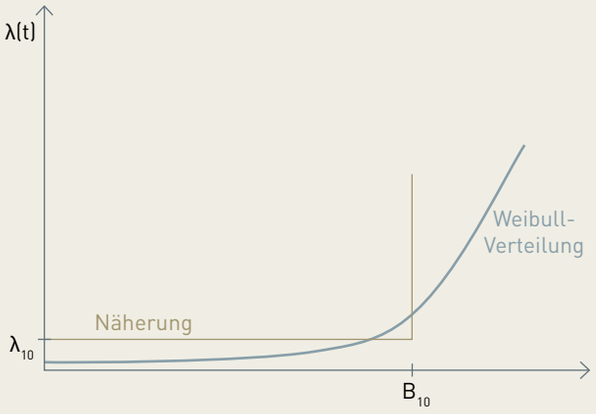


BILD 4: Annäherung der Weibull-Verteilung durch eine konstante Ausfallrate. Die Näherung ist nur innerhalb eines begrenzten Zeitraumes sinnvoll. Für große Zeiten (lange Betriebsdauern) wird die Näherung zunehmend ungenau.

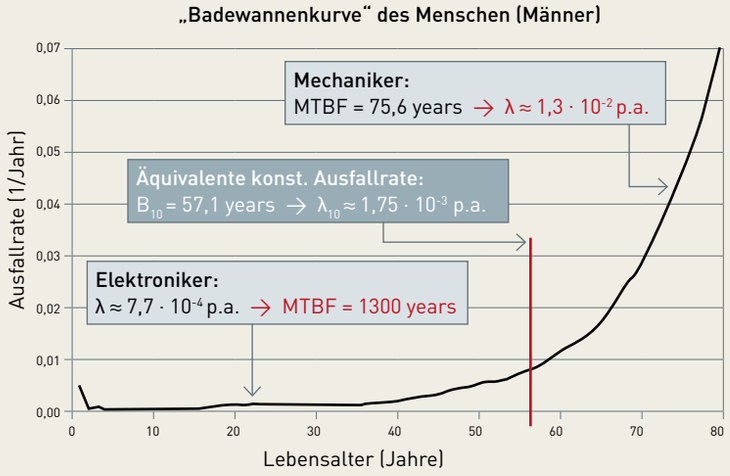


BILD 5: Ausfallrate des Menschen (Männer). Die Lebensdauer lässt sich mit Hilfe der Weibull-Verteilung beschreiben, wobei der B_{10}-Wert 57 Jahre beträgt. Bei elektronischen Geräten ist das Hauptaugenmerk auf den Boden der Badewannenkurve gerichtet. Bei mechanischen Komponenten ist vor allem der Verschleißbereich von Interesse.

ches angegeben werden. Um die Weibull-Verteilung durch eine konstante Ausfallrate anzunähern, bestimmt man eine fiktive, als konstant angenommene Ausfallrate (hier als λ_{10} bezeichnet), welche nach der dem B_{10}-Wert entsprechenden Zeit ebenfalls eine Versagenswahrscheinlichkeit von 10 % ergibt. Liegt der B_{10}-Wert dabei nicht als reine Zeitangabe vor, so muss die betreffende Angabe noch in eine Zeitangabe umgewandelt werden, indem der B_{10}-Wert durch die (applikationsspezifische) Belastung pro Zeiteinheit dividiert wird. Beträgt zum Beispiel der B_{10}-Wert eines Relais 300 000 Schaltspiele und wird das Relais 500 Mal pro Tag betätigt, so erhält man als zeitbezogenen B_{10}-Wert eine Dauer von 600 Tagen (rund 1,6 Jahre). Nach folgender Berechnungsvorschrift kann die fiktive konstante Ausfallrate λ_{10} bestimmt werden:

Gleichung 1: $$\lambda_{10} = \frac{0{,}1}{B_{10}} \quad \text{falls } B_{10} \text{ als Zeit gegeben ist, bzw.}$$

Gleichung 2: $$= \frac{0{,}1}{B_{10}} \cdot f_{Zyklus} \quad \text{falls } B_{10} \text{ als Zyklenzahl gegeben}$$

Für Zeiten, die größer sind als B_{10} (bzw. B_{10} / f_{Zyklus}) , stellt die fiktive Ausfallrate λ_{10} keine akzeptable Näherung mehr dar. Dies bedeutet, dass die entsprechende Komponente vor Erreichen dieser Zeit ausgetauscht oder gewartet werden muss.

7. BEISPIEL: MENSCH

Die Bedeutung und Anwendung des B_{10}-Werts und der daraus abgeleiteten Ausfallrate λ_{10} soll anhand eines anschaulichen Beispiels verdeutlicht werden. Hierzu wird die (Weibull-verteilte) Lebensdauer von in Deutschland lebenden Männern betrachtet. Bild 5 zeigt die „Badewannenkurve“ für Männer [3], also die Ausfallrate λ (t) über der Zeit t.

Sollen ausgehend von dieser „Badewannenkurve“ Aussagen bezüglich der Zuverlässigkeit oder Lebensdauer gemacht werden, so wird man feststellen, dass branchenabhängig verschiedene Betrachtungsweisen zu unterschiedlichen Aussagen führen, da bei Zuverlässigkeitsbetrachtungen Elektroniker und Mechaniker auf unterschiedliche Bereiche der Badewannenkurve fokussieren. Bei elektronischen Geräten ist der Boden der Badewannenkurve von besonderem Interesse, da erstens die Ausfallrate in diesem Bereich in der Regel deutlich von Null verschieden ist und zweitens der Anstieg der Ausfallrate im Verschleißbereich meist wenig ausgeprägt ist. Ein Elektroniker wird daher zur Quantifizierung der Zuverlässigkeit die Ausfallrate im flachen Teil der Badewannenkurve nennen. Für das Beispiel „Mensch“ wäre dies ein Wert von etwa $8 \cdot 10^{-4}$ pro Jahr. Um die MTBF eines Menschen zu bestimmen, würde ein Elektroniker von der genannten Ausfallrate den Kehrwert bilden

(MTBF = $1/\lambda$) und dieses Ergebnis dann als MTBF angeben. Als mittlere Lebensdauer (MTBF) würde er demnach den falschen Wert von 1300 Jahren nennen.

Anders verhält es sich, wenn ein Mechaniker die Zuverlässigkeit beurteilen würde. In der Mechanik ist es üblich, hauptsächlich den Verschleißbereich der Badewannenkurve zu betrachten. Entsprechend wird hier meist der Erwartungswert der Lebensdauer einer Komponente als Zuverlässigkeitskennwert verwendet. Für das Beispiel würde dies bedeuten, dass ein Mechaniker für den Menschen als MTBF den richtigen Wert von 76 Jahren nennen würde. Wird aus diesem Wert auf die Ausfallrate geschlossen, indem nach obiger Manier der Kehrwert der MTBF berechnet wird, erhält man einen deutlich zu großen Wert (hier $1{,}3 \cdot 10^{-2}$ pro Jahr anstelle des korrekten Werts von $8 \cdot 10^{-4}$ pro Jahr).

Um beides, sowohl die Lebensdauer als auch die Ausfallrate eines verschleißbehafteten Systems mit nur einem Wert näherungsweise beschreiben zu können, bedient man sich des B_{10}-Wertes. Im Falle des Menschen beträgt dieser 57 Jahre. Berechnet man nach Gleichung 1 daraus die fiktive Ausfallrate λ_{10}, so erhält man $1{,}7 \cdot 10^{-3}$ pro Jahr, also einen Wert, welcher lediglich rund doppelt so groß ist wie der „genaue“ Wert von $8 \cdot 10^{-4}$ pro Jahr. (Hinweis: Die PFD ist in Abhängigkeit des SIL logarithmisch skaliert. Eine Verdoppelung oder Halbierung der Ausfallrate ist daher von geringer Bedeutung. Entscheidend ist die Größenordnung; Nachkommastellen dürfen getrost auf eine signifikante Stelle gerundet werden.) Mit Hilfe des B_{10}-Wertes ist es demnach möglich, die wichtigsten Zuverlässigkeitskenngrößen (Lebensdauer und Ausfallrate) aus einem einzigen Wert abzuleiten. Es ist dabei jedoch zu beachten, dass die so ermittelte fiktive Ausfallrate λ_{10} nur für Zeiten eine akzeptable Näherung darstellt, die kleiner sind als B_{10} (im Beispiel also für $t < 57$ Jahre).

FAZIT

Abgesehen von der PFD/PFH-Berechnung können mechanische Komponenten bei der SIL-Bewertung genauso behandelt werden wie elektronische Komponenten. Die Notwendigkeit der Unterscheidung ergibt sich erst bei der Betrachtung des Ausfallverhaltens aufgrund zufälliger Fehler. Hier spielt insbesondere bei der Mechanik die Betriebsart eine entscheidende Rolle. Wird Mechanik im High Demand Mode betrieben, so fällt diese in der Regel verschleißbedingt aus. Derartige Ausfälle können weitgehend als Zufallsereignis angesehen werden und mit Hilfe der Weibull-Verteilung beschrieben werden. Eine Annäherung dieser Verteilung durch eine (zeitlich begrenzte) fiktive konstante Ausfallrate λ_{10} ermöglicht es in diesem Fall, die mechanische Komponente in die Berechnung der Ausfallwahrscheinlichkeit einer Schutzfunktion mit einzubeziehen. Basis für die besagte Approximation der Weibull-Verteilung ist der B_{10}-Wert, welcher häufig auch zur Angabe der zu erwartenden Lebensdauer herangezogen wird.

Für mechanische Komponenten, die im Low Demand Mode betrieben werden, kann in der Regel keine Ausfallrate angegeben werden, welche eine realitätsnahe Beschreibung des Ausfallverhaltens darstellt. Ausfälle sind hier in der Regel systematisch bedingt und stellen somit kein Zufallsereignis dar. Für die PFD-Berechnung stehen dann keine aussagekräftigen und belastbaren Werte zur Verfügung. Umso wichtiger ist es, in diesen Fällen mögliche Ausfälle kritisch zu beleuchten und durch entsprechende Maßnahmen (wie Diagnose, Hardware-Fehlertoleranz, Wartung und Instandhaltung) für die nötige Sicherheit zu sorgen. Technischer Sachverstand, praktische Erfahrung, sorgfältiges Arbeiten und verantwortungsbewusstes Handeln sind der Schlüssel zu sicheren Anlagen – nicht die PFD-Berechnung.

MANUSKRIPTEINGANG
14.12.2010
Im Peer-Review-Verfahren begutachtet

REFERENZEN

[1] EN 61508 Teil 1-6, „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“, November 2002
[2] Dirk Hablawetz, Norbert Matalla und Gerhard Adam, „IEC 61511 in der Praxis - Erfahrungen eines Anlagenbetreibers“, atp 10/2007
[3] Statistisches Bundesamt Wiesbaden, Sterbetafeln 2004
[4] VDI/VDE 2180, „Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT)“, 2009
[5] EN 61511; „Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 1-3“, Mai 2005

AUTOR

DR. ANDREAS HILDEBRANDT (geb. 1959) arbeitet seit 2006 als Leiter der Gruppe „Schulung und Gremienarbeit“ der Pepperl+Fuchs GmbH, Mannheim. Seine Arbeitsschwerpunkte sind unter anderem der Explosionsschutz und die funktionale Sicherheit. Daneben leitet er die ZVEI-Arbeitsgruppe „EMV“ und ist Mitglied im DKE GK 914, im DKE K 767.0.4 und im FA 6.13 der Gesellschaft Mess- und Automatisierungstechnik (GMA) des VDI/VDE.

Pepperl+Fuchs GmbH,
Lilienthalstr. 200, D-68307 Mannheim,
Tel. +49 (0) 621 776 14 54,
E-Mail: ahildebrandt@de.pepperl-fuchs.com

Wie die Sicherheit laufen lernte

Entwicklung der funktionalen Sicherheit in Deutschland

Der Beitrag zeigt die bisherige Entwicklung der Anlagensicherung mit Mitteln der Prozessleittechnik (PLT) auf und gibt einen Ausblick. Mit Herausgabe der IEC 61508/11 wird das abzudeckende Risiko in Sicherheitsintegritätsstufen (SIL) angegeben, denen eine nachzuweisende Mindestzuverlässigkeit der Schutzeinrichtung zugeordnet ist. Wegen der unterschiedlichsten Einsatzbedingungen in der chemischen Industrie liegen jedoch keine verlässlichen Fehlerraten von Feldgeräten vor. Es drohte ein Paradigmenwechsel, bei dem das Rechnen Vorrang gegenüber der korrekten Auslegung erhält. In Deutschland existiert ein sehr gutes PLT-Sicherheitskonzept, das dem ingenieurmäßigen Sachverstand entspricht und sich in der Praxis außerordentlich gut bewährt hat. In Zukunft sollten daher vornehmlich betriebsbewährte Geräte aus Standardgerätelisten in standardisierten Architekturen eingesetzt werden, für die Musterrechnungen vorliegen. Diese Vorgehensweise wird zur Zeit von deutscher Seite in die internationale Normung eingebracht. Dazu ist es aber unerlässlich, dass Unternehmen – speziell von der Anwenderseite – auch bereit sind, diese Aktivitäten finanziell zu unterstützen. In den folgenden Abschnitten wird die Evolution der Sicherheitstechnik beschrieben. Von deren sinngemäßer Steinzeit über deren Mittelalter gelangt man zu deren Neuzeit, die aus den Phasen „Der aufrechte Gang“, „Die internationale Normung“ und der sich notwendigerweise anschließenden „Wiederauferstehung“ besteht.

SCHLAGWÖRTER PLT-Schutzeinrichtung / SIL / Probabilistik / Ingenieursachverstand

How Safety Found its Feet –
The Evolution of Functional Safety in Germany

This paper outlines the development of the field “plant safety by means of process control engineering” up to now and gives an outlook on the future. With the publication of IEC 61508/11, the risk to be covered is rated by safety integrity levels (SIL). Each SIL is related to a minimum-reliability of the safety instrumented system. However, due to the different conditions in the chemical industry, there no reliable failure-rates of field device are available. There was the danger of a paradigm change towards preferring extensive mathematical calculations instead of focusing on proper design. In Germany, a very good PLT-safety-concept exists that considers the engineer’s expertise and has proven itself in practical use. In the future, only prior-use-devices from standard-device-lists should be used in standardized architectures. For these architectures, example calculations are available. These aspects are introduced to the international standardization by the German delegates right now. For that purpose, it is essential that companies – especially from the user side – support these activities financially. In the following, the evolution of safety is described. Starting with the corresponding Stone Age, going through Middle Ages, one reaches the Modern Age that consists of the phases "Upright Gait", "International Standardization", and necessarily following "Resurgence".

KEYWORDS Safety Integrated System / SIL / Probabilistic / Engineer’s Expertise

PIRMIN NETTER, Infraserv Höchst

Die technische Entwicklung schreitet seit der industriellen Revolution Anfang des 19. Jahrhunderts geradezu atemberaubend voran. Als Folge von zum Teil sehr schweren Unfällen entstanden parallel dazu Sicherheits- und Unfallverhütungskonzepte. Im Bereich der Prozessindustrie wurden früher bevorzugt die unmittelbar wirksamen Schutzeinrichtungen wie Sicherheitsventile und Berstscheiben eingesetzt. Die Themen Substitution und inhärente Sicherheit folgten später.

Mit Beginn der zweiten industriellen Revolution um 1950, deren Grundlage die Rationalisierung der industriellen Fertigung durch Automatisierung ist, trat ergänzend zu den bisherigen Sicherheitssäulen eine weitere hinzu: die Anlagensicherung mit Mitteln der Automatisierungstechnik. Nach fast 30-jährigem Umgang mit dieser speziellen Art der Sicherheitstechnik möchte der Autor einen Überblick über die bisherige Entwicklung dieses wichtigen und interessanten Fachgebiets geben.

Die Anlagensicherung mit Mitteln der Automatisierungstechnik unterliegt, wie viele andere Bereiche auch, einer ständigen Evolution. Das zeigt sich rein äußerlich bereits in der Namensgebung: Ausgehend von der MSR-Technik über die EMR- oder EMSR-Technik ist man heute beim Begriff der Prozessleittechnik angelangt.

1. STEINZEIT DER SICHERHEITSTECHNIK: 1966 BIS 1980: ERSTE GEHVERSUCHE

Im Zuge der verstärkten Automatisierung größer und komplexer werdender Anlagen der Verfahrenstechnik in der Nachkriegszeit wurden auch der MSR-Technik in vermehrten Maße Sicherheitsaufgaben übertragen, weil die anderen Methoden in bestimmten Anwendungsfällen nicht zweckmäßig oder alleine nicht ausreichend waren.

Das erste Regelwerk, das sich mit dieser Thematik beschäftigt, ist die VDI/VDE-Richtlinie 2180 [1] aus dem Jahr 1966 mit dem Titel: „Sicherung von Anlagen der Verfahrenstechnik“. Dieses Papier wurde überwiegend von Betreibern und Herstellern erarbeitet und hatte lediglich die Anlage selbst und das erzeugte Produkt als Schutzziel im Auge. Daher kommt auch der Name „Anlagensicherung“, der sich seltsamerweise bis heute gehalten hat, obwohl sich die Schutzziele im Sinne der Evolution deutlich ausgeweitet haben. Man sprach folgerichtig von Sicherungseinrichtungen und hat wesentliche Aspekte, die auch heute noch Gültigkeit haben, bereits damals formuliert:

- Verantwortlichkeiten sind festzulegen
- Frühzeitiges Festlegen der „Sicherheitskenngrößen“ wie Druck oder Temperatur nach den Kriterien: gut, zulässig, unzulässig
- Grenzwerte sind so zu legen, dass sie sicherheitstechnisch einwandfrei und wirtschaftlich angemessen sind
- Zweckdienliche und hochwertige Geräte mit langer Lebensdauer sind einzusetzen; Einbauort und -art sind zweckentsprechend zu wählen
- Funktionsprüfungen sollen Fehler aufzeigen, die auftreten können, aber auf andere Weise nicht erkennbar sind
- Unterscheidung in selbstmeldende und nicht selbstmeldende Ausfälle
- Eine Prüfanweisung und die Dokumentation der Prüfung wird empfohlen
- Ausführliche Behandlung der m-von-n-Bewertung

So hatte beispielsweise eine 1-von-2-Sicherungseinrichtung den in Bild 1 dargestellten Aufbau.

Wo stehen wir am Ende der Steinzeit der Sicherheitstechnik? Das Schutzziel war zwar lediglich die Anlage selbst und das erzeugte Produkt, aber mit den formulierten Konzepten war man bereits auf dem Wege zum aufrechten Gang!

2. MITTELALTER DER SICHERHEITSTECHNIK: 1980 BIS 1993 STÖRFALLVERORDNUNG UND MIKROPROZESSOREN

Nach dem Seveso-Unglück 1976 wurde 1980 die Störfallverordnung [2] in Kraft gesetzt. Sie fordert eine Sicherheitsanalyse, in der die sicherheitstechnisch bedeutsa-

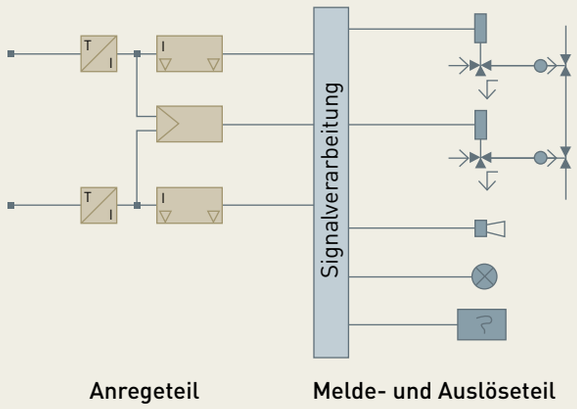


BILD 1: Aufbau einer MSR-Sicherungsein richtung im Jahre 1966

men Anlagenteile benannt werden, und verlangt Vorsorgemaßnahmen zur Verhinderung von Störfällen. Dazu gehören auch MSR-Einrichtungen und die dort so genannten Warn-, Alarm- und Sicherheitseinrichtungen. Der Widerstand gegen den damit verbundenen bürokratischen Aufwand war bei den betroffenen Firmen zum Teil erheblich. Die Dokumentationspflicht hat aber zu einer weiteren Systematisierung der Sicherheitsarbeit beigetragen.

Eine große Hilfe für Planer, Errichter und Betreiber war das 1983 erschienene Buch von G. Strohmann: „Anlagensicherung mit Mitteln der MSR-Technik“ [3]. Es enthält unter anderem eine ausführliche Diskussion des Einflusses von Gerätefehlern auf Sicherungseinrichtungen bei ein- und mehrkanaliger Auslegung. Es gibt kritische Anmerkungen zu der Zahlengläubigkeit in der „heutigen“ (1983!) Zeit. Quantitative Betrachtungen seien für Relativaussagen gut, für Absolutaussagen jedoch sehr fraglich.

Anfang der 80er-Jahre hält der Mikroprozessor in verstärktem Maße Einzug in die Sicherheitstechnik. Ein erstes Buch zu diesem Thema war von Hölscher/Rader: „Mikrocomputer in der Sicherheitstechnik“ [4] aus dem Jahr 1984. Hier wird dargestellt, dass komplexe Aufgaben zwar einfacher und kostengünstiger mit dieser Technik lösbar sind, das Fehlerverhalten aber nicht ohne Weiteres vorhersagbar ist. Als „Orientierungshilfe“ werden 5 Sicherheitsklassen aus den bisherigen Anwendungen in unterschiedlichen Bereichen „konstruiert“, je nach zu erwartendem Fehlerverhalten. Diesen Klassen werden Maßnahmenbündel technischer und organisatorischer Art zur Fehlervermeidung und Fehlerbeherrschung zugeordnet.

Mitte der 80er-Jahre werden weitere Schutzziele für die MSR-Technik „entdeckt“:

2.1. Neues Schutzziel: Personen

Im Jahre 1984 erscheint die Zweite Auflage der VDI/VDE 2180 [5]. Die Mitglieder des Arbeitskreises waren im Wesentlichen wieder die Betreiber. Die wichtigsten Neuerungen waren:

- Klassifizierung in Betriebs- und Sicherungseinrichtungen
- Sicherungseinrichtungen werden unterteilt in Überwachungs- und Schutzeinrichtungen
- Neben den Sachschäden werden Personenschäden berücksichtigt
- Die Fehleranalyse wird verbindlich eingeführt

und „Geräte, deren Eignung durch Bewährung im praktischen Einsatz unter vergleichbaren Bedingungen erwiesen ist, sind solchen vorzuziehen, deren Eignung allein analytisch oder unter Laborbedingungen ermittelt wurde. Gleichartige Geräte für Betriebs- und Sicherungseinrichtungen innerhalb einer Anlage verringern Bedienungsfehler und erleichtern die Instandhaltung.“ [5]

Diese Aussage von damals ist heute wieder außerordentlich aktuell. Wir kommen darauf im Zusammenhang mit der NE 130 im Jahr 2010 zurück.

2.2 Neues Schutzziel: Wasser

Mitte der 80er-Jahre ist auch die große Zeit der Überfüllsicherungen. Das Wasserhaushaltsgesetz und länderspezifische Verordnungen (VAwS) und die TRbF 510 [6] legen Anforderungen fest, und die NE 90 interpretiert und konkretisiert die Vorgaben. Überfüllsicherungen müssen bauartzugelassen sein und regelmäßig funktionsgeprüft werden. In der Regel handelt es sich um Überwachungseinrichtungen im Sinne der VDI/VDE 2180 und nur in Ausnahmefällen um Schutzeinrichtungen. Die intensiv betriebene Umsetzung der VAwS führte zu zahlreichen Nachrüstungen in den Betrieben und zur Entwicklung neuer Überfüllsicherungen mit überwiegend aktivem Fehlerverhalten seitens der Hersteller.

2.3 Der Risikobegriff hält Einzug

In diesem Zeitraum gewinnt auch der Begriff des Risikos stärkere Bedeutung in der Normung. Eine klare Darstellung der Zusammenhänge zwischen Risiko, Sicherheit und Gefahr liefert die DIN VDE 31000, Teil 2 [7] durch Einführung des Grenzrisikos.

Im Jahre 1989 erscheint die DIN V 19250 [8]. Sie ist anwendungs- und technologieunabhängig und beschreibt mittels des Risikographen ein qualitatives Verfahren zur Risikoabschätzung. Es werden 8 Anforderungsklassen

(AK) eingeführt, die ein Maß für das abzudeckende Risiko sind und die über objektivierbare Risikoparameter bestimmt werden. Den AK werden Maßnahmenbündel technischer und organisatorischer Art zugeordnet, die dann später in der DIN V 19251 [9] im Jahre 1995 ausführlich beschrieben werden. Man erkennt ansatzweise eine Orientierung am Sicherheitslebenszyklus, und es werden tiefer gehende Überlegungen, zum Beispiel anhand der Fehlertoleranzzeit, angestellt.

Leider konnte sich im AD Merkblatt A6 [10] diese „moderne Art" der sicherheitstechnischen Festlegung noch nicht durchsetzen. Als Ersatz für Sicherheitsventile werden zwar MSR-Sicherheitseinrichtungen in unterschiedlichen Auslegungsvarianten, wie fehlersicher, redundant oder selbstüberwachend vorgesehen, der Zusatz „je nach abzudeckendem Risiko" fehlt jedoch. Konsequenz: Noch heute werden derartige Einrichtungen grundsätzlich redundant aufgebaut.

2.4 Papier, Papier, Papier

… und wieder meldet sich die Störfallverordnung (Novelle 1988) [11] mit einer Erweiterung der Dokumentationspflicht für Prüf- und Überwachungsarbeiten.

2.5 Erstes Regelwerk für Rechner

Mit der DIN V VDE 0801 [12] werden 1990 erstmals Grundsätze für Rechner mit Sicherheitsaufgaben in einer Norm formuliert. Im Gegensatz zu konventioneller Technik liegt der Schwerpunkt der Betrachtung wegen des Softwareanteils bei den systematischen Fehlern. Auf Basis der DIN V 19250 werden Anforderungen an das Fehlerverhalten formuliert und je nach AK Maßnahmen zur Fehlervermeidung und Fehlerbeherrschung festgelegt. Die Diskussion der Fehlerarten und der Gegenmaßnahmen orientiert sich am Sicherheitslebenszyklus. Zusammen mit der Version A1 aus dem Jahr 1994 ist dieses Werk ein Vorreiter für die internationalen Normen, die im Kapitel „Neuzeit II" vorgestellt werden.

Mit Ende des Mittelalters der Sicherheitstechnik wurde also ein erheblicher Fortschritt in unserer Evolutionsgeschichte erreicht: Mit der Entdeckung von „Leib und Leben" als Schutzziel, der Orientierung am abzudeckenden Risiko über die Anforderungsklassen, der Integration von Mikroprozessoren in die Sicherheitswelt und einer sauberen, nachvollziehbaren Dokumentation geht die Entwicklung voran.

4. NEUZEIT DER SICHERHEITSTECHNIK, EPOCHE I: 1993 BIS 2002 – DER AUFRECHTE GANG

Die Neuzeit bricht Anfang der 90er-Jahre an. Es war bereits sehr vieles geregelt, insbesondere durch die VDI/VDE-Richtlinie 2180. Es gab jedoch zwei Herausforderungen:

1 | In anderen Regelwerken wurden andere Begriffe benutzt. Es gab Sicherungseinrichtungen, Sicherheitseinrichtungen, Schutzeinrichtungen, Überwachungseinrichtungen, Warn-, Alarm- und Sicherheitseinrichtungen.
2 | Historisch gewachsen entstanden verschiedene firmenspezifische PLT-Sicherheitskonzepte, die sich zwar alle stark an der VDI/VDE-Richtlinie 2180 orientierten, aber mit unterschiedlicher Terminologie: So gab es Einrichtungen für Schutz, Sicherheit, Klassen A, B, C, Kategorie I und II, Klassen A0, A1, A2 und Schadensbegrenzungseinrichtungen.

Im Zeitalter der Störfallvordnung landeten dann Sicherheitsanalysen unterschiedlicher Unternehmen auf dem Schreibtisch desselben Gutachters oder Aufsichtsbeamten. Das Erstaunen über die Vielfalt der Begriffe und Konzeptionen war bei diesen Personen verständlicherweise sehr groß. Es bestand also ein erheblicher Harmonisierungsbedarf. Dieser Aufgabe nahm sich die Namur an, und unter der Obmannschaft des Autors entstand 1993 im Namur-AK 4.5 die NE 31: „Anlagensicherung mit Mitteln der Prozessleittechnik" [13]. Dieses Papier wurde damals zur auflagenstärksten Namur-Empfehlung. Die wesentlichen Inhalte waren:

- Erstmals Einführung des Schutzziels Umwelt (als Konsequenz aus der StörfallV)
- Klassifizierung und Kennzeichnung in:
  - PLT-Schutzeinrichtungen, Klasse A: Personen- und Umweltschäden (Z)
  - PLT-Schutzeinrichtungen, Klasse B: Sachschäden (S)
  - PLT-Überwachungseinrichtungen, Klasse C (S)
  - Neu! PLT-Schadensbegrenzungseinrichtungen, Klasse X (Z)
- Einführung der Risikobereiche I und II für Schutzeinrichtungen, je nach abzudeckendem Risiko und sicherheitsbezogener Verfügbarkeit der eingesetzten Geräte
- Vorgehensweise bei Schutzeinrichtungen:
  1 | Abschätzung des abzudeckenden Risikos
  2 | Festlegung der Anforderungen
  3 | Zuordnung technischer und organisatorischer Maßnahmen
- Gegenüberstellung der Begriffe aus der NE 31 und der StörfallV

In der DIN V VDE 0801/A1 (1994) [14] wurde erstmals der Begriff „betriebsbewährt" näher gefasst: „Einsatz einer Betrachtungseinheit, die im Wesentlichen unverändert über einen ausreichenden Zeitraum in zahlreichen, verschiedenen Anwendungen betrieben wurde und bei der keine oder nur unwesentliche Fehler festgestellt wurden (mind. 10 Systeme, je 1 Jahr Betriebsdauer)." Darüber ist eine Dokumentation zu führen. Zweck der Vorgehensweise ist der Nachweis, dass das System hinreichend frei von systematischen (Entwurfs-)Fehlern ist.

Das VdTÜV-Merkblatt 372 [15] aus dem Jahre 1997 beschäftigt sich mit der Prüfung sicherheitsrelevanter MSR-Einrichtungen. Nach jeder Phase des Sicherheitslebenszyklus wird ein Haltepunkt eingeführt, und es werden die jeweilig erforderlichen Prüfschritte beschrieben.

Erfreulicherweise wurden die Empfehlungen der NE 31 in den Firmen weitgehend umgesetzt, sodass Mitte der 90er-Jahre damit begonnen werden konnte, die VDI/VDE 2180 [16] abermals zu aktualisieren. Dies erfolgte erstmals unter Einbeziehung aller am Sicherheitsprozess beteiligten Gruppen: Herstellern, Anwendern, Gutachterinstitutionen, der Wissenschaft und Aufsichtsbehörden. In der Auflage von 1998 wurden viele Aspekte der NE 31 übernommen und die StörfallV einbezogen. Daraus resultierte die klare

Unterscheidung in die nicht sicherheitsrelevanten Betriebs- und Überwachungseinrichtungen (Kennzeichnung S), die im Prozessleitsystem integriert werden dürfen, und die sicherheitsrelevanten Schutz- und Schadensbegrenzungseinrichtungen (Kennzeichnung Z), die über sicherheitsgerichtete Steuerungen realisiert werden müssen. Es wurde der Risikograph aus der DIN V 19250 übernommen, als eine Methode der qualitativen Risikoabschätzung.

Die VDI/VDE 2180 wird später (2004) in der „Vollzugshilfe zur Störfallverordnung" [17], die die Verwaltungsvorschriften ersetzt, einbezogen und wird damit zum wichtigsten Regelwerk der funktionalen Sicherheit in Deutschland. 1999 erscheint die NE 79: „Mikroprozessorbestückte Geräte in der Anlagensicherung" [18]. Sie ist unter Mitarbeit namhafter Hersteller entstanden. Seit Ende der 80er wurden sicherheitsgerichtete speicherprogrammierbare Steuerungen (SSPS) zertifiziert. Das wurde seitens der Anwender akzeptiert, da diese Systeme in den Betrieben vergleichbaren Einsatzbedingungen ausgesetzt sind („klimatisierter Schaltraum"), die wenig von den Laborbedingungen, unter denen sie getestet wurden, abweichen.

In der NE 79 wird allerdings klar festgestellt, dass die Zertifizierung von Feldgeräten, analog zu den SSPS, nicht zweckmäßig und somit auch nicht erwünscht sei, da die individuellen Prozess-, Stoff- und Umgebungsbedingungen in einem derartigen Verfahren nicht berücksichtigt werden können. Aber gerade dieses Thema, die Anpassung der am Markt erhältlichen Geräte an den eigenen Prozess, ist der Kern professioneller Sicherheitsarbeit und erfordert dringend den ingenieurmäßigen Sachverstand und umfassende Erfahrung. Deshalb wurden in der NE 79 alternativ zur Zertifizierungspraxis Wege aufgezeigt, wie man zu betriebsbewährten Geräten gelangen kann.

Die wesentlichen Inhalte sind:

- Aussagen über den Nachweis der Betriebsbewährung durch Anwender in drei Schritten:
  - Anwender-Typprüfung
  - Gezielte Erprobung
  - Einsatz einer größeren Stückzahl über einen längeren Zeitraum (10 an unterschiedlichen Stellen mit unterschiedlichen Randbedingungen, ein Jahr lang)
- Aussagen über den Nachweis der Betriebsbewährung durch Hersteller/Vorgehensweise beim Vorliegen einer Herstellerbescheinigung (Muster dafür in der Ausgabe 2004)
- Aussagen über die Vorgehensweise bei nicht betriebsbewährten Geräten
- Anforderungen an Erst- und Wiederholungsprüfungen
- Forderungen an Hersteller für künftig zu entwickelnde Geräte

Als Hauptziel wurde formuliert: Die Anwender benötigen einen Gerätetyp, der „AK-4 fähig" und einkanalig bis AK-4 und in 1v2-Redundanz für AK 5 und 6 einsetzbar ist.

Im Jahr 2000 erscheint Blatt 5 der VDI/VDE-Richtlinie 2180 [19] mit dem Titel „Einsatz von speicherprogrammierbaren Steuerungen". Ebenfalls im Jahr 2000 fordert eine weitere Novelle der StörfallV die Einführung eines Sicherheitsmanagementsystems. Die Vervollständigung in dieser Epoche war die NE 93: „Nachweis der sicherheitstechnischen Zuverlässigkeit von PLT-Schutzeinrichtungen" [20] aus dem Jahr 2001. Hiermit wurde der Grundstein für eine flächendeckende Stördatenerfassung in Deutschland gelegt. Es wurden die Mindestanforderungen für eine derartige Datensammlung formuliert und ein Konzept erstellt, wie die Zahlen über die Namur zusammengeführt und ausgewertet werden können. Als großer Erfolg darf dabei gewertet werden, dass sich mittlerweile etwa 40 Firmen an der Stördatenerfassung beteiligen mit insgesamt rund 40 000 eingesetzten PLT-Schutzeinrichtungen. Mit Hilfe dieser Daten konnte der Nachweis erbracht werden, dass die in den Regelwerken formulierten Sicherheitskonzepte in der Praxis greifen.

4. NEUZEIT DER SICHERHEITSTECHNIK, EPOCHE II: 2002 BIS 2007 – DIE INTERNATIONALE NORMUNG SCHLÄGT ZU

Ergänzend zum damit erreichten „aufrechten Gang der Sicherheitstechnik" sind zwei weitere Namur-Empfehlungen entstanden:

1 | Die NE 97: „Feldbus für Sicherungsaufgaben" [21] im Jahr 2003. Hier wird näher auf die Zertifizierungspraxis eingegangen und auf die Trennung von sicherheitsrelevanten Komponenten des Feldbusses von nicht sicherheitsrelevanten.
2 | Die NE 106: „Prüfintervalle für PLT-Schutzeinrichtungen" [22] im Jahr 2006. In diesem Papier wird beschrieben, wie das bisher übliche Mindestprüfintervall von einem Jahr verlängert werden kann. Wesentliche Voraussetzungen dafür sind die Mehrkanaligkeit und ein hoher Grad von Diagnosemöglichkeiten.

Mit der Übernahme international entstandener Normen in das nationale Regelwerk, der DIN EN 61508 (VDE 0803) [23] im Jahr 2002 und der DIN EN 61511 (VDE 0810) [24] im Jahr 2005, verbunden mit der Zurückziehung aller nationalen Normen auf diesem Gebiet am 1. August 2004, drohte jedoch ein Paradigmenwechsel. In diesen neuen Regelwerken ist die Orientierung am Sicherheitslebenszyklus und die damit verbundene Konzentration auf das Vermeiden systematischer Fehler in der Entwicklungsphase von Geräten zu begrüßen. Die Forderung nach einem Sicherheitsmanagementsystem unterstützt die notwendige systematische Vorgehensweise bei Sicherheitsaufgaben und regelt klar die Verantwortlichkeiten. Ebenso ist die Einführung von Sicherheitsintegritätsstufen (Safety Integrity Levels), den SIL, akzeptiert. Lassen sie sich doch sehr gut auf die ehemaligen AKs abbilden. Neu in der Sicherheitsbetrachtung war der Schwenk von den einzelnen Geräten hin zur gesamten Sicherheitsfunktion. Jedem SIL wird eine Mindestzuverlässigkeit für die PLT-Schutzfunktion zugeordnet, die „Probability of Failures on Demand" (PFD). Was auch noch heute erhebliches Kopfzerbrechen in diesem Zusammenhang bereitet, ist die Forderung eines rechnerischen Nachweises der PFD für derartige Schutzkreise. Die Formel für einkanalige Systeme lautet:

$$PFD = \tfrac{1}{2} \cdot \lambda_{DU} \cdot T_i \qquad (1)$$

Mit PFD: Wahrscheinlichkeit eines passiven Fehlers bei Anforderung
λ_{DU}: Fehlerrate gefährlicher, unentdeckter Fehler
T_i: Prüfintervall

In der chemischen und pharmazeutischen Industrie liegen allerdings keine verlässlichen Daten über die Ausfallraten einzelner Geräte vor, weil diese in ganz unterschiedlichen Umgebungsbedingungen eingesetzt werden. Das betrifft insbesondere die Feldgeräte, die Sensoren und Aktoren. Die Raten können um Zehnerpotenzen schwanken! Trotzdem werden zahlreiche Rechnungen durchgeführt, bei denen das Ergebnis auf vier oder mehr Stellen hinter dem Komma genau angegeben wird. Zwei Beispiele sollen die Problematik verdeutlichen:

Das erste Beispiel zeigt, wie empfindlich das Ergebnis auf die Variation der Eingangswerte reagiert. Die Schutzeinrichtung hat die in Bild 2 gezeigte Redundanzstruktur.

Die Näherungsformel aus Blatt 4 der VDI/VDE 2180 für dieses System lautet:

$$PFD_{total} = (\lambda_{DU}^{\,2} \cdot T_i^2 + \beta \cdot \tfrac{1}{2} \lambda_{DU} \cdot T_i)_{Sensor} + PFD_{Logik} + ((\lambda_{DU}^{\,2} \cdot T_i^2)/3 + \beta \cdot \tfrac{1}{2} \lambda_{DU} \cdot T_i)_{Aktor} \quad (2)$$

Mit β: Anteil unerkannter passiver Fehler gemeinsamer Ursache

Die PFD der Logik beträgt 2×10^{-5}, und für β wird ein Wert von 5 % angenommen. Aus zwei unterschiedlichen Quellen findet man für den Aktor identisches λ_A von 0,05, für den gleichen Sensor jedoch unterschiedliche Werte für λ_S von 0,3 beziehungsweise 0,02. Führt man die Berechnung alternativ mit diesen beiden Werten durch und variiert T_i zusätzlich zwischen monatlich und jährlich, so erhält man 4 Fallunterscheidungen mit folgendem interessanten Ergebnis (siehe Tabelle 1).

Die Ergebnisse variieren also zwischen SIL 1 und SIL 3, je nach Wahl der Eingangsdaten.

Welche Stilblüten die Rechnerei mitunter noch hervorbringt, zeigt das 2. Beispiel, ebenfalls aus der Praxis: Eine relativ komplexe Schutzeinrichtung (siehe Bild 3), bei der jeder der fünf Zweige nochmals eine Unterstruktur hat und in der insgesamt etwa ein Dutzend Sensoren und Aktoren eingesetzt sind, wird vom Gutachter folgendermaßen beschrieben:

„Die PFD bei dieser Einrichtung ist kleiner als $6{,}2176 \times 10^{-4}$. Dieses Ergebnis entspricht SIL 3 gemäß IEC 61511. Die Eingangsparameter sind allgemein zugänglichen Quellen entnommen." Das Ergebnis wird auf vier Stellen genau angegeben. Wissenschaftliche Untersuchungen haben jedoch ergeben, dass die Eingangsparameter bei gleichen Geräten um Größenordnungen schwanken können. Bereits im ersten Semester eines Ingenieurstudiums lernt man, wie man mit einer derartigen Aufgabenstellung richtig umgeht! Auch die SIL-Zertifizierungen von Einzelgeräten werden ohne Berücksichtigung der genannten Unschärfen durchgeführt. Die Hersteller sind dabei oft auf die Angaben von Fehlerraten der verbauten Komponenten ihrer Unterlieferanten angewiesen. Mittlerweile sehen nicht nur die Anwender, sondern auch andere am Sicherheitsprozess beteiligte Gruppen die Zertifizierung von Feldgeräten als sehr fragwürdig an.

Noch problematischer ist es, aus solchen Datenquellen eine nutzbare Lebensdauer für Geräte in Sicherheitsanwendungen abzuleiten. In der DIN EN 61508 (VDE 0803) wird zum Beispiel eine mittlere Lebensdauer von 8–12 Jahren (abgeleitet von Elektrolytkondensatoren!) angegeben. Prompt wird das auf alle Geräte, sogar rein mechanische Komponenten, übertragen. Damit nicht genug! Es gibt SIL-Zertifikate, in denen Lebensdauern angegeben werden, die nur auf Annahmen beruhen und in denen die Instandhaltungsmaßnahmen der Anwender völlig außer Acht gelassen werden, mit dem Hinweis, dass nach Ablauf dieser Lebensdauer das SIL-

BILD 2: Redundanzstruktur für Beispiel 1

Sensorik 2oo3	Logik 1oo3	Aktorik 1oo2	Total
Quelle 1 $9{,}8 \cdot 10^{-2}$ jährliche Prüfung	$2 \cdot 10^{-5}$	$2{,}1 \cdot 10^{-3}$	$1 \cdot 10^{-1}$ **SIL 1**
Quelle 2 $9 \cdot 10^{-4}$ jährliche Prüfung	$2 \cdot 10^{-5}$	$2{,}1 \cdot 10^{-3}$	$3 \cdot 10^{-3}$ **SIL 2**
Quelle 1 $1{,}3 \cdot 10^{-3}$ monatliche Prüfung	$2 \cdot 10^{-5}$	$1{,}1 \cdot 10^{-4}$	$1{,}4 \cdot 10^{-3}$ **SIL 2**
Quelle 2 $4{,}4 \cdot 10^{-5}$ monatliche Prüfung	$2 \cdot 10^{-5}$	$1{,}1 \cdot 10^{-4}$	$1{,}7 \cdot 10^{-4}$ **SIL 3**

TABELLE 1: Rechenergebnisse bei Variation der Eingangsparameter

- Quelle 1 mit jährlicher Prüfung führt zu SIL 1
- Quelle 2 mit jährlicher Prüfung zu SIL 2
- Quelle 1 und monatlicher Prüfzyklus ergibt SIL 2 und
- Quelle 2 mit monatlicher Prüfung sogar SIL 3

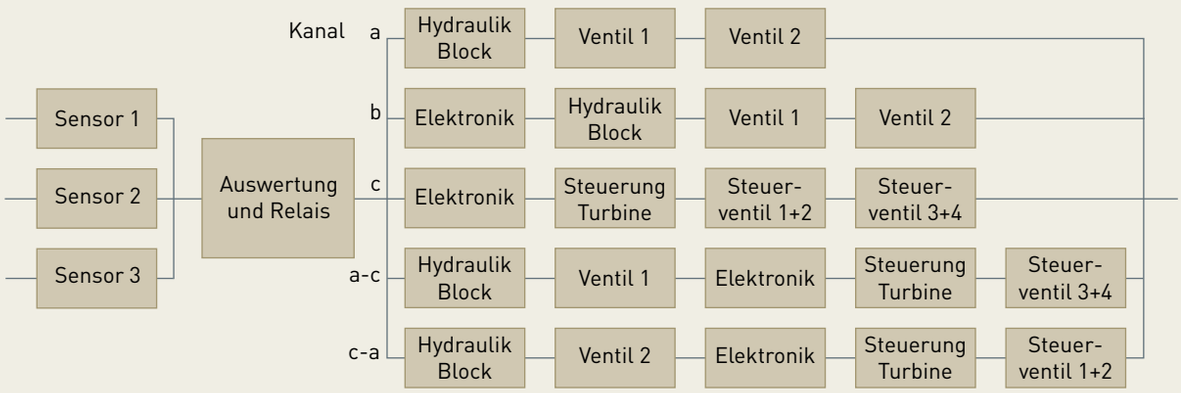


BILD 3: Blockschaltbild einer komplexen PLT-Schutzeinrichtung

Zertifikat seine Gültigkeit verliert. Abenteuerlich! Auf Basis dieser Erkenntnisse ist die Vorgehensweise einiger Anwender als sehr bedenklich anzusehen, nur noch SIL-zertifizierte Geräte einzusetzen, eine „exakte" Berechnung des kompletten Sicherheitskreises durchführen zu lassen, die Zertifikate samt Berechnung abzuheften und dann noch zu glauben, jetzt sei das Wesentliche für die Sicherheit getan.

Einem Alibidenken wird Vorschub geleistet, nach dem Motto: „Das SIL-Zertifikat ist ja vorhanden, jetzt kann nichts mehr passieren". Ein typischer Fall von „Schein"-Sicherheit. Eine wichtige Tugend des ingenieurmäßigen Sachverstands: zu prüfen, ob die Systeme auch wirklich zum konkreten Anwendungsfall passen, droht zu verkümmern. Wer die neuen Normen so versteht und lebt, muss aufpassen, dass er nicht einen erheblichen Rückschlag in seiner Sicherheitsevolution erlebt.

5. NEUZEIT DER SICHERHEITSTECHNIK, EPOCHE III: SEIT 2007 – WIEDERAUFERSTEHUNG

Die Namur passt auf! Was zu Ende des vorigen Kapitels eher negativ geschildert wurde, sind Auswüchse, die hoffentlich selten vorkommen. Die neuen Normen haben durchaus auch positive Aspekte. Sie waren der Anlass, die Systematik unserer bereits ausgereiften Sicherheitskonzepte erneut auf den Prüfstand zu stellen und einige Anregungen nutzbringend einzubinden.

Zuerst galt es, die bewährte nationale Vorgehensweise formal zu „retten". Immerhin haben sich seit Mitte der 80er-Jahre keine größeren Störereignisse aufgrund des Versagens von PLT-Schutzeinrichtungen in der Bundesrepublik ereignet. Warum sollte man dieses Know-how dann über Bord werfen? Die nationalen Normen sind zwar nicht mehr gültig, aber wer hinderte uns daran, die VDI/VDE 2180 [25] erneut zu überarbeiten und alle bewährten Konzepte aus diesen Papieren und die wesentlichen Aussagen aus den einschlägigen Namur-Empfehlungen mit einzubeziehen? Natürlich muss auch die neue international entstandene Normenwelt berücksichtigt werden. Dieser Kraftakt war 2007 bis 2010 gelungen. Abermals haben alle an dem Sicherheitsprozess beteiligten Gruppen bei der Erarbeitung dieser vierten Auflage mitgewirkt. Diese bewährte Methode stellt sicher, dass bei der späteren Anwendung der Richtlinie deren Akzeptanz besonders hoch ist. Schließlich beschreibt die VDI/VDE 2180 den Stand der Sicherheitstechnik im Sinne der Störfallverordnung.

Die wesentlichen Neuerungen sind:

- Übernahme der SIL in den Risikographen
- Zuordnung der PFD zu den SIL
- Ausführliche Beschreibung eines Sicherheitsmanagementsystems mit Themen wie Verantwortlichkeit, Qualifikation, Dokumentation
- Musterrechnungen zum Nachweis der Hardwaresicherheitsintegrität bei betriebsbewährten Geräten (Basisdaten aus NE 93 beziehungsweise NE 130)
- Empfehlungen zur Umsetzung in die Praxis
- Schadensbegrenzungseinrichtungen heißen jetzt schadensbegrenzende Schutzeinrichtungen (analog zur Terminologie der Störfallverordnung)

Im Jahr 2009 erscheint die NE 126: „Bestandsschutz für PLT-Schutzeinrichtungen" [26]. Sie füllt eine Lücke, die andere Regelwerke offen lassen. Nirgendwo findet man in Normen oder VDI-Richtlinien Aussagen über dieses wichtige Thema. Also hat man bei der Namur den gesunden Menschenverstand walten lassen und formuliert: „Bestehende PLT-Schutzeinrichtungen genießen Bestandsschutz, falls sie nach den bisher angewendeten Regelwerken geplant, errichtet und betrieben wurden." Diese Aussage wird mit Beispielen verdeutlicht.

5.1 NE 130: betriebsbewährte Geräte

Das neueste und besonders wichtige Werk aus dem Namur-AK 4.5 ist die Anfang 2010 erschienene NE 130: „Betriebsbewährte Geräte für PLT-Schutzeinrichtungen und vereinfachte SIL-Berechnung" [27].

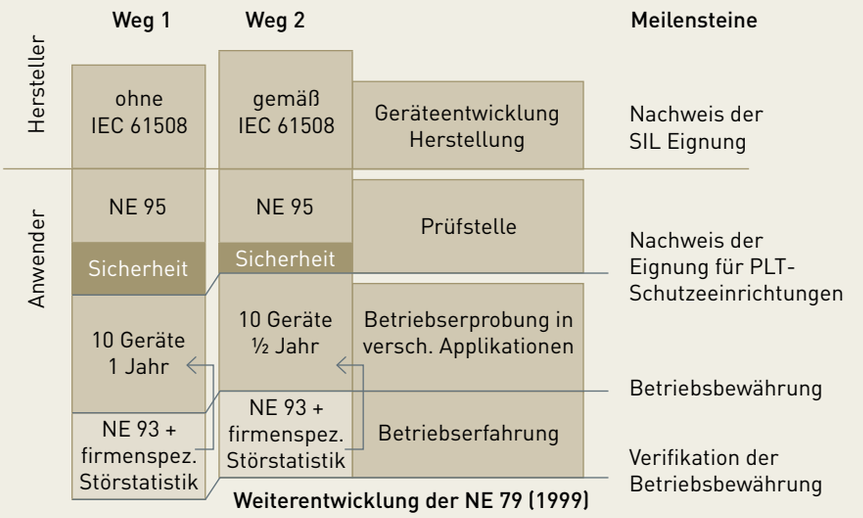


BILD 4: Prinzipielle Darstellung des Betriebsbewährungsprozesses

Fehlerbetrachtung
Zunächst wird in diesem Papier ausführlich der Unterschied zwischen systematischen und zufälligen Fehlern herausgearbeitet. Die DIN EN 61508 (VDE 0803) und auch das Konzept der Betriebsbewährtheit zielen darauf ab, die systematischen Fehler im Entwicklungsprozess der Geräte möglichst zu vermeiden und bei den ersten Anwendungsversuchen noch verbliebene Fehler dieser Art aufzudecken. Bei dem probabilistischen Ansatz wird davon ausgegangen, dass die systematischen Fehler bereits eliminiert sind und sich die PFD-Berechnungen lediglich auf die verbleibenden zufälligen Fehler beziehen, was von den Anwendern allzu leicht übersehen wird.

Betriebsbewährung
Das Konzept der Betriebsbewährung erfolgt in 4 Schritten (siehe Bild 4):

1 | Nachweis der SIL-Eignung
2 | Nachweis der Eignung für PLT-Schutzeinrichtungen
3 | Nachweis der Betriebsbewährung mit Betriebserprobung
4 | Verifikation der Betriebsbewährung

Das ist nicht neu (siehe NE 79 von 1999) und hat auch zunächst nichts mit den internationalen Normen zu tun. Eine Erleichterung tritt jedoch ein, wenn die Geräte bereits nach DIN EN 61508 (VDE 0803) entwickelt wurden. Umgekehrt widerspricht der Verzicht auf den Nachweis der Betriebsbewährtheit, nur weil ein SIL-Zertifikat oder eine Herstellerbescheinigung vorliegt, guter Ingenieurpraxis.

Musterrechnungen
In den Musterrechnungen wird vorausgesetzt, dass die seit Jahren in PLT-Schutzeinrichtungen eingesetzten Geräte betriebsbewährt sind. Aus der Sammlung der Stördaten bei der Namur seit 2002 wurden die Ausfallraten für bestimmte Gerätegruppen aus dem praktischen Einsatz ermittelt. Sie sind in der Tabelle 2 dargestellt.

Mit diesen Werten wurden die Musterrechnungen für verschiedene Redundanzgrade durchgeführt. Somit kann bei Verwendung betriebsbewährter Geräte nach NE 130 auf einen rechnerischen Einzelnachweis verzichtet werden; denn es ist bereits gerechnet! Diese Vorgehensweise ist mittlerweile auch in die VDI/VDE 2180, Blatt 4 [28] eingeflossen und erhält damit zusätzliches Gewicht. Eine weitere Effizienzsteigerung wäre möglich, wenn die Mannigfaltigkeit der eingesetzten Komponenten in PLT-Schutzeinrichtungen reduziert werden könnte, etwa durch Einführen von Standardgerätelisten. Hieran wird zurzeit auch auf Namur-Ebene intensiv gearbeitet.

5.2 Nutzen der Stördatenanalyse

Neben der firmenspezifischen Schwachstellenanalyse bietet die Störstatistik über die Sammlung der Daten bei der Namur auch übergeordnet erheblichen Nutzen. Wie wir wissen, sind Herstellerangaben zu Fehlerraten für Feldgeräte häufig konservativ. Daraus könnte die Forderung nach genereller Zweikanaligkeit von PLT-Schutzeinrichtungen abgeleitet werden. Mittels Stördatenanalyse konnte der Nachweis erbracht werden, dass die bisherige Vorgehensweise, bei kleineren Risiken einkanalig zu instrumentieren und bei höheren Risiken Redundanzen einzuführen, auch den quantitativen Anforderungen der neuen Normenwelt entspricht. Die Datenbasis beruht auf achtjähriger Beobachtung des Fehlerverhaltens von etwa 40 000 Schutzeinrichtungen in rund 40 sich beteiligenden Firmen. Damit ist die Gefahr ungerechtfertigter Nachrüstkosten von mindestens 150 Millionen Euro für die Namur-Firmen gebannt. Das gemeinsame Ziel für die Wiederauferstehung einer vernünftigen Sicherheitstechnik sollte der Einsatz von betriebsbewährten Standardgeräten sein, die nach DIN 61508 (VDE 0803) entwickelt und in typischen (Redundanz-)Strukturen implementiert wurden und für die Musterrechnungen vorliegen.

Kanalart	Kanalfehlerrrate für unerkannte passive Fehler λ_{DU}
Sensorik Messgröße P	$1 \cdot 10^{-6}\ h^{-1}$ = 1000 FiT
Sensorik Messgröße T	$5 \cdot 10^{-7}\ h^{-1}$ = 500 FiT
Sensorik Messgröße L	$4 \cdot 10^{-7}\ h^{-1}$ = 400 FiT
Sensorik Messgröße F	$1 \cdot 10^{-6}\ h^{-1}$ = 1000 FiT
Sensorik	$4 \cdot 10\text{-}7\ h^{-1}$ = 400 FiT

TABELLE 2:
Richtwerte für sicherheitstechnische Kennzahlen von betriebsbewährten Geräten

FiT = Failures in time, d.h. Fehler pro 109h

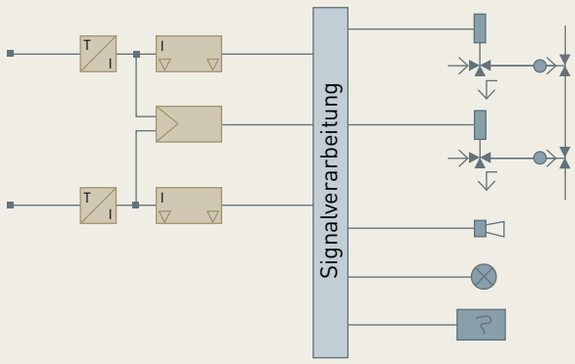


BILD 5:
Aufbau einer PLT-Schutzeinrichtung in 1v2-Bewertung im Jahre 2010

6. ZUSAMMENFASSUNG UND AUSBLICK

Der Vergleich zwischen Bild 1 aus dem Jahr 1966 und Bild 5 aus dem Jahr 2010 könnte zu dem Schluss verleiten: Eigentlich hat sich in den letzten 45 Jahren nichts verändert. Sind deshalb die „Sicherheitsmacher“ stockkonservativ? Bei näherem Hinschauen stellt man jedoch fest, dass es seit 1966 deutliche Weiterentwicklungen, sowohl technischer, als auch organisatorischer Art, gegeben hat:

- Erweiterung des Schutzziels von ehemals nur „Anlage und Produkt“ auf „Personen und Umwelt“
- Klare Unterscheidung in „sicherheitsrelevante“ und „nicht sicherheitsrelevante“ Einrichtungen
- Orientierung der Auslegung am abzudeckenden Risiko
- Einbindung aller am Sicherheitsprozess Beteiligten in die Normungsaktivitäten
- Verbessertes Fehlerverhalten der Gerätetechnik und dank der Mikroprozessortechnik zahlreiche Diagnosemöglichkeiten
- Verbindungsprogrammierbare Steuerungen (VPS) wurden durch sicherheitsgerichtete speicherprogrammierbare Steuerungen (SSPS) abgelöst
- Die Zertifizierung von SSPS stellt sicher, dass ihre Hardware frei von passiven Fehlern ist
- Die Einführung von Sicherheitsmanagementsystemen regelt die Verantwortlichkeiten und zwingt zu systematischem Arbeiten
- Die Orientierung am Sicherheitslebenszyklus mit definierten Prüfschritten senkt die Fehlerrate in allen Phasen
- Die sorgfältige Dokumentation aller Schritte im Sicherheitsprozess sorgt für Transparenz und Nachvollziehbarkeit und schützt in einem Störungsfall vor dem Vorwurf der Fahrlässigkeit
- Flexibilisierung von Prüfzyklen
- Einführung des rechnerischen Nachweises der sicherheitstechnischen Verfügbarkeit
- Flächendeckende Einführung einer Stördatenerfassung und -analyse

Im Sicherheitsgeschäft gilt es, Änderungen behutsam, nach hinreichender Erprobung, einzuführen und rechtzeitig vor Übertreibungen und Fehlentwicklungen zu warnen. Wir haben nach Einschätzung des Autors ein sehr gutes PLT-Sicherheitskonzept in Deutschland, das auch im Zuge der Deregulierung ausgewogene Handlungsanweisungen an die beteiligten Gruppen gibt. Deshalb ist es auch glücklicherweise nicht erforderlich, wie in anderen Ländern zum Teil üblich, kleinlich bürokratisch und praxisfern überzureglementieren. Es geht darum, die Regelwerke auch tatsächlich umzusetzen und die gegebenen Freiheitsgrade unter „Einschaltung von Gehirn und ingenieurmäßigem Sachverstand“ zu nutzen. Wir müssen deshalb unsere Kompetenz als Anwender selbstbewusst in die internationale Normung einbringen! Somit können wir darauf hinwirken, dass sich

die Sicherheit nach Kochbuch in Grenzen hält. In anderen Ländern herrschen andere Rahmenbedingungen. Es seien nur das Stichwort „Produkthaftung“ und die Angst vor exorbitant hohen Regressforderungen genannt. Daran ausgerichtete Vorgehensweisen weltweit in ganz anderen Rechtsräumen und gewachsenen Kulturen einführen zu wollen, führt lediglich zu überflüssigem Aktionismus, ohne die Sicherheit der Anlagen zu verbessern. Dazu gehört aber zwangsläufig auch, dass Unternehmen der Anwenderseite bereit sind, unsere Normungsaktivitäten finanziell zu unterstützen. Aussagen wie „Lasst uns mal sportlich 10 % in der Regelwerksverfolgung und der Gremienarbeit einsparen“ sind das falsche Signal und gehören in die Steinzeit! Zurzeit bringt die deutsche Delegation bei der anstehenden Überarbeitung der IEC 61511 folgende Themen ein:

- Betriebsbewährte Geräte (NE 130)
- Vorgehen bei elektromechanischen Komponenten
- Mitbenutzung von PLT-Betriebseinrichtungen und
- Nutzbare Lebensdauer von Geräten

Es wird Kompromisse geben müssen, aber die Ergebnisse werden der Sicherheitsevolution sicher zuträglich sein.

MANUSKRIPTEINGANG
13.12.2010
Im Peer-Review-Verfahren begutachtet

AUTOR

DR. PIRMIN NETTER
(geb. 1949) studierte Experimentalphysik in Heidelberg. Von 1981 bis 1996 hatte er verschiedene Positionen in der EMR-Betriebsbetreuung der Hoechst AG inne. Von 1997 bis 2009 war er Leiter der Sicherheitsüberwachung Hoechst AG beziehungsweise Abt. Arbeitsschutz und Anlagensicherheit der Infraserv Höchst. Sein Hauptarbeitsgebiet ist Anlagensicherung mit Mitteln der Prozessleittechnik. Dr. Netter ist Mitglied in mehreren nationalen Gremien. Bis 2010 war er deutscher Sprecher im IEC SC65A. Er ist bekannt gegebener Sachverständiger gem. § 29a BImschG.

Infraserv GmbH & Co. Höchst KG,
Industriepark Höchst, C 769,
D-65926 Frankfurt am Main,
Tel. +49 (0) 69 305 64 98,
E-Mail: Pirmin.Netter@infraserv.com

REFERENZEN

[1] VDI/VDE-Richtlinie 2180, Blatt 1-7: Sicherung von Anlagen der Verfahrenstechnik, 1966ff
[2] Störfallverordnung: Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes,1980
[3] G. Strohmann: Anlagensicherung mit Mitteln der MSR-Technik,1983
[4] Hölscher/Rader: Mikrocomputer in der Sicherheitstechnik, 1984
[5] VDI/VDE-Richtlinie 2180, Blatt 1-5: Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der MSR-Technik, 1984ff
[6] TRbF 510: Richtlinie/Bau- und Prüfgrundsätze für Überfüllsicherungen, 1985
[7] DIN VDE 31000 Teil 2: Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse, 1987
[8] DIN V 19250: Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen, 1989
[9] DIN V 19251: MSR-Schutzeinrichtungen, Anforderungen und Maßnahmen zur gesicherten Funktion, 1995
[10] AD-Merkblatt A6: Sicherheitseinrichtungen gegen Drucküberschreitung, MSR-Sicherheitseinrichtungen, 1986
[11] Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfall-Verordnung) – 12. BImSchV– Novelle 1988
[12] DIN V VDE 0801: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben, 1990
[13] NE 31: Anlagensicherung mit Mitteln der Prozessleittechnik, 1993
[14] DIN V VDE 0801/A1: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben, 1994
[15] VdTÜV-Merkblatt 372: Leitlinie für die Prüfung sicherheitsrelevanter MSR-Einrichtungen in Anlagen, 1997
[16] VDI/VDE-Richtlinie 2180, Blatt 1-5: Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik, 1998
[17] Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: Vollzugshilfe zur Störfallverordnung, 2004
[18] NE 79: Mikroprozessorbestückte Geräte in der Anlagensicherung, 1999
[19] VDI/VDE-Richtlinie 2180, Blatt 5: Einsatz von speicherprogrammierbaren Steuerungen, 2000
[20] NE 93: Nachweis der sicherheitstechnischen Zuverlässigkeit von PLT-Schutzeinrichtungen, 2001
[21] NE 97: Feldbus für Sicherungsaufgaben, 2003
[22] NE 106: Prüfintervalle für PLT-Schutzeinrichtungen, 2006
[23] DIN EN 61508 (VDE 0803): Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbar elektronischer Systeme, 2002
[24] DIN EN 61511 (VDE 0810): Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie, 2005
[25] VDI/VDE-Richtlinie 2180, Blatt 1-5: Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik, 2007-2010
[26] NE 126: Bestandsschutz für PLT-Schutzeinrichtungen, 2009
[27] NE 130: Betriebsbewährte Geräte für PLT-Schutzeinrichtungen und vereinfachte SIL-Berechnung, 2010
[28] VDI/VDE-Richtlinie 2180, Blatt 4: Nachweis der Hardware-Sicherheitsintegrität einer PLT-Schutzeinrichtung, 2010

Batch-Prozessführung

Potenziale und Herausforderungen

Batchprozesse, An- und Abfahrprozesse sowie Last- und Produktwechsel kontinuierlicher Anlagen stellen unter anderem aufgrund ihrer inhärenten, nicht-linearen Dynamik, der häufig nicht komplett verstandenen Chemie und der Komplexität der Steuerungen eine Herausforderung für die Automatisierung und Optimierung dar. Der Beitrag des Namur-AK 2.2 „Prozessführung“ beschreibt diese Herausforderungen und stellt aktuelle Lösungsansätze aus der industriellen Praxis vor.

SCHLAGWÖRTER Prozessführung / Batchprozess / An- und Abfahrprozesse / Last- und Produktwechsel / Advanced Process Control

Batch process optimization–
Opportunities and Challenges

Batch processes, start-up, shut-down as well as load and product changes of continuous processes are challenging to automate and optimize, because of their inherent, non-linear dynamics, the often limited process understanding and the control systems complexity. This contribution of Namur AK 2.2 “Prozessführung” describes these challenges and presents current solution approaches from industrial practice.

KEYWORDS Process management / batch process / start-up / shut-down / load change / product change / advanced process control.

OLAF KAHRS, BASF SE;
GUIDO DÜNNEBIER, Bayer Technology Services;
STEFAN KRÄMER, Ineos Köln;
HEIKO LUFT, Evonik Degussa

Die Produktion in Chargen ist ein wichtiger Produktionstyp, der für die Herstellung von Polymeren, Fein- und Spezialchemikalien, Pharmazeutika, Tensiden und anderen Produkten weit verbreitet ist. Die Automatisierung von An- und Abfahrprozessen sowie Last- und Produktwechseln kontinuierlicher Anlagen gewinnt an Bedeutung aufgrund schwankender Produktnachfrage und dem fortwährenden Trend zu einer Produktionskostenreduktion. Aufgrund der inhärenten Dynamik dieser Prozesse ergeben sich für folgende Aufgabenstellungen ähnliche Lösungsansätze:

- Erhöhung der Flexibilität zur kurzfristigen Deckung der Marktnachfrage
- Erhöhung der Reproduzierbarkeit und Verringerung von nicht normgerechten Anteilen
- Minimierung der Energiekosten und Erhöhung des Durchsatzes
- Unterstützung der Anlagenfahrer

Die Erreichung dieser Ziele stellt eine komplexe und interdisziplinäre Aufgabe dar. Sie umfasst unter anderem die Erstellung eines Rezeptursystems, das Scheduling der Produkte und Mengen, die Erstellung von Schrittketten, die Planung und Einhaltung der Sollwert-Trajektorien innerhalb der Schrittkettenabschnitte, die Erstellung von Schutzschaltungen sowie die Datenerfassung und -verarbeitung. Der Fokus dieses Beitrags wird im Folgenden auf die Prozessführung gelegt, insbesondere auf die Planung und Einhaltung der Sollwert-Trajektorien.

1. UNGENUTZTES POTENZIAL FÜR INNOVATIVE PROZESSFÜHRUNGSMETHODEN

Im Jahr 2008 führte der Namur-AK 2.2 mit Unterstützung des ARC eine Expertenbefragung durch [1]. Bild 1 zeigt ein Ergebnis der Umfrage: die Wichtigkeit von Technologien für Batchprozesse in der industriellen Praxis. Der Fokus liegt bisher auf eher grundlegenden Technologien; fortschrittliche Prozessführungskonzepte wie Modellprädiktive Regelungen (MPC) besitzen demnach bisher nur eine geringe Bedeutung.

Die Prozessführung für Batchprozesse erfolgt in der Praxis häufig durch Übertragung von Laborvorgaben in die Produktion in Form einfacher Dosier- und Temperaturtrajektorien, die aus wenigen Rampen und Sprüngen zusammengesetzt sind. Bedingt durch diese Vorgehensweise können sich signifikante Sollwertabweichungen ergeben, die die Reproduzierbarkeit der Produktqualität einschränken. Außerdem wird insbesondere bei exothermen Prozessen die Kühlkapazität nicht zu jedem Zeitpunkt voll ausgenutzt, so dass Potenziale für eine Batchzeitreduktion durch fortschrittliche Prozessführungskonzepte bestehen.

Bild 2 zeigt einige APC-Methoden zur Führung von Batchprozessen. Die Methoden sind grob nach Leistungsfähigkeit und Implementierungsaufwand sortiert. Abhängig von den Prozessführungsanforderungen und Prozesseigenschaften sollte die passende Methode gewählt werden. In der industriellen Praxis wurden mehrere der Methoden bereits erfolgreich eingesetzt (siehe beispielsweise [2], [3]). Beachtenswert ist, dass diese beiden Methoden federführend durch Anwenderfirmen vorangetrieben und für eine Vielzahl von Batchreaktoren implementiert wurden. Kommerzielle Lösungen, insbesondere nicht-lineare Modellprädiktive Regelungen (NMPC), scheinen momentan bei den befragten Namur-Mitgliedsfirmen erst zu einem geringen Grad implementiert zu sein. Mittelfristig können kommerzielle Lösungen jedoch aufgrund der größeren Kundenbasis, der besseren Wartbarkeit der Applikationen, einer umfangreichen Dokumentation und der Unterstützung bei der Projektdurchführung durch Dienstleister deutliche Vorteile bieten.

Obwohl zuvor genannte Prozessführungsmethoden ([2], [3]) in der industriellen Praxis ihre Wirtschaftlichkeit bereits unter Beweis gestellt haben, ist bisher nur in einem Teil der in Frage kommenden Produktionsbetriebe eine solche Technologie im Einsatz. Die Umfrageergebnisse des Namur-AK 2.2 zeigen die Gründe hier-

für auf [1]. Die Hindernisse für den Einsatz innovativer Prozessführungskonzepte sind in Bild 3 zusammengefasst. Die Mehrzahl der Nennungen bezieht sich auf Hindernisse nicht-technischer Natur, wie beispielsweise die unzureichende Quantifizierung des Nutzens eines Prozessführungsprojektes oder der Mangel an qualifiziertem Personal.

Ein Teil dieser Hürden lässt sich durch Standardisierung der Technologien und Vorgehensweisen bei der Projektdurchführung senken. Ein wichtiges Element hierbei ist die aufgabenorientierte Beschreibung der Vielzahl verfügbarer Prozessführungsmethoden, z.B. in Form von Technologie-Steckbriefen, die typische Anwendungsgebiete und Einsparpotenziale, Besonderheiten bei der Implementierung (beispielsweise benötigte Infrastruktur), Referenzanwendungen sowie verfügbare kommerzielle Lösungen nennen. Nachdem der Werkzeugkasten der Batch-Prozessführungsmethoden hierdurch beschrieben ist, ergibt sich weiterhin die Möglichkeit der Konsolidierung und Identifikation der Lücken für die eventuelle Entwicklung neuer oder verbesserter Methoden.

2. ERFOLGSFAKTOREN FÜR DIE UMSETZUNG INNOVATIVER PROZESSFÜHRUNGSMETHODEN

Auf Basis der Erfahrungen mit der Umsetzung innovativer Prozessführungsmethoden möchten die Autoren auf folgende Punkte bei der Projektdurchführung besonders hinweisen:

- Zu Beginn des Projektes sollte in einer Benefit-Studie durch Diskussion des bisherigen Anlagenbetriebs und technischer sowie wirtschaftlicher Randbedingungen geklärt werden, worin das wirtschaftliche

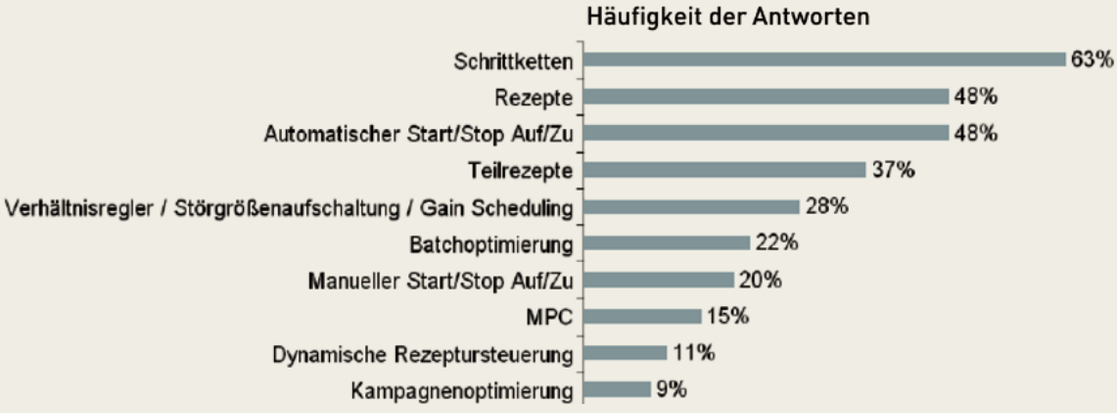


BILD 1: Wichtigkeit von Technologien für Batchprozesse in der industriellen Praxis [1]

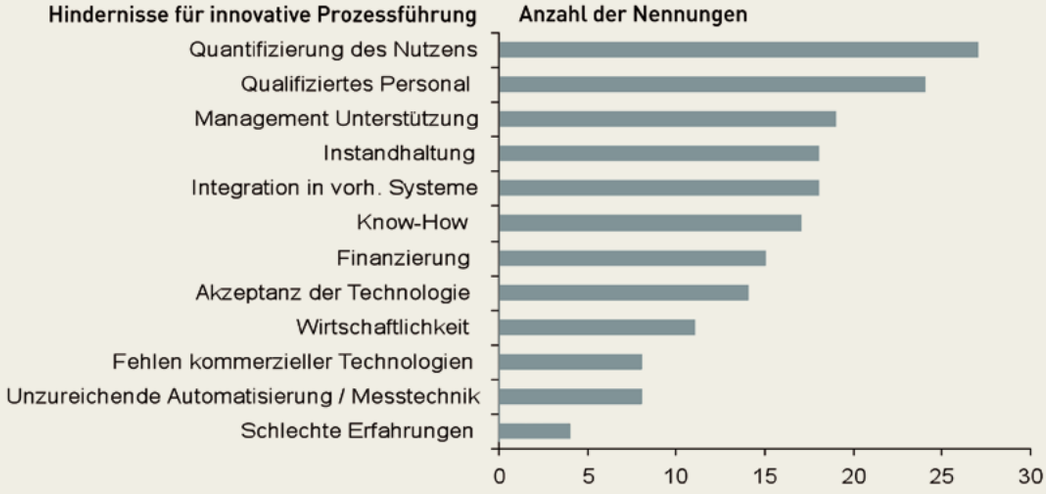


BILD 3: Umfrageergebnisse des Namur-AK 2.2 zu den Hindernissen beim Einsatz innovativer Prozessführungskonzepte [1]

Potenzial liegt. Zum Beispiel können die zwei alternativen Anforderungen (i) Erhöhung der Reproduzierbarkeit und (ii) Erhöhung der Anlagenkapazität zur Auswahl zweier unterschiedlicher Technologien führen. Prozessverständnis sollte auch durch Nutzung vorhandenen Modellwissens und Auswertung historischer Daten aufgebaut werden.

- Bei der Konzepterstellung sollten anhand eines Kriterienkataloges, wie beispielhaft in Bild 4 gezeigt, geeignete Lösungskonzepte entwickelt und anhand der Kosten und des erwartbaren Nutzens bewertet werden. Diese Aufgabe sollte interdisziplinär durchgeführt werden, da verfahrenstechnische Maßnahmen und Rezepturänderungen den Nutzen weiter steigern können.
- Zwei wichtige Aspekte bei der Implementierung einer APC-Lösung sind die Integrierbarkeit in die bestehende Infrastruktur (manche Lösungen sind direkt ins Prozessleitsystem implementierbar) und die Verfügbarkeit einer gut funktionierenden Instrumentierung und Basisautomatisierung (inklusive einer Fallback-Strategie, die bei Ausfall der APC-Applikation die Prozessführung übernimmt).
- Wichtige Erfolgsfaktoren für die nachhaltige Nutzung der Lösung sind deren Akzeptanz innerhalb des Produktionsbetriebes und ein Konzept für die Applikationspflege.

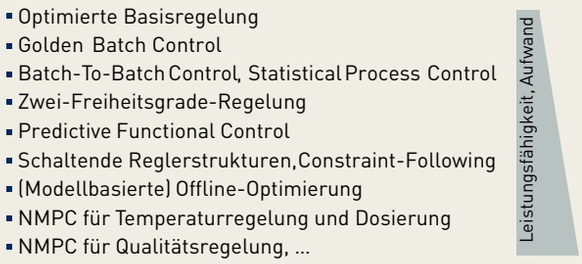


BILD 2: APC-Methoden für die Führung von Batchprozessen (Auszug)

BILD 4: Kriterien für die Auswahl einer Technologie zur Optimierung der Batch-Prozessführung

3. ANFORDERUNGEN UND WÜNSCHE

Für den mittelfristigen Erfolg ist die Zusammenarbeit mehrerer Interessengruppen notwendig. Hierzu haben die Autoren dieses Beitrags folgende Anforderungen und Wünsche an die fünf beteiligten Gruppen formuliert:

Namur/Hochschulen

- Einheitliche Beschreibung der unterschiedlichen Ansätze und Schaffung von Standards, welche auch Grundlage für kommerzielle Angebote ein können
- Förderung der Ausbildung qualifizierter Fachkräfte (PLT, APC)

Anbieter

- Standardisierung der Technologien und Kapselung der Komplexität für die Anwender mittels geeigneter Automatisierungstechnologie
- Integrierbarkeit in heterogene IT-/AT-Landschaften
- Gute Bedien-, Anwend- und Wartbarkeit

PLT-Ingenieure

- Bewusstsein für die Methoden der Prozessführung und Erkennung von Potenzialen

Betriebsleiter

- Schärfung der Beurteilungs- und Beauftragungskompetenz
- Nutzung firmeninterner Fachkräfte als Wettbewerbsvorteil
- Prozessmodelle als Assets betrachten und pflegen lassen

Prozessführungsexperten

- Weiterbildung der Mitarbeiter und Bildung interdisziplinärer Teams
- Überzeugung der Entscheidungsträger durch klare Kommunikation der Technologien und Abschätzung deren Wirtschaftlichkeit

4. ZUSAMMENFASSUNG UND AUSBLICK

Industriell eingesetzte Methoden zur Optimierung der Prozessführung von Batchprozessen haben ihr hohes wirtschaftliches Potenzial bewiesen. Für eine flächendeckende Implementierung sind allerdings noch verschiedene Hindernisse zu überwinden, die zum Teil durch eine Standardisierung der Vorgehensweise bei Prozessführungsprojekten und durch den Aufbau eines Methoden-Werkzeugkastens gesenkt werden können. Für den mittelfristigen Erfolg ist hierzu die Zusammenarbeit mehrerer Interessengruppen notwendig.

Methodische Weiterentwicklungen zur simultanen Betrachtung der verschiedenen Automatisierungsebenen (Scheduling, Rezepte, Schrittketten, Trajektorienoptimierung und -regelung) sind wünschenswert [4]. Komponenten darin könnten Werkzeuge zur Erzeugung einer Steuerung aus einer Funktionsbeschreibung sowie Optimierungsalgorithmen für hybride Systeme (kontinuierliche und diskrete Optimierungsvariablen) sein.

MANUSKRIPTEINGANG
14.12.2010
Im Peer-Review-Verfahren begutachtet

DANKSAGUNG

Die Autoren bedanken sich für die Unterstützung bei der Vorbereitung dieses Beitrags durch die Mitglieder des Namur-AK 2.2 und durch Hr. Dipl.-Ing. Marcus Nohr und Hr. Dipl.-Ing. Axel Schild von der BASF SE.

REFERENZEN

[1] Hagenmeyer, V. und Piechottka, U.: Innovative Prozessführung – Erfahrungen und Perspektiven. atp, 1:46–63, Januar 2009.

[2] Deis, W.: Ganzheitlich optimierte Prozesse - Effiziente Prozessführung endet nicht mit der schnellen Lösung der Regelungsaufgabe, Tagungsband zur Automation 2009, VDI-Berichte 2067, S. 213ff, VDI-Verlag, Düsseldorf, 2009.

[3] Hagenmeyer, V. und .Nohr, M.: Flatness-based two-degree-of-freedom control of industrial semi-batch reactors using a new observation model for an extended Kalman filter approach. Int. J. Contr., 81(3):428-438, 2008.

[4] Nohr, M., Kahrs, O., Münnemann, A. und Hesse, P.: Optimierung von Batch- und Semibatchprozessen – Auf dem Weg zu einem ganzheitlichen Ansatz. atp edition, 12/2010, S.62-69.

AUTOREN

DR.-ING. OLAF KAHRS (geb. 1975) ist im Fachzentrum für Automatisierungstechnik der BASF SE für die Fachgruppe „Optimierung der Prozessführung“ verantwortlich. Arbeitsschwerpunkte bilden sowohl Entwicklungen als auch Anwendungen in den Bereichen Prozessdiagnose, gehobene Regelungstechnik, dynamische Simulation und modellbasierte Optimierung verfahrenstechnischer Prozesse. Nach einem Studium des Maschinenbaus an der RWTH Aachen und am Dartmouth College (USA) promovierte er am Lehrstuhl für Prozesstechnik in Aachen. In der Namur ist er Mitglied im Arbeitskreis 2.2 „Prozessführung“.

BASF SE,
L440, 67056 Ludwigshafen,
Tel.: +49 (0) 621 607 95 69,
E-Mail: olaf.kahrs@basf.com

DR.-ING. GUIDO DÜNNEBIER (geb. 1970) leitet die Gruppe Process Management Consulting bei Bayer Technology Services GmbH und ist verantwortlich für die Aktivitäten im Bereich Operational Excellence und technischer Beratung für die chemische und pharmazeutische Industrie. Mit einer verfahrenstechnischen Ausbildung hat er mehr als 10 Jahre Berufserfahrung in der Anwendung und Entwicklung von Methoden der Prozessoptimierung und Systemverfahrenstechnik. Er ist ein zertifizierter Six Sigma Master Black Belt und erfahrener Trainer und Coach.

Bayer Technology Services,
Bayerwerk, 51368 Leverkusen,
Tel. +49 (0) 214 304 88 41,
E-Mail: guido.duennebier@bayertechnology.com

DR.-ING. STEFAN KRÄMER (geb. 1972) studierte Verfahrenstechnik und Chemieingenieurwesen an der University of Newcastle upon Tyne, GB, und promovierte im Bereich der Optimierung der Prozessführung von Emulsionspolymerisationen am Lehrstuhl Systemdynamik und Prozessführung (Prof. Engell) der Technischen Universität Dortmund. Er unterrichtet dort als Lehrbeauftragter „Batch Process Operation“. Seit 2004 ist er Ingenieur für Advanced Process Control bei der Ineos in Köln und seit 2009 Leiter der Gruppe „Process Control and Application Engineering“. Hauptarbeitsgebiete sind Prozessregelung und -optimierung, Zustandsschätzung und Advanced Control. Stefan Krämer ist Obmann des Namur-Arbeitskreises 2.2 „Prozessführung“.

Ineos Köln,
TS-SCE-PLS, Alte Straße 201, 50769 Köln,
Tel. +49 (0) 221 355 52 65 78,
E-Mail: stefan.kraemer@ineos.com

DIPL.-ING. HEIKO LUFT (geb. 1973) ist Mitarbeiter der Abteilung Prozessdatenverarbeitung und Informationstechnik im Servicebereich Verfahrenstechnik und Engineering der Evonik Degussa GmbH. Seit 1999 ist sein Arbeitsschwerpunkt die Beratung und Realisierung von gehobenen Prozessführungsstrategien. In der Namur ist er Mitglied im Arbeitskreis 2.2 „Prozessführung“.

Evonik Degussa GmbH,
HPC 1024-319, Rodenbacher Chaussee 4,
63457 Hanau-Wolfgang,
Tel. +49 (0) 6181 59 20 87,
E-Mail: heiko.luft@evonik.com

WISSEN für die ZUKUNFT

NEU
Abo *plus*
mit Heft
+ ePaper

Die Referenzklasse für die Automatisierungstechnik

Erfahren Sie auf höchstem inhaltlichen Niveau, was die Automatisierungsbranche bewegt. Alle Hauptbeiträge werden in einem Peer-Review-Verfahren begutachtet, um Ihnen maximale inhaltliche Qualität zu garantieren.

Sichern Sie sich jetzt das doppelte Lektüreerlebnis. Als exklusiv ausgestattetes Heft und als praktisches ePaper – ideal für unterwegs, auf mobilen Endgeräten oder zum Archivieren.

Gratis für Sie: Das NAMUR-Kompendium 2010 Automatisierung für die Prozessindustrie als ePaper

Schärfen Sie Ihren Blick für neue Märkte und verschaffen Sie sich einen Überblick zum aktuellen Stand der Technik. Mit diesem Sammelband bekommen Sie nützliche Anregungen zu den Themen Feldbus, Asset-Management, Geräteintegration, Instandhaltung, Anlagensicherheit oder Umbau bestehender Produktionseinrichtungen.

atp edition erscheint in der Oldenbourg Industrieverlag GmbH, Rosenheimerstr. 145, 81671 München

Oldenbourg-Industrieverlag
www.atp-online.de

Vorteilsanforderung per Fax: +49 (0) 931 / 4170 - 492 oder im Fensterumschlag einsenden

Ja, ich möchte atp edition im Abo-*plus*-Paket lesen.

Bitte schicken Sie mir die Fachpublikation als gedrucktes Heft + digital als ePaper (PDF-Datei als Einzellizenz) für € 598,- zzgl. Versand (Deutschland: € 30,- / Ausland: € 35,-) pro Jahr. Zudem erhalte ich das NAMUR-Kompendium 2010 „Automatisierung für die Prozessindustrie“ gratis als ePaper.

Nur wenn ich nicht bis von 8 Wochen vor Bezugsjahresende kündige, verlängert sich der Bezug um ein Jahr.

Die sichere, pünktliche und bequeme Bezahlung per Bankabbuchung wird mit einer Gutschrift von € 20,- auf die erste Jahresrechung belohnt.

Antwort
Leserservice atp
Postfach 91 61

97091 Würzburg

Firma/Institution

Vorname/Name des Empfängers

Straße/Postfach, Nr.

Land, PLZ, Ort

Telefon Telefax

E-Mail

Branche/Wirtschaftszweig

Bevorzugte Zahlungsweise ☐ Bankabbuchung ☐ Rechnung

Bank, Ort

Bankleitzahl Kontonummer

✘

Datum, Unterschrift PAATPE0111

Widerrufsrecht: Sie können Ihre Vertragserklärung innerhalb von 14 Tagen ohne Angabe von Gründen in Textform (Brief, Fax, E-Mail) oder durch Rücksendung der Sache widerrufen. Die Frist beginnt nach Erhalt dieser Belehrung in Textform. Zur Wahrung der Widerrufsfrist genügt die rechtzeitige Absendung des Widerrufs oder der Sache an den Leserservice atp, Postfach 91 61, 97091 Würzburg.
Nutzung personenbezogener Daten: Für die Auftragsabwicklung und zur Pflege der laufenden Kommunikation werden personenbezogene Daten erfasst, gespeichert und verarbeitet. Mit dieser Anforderung erkläre ich mich damit einverstanden, dass ich vom Oldenbourg Industrieverlag oder vom Vulkan-Verlag ☐ per Post, ☐ per Telefon, ☐ per Telefax, ☐ per E-Mail, ☐ nicht über interessante Fachangebote informiert und beworben werde. Diese Erklärung kann ich mit Wirkung für die Zukunft jederzeit widerrufen.

Modellbasiertes Format für RI-Informationen

Verbesserter Datenaustausch für das PLT-Engineering

Die im Rohrleitungs- und Instrumenten-Fließbild (RI-Fließbild) festgelegten Funktionen und Zusammenhänge sind für die PLT-Planung und -Betriebsbetreuung eine zentrale Informationsgrundlage. Im Beitrag wird ein auf alle kontinuierlichen Prozesse anwendbares modellbasiertes Format für diesen Informationsaustausch vorgestellt. Damit wird eine wichtige Lücke im digitalen Informationsfluss einer Anlage geschlossen. Die auf die Prozessführung und Überwachung fokussierte Spezifikation erlaubt eine einfache automatisierte Interpretation und Auswertung der übertragenen Daten. Damit eröffnen sich interessante Möglichkeiten zur Qualitätssteigerung und Effizienzverbesserung der nachgelagerten PLT-Ingenieurprozesse.

SCHLAGWÖRTER Anlagenfunktion / Rohrleitungs- und Instrumentenfließbild / RI-Fließbild / Digitale Fabrik / XML-Export / PLT-Engineering

Model-based Format for P&ID Informationen – Improved Data Exchange for Continuous Processes

The P&I-diagram (P&ID) determines the product flow structure and the functionality of a process plant. These data are a central base for the downstream control engineering and maintenance processes. In this paper, a model is presented which allows a simple, formal and unambiguous data exchange for all contiuous processes. A significant gap in the information flow between process plant and control engineering is bridged in this way.
The special focus of the specification on process control and supervision allows an easy automated interpretation and evaluation of the transmitted data. Interesting possibilities to increase quality and improve efficiency of the downstream engineering processes are now given.

KEYWORDS Plant function / Pipe and Instrumentation Diagram / P&ID / Digital Factory / XML-Export / Process Controll Engineering

ULRICH EPPLE, RWTH Aachen;
MARKUS REMMEL, OLIVER DRUMM, Siemens AG

Die Errichter und Betreiber von verfahrenstechnischen Anlagen sind bestrebt, diese möglichst wirtschaftlich zu planen, zu errichten und zu betreiben. In diesem Zusammenhang ist die Verwaltung sämtlicher Informationen über den Lebenszyklus einer Anlage von zentraler Bedeutung. Die zur Verfügung stehenden Informationen bilden die Grundlage zur Optimierung des Produktionsprozesses und die Voraussetzung für eine effiziente Gestaltung der Ingenieurprozesse. Unter dem Schlagwort „Digitale Fabrik" vereinen sich derzeit die Wünsche, Hoffnungen und Forderungen der Errichter und Betreiber von Anlagen an EDV-Werkzeuge, die eine konsistente und durchgängige Datenhaltung unterstützen und die von den einzelnen Gewerken über alle Lebenszyklusphasen effizient genutzt werden können.

Einen großen Fortschritt verspricht man sich bei der „Digitalen Fabrik" dadurch, dass Informationen so abgelegt werden, dass sie zwischen verschiedenen Anwendungen elektronisch ausgetauscht werden können. Damit entfallen eine fehleranfällige, redundante manuelle Eingabe von Planungsdaten ebenso wie die Speziallösungen zur Übertragung von einzelnen Datensätzen in individuellen Listen.

Ziel ist, dass jedes Datum zukünftig nur einmal an einer Stelle eingegeben und gepflegt wird, dieses Datum aber von allen Anwendungen ohne zusätzlichen Projektieraufwand genutzt werden kann.

Eine Workflow-Analyse im verfahrenstechnischen Anlagenbau zeigt, dass das RI-Fließbild (P&ID) das zentrale Dokument bei der Planung darstellt (siehe Bild 1). Dieses Diagramm dient mehreren Gewerken als Grundlage ihrer Arbeiten und dies in der Planungsphase und während der gesamten Betriebsphase einer Anlage. Für die Automatisierungstechnik enthält das RI-Fließbild eine Vielzahl wichtiger Informationen.

Trotz dieser großen Bedeutung des RI-Fließbilds für die Automatisierungstechnik gilt es nach wie vor als Stand der Technik, wesentliche strukturelle und funktionale Informationen grafisch zu interpretieren und manuell zu übernehmen. Auf dem Weg zur „Digitalen Fabrik" ist es zwingend erforderlich, diesen Bruch der Durchgängigkeit zu schließen. Dazu wird neben einem Austauschformat für die visuelle Darstellung vor allem ein Datenformat benötigt, das die für die Automatisierungstechnik wichtigen strukturellen und funktionalen Informationen datentechnisch interpretierbar erfasst.

1. STAND DER TECHNIK

Im Gegensatz zu der früher üblichen rein grafischen Handhabung werden in modernen CAE-Systemen RI-Fließbilder primär als Informationsmodelle gesehen und in Datenbanken explizit verwaltet. Die Grafik ist nur noch eine spezielle Sicht auf das RI-Informationsmodell. Diese Technik eröffnet die Möglichkeit, Informationen explizit aus den Datenmodellen abzugreifen. Leider gibt es dabei drei wesentliche Schwierigkeiten:

1 | **Vollständigkeit der Abbildung**
Nach wie vor steckt in vielen Fällen in der Grafik zusätzliche Information, die im Datenmodell nicht abgebildet ist.

2 | **Uneinheitliche Abbildung**
In der Praxis unterscheiden sich die Abbildungen von Fall zu Fall erheblich. Hintergrund ist die unterschiedliche Vorstellung der Anwender, die das Modell je nach Gewerk, Weltgegend, Firmenrichtlinien oder persönlichem Stil konfigurieren.

3 | **Umfang der Abbildungen**
Das RI-Fließbild ist für verschiedene Gewerke eine wichtige Grundlage. Daher versuchen diese Gewerke, eine Vielzahl spezifischer Informationen in der aus Gewerkesicht geeigneten Struktur im RI-Fließbild zu hinterlegen. Dies führt zu einer Fülle von Informationen und Strukturen, die für die Automatisierungstechnik nicht von Interesse sind.

Diese Schwierigkeiten verhindern einen einheitlichen automatischen Zugriff auf die im RI-Modell hinterlegten

Informationen und führen dazu, dass auch heute noch, abgesehen von einfachen Listenexporten, die Übertragung zum Beispiel der Strukturinformationen durch Interpretation des grafischen Fließbildes durch den PLT-Planer erfolgt. Aufgrund der unterschiedlichen Auffassungen zum Umfang und zu der Bedeutung der in einem Fließbild zu hinterlegenden Informationen erscheint eine stringentere weltweite Standardisierung der bestehenden Fließbildnormen derzeit wenig aussichtsreich.

Deshalb geht das hier vorgeschlagene Modell PandIX einen anderen Weg. PandIX steht für „Piping and Instrumentation Diagram Exchange“, es geht von der leittechnischen Aufgabenstellung aus und fragt: Welche Informationen benötige ich aus einem RI-Fließbild, um eine ganz bestimmte Fragestellung bei der PLT-Planung oder PLT-Betriebsbetreuung eindeutig beantworten zu können. Aus dieser Sicht heraus wurde ein Referenzmodell entwickelt, das beschreibt, wie sich ein funktionales Modell der verfahrenstechnischen Anlage für die Leittechnik darstellen sollte.

1.1 Bestehende Festlegungen zu den Inhalten

Unabhängig von den speziellen Ausprägungen, Erweiterungen und Realisierungen gibt es weltweit ein einheitliches Verständnis über die Kerninhalte eines P&ID. Ziel ist die Darstellung der prozesstechnischen Funktionalität einer Anlage. Dazu gehören:

- die Beschreibung des Netzwerks der Produkträume und Produktförderwege mit ihren Förder- und Sperrorganen
- die Beschreibung der prozesstechnischen Hauptfunktionalität der beteiligten Apparate
- die Beschreibung sämtlicher PLT-Stellen, an denen entweder Information aus der physikalischen Anlage gewonnen (Sensorstelle) oder Information in physikalische Eingriffe verwandelt (Aktorstelle) wird

Wie die Beschreibung zu erfolgen hat, ist in grundlegenden Normenreihen festgelegt. Die Normenreihe DIN 28004 [1] beschreibt die wichtigsten Funktionstypen prozesstechnischer Anlagenteile mit ihrer grafischen Darstellung. Sie wird zur Zeit durch die Normenreihe ISO 10628 [2] abgelöst. In der ISO 15519 [3] werden allgemeine Regeln zur Darstellung von Eigenschaften, zur Notation der Objektreferenzen und so weiter in einem Diagramm festgelegt. Diese ISO-Normenreihen sind tendenziell eher geräte- als funktionsorientiert. Die zur Beschreibung der MSR-Funktionen im Fließbild gedachte ISO 3511 [4] wird als wenig geeignet angesehen und kaum angewandt. Für die Beschreibung von PLT-Stellen wurden daher aus automatisierungstechnischer Sicht getriebene funktionsorientierte Normen entwickelt. Das zentrale Dokument ist heute die IEC 62424 [5]. Sie hat die DIN 19227 [6] in der Zwischenzeit vollständig abgelöst.

Insgesamt bleibt festzustellen, dass alle diese im praktischen Engineering-Prozess verbreiteten und angewendeten Normen in erster Linie die grafische Beschreibung der Anlagenfunktion im Fokus haben. Einen primär informationsorientierten Ansatz findet man nicht. Die Datenmodelle der ISO 15926 und der IEC 62424 (CAEX) sind eher generischer Art und reichen als Arbeitsgrundlage für eine einheitliche konsistente Projektierung im konkreten Anwendungsfall nicht aus.

1.2 Bestehende Austauschformate

Neben der Beschreibung des P&ID-Modells sind in dem hier verfolgten Zusammenhang insbesondere die Schnittstellen zwischen P&ID und den Planungssystemen der PLT von Interesse. Dabei bieten sich folgende Technologien an:

CAEX
CAEX ist ein Standard zum elektronischen Austausch von Modellinformationen in Form von XML-Dateien. CAEX ist als Austauschformat für Fließbilddaten in IEC 62424 normiert. CAEX wurde allerdings ganz allgemein zum Austausch von CAE-Systeminformationen entwickelt. Es erlaubt den Austausch beliebiger hierarchischer Systemmodelle. Diese Eigenschaft von CAEX wird zum Beispiel in der AutomationML-Initiative genutzt. Wie CAEX speziell zum Austausch von P&ID-Informationen konfiguriert werden kann, ist beispielhaft im Anhang der IEC 62424 beschrieben. Diese Beschreibung ist jedoch eher informativ. Sie lässt viele Abbildungsvarianten zu und reicht bei Weitem nicht für einen automatisiert interpretierbaren Informationsaustausch. PandIX schließt genau diese Lücke. PandIX baut auf dem Metamodell von CAEX auf und prägt das Metamodell semantisch aus (vergleiche auch [7]).

XMpLant
XMpLant ist eine Spezifikation zum Austausch von P&ID-Daten auf der Grundlage des Datenmodells der ISO 15926. Sowohl das mit der ISO 15926 Teil 2 zugrundeliegende Metamodell als auch das P&ID-Referenzmodell (mit den Definitionen aus ISO 15926) ist sehr komplex. Zweifellos ist es mit XMpLant möglich, alle Informationen eines RI-Fließbildes zu übertragen. Dabei muss man jedoch feststellen, dass bei diesem Austauschformat nach wie vor der grafische Aspekt im Vordergrund steht. Die Vermischung von grafischen Informationen, funktionalen Informationen, Gerätedaten und Lebenszyklusdaten macht eine einfache Interpretation der PLT-relevanten Funktionalität sehr schwer.

Individuelle Exportformate
Von den CAE-Systemlieferanten werden eine Reihe von individuellen Exportformaten angeboten. Dies ist für den Planungsalltag sehr hilfreich. So können beispielsweise PLT-Stellenlisten aus dem RI-System extrahiert und automatisiert in das PLT-CAE-System eingelesen werden. Im Allgemeinen sind diese Formate jedoch nicht in der Lage, strukturelle Eigenschaften der Anlagentopologie abzubilden. Ein weiterer Nachteil ist der individuelle Charakter der Lösung.

2. ZIELSETZUNG VON PANDIX

In der Prozessautomatisierung basieren sowohl die Erstellung der PLT-Funktionspläne als auch fortgeschrittene Laufzeitanwendungen auf der expliziten Kenntnis der funktionalen Anlagenstruktur. Diese wird üblicherweise in einem P&ID-System der Anlagenplanung erstellt, verwaltet und dem Anwender zur Verfügung gestellt. Ziel von PandIX ist es, die funktionale Anlagenstruktur auf einfache und standardisierte Weise zu modellieren und Schnittstellen zu spezifizieren, wie diese Modelldaten zwischen einem Anlagenplanungssystem und den PLT-Systemen ausgetauscht werden können. Die Einordnung wird in Bild 2 verdeutlicht.

PandIX ist also eine sehr schmale Schnittstelle, die ausschließlich die funktionale Anlagenstruktur modelliert. Sie basiert auf dem Modell der IEC 62424 [5], die genau

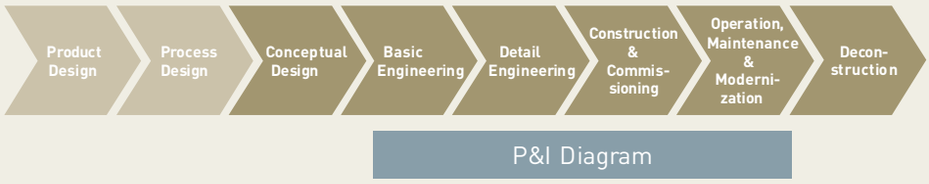


BILD 1: P&ID im Workflow

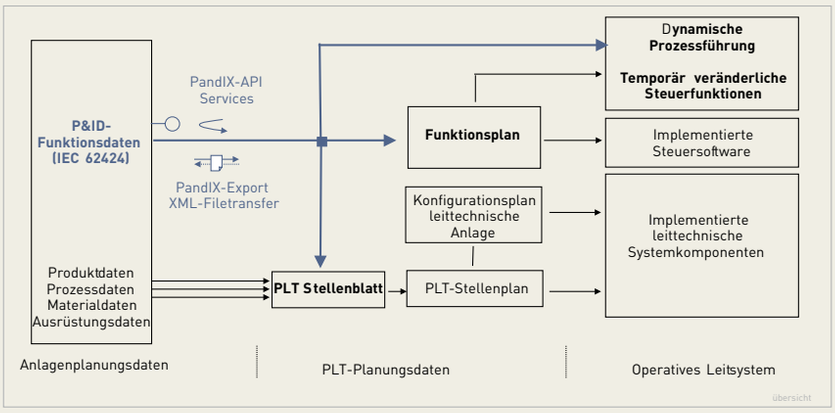


BILD 2: Einordnung von PandIX im Workflow

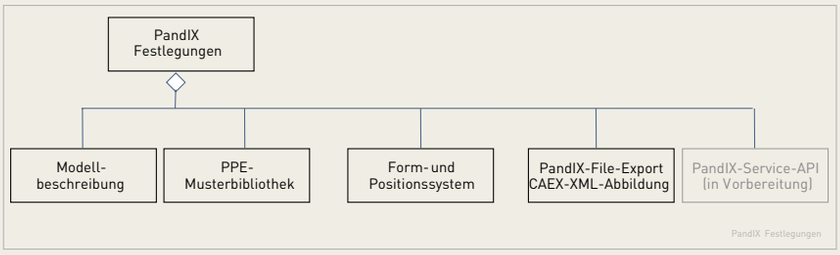


BILD 3: Festlegungen in PandIX

diesen Fokus besitzt. Wie in Bild 2 veranschaulicht, werden in Anlagenplanungssystemen oft weitere, für die PLT-Planung erforderliche Informationen verwaltet und meist auch im P&ID „irgendwie" dargestellt, so zum Beispiel Informationen zu den Produktdaten (beteiligte Stoffe, spezifische Dichte, ...), zu den Prozessdaten (Minimal-/Normal-/Maximal-Werte für Druck, Temperatur, Durchfluss, ...), zu den Materialdaten der Einrichtungen (Korrosionsbeständigkeit, Auskleidung, ...) zur Wahl der Ausrüstung (Typdaten der Einrichtungen, ...) und zu organisatorischen Rahmenbedingungen (sicherheitsrelevant, GMP-relevant, ...). Diese Informationen werden von PandIX nicht erfasst.

Das PandIX-Modell ist als Metamodell formuliert. Es beinhaltet die Konstruktionsregeln zur Darstellung des prozesstechnischen Anlagenaufbaus und zur Gestaltung der PLT-Stellen. In seiner Modellbeschreibung baut PandIX auf dem CAEX-Systemmodell auf.

PandIX besteht aus verschiedenen Festlegungen (vergleiche Bild 3):

- der eigentlichen Modellbeschreibung
- einer Bibliothek standardisierter Prozessanlagenelemente
- einem Vorschlag für ein Form- und Positionssystem
- Abbildungsvorschriften auf CAEX für den Modell-Export als XML-Datei

Diese Festlegungen liegen vor und können als Whitepaper von der Webseite des Lehrstuhls für Prozessleittechnik der RWTH Aachen heruntergeladen werden (www.plt.rwth-aachen.de). Die Festlegung der PandIX-Service-API ist derzeit noch in Vorbereitung.

3. CHARAKTERISTISCHE EIGENSCHAFTEN

3.1 Anlagenteile als Elemente der prozesstechnischen Anlage

Kern des PandIX-Modells ist die Beschreibung des funktionalen Aufbaus einer prozesstechnischen Anlage als flaches System aus miteinander verbundenen Anlagenteilen. PandIX unterscheidet, wie in Bild 4 dargestellt, zwischen zwei grundsätzlich unterschiedlichen Arten von Anlagenteilen: Prozessanlagenelementen und PLT-Stellen.

Prozessanlagenelemente (CAEX: PPE_Request) entsprechen in der Prozesstechnik den produktführenden Anlagenteilen wie Pumpen, Ventilen, Behältern, Rohrleitungen. Für die Darstellung im P&I-Diagramm gibt es für jeden Typ ein eigenes grafisches Symbol.

PLT-Stellen (CAEX: PCE_Request) sind funktionale Elemente, die als Brücke zwischen der Informationswelt und der physikalischen Welt wirken. Sensoren wandeln physi-

kalische Größen in Messwerte, Aktoren wandeln Stellinformationen in physikalische Einflussgrößen. PLT-Stellen haben im P&ID ein gemeinsames grafisches Symbol. Die Funktion wird durch mehrere Buchstaben-Funktionscodes beschrieben. Die grafische Darstellung und die Buchstabenfunktionscodes sind in der IEC 62424 [5] enthalten.

Wie in Bild 5 dargestellt, werden die Anlagenteile (CAEX: InternalElement) an entsprechenden Interfaces (CAEX: ExternalInterfaces) durch Links (CAEX: InternalLink) miteinander verbunden. Dies gilt für Verbindungen zwischen Prozessanlagenelementen, für Verbindungen zwischen PLT-Stellen und für Verbindungen zwischen Prozessanlagenelementen und PLT-Stellen.

Die Art der Verbindungen ergibt sich aus der Klasse der beteiligten Anlagenteile und Interfaces. Die Verbindungen selbst sind nur Links und besitzen gemäß dem CAEX-Modell keine funktionalen Eigenschaften. Verbindungen mit technologischen Eigenschaften wie zum Beispiel Rohrleitungen werden in PandIX daher nicht als Links, sondern als Anlagenteile modelliert. Im PandIX-Modell sind die in Bild 6 dargestellten Interface-Typen festgelegt und erlaubt.

Bild 7 zeigt ein Beispiel, in dem alle in PandIX erlaubten Interface-Typen und Links auftreten. Diese Interface-Typen und die dazugehörigen Links charakterisieren das P&ID-Modell von PandIX und sollen im Folgenden noch etwas ausführlicher erläutert werden.

3.2 Das Produktraumnetzwerk

In der Prozesstechnik sind die Produkte formlos (Gase, Flüssigkeiten, Schüttgüter) und werden typischerweise in geschlossenen Behältern und Rohrleitungen gehalten und transportiert. Ein wesentlicher Aspekt des P&ID ist die Beschreibung dieser Produkträume und ihrer Verbindungen. Die Produkträume sind untereinander durch punktuelle Koppelpunkte miteinander verbunden. Die verkoppelten Produkträume bilden das Produktraumnetzwerk.

Produkträume

Jedes Prozessanlagenelement besitzt mindestens einen Produktraum. Ein Rohr oder ein einfacher Behälter be-

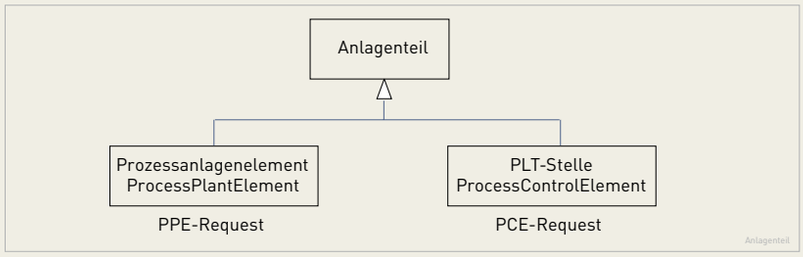


BILD 4: Die zwei unterschiedlichen Arten von Anlagenteilen

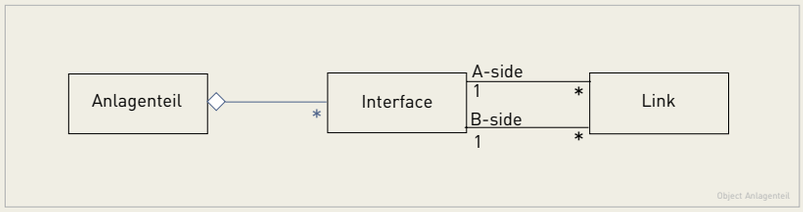


BILD 5: Netzwerk aus Anlagenteilen

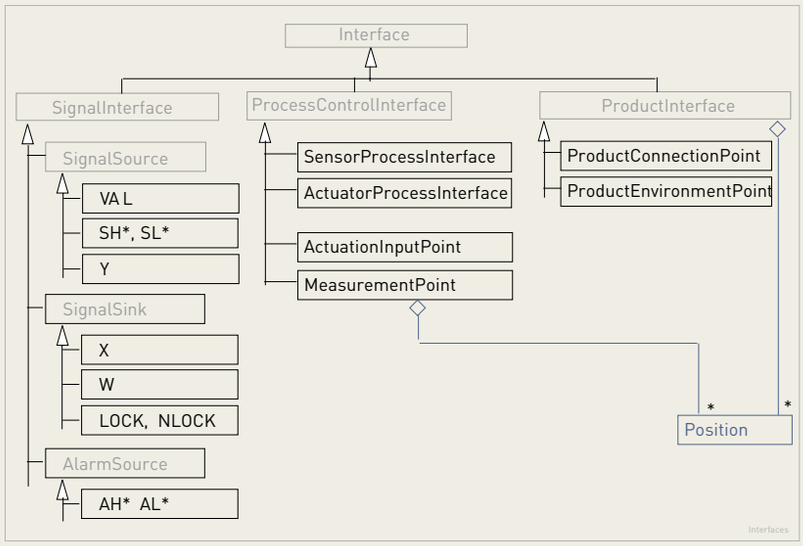


BILD 6: Interface-Typen in PandIX

sitzen genau einen Produktraum, ein Wärmetauscher besitzt zum Beispiel zwei Produkträume.

Die Modellierung der Produkträume erfolgt in PandIX nach dem RIVA-Kanalmodell [8]. Jeder Produktraum entspricht einem Kanal (ProductChannel). Jedes Prozessanlagenelement hat also einen oder mehrere Kanäle. Zur Vereinfachung bezeichnen wir einen Kanal als Hauptkanal und die eventuell vorhandenen weiteren Kanäle als Nebenkanäle. Zur Vereinfachung der Abbildung erben alle Prozessanlagenelementrollen die Kanaleigenschaft des Hauptkanals direkt von der Basisklasse PPE-Request. Sollen Nebenkanäle ebenfalls explizit modelliert werden, dann ist für den jeweiligen Elementtyp eine eigene SystemUnitClass anzulegen. In der SystemUnitClass werden die Kanäle, wie am Beispiel des Wärmetauschers in Bild 8 verdeutlicht, explizit als interne Elemente angelegt und verschaltet. Dies ermöglicht die eindeutige Verschaltung und die eindeutige Zuordnung und Verortung zum Beispiel von Messstellen innerhalb eines Kanals in einem komplexen mehrkanaligen Apparat.

Produktkopplung

Eine Produktkopplung beschreibt das dichte Verbinden von zwei Produkträumen (Kanälen) über zwei Produktanschlusspunkte (ProductConnectionPoints). Ein Produktanschlusspunkt beschreibt eine Öffnung eines Produktraums, die als Übergang zu Nachbarprodukträumen explizit vorgesehen ist. Darüber kann ein Produkt in den Produktraum ein- und austreten. Mit der Produktkopplung werden zwei genau zueinander passende Produktanschlusspunkte räumlich und funktional verbunden und zur Umgebung hin dicht verschlossen.

Im bestimmungsgemäßen Zustand muss jeder Produktanschlusspunkt mit einem anderen Produktanschlusspunkt verbunden (das heißt im PandIX-Modell verlinkt) sein. Jede Produktkopplung befindet sich an einem definierten physikalischen Ort. Zwei verlinkte Produktanschlusspunkte müssen sich also zwingend am gleichen Ort befinden.

Auslass

Ein Auslass ist eine Öffnung eines Produktraums zur Umgebung. In Bild 9 sind verschiedene Beispiele für Auslässe dargestellt. In PandIX wird ein Auslass durch ein Interface

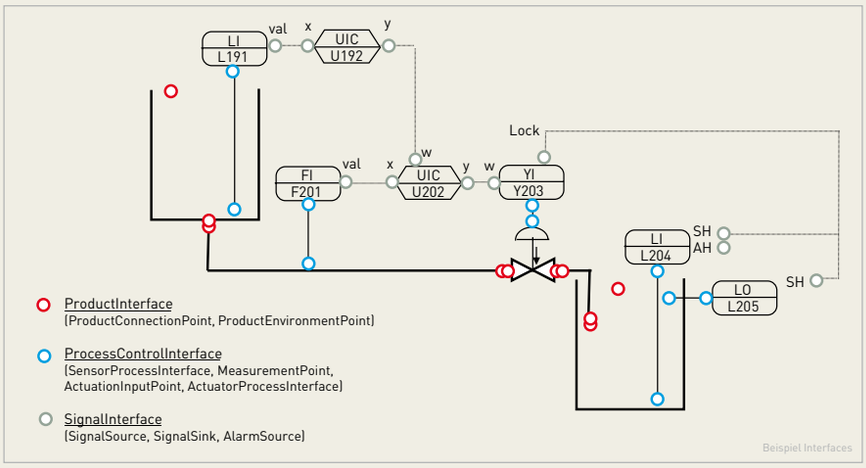


BILD 7: Beispiel mit den in PandIX erlaubten Interface-Typen

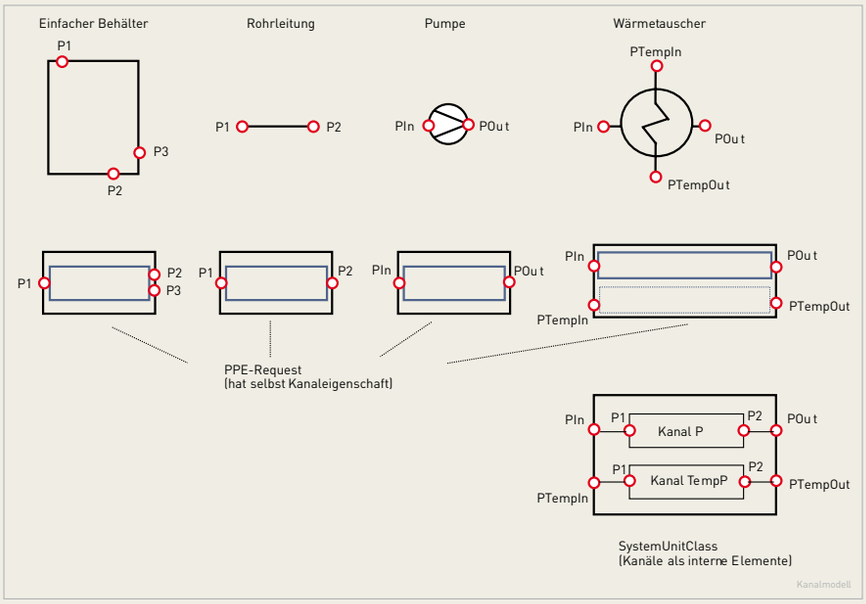


BILD 8: Explizite Modellierung der Produkträume als Kanäle in PandIX

des Typs Produktauslasspunkt (ProductEnvironment-Point) modelliert. Dieses Interface ist immer einem Produktraum zugeordnet und kann nicht verlinkt werden. Auch wenn dies im P&ID bildlich nicht explizit dargestellt ist, hat jeder drucklose offene Behälter einen Auslass.

PLT-Stellen

PLT-Stellen sind funktionale Elemente, die als Brücke zwischen der Informationswelt und der physikalischen Welt wirken. Die Funktionalität von PLT-Stellen ist in der IEC 62424 [5] standardisiert.

Restriktive Regeln in PandIX

PandIX geht von den Festlegungen der IEC 62424 aus, ist also mit dieser Norm konform. PandIX macht jedoch weitere restriktive Vorschriften, um die eindeutige Interpretierbarkeit sicherzustellen. So werden zum Beispiel redundante Darstellungsarten vermieden und informelle, nicht eindeutig interpretierbare Informationen eliminiert. Wichtige Vorschriften sind:

- Verpflichtende Angabe des Signalcodes.
  Für das Verständnis der PLT-Stelle ist der grundsätzliche Wertebereich der ausgetauschten Information von zentraler Bedeutung. In PandIX ist daher die Angabe von O (binärer Wertebereich) beziehungsweise I (mehrwertiger oder analoger Wertebereich) als Zweitbuchstabe (Drittbuchstabe bei Differenzmessungen) zwingend.
- C-Funktion ist ausschließlich in U-Stelle erlaubt. Werden zwei PLT-Stellen durch eine C-Funktion verknüpft, dann muss dazu in PandIX zwingend eine eigene U-Stelle angelegt werden. Die Verwendung der C-Funktion in Aktor- oder Sensorstellen ist nicht erlaubt.
- Die U-Stelle ist ausschließlich zur Beschreibung eines einfachen SISO-Reglers erlaubt.
  Komplexe U-Funktionen können aus dem P&ID nicht interpretiert werden und sind daher für PandIX wertlos. Sie tauchen in PandIX nicht auf. In PandIX entspricht eine U-Funktion immer einem einfachen SISO-Regler.

Prozess-Sensor-Kopplung

Eine Prozess-Sensor-Kopplung beschreibt die Zuordnung einer Messfunktion zu ihrem physikalischen Messort. In PandIX wird diese Kopplung durch einen Sensor-Prozessanschluss (SensorProcessInterface) modelliert, der mit einem Messpunkt (MeasurementPoint) verlinkt ist. In Bild 10 wird der Sensor-Prozessanschluss erläutert.

Jeder Sensor-Prozessanschluss muss wie im Beispiel in Bild 10 zwingend mit genau einem Messpunkt verlinkt sein. Umgekehrt dürfen jedoch bei Multisensoren mehrere Sensor-Prozessanschlüsse auf einen Messpunkt verlinkt sein. In Bild 10 ist dies bei dem dargestellten Durchflussmesser

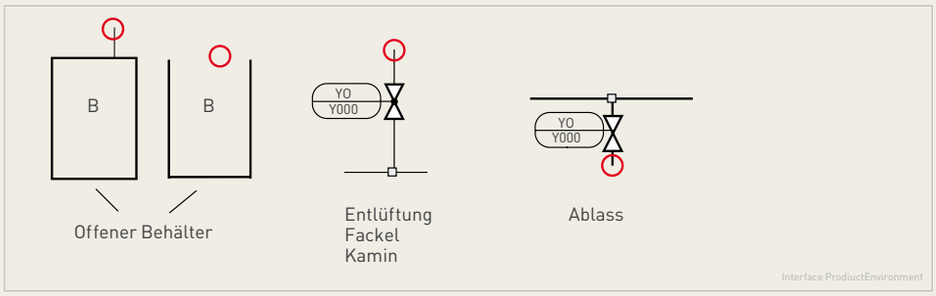


BILD 9: Beispiele für Auslässe

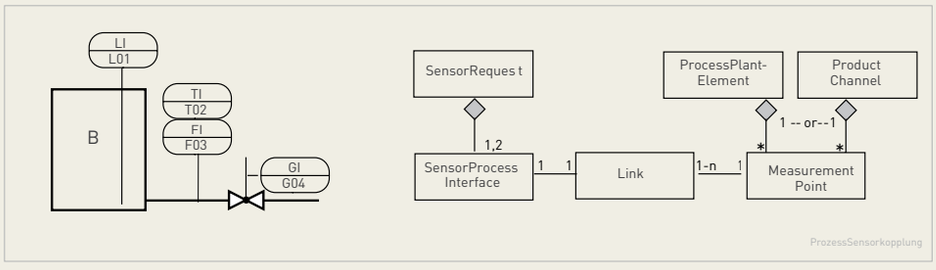


BILD 10: Die Prozess–Sensor-Kopplung

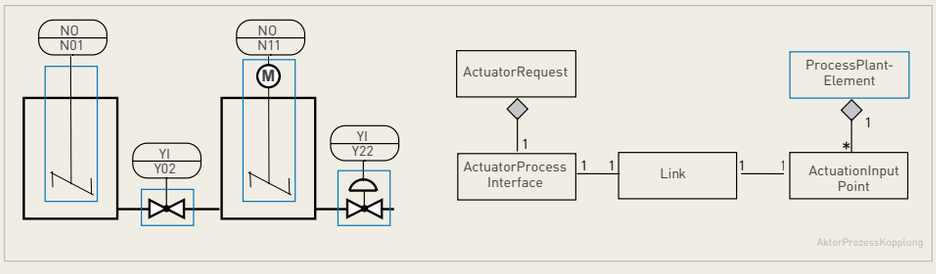


BILD 11: Die Aktor–Prozess-Kopplung

der Fall, der gleichzeitig eine Temperaturmessung beinhaltet. Die räumliche Platzierung der Sensorstellen und der Prozessanschlusslinie im P&ID hat im Gegensatz zum Ort des Messpunkts keinerlei technologische Bedeutung.

Aktor-Prozess-Kopplung
Eine Aktor-Prozess-Kopplung beschreibt die Zuordnung einer Stellfunktion zu einem physikalischen Aktor. In PandIX wird diese Kopplung durch einen Aktor-Prozessanschluss (ActuatorProcessInterface) modelliert, der mit einem Aktoreingangspunkt (ActuationInputPoint) verlinkt ist. Die Zusammenhänge werden in Bild 11 erläutert. Jeder Aktor-Prozessanschluss muss zwingend mit genau einem Aktoreingangspunkt verlinkt sein. Umgekehrt muss jeder Aktoreingangspunkt mit genau einem Aktor-Prozessanschluss verlinkt sein.

Signalkopplung
Eine Signalkopplung beschreibt die Zuordnung eines Signaleingangs (SignalSink) einer PLT-Stelle zu einem Signalausgang (SignalSource) einer PLT-Stelle. Signalquellen und Signalsenken können, müssen jedoch nicht verlinkt sein. Alarmquellen sind grundsätzlich nicht verlinkt. Signalverbindungen besitzen im Rahmen des P&ID keinerlei funktionale Eigenschaften und können daher als Links modelliert werden. Sämtliche erlaubten Signalein- und -ausgänge sind in PandIX standardisiert. Sie sind in Bild 7 dargestellt. In PandIX dürfen nur diese Signalein- und -ausgänge verwendet werden.

4. DIE PPE-BASISBIBLIOTHEK

Die Prozessanlagenelemente (ProcessPlantElements, PPE-Requests) beschreiben die prozesstechnischen Komponenten, aus denen die Anlage aufgebaut ist. In der PPE-Basisbibliothek werden die wichtigsten Rollentypen wie Rohre, Pumpen und Behälter beschrieben. Es zeigt sich, dass man mit einer Liste von etwa 10 bis 20 Typen eine recht hohe Abdeckung für die chemische und petrochemische Industrie erreicht. Für spezielle Anlagentypen müssen nur noch wenige spezielle Rollentypen nachgepflegt werden. Dies ist ohne großen Aufwand möglich. Bild 12 zeigt einen Ausschnitt aus der Basisbibliothek.

Unabhängig von den speziellen Ausprägungen besitzen alle PPE-Elemente einen einheitlichen Grundaufbau und werden in der Bibliothek einheitlich beschrieben. In den Bildern 13 und 14 sind die Grundmuster für ein einfaches PPE-Element, modelliert als RoleClass, und ein strukturiertes PPE-Element, modelliert als SystemUnitClass, dargestellt. Für eine Pumpe als einfaches PPE-Element ergibt sich dann z. B. der in Bild 15 dargestellte Rollentyp.

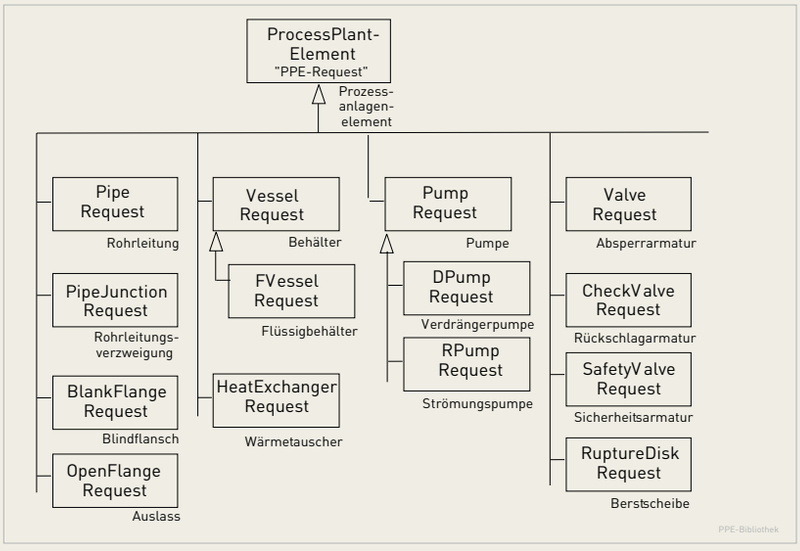


BILD 12: PPE-Basisbibliothek

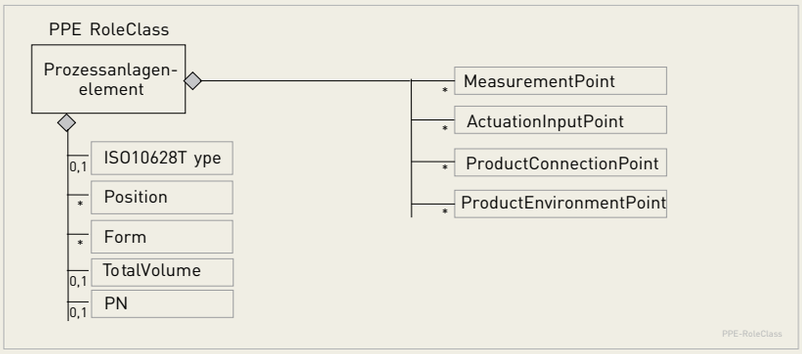


BILD 13: Grundmuster einer PPE RoleClass

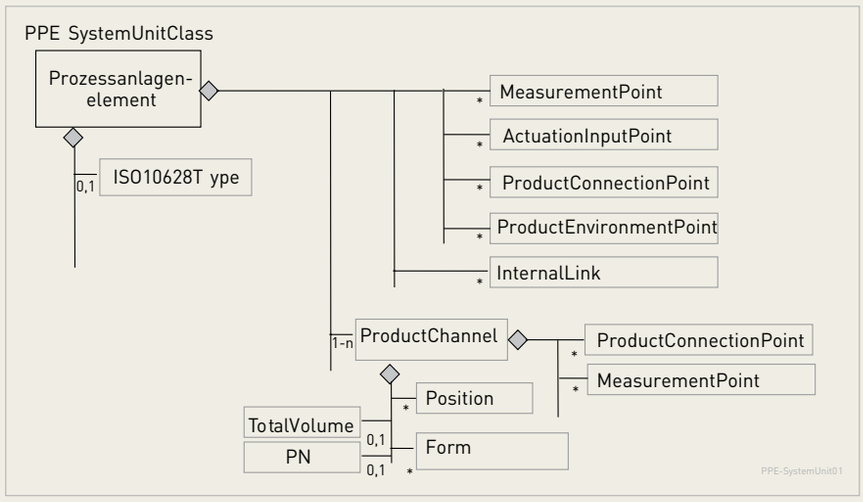


BILD 14: Grundmuster einer PPE System-UnitClass

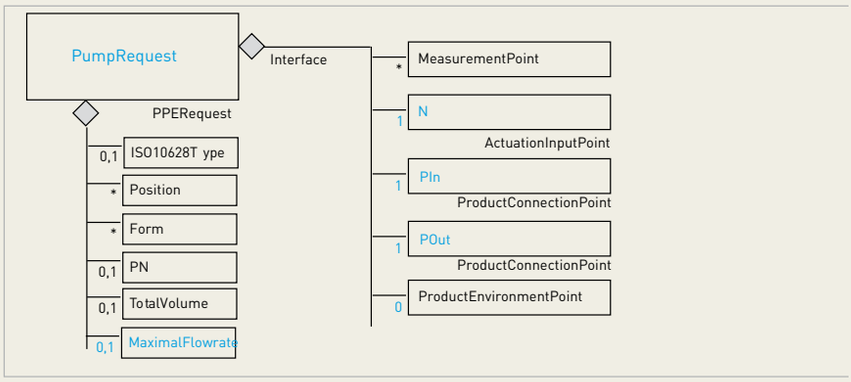


BILD 15: Attribute und Interfaces einer Pumpe

5. FORM- UND POSITIONSSYSTEM

Um die Struktur des Produktraummodells in automatisierungstechnische Zusammenhänge umsetzen zu können, sind einige wenige ergänzende geometrische Informationen erforderlich. Dazu gehören beispielsweise die Volumen-Füllstands-Kennlinien von Behältern, die Positionen von Rohranschluss- und Messpunkten und die Höhenverläufe zur Abschätzung von hydrostatischen Zusammenhängen. Diese Informationen sind prinzipiell in den 3D-Anlagenmodellen vorhanden. P&I-Diagramme enthalten diese Informationen typischerweise nur angedeutet und unvollständig. Die direkte Erfassung aus den 3D-Anlagenmodellen ist jedoch schwierig, da die relevanten Informationen in nicht standardisierter Weise in den (standardisierten) Exportdatendateien versteckt sind. In vielen Fällen stehen die 3D-Anlagendaten auch nicht oder nicht aktuell für die Automatisierungstechnik zur Verfügung. Um diese Lücke zu schließen, ist dem PandIX-Modell ein Form- und Positionsschema angefügt, nach dem die benötigten geometrischen Informationen einfach übertragen und automatisch interpretiert werden können.

Gefüllt werden kann dieses Form- und Positionsschema im Einzelfall durch einen geeigneten Export aus dem 3D-Anlagenmodell, aber auch zumindest teilweise aus der P&ID-Datenbasis. Aus der P&ID-Datenbasis sind die Informationen jedoch nicht zweifelsfrei erkennbar. Höhenverhältnisse, Formen und Positionen von Anschlusspunkten sind nur informativ grafisch angedeutet, jedoch nicht explizit in der Datenbasis abgelegt. Aus diesem Grund müssen bei einem Export aus der P&ID-Datenbasis Form- und Positionsinformationen teilweise händisch und nach Rücksprache mit dem Verfahrenstechniker nachgepflegt werden.

Um diese Arbeit so gering wie möglich zu halten, beschränkt sich das PandIX-Form- und -Positionssystem auf die unbedingt notwendigen Informationen. Es müssen im Einzelfall auch nur die Informationen eingepflegt werden, die tatsächlich später benutzt werden. Es sei darauf hingewiesen, dass dies keine Mehrarbeit ist. Diese Informationen müssen in jedem Fall für die PLT-Systeme erfasst werden. PandIX definiert dazu jedoch ein einheitliches Format zur einfachen Eingabe und zur automatisierten Übernahme zum Beispiel aus 3D-Anlagenplanungssystemen.

6. ZUSAMMENFASSUNG UND AUSBLICK

PandIX steht für „Piping and Instrumentation Diagram Exchange“ und bietet eine Modellspezifikation zur Erfassung der Rohrleitungs- und Instrumentierungsstruktur einer prozesstechnischen Anlage. Diese Spezifikation wird aus Sicht der Automatisierungstechnik formuliert.

Ziel ist es, mit PandIX eine formale Beschreibung eines RI-Fließbildes zur maschinellen Auswertung in der Automatisierungstechnik zur Verfügung zu haben. Damit wird ein Teil des Informationsbruchs zwischen der Verfahrenstechnik und der Automatisierung geschlossen. Informationen, die bisher nur durch optische Interpretation des RI-Fließbildes oder spezielle Listenexporte erfasst wurden, können mit Hilfe von PandIX formalisiert beschrieben, elektronisch ausgetauscht und von der automatisierungstechnischen Anwendung interpretiert werden. Damit wird eine Grundlage geschaffen, um mit intelligenten Assistenzfunktionen die automatisierungstechnischen Ingenieurprozesse effizient zu unterstützen, in Teilbereichen zu automatisieren und die Ergebnisse zu verifizieren.

Als ein wesentliches Problem sind die Informationen zu Position und Form von Prozessanlagenelementen anzusehen, die nicht explizit im Datenmodell abgelegt sind und nur durch die Grafik informell vermittelt werden. Diese Informationen werden für die Prozessautomation jedoch unbedingt benötigt. Es erscheint von PLT-Seite aus sinnvoll, diese Informationen in die P&ID-Datenbanken, gegebenenfalls übergangsweise händisch, als zusätzliche Objektparameter explizit nachzupflegen. Das PandIX-Form- und -Positionspapier macht dazu einen Vorschlag.

Damit in Zukunft die PLT-Engineering-Funktionen direkt auf die P&ID-Datenbasis zurückgreifen können, bietet sich die Spezifikation und Implementierung einer PandIX-Serviceschnittstelle als API an, über die dann dynamisch interaktiv Modellinformationen mit dem P&ID ausgetauscht werden können. Die Entwicklung dieser Serviceschnittstelle ist eine interessante Aufgabe der nächsten Zeit.

MANUSKRIPTEINGANG
07.10.2010
Im Peer-Review-Verfahren begutachtet

REFERENZEN

[1] DIN 28004: Fließbilder verfahrenstechnischer Anlagen. DIN. Beuth-Verlag
[2] ISO 10628: Flow Diagrams for Process Plants. Publication ISO
[3] ISO 15519: Specifications for diagrams for process industry. Publication ISO
[4] ISO 3511: Process measurement control functions and instrumentation. Publication ISO
[5] IEC 62424: Specification for representation of process control engineering requests in P&I Diagrams and for data exchange between P&ID tools and PCE-CAE. Publication IEC 62424-Ed.1. CDV-6:2007
[6] DIN 19227: Grafische Symbole und Kennbuchstaben für die Prozessleittechnik. DIN. Beuth-Verlag
[7] Epple, U.; Austausch von Anlagenplanungsdaten auf der Grundlage von Metamodellen. atp - Automatisierungstechnische Praxis 45 (2003), Heft 7, Oldenbourg Industrieverlag, München.
[8] Jorewitz, R., Quirós, G., Epple, U.: Modelling of Multiple, Semantically-Coupled Flow-Graphs, in: SOLI 2008: 2008 IEEE International Conference on Service Operations and Logistics, and Informatics, 12. – 15. Okt. 2008, Beijing, China, S. 965 – 971

AUTOREN

PROF. DR.-ING. ULRICH EPPLE (geb. 1953) leitet den Lehrstuhls für Prozessleittechnik an der RWTH Aachen. Seine Hauptarbeitsgebiete sind der Einsatz von formalen Methoden in der Prozessautomation, modellgetriebene Entwicklungskonzepte, Automation der Automation, Prozessführung, Prozess- und Anlagenüberwachung.

**Lehrstuhl für Prozessleittechnik,
RWTH Aachen, D-52056 Aachen,
Tel. +49 (0) 241 809 77 37,
E-Mail: epple@plt.rwth-aachen.de**

DIPL.-ING. MARKUS REMMEL (geb. 1980) ist Entwicklungsingenieur in der Vorfeldentwicklung des Sektors Industry in der Division Industry Automation der Siemens AG. Seine Hauptarbeitsgebiete sind die durchgängige Nutzung von Engineering-Daten im Lebenszyklus einer verfahrenstechnischen Anlage und die Entwicklung von Konzepten für den Datenaustausch zwischen Engineering-Werkzeugen.

**Siemens AG,
I IA&DT ATS 3,
Östliche Rheinbrückenstraße 50,
D-76187 Karlsruhe,
Tel. +49 (0) 721 596 45 98,
E-Mail: markus.remmel@siemens.com**

DR.-ING. OLIVER DRUMM (geb. 1972) ist Entwicklungsingenieur in der Vorfeldentwicklung des Sektors Industry in der Division Industry Automation der Siemens AG. Er beschäftigt sich mit durchgängigen Prozessen und Werkzeugen im Engineering für verfahrenstechnische Anlagen entlang des gesamten Lebenszyklus.

**Siemens AG,
I IA&DT ATS 3,
Östliche Rheinbrückenstraße 50,
D-76187 Karlsruhe,
Tel. +49 (0) 721 595 45 98,
E-Mail: oliver.drumm@siemens.com**

Sicher und flexibel just in sequence produzieren

Processing statt Tracing: QRV-Software vereinfacht Montage von Pkw-Dachhimmeln

Beim Aufbau einer Just-in-sequence-Fertigung für Pkw-Dachhimmelmodule erreichte die Grupo Antolin Logistik GmbH mit einer Qualitätssicherungs- und Rückverfolgungssoftware sichere Prozesse und hohe Flexibilität. Zudem konnten die indirekten Fertigungskosten reduziert werden. Die unproduktiven Tätigkeiten konnten gesenkt und das gewünschte Preis-Leistungs-Verhältnis erreicht werden.

Neben der klassischen Logistikarbeit haben auch moderne Logistikunternehmen schon längst Teilproduktionen als Zulieferer übernommen. Diese Kombination aus Produktion und Logistik setzt ein hohes Maß an Flexibilität und Prozesssicherheit voraus.

Auch die Niederlassung der Grupo Antolin Logistik GmbH in Neutraubling stand vor einigen Jahren vor einer besonderen Herausforderung. Der neue Montageprozess für Dachhimmelmodule für Pkw im Mehrschichtbetrieb sollte flexibel und sicher gestaltet und dabei die Kosten gesenkt werden. Die geforderte Just-in-sequence-Fertigung sollte vom Start an sicher laufen, um den sehr anspruchsvollen Kunden, einen Pkw-Premiumhersteller, langfristig zufriedenzustellen.

Die Komplexität und die Anforderungen an die Flexibilität sind sehr hoch: Die Dachhimmelherstellung umfasst mehr als 250 verschiedene Ausstattungsvarianten. Und bis zu einer Stunde vor der Anlieferung an das Montageband des Automobilherstellers müssen noch Änderungen im größeren Umfang möglich sein.

Die Lösung fand der Hersteller bei seinem Sondermaschinenlieferanten, der Firma PaCo GmbH aus dem thüringischen Saalfeld. Das mittelständische Unternehmen hatte aufgrund der langjährigen Erfahrung im Sondermaschinenbau die QRV-Software entwickelt. QRV steht für Qualitätssicherungs- und Rückverfolgungs-System. Es erlaubt eine kundenspezifische lückenlose Prozesssteuerung mit integrierter Qualitätskontrolle und Prozessdokumentation sowie nahtloser Rückverfolgung. Diese permanent weiterentwickelte Software ist sehr flexibel und für unterschiedlichste Produktionsprozesse einsetzbar. Sie wird von Automobilzulieferern unter anderem bei der Produktion von Airbags, Scheinwerfern, Sicherheitsgurten, Lenkgetrieben und Schweißbaugruppen verwendet.

Aufgrund der Systemoffenheit der QRV-Software konnten die vorhandenen Prozessdaten ohne Behinderung der laufenden Produktion entsprechend aufbereitet werden. Nur jene Programmmodule wurden eingebunden, die für die Prozesssicherheit benötigt wurden. So konnte Grupo Antolin Logistik unnötige Kosten vermeiden. Die benötigten Reports kann der Kunde selbstständig erstellen und bearbeiten. Direkte Exporte in MS-Excel, ASCII, Q-DAS oder SAP sind durch die jeweiligen Module gewährleistet.

Im Montagewerk in Neutraubling wurde durch die QRV-Software die Flexibilität der Arbeitsvorbereitung erhöht und die damit verbundene, lückenlose Dokumentation der Arbeitsanweisungen vereinfacht und nahezu papierlos gestaltet. Die Mitarbeiter in der Produktion und Logistik sind seither von unnötigen Schreibarbeiten entlastet und können sich auf den eigentlichen Fertigungsprozess konzentrieren. Sicher überwacht wird zudem die Einhaltung wichtiger Wartungsintervalle innerhalb des Fertigungsprozesses. Entlastet werden die Mitarbeiter auch durch die visualisierte Führung: Stets wird ihnen die aktuellste Arbeitsanweisung auf einem Bildschirm angezeigt. Deren Ausführung wird schließlich von den Mitarbeitern bestätigt.

Dank ihrer offenen Schnittstellen konnte die QRV-Software störungsfrei mit dem beim Kunden eingesetzten ERP-System von SAP verbunden werden. Die Übernahme der Stücklistendaten war neben der gewünschten Generierung der Barcodes nur ein Teil der umfangreichen Datenübernahme. Im Rahmen der Qualitätssicherung werden analoge und digitale Messwerte erfasst und ausgewertet sowie optische Messungen integriert. Mit dem neuen System konnte der Hersteller auch den Aufwand für die Prozesszertifizierung reduzieren.

PACO GMBH,
Zum Silberstollen 2,
D-07318 Saalfeld,
Tel. +49 (0) 3671 45 56 60,
Internet: www.paco-gmbh.com

Ohne QRV-System

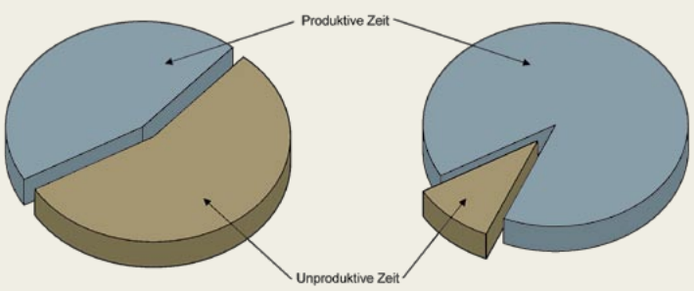
Arbeitsinhalt	Kosten bzw. Aufwand pro				entspricht Stunden im Jahr
	Tag	Woche	Monat	Jahr	
Produktion bzw. Fertigung	8 h				1824 h
Endkontrolle, Verpacken	2 h				456 h
Verwalten von Qualitätsanforderungen		4 h			182 h
Verwalten & Auswertung von Proben	3 h				684 h
Verwaltung von Arbeitsanweisungen		4 h			182 h
Auswertung von Maschinenparametern		3 h			137 h
Durchführen von Inventuren				32 h	32 h
Fehlererkennung und -auswertung			12 h		126 h
Erfassen und erstellen von Zeitnachweisen	2 h				456 h

Produktive Zeit	**1824 h**
Unproduktive Zeit	**2255 h**
Gesamtstunden pro Jahr	**4079 h**

Mit QRV-System

Arbeitsinhalt	Kosten bzw. Aufwand pro				entspricht Stunden im Jahr
	Tag	Woche	Monat	Jahr	
Produktion bzw. Fertigung	8 h				1824 h
Endkontrolle, Verpacken		3 h			137 h
Verwalten von Qualitätsanforderungen					0 h
Verwalten & Auswertung von Proben					0 h
Verwaltung von Arbeitsanweisungen					0 h
Auswertung von Maschinenparametern		1 h			46 h
Durchführen von Inventuren				6 h	6 h
Fehlererkennung und -auswertung			2 h		21 h
Erfassen und erstellen von Zeitnachweisen					0 h

Produktive Zeit	**1824 h**
Unproduktive Zeit	**210 h**
Gesamtstunden pro Jahr	**2034 h**



Durchschnittliche Arbeitszeit für 1 Mitarbeiter pro Jahr:		
	Stunden	1824
	Tage	228
	Wochen	45,6
	Monate	10,5

UNPRODUKTIVE ZEIT BEDEUTEND REDUZIERT: Die Grupo Antolin Logistik konnte im Werk Neutraubling die Arbeitszeit effektiver ausnutzen. Quelle: PaCo

IMPRESSUM

Verlag:
Oldenbourg Industrieverlag GmbH
Rosenheimer Straße 145
D-81671 München
Telefon +49 (0) 89 4 50 51-0
Telefax +49 (0) 89 4 50 51-3 23
www.oldenbourg-industrieverlag.de

Geschäftsführer:
Carsten Augsburger
Jürgen Franke
Hans-Joachim Jauch

Publisher:
Wolfgang Mönning

Herausgeber:
Dr. V. Huck
Dr. G. Kegel
Dipl.-Ing. H. Kumpfmüller
Dr. N. Kuschnerus

Beirat:
Dr.-Ing. K. D. Bettenhausen
Prof. Dr.-Ing. Ch. Diedrich
Prof. Dr.-Ing. U. Epple
Prof. Dr.-Ing. A. Fay
Prof. Dr.-Ing. M. Felleisen
Prof. Dr.-Ing. G. Frey
Prof. Dr.-Ing. P. Göhner
Dipl.-Ing. Th. Grein
Prof. Dr.-Ing. H. Haehnel
Dr.-Ing. J. Kiesbauer
Dipl.-Ing. R. Marten
Dipl.-Ing. G. Mayr
Dr. J. Nothdurft
Dr.-Ing. J. Papenfort
Dipl.-Ing. W. Setzwein
Dipl.-Ing. D. Westerkamp
Dr. Ch. Zeidler

Organschaft:
Organ der GMA (VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik) und der NAMUR (Interessengemeinschaft Automatisierungstechnik der Prozessindustrie).

Redaktion:
Gerd Scholz
(verantwortlich)
Telefon +49 (0) 89 4 50 51-3 44
Telefax +49 (0) 89 4 50 51-3 23
E-Mail: atp.redaktion@oldenbourg.de

Anne Hütter
Telefon +49 (0) 89 4 50 51-4 18
Telefax +49 (0) 89 4 50 51-3 23
E-Mail: atp.redaktion@oldenbourg.de

Einreichung von Hauptbeiträgen:
Prof. Dr.-Ing. Frank Schiller
(Chefredakteur, verantwortlich für die Hauptbeiträge)
Technische Universität München
Lehrstuhl f. Informationstechnik in Maschinenwesen
GF Automatisierungstechnik
Boltzmannstraße 15
D-85748 Garching bei München
Telefon +49 (0) 89 28 91 64 02
E-Mail: schiller@oldenbourg.de

Fachredaktion:
M. Blum
Prof. Dr. J. Jasperneite
Dr. B. Kausler
Dr. N. Kiupel
Dr. W. Morr
I. Rolle

Bezugsbedingungen:
„atp edition – Automatisierungstechnische Praxis" erscheint monatlich mit einer Doppelausgabe im Januar/Februar und Juli/August.

Bezugspreise:
Abonnement (Deutschland):
€ 460,– + € 30,– Versand
Abonnement (Ausland):
€ 460,– + € 35,– Versand
Einzelheft: € 55,– + Versand
Die Preise enthalten bei Lieferung in EU-Staaten die Mehrwertsteuer, für alle übrigen Länder sind es Nettopreise.
Mitglieder der GMA: 30% Ermäßigung auf den Heftbezugspreis.
Bestellungen sind jederzeit über den Leserservice oder jede Buchhandlung möglich.
Die Kündigungsfrist für Abonnementaufträge beträgt 8 Wochen zum Bezugsjahresende.

Abonnement-/ Einzelheftbestellung:
Leserservice atp
Postfach 91 61, D-97091 Würzburg
Telefon +49 (0) 931 4170-1615
Telefax +49 (0) 931 4170-492
E-Mail: leserservice@oldenbourg.de

Verantwortlich für den Anzeigenteil:
Thomas Hoffmann
Telefon +49 (0) 89 4 50 51-2 06
Telefax +49 (0) 89 4 50 51-2 07
E-Mail: hoffmann@oldenbourg.de
Anschrift siehe Verlag.
Zurzeit gilt Anzeigenpreisliste Nr. 48.

Anzeigenverwaltung:
Brigitte Krawczyk
Telefon +49 (0) 89 4 50 51-2 26
Telefax +49 (0) 89 4 50 51-3 00
E-Mail: krawczyk@oldenbourg.de

Druck:
druckpartner
Am Luftschacht 12
45292 Essen
Gedruckt auf chlor- und säurefreiem Papier.

Die atp wurde 1959 als „Regelungstechnische Praxis – rtp" gegründet.

ISSN 2190-4111

VORSCHAU

DIE AUSGABE 3/2011 DER

atp edition
Automatisierungstechnische Praxis

ERSCHEINT AM 9.3.2011
MIT FOLGENDEN BEITRÄGEN:

Modellgestützter Entwurf portabler, eingebetteter Steuerungssysteme

Maschinensicherheit und Zuverlässigkeit nach ISO 13849

Modellierung und Analyse von Verlässlichkeitsanforderungen mittels Prozess- und Ressourcenbeschreibung

Automatische Optimierung in der Profilextrusion

...und vielen weiteren Themen.

Aus aktuellem Anlass können sich die Themen kurzfristig verändern.

LESERSERVICE

E-MAIL:
leserservice@oldenbourg.de

TELEFON:
+49 (0) 931 4170-1615

WISSEN für die ZUKUNFT

Sonderpreise für Abonnenten der atp edition

atp kompakt

Methoden Verfahren Konzepte

Die Automatisierungstechnik wird durch neue Forschungen und Entwicklungen bestimmt. Damit Ingenieure fit für ihren Job sind und die entscheidenden Trends in der Automatisierungstechnik schnell zur Hand haben, legt die Fachpublikation atp edition die Buchreihe atp kompakt auf. Alle darin enthaltenen Beiträge haben ein wissenschaftliches Gutachterverfahren durchlaufen.
Herausgeber Prof. Dr.-Ing. Frank Schiller leitet am Lehrstuhl für Informationstechnik im Maschinenwesen der TU München das Fachgebiet Automatisierungstechnik.

atp kompakt Band 1

Erfolgreiches Engineering – Die wichtigsten Methoden

Diese Ausgabe befasst sich mit den Methoden, Verfahren und Standards, die Sie in den nächsten Jahren im Engineering beschäftigen werden. Wichtige Kriterien sind die einfache Wiederverwendbarkeit von Komponenten, die Unterstützung durch geeignete Werkzeuge, die Erhöhung der Flexibilität von Anlagen sowie geeignete Modellierungs- und Gerätebeschreibungssprachen.

1. Auflage 2010, 138 Seiten mit CD-ROM, Broschur, € 79,- • ISBN: 978-3-8356-3210-3

atp kompakt Band 2

Effiziente Kommunikation – Die bedeutendsten Verfahren

Sie bekommen Einblick in die wachsende Bedeutung der industriellen Kommunikation und dem Wandel in der Gerätekommunikation. Einen Schwerpunkt bildet die Kommunikationstechnik in der Prozessautomatisierung mit deren besonderen Rahmenbedingungen wie dem Explosionsschutz. Die bedeutendsten Verfahren und Methoden der modernen Kommunikation werden praxisnah veranschaulicht.

1. Auflage 2010, 72 Seiten mit CD-ROM, Broschur, € 59,- • ISBN: 978-3-8356-3212-7

atp kompakt Band 3

Praktische Messtechnik – Die besten Konzepte

Dieser Band vermittelt wertvolles Know-how zu allen Aspekten der praktischen Messtechnik und fokussiert besonders die Prozessmesstechnik. Lernen Sie die Fortschritte in der Sensortechnik entlang der Technologie-Roadmap kennen und profitieren Sie von erstklassigen Konzepten zu kostengünstigen und effizienten Lösungen.

1. Auflage 2010, 72 Seiten mit CD-ROM, Broschur, € 59,- • ISBN: 978-3-8356-3213-4

atp kompakt Kollektion (Bände 1-3)

Erfolgreiches Engineering Effiziente Kommunikation Praktische Messtechnik

Mit dieser dreibändigen Kollektion zu den Themen Engineering, Kommunikation und Messtechnik erhalten Sie ein nützliches, kompakt und praxisnah aufbereitetes Kompendium zu den Kernthemen der Automatisierungstechnik. Die wertvolle Grundlage für Ihre tägliche und zukünftige Arbeit.

1. Auflage 2010, ca. 282 Seiten mit CD-ROM, Broschur • € 179,- • ISBN: 978-3-8356-3221-9

Sofortanforderung im Online-Shop www.oldenbourg-industrieverlag.de oder telefonisch +49 (0)201 / 82002-14

OLDENBOURG INDUSTRIEVERLAG GMBH
VULKAN-VERLAG GMBH
www.oldenbourg-industrieverlag.de • www.vulkan-verlag.de