Steuerungs- und Schutzsysteme an industriellen Thermoprozessanlagen

Control- and protective on industrial thermal processing installations

Von Klaus Kroner

An die Steuerung einer Thermoprozessanlage werden hohe Anforderungen bezüglich Anlagen- und Betriebssicherheit, Funktionalität, Verfügbarkeit und Wirtschaftlichkeit gestellt. Dabei gilt es, für die elektrische und elektronische Ausrüstung dieser Anlagen eine Vielzahl relevanter EG-Richtlinien und Normen zu berücksichtigen. Dieser Artikel erklärt die Zusammenhänge. Zudem erläutert er die Anforderungen an die Ausführung von Schutzsystemen und beschreibt die notwendigen Schritte der Risikobeurteilung. Darüber hinaus wird die Ermittlung von sogenannten „SIL/PL-Level" von Sicherheitsfunktionen beschrieben.

A control system for Industrial thermoprocessing equipment must meet stringent requirements in terms of plant and operating safety, functionality, availability and costeffectiveness. The electrical and electronic equipment for these installations must comply with a number of relevant EG directives and standards. This article explains the context. It also explains the requirements for the design of protective systems and describes the necessary steps of risk assessment. In addition the determination of so-called „SIL/PL-Level" for safety functions is described.

Bedingt durch das Inkrafttreten der neuen Maschinenrichtlinie 2006/42/EG, welche seit dem 29.12.2009 gültig ist, werden auch an Thermoprozessanlagen Anforderungen bezüglich der funktionalen Sicherheit beschrieben. Die internationale Normung definiert Anforderungen in Bezug auf die Zuverlässigkeit von Sicherheitsfunktionen (Safety Integrity Level SIL bzw. Performance Level PL) mit dem Ziel der Risikominimierung für Personen, Umwelt, Produkte und Prozesse im Falle einer Fehlfunktion. Mit dieser Thematik müssen sich nun Hersteller von Thermoprozessanlagen und insbesondere Steuerungsbauer befassen.

Die elektrische und elektronische Ausrüstung einer Thermoprozessanlage besteht aus der übergeordneten Prozess-Steuerung (**Bild 1**) sowie den elektrisch angesteuerten Geräten (Sensoren/Aktoren), die dezentral verteilt an einer Thermoprozessanlage angeordnet sind.

Beispielhaft für eine Thermoprozessanlage ist in **Bild 2** schematisch ein Industrieofen für Hochtemperaturbetrieb dargestellt. Die Prozess-Steuerung ist funktional verknüpft mit einer Vielzahl von Komponenten, welche in der Gaseingangsstrecke 1, der Lufteingangsstrecke 2, der Brennerregelung 3 sowie im Verbrennungsraum, dem Abgassystem und dem Leistungsteil (Antriebe) der Thermoprozessanlage angeordnet sind. Der erforderliche Signalaustausch zwischen den beteiligten Steuerungskomponenten und der Feldebene unterscheidet dabei sicherheitsrelevante und nicht sicherheitsrelevante Signale.

Die Prozess-Steuerung selbst besteht zum einen aus der Leittechnik/Bedienebene. Hier sind die zur Visualisierung und Bedienung der Anlage erforderlichen Betriebsmittel untergebracht. Es werden Steuerungsabläufe und Regelkreise für den Prozess implementiert und visualisiert (nicht fehlersicherer Teil der Prozess-Steuerung).

Des Weiteren besteht die Prozess-Steuerung aus dem sogenannten Schutzsystem, welches alle Einrichtungen, Geräte und die Steuerung für Sicherheitsfunktionen beinhaltet, deren Hauptzweck dem Schutz von Personen, der Anlage und der Umwelt dient.

Bild 1: Prozess-Steuerung
Fig. 1: Process control system

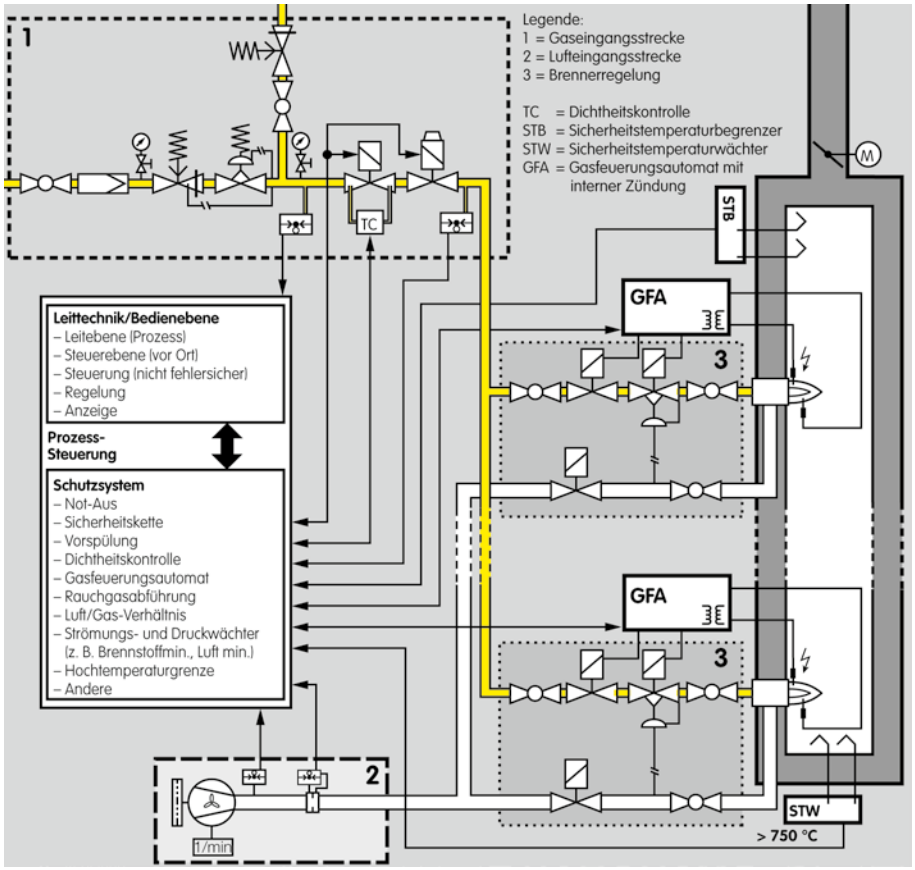


Bild 2: Industrieofen für Hochtemperaturbetrieb
Fig. 2: High-temperature industrial furnace

„Das Schutzsystem beinhaltet alle Komponenten, die zur Ausführung der Sicherheitsfunktionen erforderlich sind, z. B. Signalgeber, die sicherheitsrelevanten Größen (z. B. Flammenüberwachung), Geräte für die Unterbrechung der Brennstoffzufuhr, die Belüftung des Feuerraumes und den Schutz des beheizten Systems. Ein Schutzsystem besteht typischerweise aus Signalgebern, einer Schutzeinrichtung, die die Signale logisch verarbeitet und Stellgeräten. Wenn dies durch ein mehrkanaliges System erreicht wird, dann sind alle Kanäle und die Überwachungsgeräte, die für Sicherheitszwecke verwendet werden, in das Schutzsystem eingeschlossen." (Quelle DIN EN 746-2:2011).

Konstruktive Anforderungen an die Prozess-Steuerung

An die Steuerung einer Thermoprozessanlage werden hohe Anforderungen bezüglich Sicherheit, Verfügbarkeit und Wirtschaftlichkeit gestellt. Die Aufgabe im Steuerungsengineering besteht nun darin, neben der Funktionalität auch die grundlegenden Anforderungen an die Anlagen- und Betriebssicherheit gemäß der entsprechenden EG-Richtlinien und Normen konstruktiv in Schaltungstechnik, Hardware und Steuerungsprogramme (Software) umzusetzen.

EG-Richtlinien, horizontale Anwendung

EG-Richtlinien sind horizontal anzuwenden, d. h. alle für ein Produkt zutreffenden Richtlinien sind in der Konstruktion anzuwenden und stellen die gesetzlichen Anforderungen dar (**Bild 3**). Die von den EG-Richtlinien spezifizierten Anforderungen werden durch entsprechende Gesetze in nationales Recht umgesetzt. Die grundlegenden Anforderungen der Richtlinien müssen vom Maschinenhersteller und ebenfalls vom Steuerungsbauer berücksichtigt und umgesetzt werden.

Jedoch stellen die in den EG-Richtlinien festgelegten grundlegenden Anforderungen ausschließlich Mindestanforderungen an die elektrische Ausrüstung einer Thermoprozessanlage dar. Entscheidend für die konkrete Umsetzung aller Anforderungen an die Ausführung der elektrischen Ausrüstung einer Thermoprozessanlage sind die vertraglichen Vereinbarungen zwischen den Vertragspartnern, Hersteller und Betreiber, einer Thermoprozessanlage. Über die grundlegenden Anforderungen der EG-Richtlinien hinausgehende betreiberspezifische Anforderungen können beispielsweise in Werksnormen spezifiziert werden, auf welche dann vertraglich verwiesen wird.

In der Maschinen-Richtlinie 2006/42/EG werden grundlegende Anforderungen bezüglich Sicherheits- und Gesundheitsanforderungen bei Konzipierung und Bau von Maschinen formuliert. Die Umsetzung in nationales (deutsches) Recht

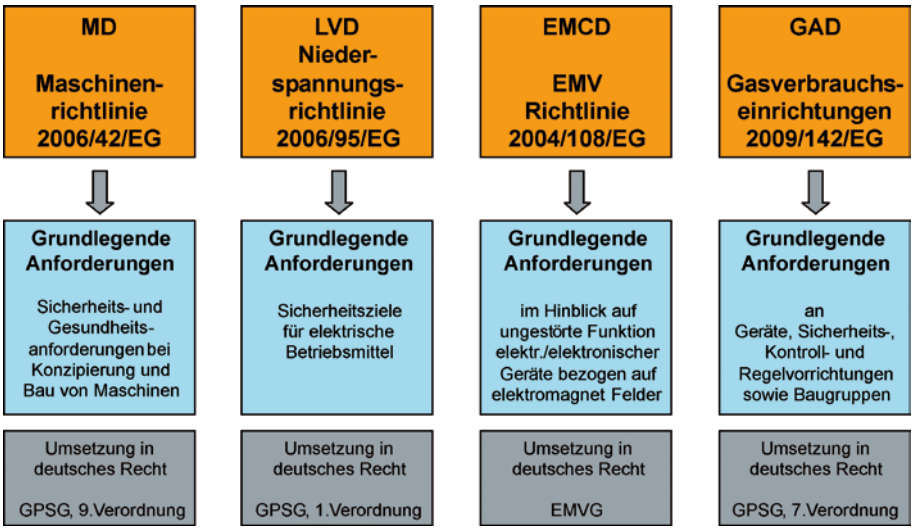


Bild 3: EG Richtlinien, Gesetzliche Anforderungen
Fig. 3: EC directives and legal requirements

erfolgt im Geräte- und Produktsicherheitsgesetz (GPSG), 9. Verordnung.

In der Niederspannungsrichtlinie 2006/95/EG werden grundlegende Anforderungen bezüglich der Sicherheitsziele für elektrische Betriebsmittel formuliert. Die Umsetzung in nationales (deutsches) Recht erfolgt im Geräte- und Produktsicherheitsgesetz (GPSG), 1. Verordnung. Die hier beschriebenen Schutzziele behandeln vorrangig die Einhaltung der Schutzmaßnahmen zum Personen- und Anlagenschutz, bezogen auf die Verwendung elektrischer Betriebsmittel und deren Dimensionierung.

Die EMV-Richtlinie 2004/108/EG formuliert grundlegende Anforderungen im Hinblick auf die ungestörte Funktion elektrischer/elektronischer Geräte bezogen auf elektromagnetische Felder. Die Umsetzung in nationales (deutsches) Recht erfolgt im EMV-Gesetz EMVG. Danach sollen Geräte und Anlagen möglichst selbst keine Störungen aussenden, jedoch gegenüber Störeinstrahlung bzw. leitungsgebundenen Störungen möglichst resistent sein.

Die Gasverbrauchseinrichtungen Richtlinie 2009/142/EG formuliert grundlegende Anforderungen an Geräte, Sicherheits-, Kontroll- und Regelvorrichtungen sowie Baugruppen. Die Umsetzung in nationales (deutsches) Recht erfolgt im Geräte- und Produktsicherheitsgesetz (GPSG), 7. Verordnung.

Geräte, Sicherheits-, Kontroll- und Regelvorrichtungen sowie Baugruppen für Gasverbrauchseinrichtungen sind so auszulegen, herzustellen und zu verwenden, dass durch deren Ausfall keine gefährliche Situation entstehen kann.

Anforderungen an Hersteller

Hersteller von Thermoprozessanlagen (IThE, Industrielle Thermoprozessanlagen) wenden die Maschinenrichtlinie 2006/42/EG an und müssen durch das Ausstellen einer Konformitätserklärung für die Thermoprozessanlage deren Richtlinienkonformität und damit die Gesetzeskonformität (gemäß GPSG) bescheinigen.

Gerätehersteller wenden in erster Linie die Richtlinie über Gasverbrauchseinrichtungen 2009/142/EG an. Bei elektrisch betriebenen Geräten sind zusätzlich die Niederspannungsrichtlinie 2006/95/EG und die EMV-Richtlinie 2004/108/EG anzuwenden.

Steuerungsbauer wenden die Niederspannungsrichtlinie 2006/95/EG und die EMV-Richtlinie 2004/108/EG an. Weiterhin muss die Steuerung auch die betreffenden Sicherheits- und Gesundheitsanforderungen der Maschinenrichtlinie 2006/42/EG erfüllen, da sie ja die Steuerungsaufgaben für eben diese Maschine übernimmt. Die Steuerung für sich allein betrachtet unterliegt jedoch ausschließlich der Niederspannungsrichtlinie 2006/95/EG und der EMV-Richtlinie 2004/108/EG.

EG-Richtlinien, grundlegende Anforderungen

Hier ist ein Auszug (Punkt 1.2 „Steuerungen und Befehlseinrichtungen“) des Anhang I der Maschinenrichtlinie 2006/42/EG (gültig seit 29.12.2009) dargestellt:

Grundlegende Sicherheits- und Gesundheitsschutzanforderungen für Konstruktion und Bau von Maschinen:

1.2 Steuerungen und Befehlseinrichtungen

1.2.1 Sicherheit und Zuverlässigkeit von Steuerungen

Steuerungen sind so zu konzipieren und zu bauen, dass es nicht zu Gefährdungssituationen kommt.

Insbesondere müssen sie so ausgelegt und beschaffen sein, dass

– sie den zu erwartenden Betriebsbeanspruchungen und Fremdeinflüssen standhalten
– ein Defekt der Hardware oder der Software der Steuerung nicht zu Gefährdungssituationen führt
– Fehler in der Logik des Steuerkreises nicht zu Gefährdungssituationen führen
– vernünftigerweise vorhersehbare Bedienungsfehler nicht zu Gefährdungssituationen führen.

(Quelle Maschinenrichtlinie 2006/42/EG)

Anhand dieses Auszugs wird deutlich, dass in der Richtlinie die Schutzziele (Grundlegende Anforderungen) beschrieben werden, welche vom Konstrukteur umzusetzen sind. Konkrete Hilfe zur praxisorientierten Umsetzung dieser Schutzziele findet der Konstrukteur der Steuerung dann in den relevanten Normen, wo konstruktive Details beschrieben werden.

Europäische Normen bekommen nach der Veröffentlichung im Amtsblatt der Europäischen Gemeinschaft den Status „Harmonisierte Norm“. Harmonisierte Normen sind danach ohne Änderungen in nationale Normen zu übernehmen. In harmonisierten Normen ist niedergelegt, wie nach dem derzeitigen Stand der Technik die grundlegenden Anforderungen der EG-Richtlinien erfüllt werden können. Die Übereinstimmung von Produkten mit harmonisierten Normen lässt die Übereinstimmung mit den grundlegenden Anforderungen der EG-Richtlinien vermuten.

Normen haben keine Gesetzeskraft, ihre Anwendung ist freiwillig, aber dennoch

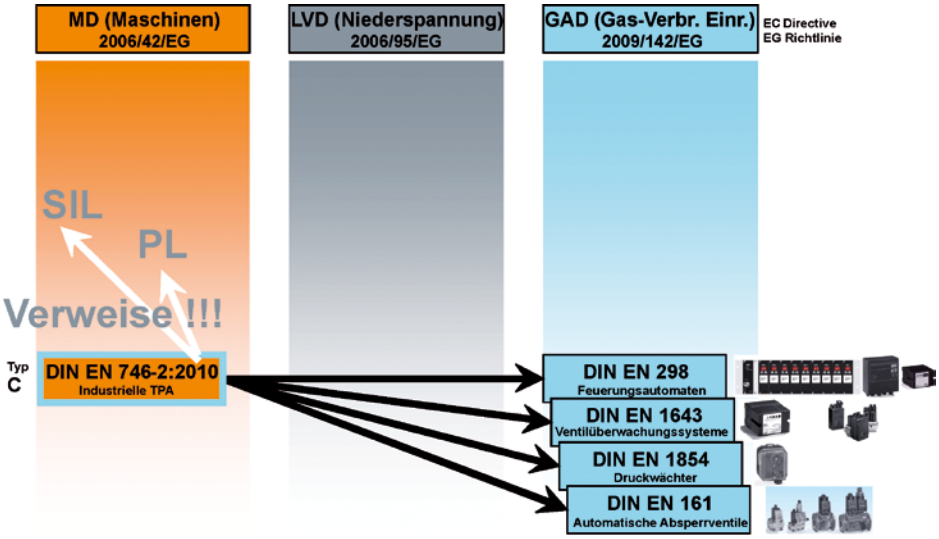


Bild 4: Maschinensicherheits- Produktnormen
Fig. 4: Machine-safety product standards

empfehlenswert. Dem Hersteller steht es frei, ob er bei der Herstellung seiner Produkte auf harmonisierte Normen zurückgreift oder auf andere Art und Weise die festgelegten grundlegenden Anforderungen der EG-Richtlinien erfüllt.

Normative Zusammenhänge, Maschinensicherheits-Produktnormen

Um wesentliche Zusammenhänge aufzuzeigen, wird in **Bild 4** eine Darstellung gewählt, in der die Beziehungen zwischen den harmonisierten Normen untereinander und zu den zugehörigen Richtlinien deutlich werden.

In der Waagerechten sind die relevanten EG-Richtlinien dargestellt, darunter sind jeweils die entsprechenden harmonisierten Normen zugeordnet.

Die EN 746-2:2010 (Industrielle Thermoprozessanlagen – Teil 2: Sicherheitsanforderungen an Feuerungen und Brennstoffführungssysteme) ist eine harmonisierte Typ-C-Norm zur Maschinenrichtlinie.

Im Anwendungsbereich der EN 746-2 wird erläutert, dass sie zusammen mit der EN 746-1 die Sicherheitsanforderungen für Einzelbrenner und Mehrbrenner-Systeme festlegt, die Teile einer Industriellen Thermoprozessanlagen sind. (Im Folgenden werden Industrielle Thermoprozessanlagen als „IThE" bezeichnet). Dieses Dokument behandelt die signifikanten Gefährdungen, Gefährdungssituationen und Ereignisse für Feuerungen und Brennstoffführungssysteme an IThE, auf der Grundlage, dass diese wie vorgesehen und unter den vom Hersteller vorgesehenen Bedingungen eingesetzt werden.

Die EN 746-2 gilt für Brennstoff-Leitungssysteme in Strömungsrichtung, beginnend mit dem handbetätigten Hauptabsperrventil, Brenner, Brennersysteme und Zündeinrichtungen sowie für das sicherheitsbezogene Steuerungssystem (Schutzsystem).

Diese europäische Norm ist jedoch nicht anwendbar für elektrische Verkabelung und Starkstromverkabelung, die dem IThE Steuerungsschrank/Bedienerfeld/Schutzsystem vorgeschaltet sind (Quelle EN 746-2:2010).

Die Produktnormen DIN EN 298, DIN EN 1643, DIN EN 1854 und DIN EN 161 sind harmonisierte Produktnormen zur Richtlinie über Gasverbrauchseinrichtungen. Den Bezug zur Maschinenrichtlinie, unter welcher sie nicht harmonisiert sind, bekommen diese Produktnormen durch Verweise in der EN 746-2.

Die EN 746-2 verweist z. B. beim Einsatz von Flammenüberwachungseinrichtungen und Feuerungsautomaten auf die EN 298, welche die sicherheitstechnischen und konstruktiven Anforderungen an diese Geräte sehr ausführlich und detailliert beschreibt.

Feuerungsautomaten werden gemäß Produktnorm DIN EN 298 (Feuerungsautomaten für Gasbrenner und Gasgeräte mit oder ohne Gebläse) entwickelt und gefertigt. Ventilüberwachungssysteme wie z. B. Dichtheitskontrolleinrichtungen werden entsprechend der Produktnorm DIN EN 1643 (Ventilüberwachungssysteme für automatische Absperrventile für Gasbrenner und Gasgeräte), Druckwächter entsprechend der Produktnorm DIN EN 1854 (Druckwächter für Gasbrenner und Gasgeräte) und Automatische Absperrventile entsprechend der Produktnorm DIN EN 161 (Automatische Absperrventile für Gasbrenner und Gasgeräte) entwickelt und konstruiert.

Des Weiteren wird nun auch auf Normen für die Funktionale Sicherheit verwiesen, in welchen die Anforderungen bezüglich SIL bzw. PL-Level beschrieben werden.

Normative Zusammenhänge, Normen elektrische Sicherheit

Die Elektrische Sicherheit wird in den Normen DIN EN 60204 (Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen), harmonisiert unter Maschinenrichtlinie sowie unter Niederspannungsrichtlinie und der DIN EN 61439 (Niederspannungs-Schaltgerätekombinationen), harmonisiert unter der Niederspannungsrichtlinie, beschrieben (**Bild 5**).

In diesen Normen werden Festlegungen und Empfehlungen für die Sicherheit, Funktionsfähigkeit und Instandhaltung der elektrischen Ausrüstung geregelt und Schutzmaßnahmen wie z. B. Schutz gegen elektrischen Schlag, Dimensionierung und Auslegung von Schaltgeräten, Leitungen und Überstromeinrichtungen, Potenzialausgleich usw. beschrieben.

Die elektrische Ausrüstung von Thermoprozessanlagen muss den Anforderungen gemäß EN 60204-1 entsprechen und die Gefährdungen berücksichtigen, welche in der von der Maschinenrichtlinie geforderten Risikobeurteilung während der Konstruktionsphase identifiziert wurden.

Normative Zusammenhänge, Normen Funktionale Sicherheit

Die Norm IEC 61508 (Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme) definiert Anforderungen an sicherheitsbezogene Systeme (**Bild 6**). Der Geltungsbereich dieser Norm umfasst den gesamten Lebenszyklus sicherheitsbezogener Systeme und erstreckt sich vom Konzept über die Planung, die Entwicklung, die Realisierung und den Betrieb des Systems bis hin zur Außerbetriebnahme einer Anlage. Die IEC 61508 ist eine generische Norm, die nicht auf ein bestimmtes Anwendungsgebiet eingeschränkt ist. Von wei-

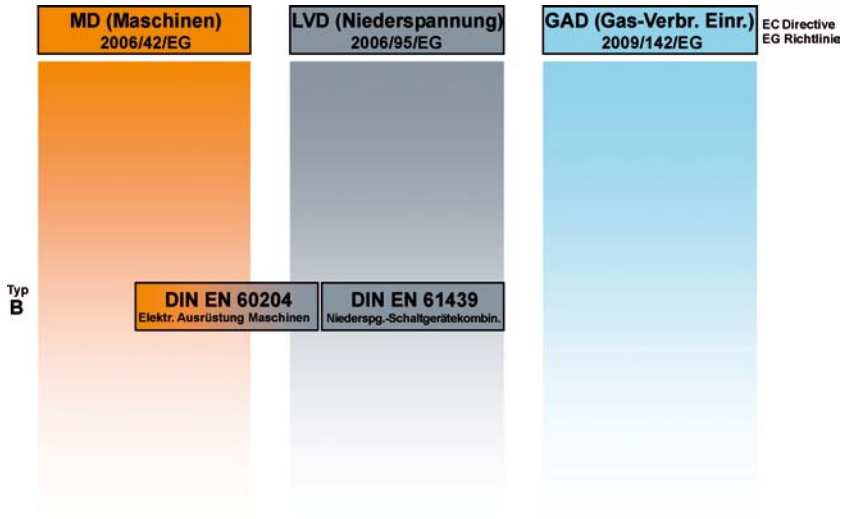


Bild 5: Normen Elektrische Sicherheit
Fig. 5: Electrical safety standards

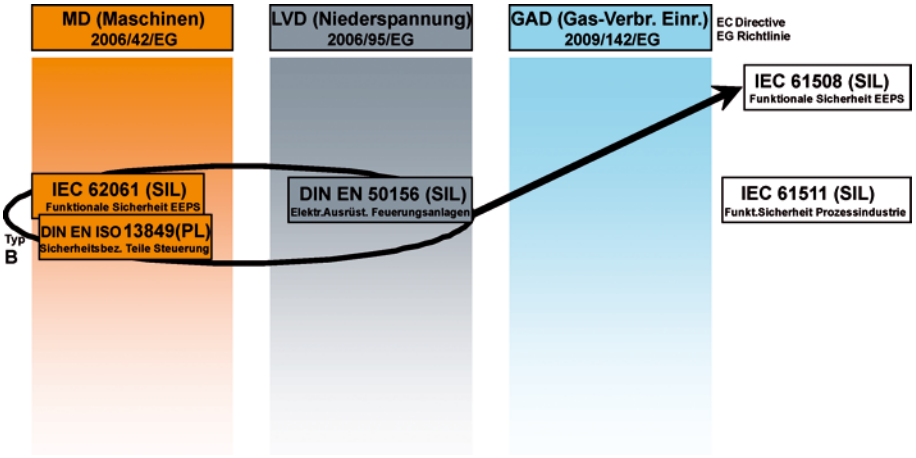


Bild 6: Normen Funktionale Sicherheit
Fig. 6: Functional safety standards

teren Normengremien wurden folgende branchenspezifische Sektor-Normen von dieser Norm abgeleitet:

IEC 61511 – Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie

EN 50156 – Elektrische Ausrüstung von Feuerungsanlagen

IEC 62061 – Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme

ISO 13849 – Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen

Die IEC 61508 und die Sektornorm IEC 61511 werden an Prozesstechnischen Anlagen in der chemischen Industrie angewendet. Beide IEC-Normen sind nicht unter einer EG-Richtlinie harmonisiert.

Nachdem die SIL-Betrachtung von Sicherheitsfunktionen in der chemischen Industrie bereits seit einigen Jahren angewendet werden, wurde diese Betrachtung nun auch auf Maschinen und Maschinenanlagen gemäß der Maschinenrichtlinie ausgeweitet. Da gerade für Hersteller von Thermoprozessanlagen und für Hersteller von Sicherheitsgeräten für Thermoprozessanlagen diese Thematik noch relativ neu ist, müssen häufig die hierzu erforderlichen Kenntnisse und Erfahrungen noch erworben werden, um neue Anlagen an die zusätzlichen Anforderungen der Funktionalen Sicherheit anzupassen.

Die Normen EN IEC 62061 und die EN ISO 13849 sind harmonisierte Normen zur Maschinenrichtlinie und finden Anwendung an Maschinen wie z. B. Thermoprozessanlagen.

Die EN 50156 ist eine harmonisierte Norm zur Niederspannungsrichtlinie und wird z. B. an Dampfkesselanlagen angewendet.

Alle drei Sektornormen befassen sich mit den Anforderungen an die funktionale Sicherheit von Systemen und beschreiben die Bestimmung sowie die Berechnung der erforderlichen SIL-Level oder PL-Level. An verschiedenen Stellen wird in diesen Sektor-Normen wiederum auf die generische IEC 61508 verwiesen.

Fehlersichere SPS, Sicherheitsrelais sowie auch neuere Feuerungsautomaten bzw. Schutzsystemelektronik entsprechen den Anforderungen aus der IEC 61508 bzw. der IEC 62061 oder der ISO 13849. Für diese Geräte sind SIL-Zertifikate bzw. PL-Zertifikate verfügbar.

Normative Zusammenhänge, Deterministischer und Probabilistischer Ansatz

Die einschlägigen Produktnormen für Sicherheitsgeräte wie z. B. die DIN EN 298 für Feuerungsautomaten oder die DIN EN 161 für Automatische Absperrventile wurden auf der Grundlage des deterministischen Ansatzes zur Beurteilung von Fehlern und Ausfällen entwickelt (**Bild 7**). D. h. man betrachtet bei der Geräteentwicklung definierte und reproduzierbare gefährliche Ausfälle, welche es zu vermeiden gilt.

Der probabilistische Ansatz stellt lediglich eine weitere Betrachtungsweise zur Beurteilung von Fehlern und Ausfällen dar. Hier wird die statistische Wahrscheinlichkeit gefährlicher Ausfälle ermittelt, die während der Entwicklung von Sicherheitsgeräten durch Rechnungen und Dauerversuche in einem komplexen Prozess vom Hersteller von Sicherheitsgeräten nachgewiesen werden muss.

Bei der Entwicklung von Sicherheitsgeräten werden nun zusätzlich zu den deterministischen Produktnormen, wo wesentliche Anforderungen (grundsätzliche funktionale Anforderungen wie z. B. Anforderungen an die Dichtheit von Geräten, Sicherheitszeiten usw.) beschrieben werden, auch die neuen Normen für die Funktionale Sicherheit gemäß dem probabilistischem Ansatz angewendet. Durch die zusätzliche Anwendung dieser neuen Normen, welche als SIL-Anhang oder PL-Anhang zu bestehenden Produktnormen herausgegeben werden, wird es den Geräteherstellern ermöglicht, Sicherheitsgeräte mit Baumusterprüfung gemäß Richtlinie über Gasver-

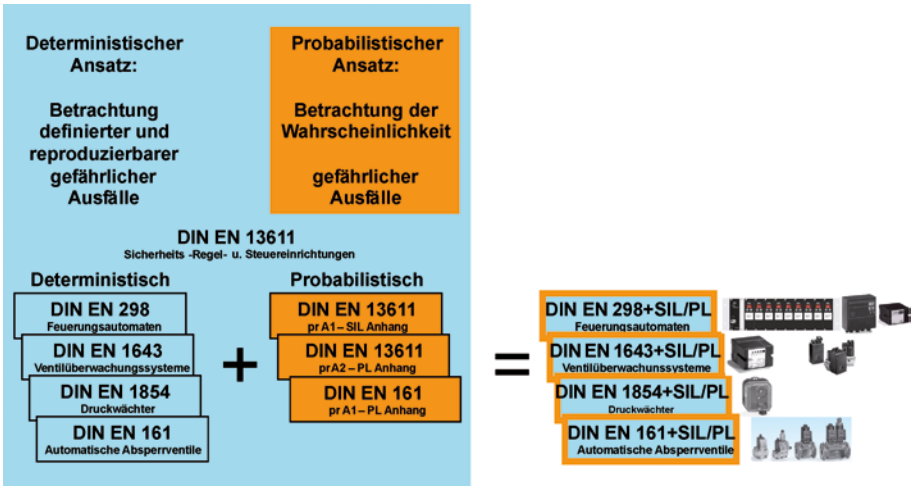


Bild 7: Normative Zusammenhänge, Deterministischer + Probabilistischer Ansatz
Fig. 7: Normative correlations, deterministic + probabilistic approach

brauchseinrichtungen zusätzlich auch mit einem SIL/PL-Zertifikat zu liefern.

Da die Erstellung von SIL/PL-Zertifikaten für Sicherheitsgeräte ein umfangreicher, zeitaufwendiger und sehr komplexer Prozess ist, der üblicherweise und sinnvollerweise parallel zur Geräteentwicklung bearbeitet wird und auch die dazu erforderlichen Normen zum Teil noch in den Normengremien in Bearbeitung sind bzw. derzeit nur als Vornorm (pr-Norm) vorliegen, werden die Gerätehersteller erst nach und nach den Herstellern von Thermoprozessanlagen Sicherheitsgeräte mit zusätzlichem SIL/PL-Zertifikat zu Verfügung stellen können.

SIL/PL-Zertifikate für Sicherheitsgeräte der Elster GmbH

Feuerungsautomat:

Für Elster Kromschröder Gasfeuerungsautomaten der Baureihe PFU 700 ist ein SIL 3/PL e Zertifikat verfügbar. Das Zertifikat wurde in Zusammenarbeit mit dem TÜV Süd erstellt. Die erfüllten Normen, SIL- und PL-Werte sowie alle relevanten Werte sind im Zertifikat angegeben.

Automatische Absperrventile:

Für Elster Kromschröder Automatische Absperrventile der Baureihe VAS 1 ist ein SIL/PL-Zertifikat (einsetzbar bis SIL 3/PL e) verfügbar. Der SIL/PL Level ist bei diesem Produkt abhängig von der Anzahl (1 oder 2 Ventile) und der Schaltspielzahl des jeweiligen Einsatzfalls. Der tatsächliche SIL/PL-Wert wird aus verschiedenen Kennwerten des Produktes und der Schaltspielzahl der Anwendung ermittelt. Die Berechnungsformel ist im Zertifikat abgedruckt. Das Zertifikat wurde in Zusammenarbeit mit dem TÜV Rheinland erstellt. Die Berechnung der relevanten Werte in Abhängigkeit der Schaltspielzahl kann interaktiv in der technischen Information (TI) ermittelt werden.

Druckwächter:

Für Elster Kromschröder Druckwächter der Baureihe DG ist ein SIL/PL-Zertifikat (einsetzbar bis SIL 3/PL e) verfügbar. Der SIL/PL-Level ist auch bei diesem Produkt abhängig von der Anzahl (1 oder 2 Druckwächter) und von der Schaltspielzahl des jeweiligen Einsatzfalls. Der tatsächliche SIL/PL-Wert wird aus verschiedenen Kennwerten des Produktes und der Schaltspielzahl der Anwendung ermittelt. Die Berechnungsformel ist im Zertifikat abgedruckt. Das Zertifikat wurde in Zusammenarbeit mit dem TÜV Rheinland erstellt. Die Berechnung der relevanten Werte in Abhängigkeit der Schaltspielzahl kann interaktiv in der technischen Information (TI) ermittelt werden.

Alle Zertifikate sowie weitere Informationen zu den Sicherheitsgeräten der Elster GmbH werden online in der Dokuthek http://www.docuthek.com bereitgestellt.

Safety Integrity Level (SIL – Level)

Safety Integrity Level (SIL) werden definiert in den Sicherheitsnormen IEC 61508 und IEC 62061 (Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer Steuerungssysteme). Es wird die Wahrscheinlichkeit eines gefährlichen Ausfalls von elektrischen Geräten/Systemen betrachtet.

Man unterscheidet drei Stufen SIL 1 – SIL 3 (4):

SIL – Level 1 = niedrigste Stufe

SIL – Level 3 = höchste Stufe

Die Anforderungsstufe SIL 4 findet in den harmonisierten Normen zur Maschinenrichtlinie keine Berücksichtigung. Zu SIL 4 siehe IEC 61508-1.

Performance Level (PL)

Performance Level (PL) werden definiert in der Sicherheitsnorm ISO 13849 (Sicherheitsbezogene Teile von Steuerungen). Es wird die Wahrscheinlichkeit eines gefährlichen Ausfalls von elektrischen, hydraulischen, pneumatischen und mechanischen Geräten/Systemen betrachtet.

Man unterscheidet fünf Stufen PL a – PL e:

PL a = niedrigste Stufe

PL e = höchste Stufe

Gegenüberstellung PL/SIL

Bild 8 zeigt den Performance Level (PL) und Sicherheits-Integritätslevel (SIL) als Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde (PFH_D).

Die Absicherung von hohen Risiken erfolgt mit SIL 3 bzw. PL e, in beiden Fällen liegt die Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde zwischen 10^{-8} und 10^{-7}. Die Absicherung niedriger Risiken erfolgt z. B. mit SIL 1 bzw. PL b/c, in beiden Fällen liegt die Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde zwischen 10^{-6} und 10^{-5}. Je höher das Risiko ist, desto kleiner muss die Ausfallwahrscheinlichkeit der verwendeten Sicherheitsgeräte sein.

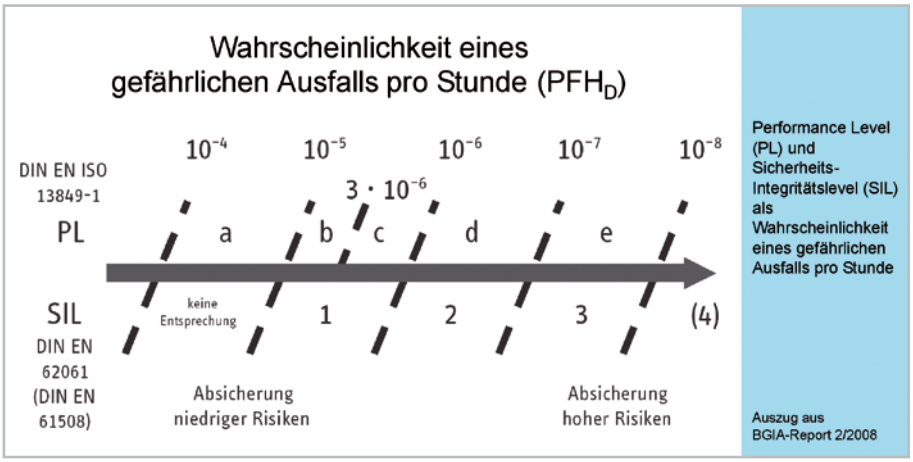


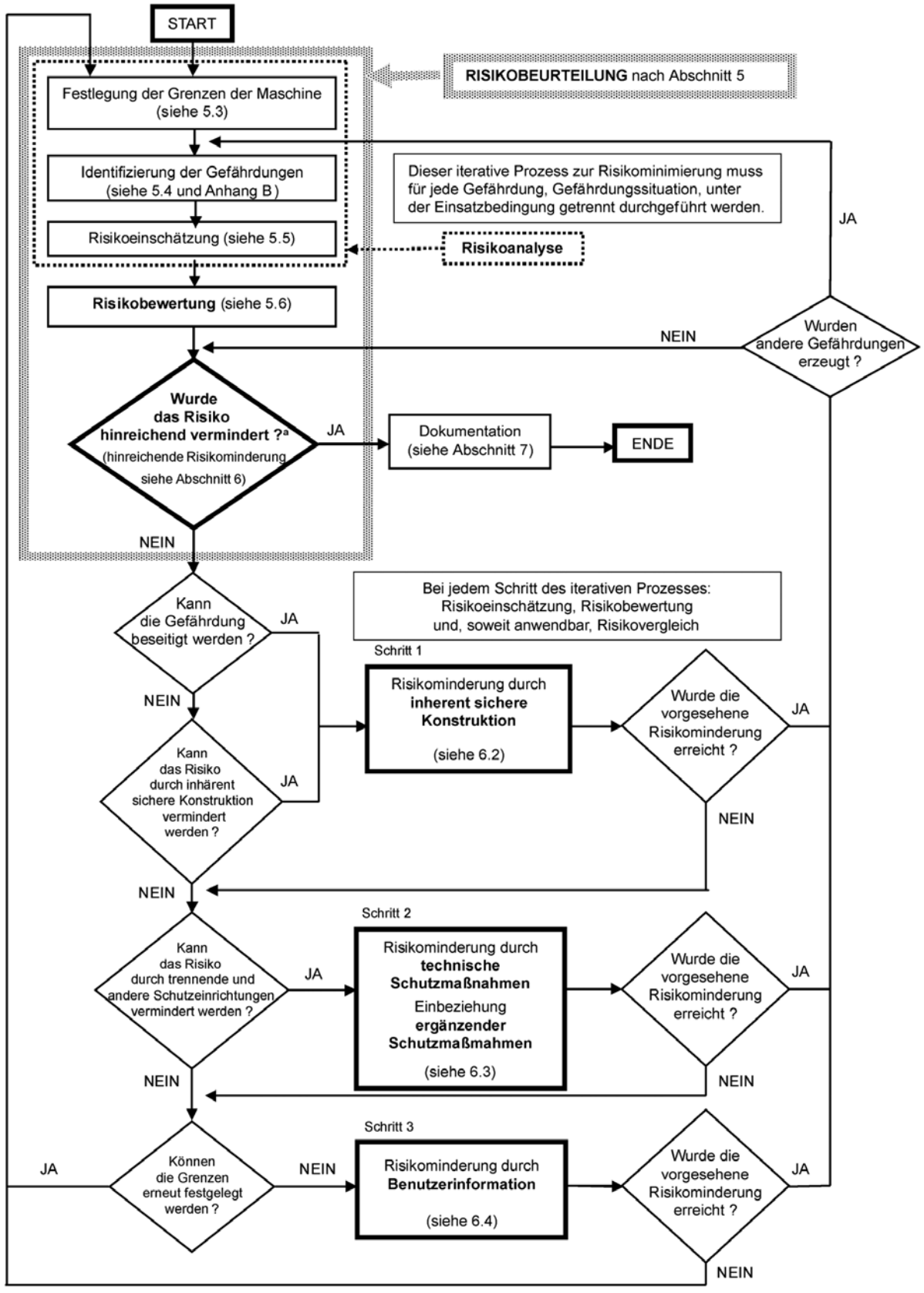
Bild 8: Gegenüberstellung PL/SIL, Quelle – Report 2/2008 IFA (BGIA)

Fig. 8: Comparative assessment of PL/SIL, source: report 2/2008 IFA (BGIA)

Normative Zusammenhänge, Gefahrenanalyse und Risikobeurteilung

Im Bereich Sicherheit von Maschinen gibt die DIN EN ISO 12100:2011-03 (Sicherheit von Maschinen – allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung) einen Gesamtrahmen zur systematischen Risikominderung vor. Die Risikobeurteilung erfolgt dabei nach den hier dargestellten Prinzipien. Die Norm DIN EN ISO 12100 ist eine harmonierte Norme zur Maschinenrichtlinie.

Innerhalb des Rahmens der DIN EN ISO 12100 legt die Norm IEC 62061 Sicher-



[a] Beim erstmaligen Stellen der Frage, wird diese mit dem Ergebnis der Ausgangsrisikobewertung beantwortet.

Bild 9: Risikobeurteilung / Risikominderung nach EN ISO 12100, Quelle DIN EN ISO 12100:2011-03

Fig. 9: Risk assessment / Risk reduction in accordance with EN ISO 12100, source: DIN EN ISO 12100:2011-03

heitsanforderungen für elektrisch/elektronische und programmierbar elektronische (E/E/PE) Steuerungen fest. Des Weiteren stellt sie eine Methodologie und Anforderungen bereit, um in Übereinstimmung mit ISO 13849 entworfene sicherheitsbezogene Teilsysteme zu integrieren. So können auch Risiken von hydraulischen, pneumatischen und mechanischen Geräten/Systemen betrachtet werden. „Der Hersteller einer Maschine oder sein Bevollmächtigter hat dafür zu sorgen, dass eine Risikobeurteilung vorgenommen wird, um die für die Maschine geltenden Sicherheits- und Gesundheitsschutzanforderungen zu ermitteln. Die Maschine muss dann unter Berücksichtigung der Ergebnisse der Risikobeurteilung konstruiert und gebaut werden."

(Quelle: Maschinenrichtlinie 2006/42/EG – Anhang I).

Der Hersteller einer Maschine erstellt die in der Maschinenrichtlinie vorgeschriebene Risikobeurteilung, baut dann die Maschine unter Berücksichtigung der Risikobeurteilung und unter Anwendung harmonisierter Normen. Für die so erstellte sichere Maschine erstellt der Hersteller eine Konformitätserklärung, an der Maschine wird eine CE-Kennzeichnung angebracht.

Der Betreiber einer Maschine erstellt gemäß Arbeitsmittelrichtlinie, Arbeitsschutzgesetz und Betriebssicherheitsverordnung die Gefährdungsanalyse am Arbeitsplatz seiner Mitarbeiter. Durch die Bereitstellung sicherer Arbeitsmittel, Schulung und Unterweisung der Mitarbeiter übernimmt er die Betreiberverantwortung und sorgt für sichere Arbeitsplätze sowie den sicheren Betrieb der Maschine.

Der sichere Betrieb einer Thermoprozessanlage umfasst auch die regelmäßige Wartung der Anlage.

Risikobeurteilung nach DIN EN ISO 12100, iterativer Prozess

Die einzelnen Schritte der Risikobeurteilung werden in EN ISO 12100 beschrieben (**Bild 9**). Die Risikoanalyse beinhaltet die Festlegung der Grenzen der Maschine, die Identifizierung der Gefährdungen und die Risikoeinschätzung.

Die Risikobeurteilung beinhaltet zusätzlich die Risikobewertung. Anhand des Bewertungsergebnisses, ob das Risiko als hinreichend klein erachtet werden kann, oder hinreichend vermindert wurde, ist die Risikobeurteilung entweder für die bewertete Sicherheitsfunktion abgeschlossen, oder es muss eine weitere Risikominderung betrieben werden.

Der Prozess wird iterativ solange durchlaufen, bis die Frage „Risiko hinreichend vermindert?" mit Ja beantwortet werden kann.

Der Prozess der Risikobeurteilung muss für jede Sicherheitsfunktion separat durchgeführt werden. Die Risikobeurteilung betrifft alle Gefährdungen, welche an der Maschine auftreten können.

Prozess zur Risikominderung aus Sicht des Konstrukteurs

Die DIN EN ISO 12100 Norm legt die grundsätzliche Terminologie und Methodik fest, die für das Erreichen der Sicherheit von Maschinen angewandt werden. Die Festlegungen in dieser Norm sind für Konstrukteure vorgesehen.

Alle Schutzmaßnahmen, die zum Erreichen dieses Ziels angewendet werden, sind in der als „3-Stufen-Methode" bezeichneten Reihenfolge zu ergreifen.

Schritt 1: Inhärent sichere Konstruktion:

Diese Phase ist die einzige, in der Gefährdungen beseitigt werden können.

Dadurch erübrigt sich die Notwendigkeit für zusätzliche Schutzmaßnahmen wie technische Schutzmaßnahmen oder ergänzende Schutzmaßnahmen.

Schritt 2: Technische Schutzmaßnahmen und eventuell ergänzende Schutzmaßnahmen

Schritt 3: Benutzerinformation hinsichtlich des Restrisikos

Die Anwendung dieser Schritte soll mit der inhärent sicheren Konstruktion beginnen, erst wenn hier keine Risikominderung mehr erreicht werden kann, sollen zusätzliche Schutzmaßnahmen in Erwägung gezogen werden. Die Benutzerinformation hinsichtlich des Restrisikos soll erst an 3. Stelle gewählt werden, da die Wirksamkeit dieser Maßnahme grundsätzlich davon abhängig ist, ob die Informationen dem Betreiber bzw. Bediener der Maschine/Thermoprozessanlage auch vorliegen und ob die Benutzerinformation verstanden wurde.

Prozess zur Risikominderung aus Sicht des Betreibers

Schutzmaßnahmen, die anschließend vom Benutzer bzw. Betreiber durchzuführen sind, beziehen sich auf organisatorische Maßnahmen, Bereitstellung und Anwendung zusätzlicher Schutzeinrichtungen, Anwendung persönlicher Schutzausrüstung, Ausbildung, Schulung usw.

SIL/PL-Level einer Sicherheitsfunktion

Für eine Sicherheitsfunktion (bestehend aus Sensor + Logik + Aktor) wird der SIL/PL-Level ermittelt (**Bild 10**). Da Thermoprozessanlagen unterschiedliche Sicherheitsfunktionen enthalten, kann ein SIL/PL-Level nicht pauschal für eine komplette Anlage ermittelt bzw. berechnet werden, sondern muss separat für jede Sicherheitsfunktion ermittelt werden.

Unter einer Sicherheitsfunktion eines Systems versteht man die Verschaltung von „Sensor" (erfassen), „Steuerung/Logik" (verarbeiten) und „Aktor" (schalten).

Ermittlung des benötigten SIL/PL-Level

Wenn die Risikobeurteilung der Thermoprozessanlage ergeben hat, dass zur Risikominimierung die Notwendigkeit einer zusätzlichen Schutzmaßnahme besteht und diese in Form einer elektrischen

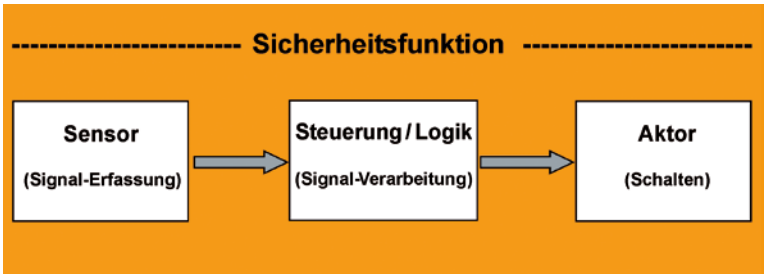


Bild 10: SIL/PL – Level einer Sicherheitsfunktion
Fig. 10: SIL/PL level of a safety function

Schutzeinrichtung/Sicherheitsfunktion ausgeführt werden soll, dann ist es erforderlich, zunächst den erforderlichen SIL-Level oder PL-Level zu ermitteln. Hier kommt die Verwendung der sogenannten Risikoelemente zu tragen.

RISIKO = AUSMASS und WAHRSCHEINLICHKEIT DES SCHADENSEINTRITTS

Das mit einer bestimmten Gefährdungssituation zusammenhängende Risiko hängt von folgenden Elementen ab:

a) dem Schadensausmaß;

b) der Eintrittswahrscheinlichkeit dieses Schadens als Funktion

1) der Gefährdungsexposition einer Person/von Personen,

2) des Eintritts eines Gefährdungsereignisses,

3) der technischen und menschlichen Möglichkeiten zur Vermeidung oder Begrenzung des Schadens.

Ermittlung des erforderlichen Performance Level gemäß DIN EN ISO 13849-1

Die Ermittlung des erforderlichen PL-Levels erfolgt unter Berücksichtigung der Schwere der Verletzung (S = S1 oder S2), Häufigkeit und/oder Dauer der Gefährdungsexposition (F = F1 oder F2) und der Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens (P = P1 oder P2).

Für die in **Bild 11** dargestellte spezifische Gefährdung, für die S als S2, F als F2 und P als P1 bestimmt worden sind, ergibt sich ein erforderlicher PL-Level von PL d.

Ermittlung des erforderlichen SIL-Level gemäß EN 62061

Die Ermittlung des erforderlichen SIL-Levels erfolgt unter der Berücksichtigung der Schwere der Auswirkungen (S = 4, 3, 2 oder 1), Häufigkeit und Dauer der Gefährdungsexposition (F = 5, 4, 3 oder 2), Wahrscheinlichkeit des Auftretens des gefahrbringenden Ereignisses (W = 5, 4, 3, 2 oder 1) und der Möglichkeit der Vermeidung oder Begrenzung des Schadens (P = 5, 3 oder 1).

Die Klasse K wird gemäß der Formel K = F + W + P berechnet. Der Schnittpunkt aus der Schwere S und der Klasse K ergibt den erforderlichen SIL-Level.

Für die in **Bild 12** dargestellte spezifische Gefährdung, für die S als 3, F als 4, W als 5 und P als 5 bestimmt worden sind, ergibt sich: K = F + W + P = 4 + 5 + 5 = 14 Bei Anwendung der Tabelle ergibt dies im Schnittpunkt aus S = 3 und K = 14 einen erforderlichen SIL-Level von SIL 3.

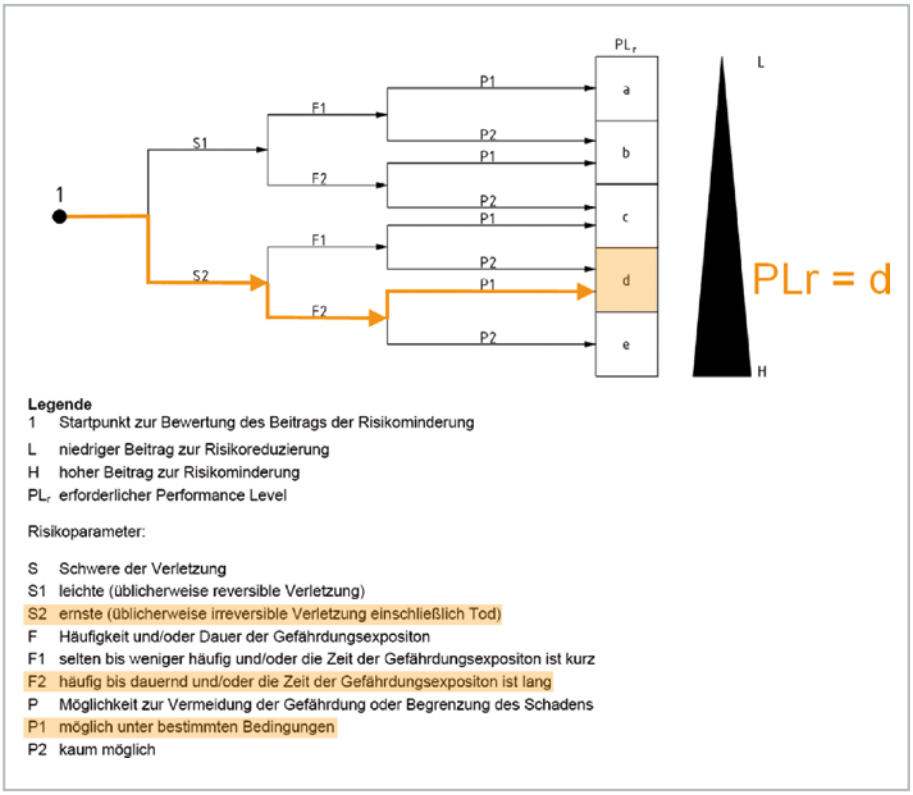


Bild 11: Ermittlung des Performance Level, Quelle DIN EN ISO 13849-1
Fig. 11: Determination of Performance Level, source: DIN EN ISO 13849, Part 1

EN 746-2:2010 Elektrische Ausrüstung und Schutzsystem

Die generelle Anforderung der EN 746-2:2010 besagt, dass die elektrische Ausrüstung von Thermoprozessanlagen in Übereinstimmung mit der DIN EN 60204 (Elektrische Ausrüstung von Maschinen) auszuführen ist.

Eine wesentliche Neuerung in der aktuellen Norm sind die Anforderungen bezüglich der funktionalen Sicherheit an das Schutzsystem. Das Schutzsystem ist wahlweise gemäß der Ausführung A, B, C oder D aufzubauen.

EN 746-2:2010 Anforderungen Schutzsystem

Die Norm beschreibt eine pauschalisierte Einstufung von Funktionen:

Nicht gefährliche Funktionen:

Hier werden keine Anforderungen an die funktionale Sicherheit spezifiziert.

Überwachungsfunktionen, welche nicht unmittelbar gefährlich sind:

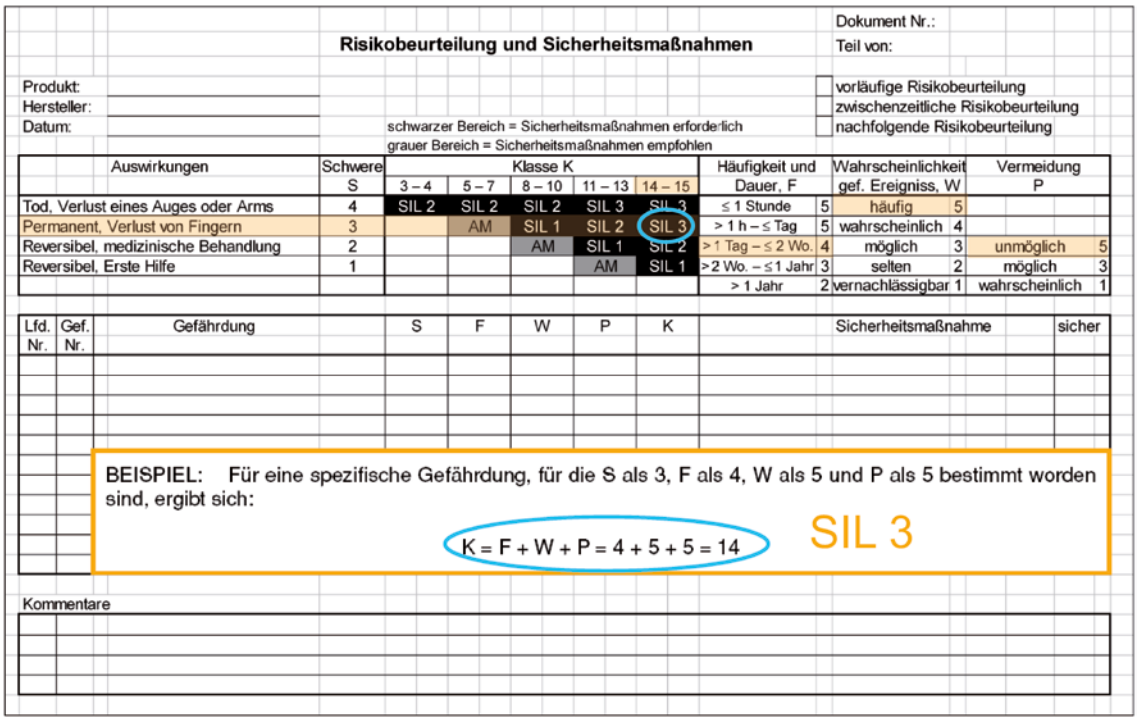
Hier wird der Einsatz von Komponenten gemäß Produktnormen (siehe EN 746-2, Abschnitt 5.2–5.6) oder Komponenten mit SIL 2/PL d Zertifizierung gefordert. Beispielhaft werden in der Norm Überwachungsfunktionen wie z. B. Gasdruck und Temperatur aufgeführt.

Unmittelbar gefährliche Funktionen:

Hier wird der Einsatz von Komponenten gemäß Produktnormen (siehe EN 746-2, Abschnitt 5.2–5.6) oder Komponenten mit SIL 3/PL e Zertifizierung gefordert. Diese Anforderungen gehen aus der Beschreibung der Ausführungen A, B, C und D hervor. Beispielhaft werden in der Norm unmittelbar gefährliche Funktionen wie z. B. Flammenüberwachung und Verhältnisüberwachung aufgeführt.

EN 746-2:2010 Schutzsystem Ausführung A

Das Schutzsystem Ausführung A ist ein fest verdrahtetes Schutzsystem (nicht programmierbar) und beschreibt die Verwendung von Sicherheitsgeräten gemäß Produktnormen (siehe Abschnitt



Risikobeurteilung und Sicherheitsmaßnahmen

Dokument Nr.:
Teil von:

Produkt:
Hersteller:
Datum:

schwarzer Bereich = Sicherheitsmaßnahmen erforderlich
grauer Bereich = Sicherheitsmaßnahmen empfohlen

☐ vorläufige Risikobeurteilung
☐ zwischenzeitliche Risikobeurteilung
☐ nachfolgende Risikobeurteilung

Auswirkungen	Schwere S	Klasse K 3 – 4	5 – 7	8 – 10	11 – 13	14 – 15	Häufigkeit und Dauer, F		Wahrscheinlichkeit gef. Ereigniss, W		Vermeidung P	
Tod, Verlust eines Auges oder Arms	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≤ 1 Stunde	5	häufig	5		
Permanent, Verlust von Fingern	3		AM	SIL 1	SIL 2	SIL 3	> 1 h – ≤ Tag	5	wahrscheinlich	4		
Reversibel, medizinische Behandlung	2			AM	SIL 1	SIL 2	> 1 Tag – ≤ 2 Wo.	4	möglich	3	unmöglich	5
Reversibel, Erste Hilfe	1				AM	SIL 1	> 2 Wo. – ≤ 1 Jahr	3	selten	2	möglich	3
							> 1 Jahr	2	vernachlässigbar	1	wahrscheinlich	1

Lfd. Nr.	Ges. Nr.	Gefährdung	S	F	W	P	K	Sicherheitsmaßnahme	sicher

BEISPIEL: Für eine spezifische Gefährdung, für die S als 3, F als 4, W als 5 und P als 5 bestimmt worden sind, ergibt sich:

K = F + W + P = 4 + 5 + 5 = 14 SIL 3

Kommentare

Bild A.3 – Beispiel-Formblatt für den Prozess der Bestimmung des SIL

Bild 12: Ermittlung des SIL Level, Quelle EN 62061
Fig. 12: Determination of SIL level, source: EN 62061

5.2–5.6) (**Bild 13**). D. h. die hier zur Anwendung kommenden Sicherheitsgeräte entsprechen speziellen auf den Einsatzbereich und die funktionalen Anforderungen an diese Geräte abgestimmten Sicherheitsanforderungen, wie sie in den entsprechenden Produktnormen für Feuerungsautomaten, Ventilüberwachungssysteme, Druckwächter, Automatische Absperrventile und Gas/Luft-Verhältnisregelung gefordert werden.

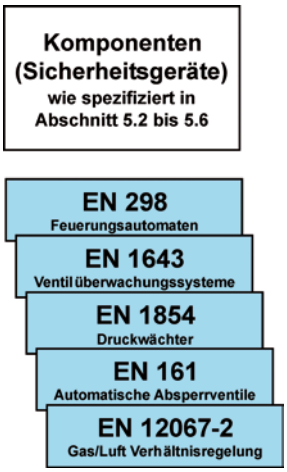


Bild 13: Schutzsystem Ausführung A, Quelle EN 746-2:2010,
Fig. 13: Safety system, Version A, source: EN 746, Part 2:2010

Eine Anwendung der EN 62061 oder EN ISO 13849 ist nicht möglich.

Beispiel:

Die „Sicherheitsfunktion Dichtheitskontrolle" wird gemäß Ausführung A mittels der Verschaltung eines Sensors (Druckwächter gemäß DIN EN 1854) mit der Logik (Dichtheitskontrolle gemäß DIN EN 1643) und den Aktoren (Gasventile gemäß DIN EN 161) aufgebaut.

Für die Feuerungstechnik liegen seit Jahrzehnten umfangreiche ständig an den Stand der Technik angepasste Produktnormen vor. Die nach diesen Normen ausgeführten Anlagen und Produkte weisen ein sehr hohes Sicherheitsniveau auf. Am Beispiel der millionenfach im Feld befindlichen Feuerungsautomaten ist festzustellen, dass es nie zu Schadensfällen gekommen ist, die auf mangelnde Anforderungen in Normen zurückzuführen sind.

Auch ohne zusätzliche SIL/PL Zertifizierung von Sicherheitsgeräten ist nach wie vor die Sicherstellung der Schutzziele und Sicherheitsanforderungen für den Einsatz von Sicherheitsgeräten gemäß Produktnormen gegeben und damit die Realisierung eines Schutzsystems Ausführung A als eine von mehreren alternativen Möglichkeiten anzusehen.

Um darüber hinaus zukünftig auch zusätzliche Anforderungen aus den Normen für funktionale Sicherheit einzubeziehen, wird derzeit intensiv in Normengremien und Arbeitsgruppen mit Herstellern und Prüfstellen an sektorspezifischen Erweiterungen zu den oben genannten Produktnormen gearbeitet. Als Ergebnis dieser Anstrengungen ist die zusätzliche SIL/PL-Zertifizierung von Sicherheitsgeräten zu erwarten und aktuell bereits teilweise bei Herstellern von Sicherheitsgeräten in der Umsetzung.

Die zusätzliche SIL/PL-Zertifizierung von Sicherheitsgeräten wird jedoch in der Regel (Ausnahme – Nachweis der Betriebsbewährtheit) nicht für ältere Sicherheitsgeräte möglich sein, da der Zertifizierungsprozess entwicklungsbegleitend erfolgt und damit nicht rückwirkend möglich ist.

EN 746-2:2010 Schutzsystem Ausführung B

Das Schutzsystem Ausführung B ist ein fest verdrahtetes Schutzsystem (nicht programmierbar) und beschreibt die Verwendung von Sicherheitsgeräten gemäß Produktnormen (siehe Abschnitt 5.2–5.6) in Kombination mit Sicherheitsgeräten für welche ein entsprechender SIL/PL Level definiert und nachgewiesen ist (**Bild 14**).

Für „Überwachungsfunktionen, welche nicht unmittelbar gefährlich“ sind (z. B. Gasdruck, Temperatur), müssen Komponenten gemäß Produktnormen (siehe Abschnitt 5.2 – 5.6) oder Komponenten mit mindestens SIL 2 / PL d Zertifizierung eingesetzt werden.

Für „Unmittelbar gefährliche Funktionen“ (z. B. Flammenüberwachung) müssen Komponenten gemäß Produktnormen (siehe Abschnitt 5.2 – 5.6) oder Komponenten mit SIL 3 / PL e Zertifizierung eingesetzt werden.

Beispiel:

Die „Sicherheitsfunktion Hochtemperatur Grenzwertüberwachung“ wird gemäß Ausführung B mittels der Verschaltung eines Sensors (Sicherheits-Temperaturbegrenzer mit SIL/PL Zertifizierung) mit der Logik (Feuerungsautomat gemäß DIN EN 298) und den Aktoren (Gasventile gemäß DIN EN 161) aufgebaut.

EN 746-2:2010 Schutzsystem Ausführung C

Das Schutzsystem Ausführung C ist ein SPS-basiertes Schutzsystem (programmierbar) und beschreibt die Verwendung von Sicherheitsgeräten gemäß Produktnormen (siehe Abschnitt 5.2–5.6) in Kombination mit Sicherheitsgeräten für welche ein entsprechender SIL/PL Level definiert und nachgewiesen ist und/ oder in Kombination mit einer SPS für welche ein entsprechender SIL/PL-Level definiert und nachgewiesen ist (**Bild 15**).

Für „Überwachungsfunktionen, welche nicht unmittelbar gefährlich“ sind (z.B. Gasdruck, Temperatur), müssen Komponenten gemäß Produktnormen (siehe Abschnitt 5.2–5.6) oder Komponenten mit mindestens SIL 2/PL d Zertifizierung eingesetzt werden.

Für „Unmittelbar gefährliche Funktionen“ (z. B. Flammenüberwachung) müssen Komponenten gemäß Produktnormen (siehe Abschnitt 5.2 – 5.6) oder Komponenten mit SIL 3/PL e Zertifizierung eingesetzt werden.

Die Hard- und Software der SPS muss den Anforderungen gemäß EN IEC 62061 bzw. EN ISO 13849 entsprechen und auch die funktionalen Anforderungen (z. B. Gesamtschließzeit), wie in Abschnitt 5.2 bis 5.6 spezifiziert, berücksichtigen.

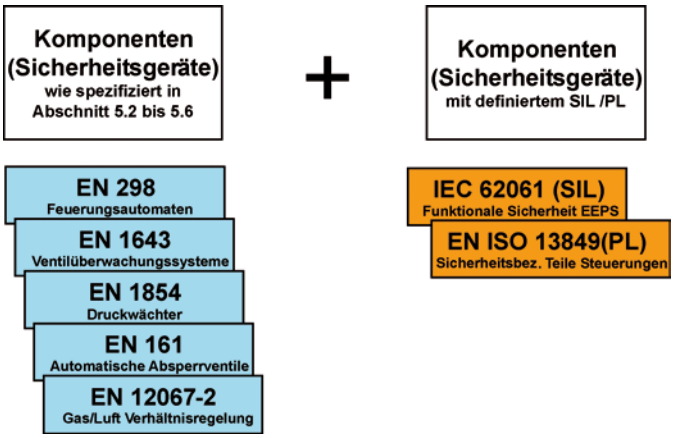


Bild 14: Schutzsystem Ausführung B, Quelle EN 746-2:2010,
Fig. 14: Safety system, Version B, source: EN 746, Part 2:2010

Beispiel:

Die „Sicherheitsfunktion Sicherheitskette Gas Max. Drucküberwachung“ wird gemäß Ausführung C mittels der Verschaltung eines Sensors (Druckwächter gemäß DIN EN 1854) mit der Logik (Sicherheits-SPS mit SIL/PL-Zertifizierung) und den Aktoren (Gasventile gemäß DIN EN 161) aufgebaut.

EN 746-2:2010 Schutzsystem Ausführung D

Das Schutzsystem Ausführung D ist ein SPS-basiertes Schutzsystem (programmierbar) und beschreibt die Verwendung von Sicherheitsgeräten, für welche ein entsprechender SIL/PL-Level definiert und nachgewiesen ist in Kombination mit einer SPS, für welche ein entsprechender SIL/PL-Level definiert und nachgewiesen ist (**Bild 16**).

Alle Komponenten sollen gemäß der Norm eine SIL 3/PL e Zertifizierung aufweisen.

Die Hard- und Software der SPS muss den Anforderungen gemäß EN IEC 62061 bzw. EN ISO 13849 entsprechen und auch die funktionalen Anforderungen (z. B. Gesamtschließzeit), wie in Abschnitt 5.2 bis 5.6 spezifiziert, berücksichtigen.

Beispiel:

Die „Sicherheitsfunktion Sicherheitskette Gas. Max. Drucküberwachung“ wird gemäß Ausführung D mittels der Verschaltung eines Sensors (Druckwächter gemäß DIN EN 1854 und SIL/PL-Zertifizierung) mit der Logik (Sicherheits-SPS oder Sicherheitselektronik mit SIL/PL-Zertifizierung) und den Aktoren (Gasventile gemäß DIN EN 161 und SIL/PL-Zertifizierung) aufgebaut.

Anmerkung:

Durch die ausschließliche Forderung nach SIL 3/PL e ergibt sich hier ein Widerspruch zu den anderen Ausführungen des Schutzsystems in der Norm. Praktikabel erscheint hier eine Unterscheidung in

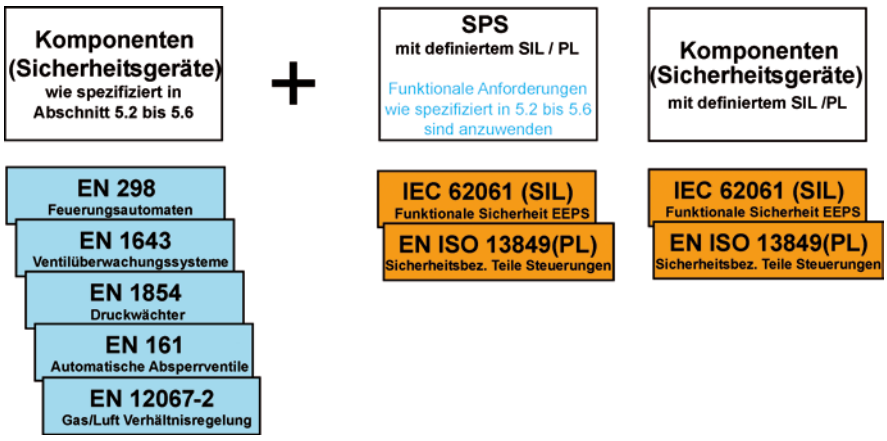


Bild 15: Schutzsystem Ausführung C, Quelle EN 746-2:2010
Fig. 15: Safety system, Version C, source: EN 746, Part 2:2010

Bild 16: Schutzsystem Ausführung D, Quelle EN 746-2:2010,
Fig. 16: Safety system, Version D, source: EN 746, Part 2:2010

SIL 2/PL d und SIL 3/PL e vorzunehmen, wie in Ausführung B und C beschrieben.

V-Modell für Softwareentwicklung für Sicherheits-SPS

Für die Softwareentwicklung für Sicherheits-SPS sowie Programmierbarer Sicherheitsgeräte wird z. B. die Vorgehensweise gemäß V-Modell empfohlen.

Alle Tätigkeiten im Lebenszyklus von sicherheitsbezogener Embedded- oder Anwendungssoftware müssen hauptsächlich die Vermeidung von Fehlern berücksichtigen, die während des Softwarelebenszyklus eingebracht werden. Das Hauptziel der Anforderungen an die Software ist es, lesbare, verständliche, testbare und wartbare Software zu erhalten.

Die konstruktiven Tätigkeiten umfassen die sicherheitsbezogene Software-Spezifikation, die Systemgestaltung, die Modulgestaltung und die Codierung (das SPS-Programm). Die überprüfenden Aktivitäten umfassen die Modultests, die Integrationstests und die Validierung der Software.

(Quelle EN ISO 13849-1; IEC 61508-3)

Die sichere Programmgestaltung ist sehr wichtig, damit die Kombination aus SIL/PL zertifizierter SPS-Hardware zusammen mit der Software der Sicherheits-SPS eine sichere Einheit bildet. Softwarefehler können unmittelbar zu einem Sicherheitsrisiko führen. Um Softwarefehler zu vermeiden, sind entsprechende Maßnahmen zu ergreifen. Häufig werden entsprechende Sofwaremodule von den Steuerungsherstellern angeboten. Speziell der Teil 3 der IEC 61508 befasst sich mit der Softwareerstellung.

Sicherheitsfunktionen einer Prozess-Steuerung

In **Bild 17** sind die wesentlichen Sicherheitsfunktionen des Schutzsystems der Prozess-Steuerung einer Thermoprozessanlage dargestellt. Elektronische Sicherheitsgeräte sind orange eingefärbt.

Die Einspeisung (100) versorgt die Steuerung mit der Versorgungsspannung. Der Start der Verbrennungsluftgebläsesteuerung (210) erfolgt unter Einbeziehung der Wechselüberwachung des Luft min. Druckwächters (311).

Der Steuerungsblock für die Überwachung der Sicherheitsgrenzen (300) übernimmt die sicherheitsrelevante Überwachung der Safety Limits Luft min. (311), Gas min. (321), Gas max. (322), Not-Halt (331) und die Überwachung

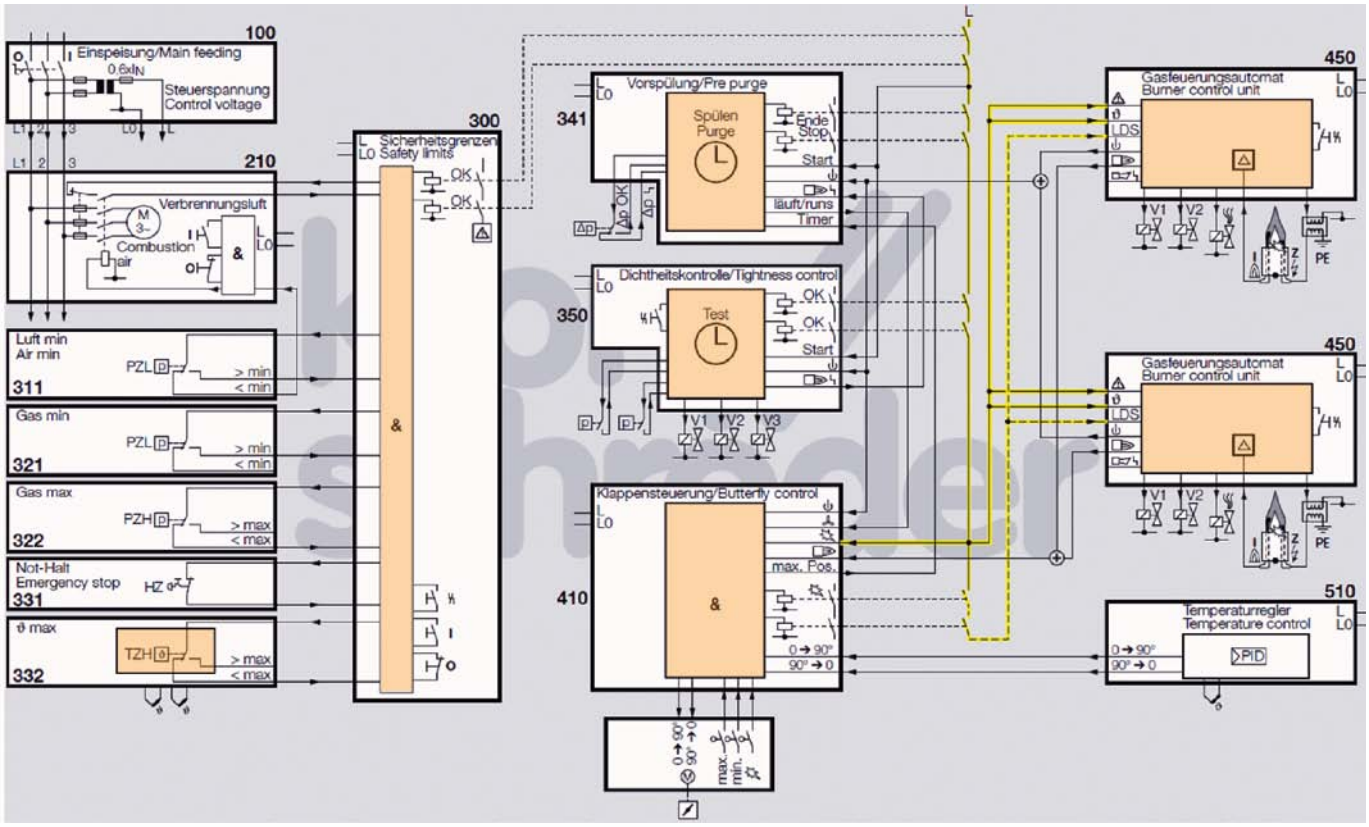


Bild 17: Sicherheitsfunktionen Prozess-Steuerung
Fig. 17: Process control system safety functions

Tabelle 1: Erforderliche SIL/PL-Level von Sicherheitsfunktionen
Table 1: SIL/PL levels necessary for safety functions

Sicherheitsfunktion :	Betriebsart:	EN 746-2 SIL:	EN 746-2 PL:	IEC 62061 (ermittelt) SIL:	ISO 13849 (ermittelt) PL:
Gas max. Überwachung	High / Low Demand	2	d	2	d
Gas min. Überwachung	High / Low Demand	2	d	2	d
Luft min. Überwachung	High Demand			2	d
Vorspülung	High Demand			2 (3)	d (e)
Dichtheitskontrolle / Ventilüberwachungssystem	High Demand			2 (3)	d (e)
Flammenüberwachung / Gasfeuerungsautomat	High Demand	3	e	3	e
Überwachung Zündstellung (Einzel / Mehrbrenner)	High Demand			2 / 1	d / c
Luft / Gas - Verhältnisüberwachung	High Demand	3	e	3	e
Hochtemperatur Grenzwertüberwachung	High Demand	3	e	3	e
Not - Halt / Not - Aus	High / Low Demand			2 / 3	d / e

des Sicherheitstemperaturbegrenzers (332). Nach dem Anlagenstart und dem Vorhandensein aller Sicherheits-Grenzwerte (300) beginnt die Vorspülung (341) der Thermoprozessanlage sowie die Dichtheitskontrolle (350) der Ventile. Nach Abschluss der Vorspülung (341) und dem OK-Signal der Dichtheitskontrolle (350) ist die Sicherheitskette (gelb dargestellt) gesetzt und die Brenner werden in Zündstellung gestartet. Nach Rückmeldung der Flammensignale an die Gasfeuerungsautomaten (450) gehen die Brenner in Betrieb. Der Temperaturregler (510) übernimmt die Temperaturregelung der Beheizungseinrichtung.

Die Anforderungen bezüglich der erforderlichen SIL/PL-Level an die in Bild 17 dargestellten Sicherheitsfunktionen werden in der **Tabelle 1** aufgeführt.

Erforderliche SIL/PL-Level von Sicherheitsfunktionen

Die in Tabelle 1 aufgeführten Sicherheitsfunktionen werden zunächst auf ihre Betriebsart hin betrachtet. Generell werden der sogenannte Low Demand Mode (Betriebsart mit niedriger Anforderungsrate, nicht mehr als einmal pro Jahr betätigt) und der sogenannte High Demand Mode (Betriebsart mit hoher Anforderungsrate, mehr als einmal pro Jahr betätigt) unterschieden. Praktisch hat der Low Demand Mode an Maschinen/ Thermoprozessanlagen keine Bedeutung, da einerseits nur wenige Sicherheitsfunktionen überhaupt so eingestuft werden könnten, andererseits wird in der EN 62061 der Low Demand Mode für die Anwendung an Maschinen als nicht relevant betrachtet.

ANMERKUNG aus EN 62061 – 3.2.26:

Einrichtungen, die nur in Übereinstimmung mit den Anforderungen zur Betriebsart mit niedriger Anforderungsrate gemäß IEC 61508-1 und IEC 61508-2 entworfen worden sind, können für die Verwendung als Teil eines sicherheitsbezogenen elektrischen Steuerungssystems (SRECS) nach EN 62061 ungeeignet sein. Die Betriebsart mit niedriger Anforderungsrate wird für die Anwendung von SRECS an Maschinen als nicht relevant betrachtet. (Quelle EN 62061).

Wie in der EN 62061 beschrieben, wird an Maschinen wie Thermoprozessanlagen für die Komponenten des Schutzsystems nur die Betriebsart mit hoher Anforderungsrate (High Demand) betrachtet.

Erforderliche SIL/PL-Level:

Zum einen sind in Tabelle 1 die in der EN 746-2 geforderten SIL/PL-Level eingetragen. Daneben sind SIL/PL-Level aufgeführt, welche in Gesprächen mit Herstellern von Thermoprozessanlagen gemäß der Risikobeurteilung aus IEC 62061 und ISO 13849 ermittelt wurden. Die Tabelle 1 als Beispiel aufgeführten Werte beziehen sich auf typische Thermoprozessanlagen. Die erforderlichen SIL/PL Level können in Abhängigkeit der Risikobeurteilung abweichen.

Folgendes lässt sich feststellen:

Bei den Anforderungen an die Überwachung des Gas- und Luftdruckes besteht mit der Anforderung SIL 2/PL d aus EN 746-2 große Übereinstimmung.

Für die Sicherheitsfunktionen Vorspülung und Dichtheitskontrolle macht die EN 746-2 keine direkten Angaben. Die Ermittlung der Werte SIL 2/PL d beruht auf einer Beurteilung dahingehend, dass diese Sicherheitsfunktion in der Regel immer zusammen mit anderen Sicherheitsfunktionen (z. B. Verwendung von zwei automatischen Absperrventilen gemäß EN 161 oder Vorspülung und Dichtheitskontrolle) zur Anwendung kommen, d.h. ein Ausfall führt in der Regel nicht zu einer unmittelbaren Gefährdung. In Einzelfällen kann je nach Risikobeurteilung SIL 3/PL e erforderlich sein.

Für die Anforderung an die Sicherheitsfunktion Flammenüberwachung/Gasfeuerungsautomat besteht mit SIL 3/PL e wiederum Übereinstimmung mit der Anforderung aus EN 746-2. Hier ist klar, dass bei nicht vorhandener Flamme am Brenner unverbranntes Gas in den Feuerungsraum strömt und eine unmittelbare Gefährdung besteht.

Die Risikobeurteilung für die Überwachung der Zündstellung ergab für Einzelbrenner SIL 2/PL d und für Mehrbrennersysteme SIL 1/PL c, da im Falle einer Mehrbrenneranlage (z. B. Zündung eines Brenners von vielen Brennern) das Risiko deutlich sinkt.

Die Beurteilung der Luft/Gas-Verhältnisüberwachung gestaltete sich äußerst schwierig. Abgesehen davon, daß die Forderung der EN 746-2 nach SIL 3/PL e und die üblicherweise anzutreffende Realisierung an Thermoprozessanlagen

häufig deutlich voneinander abweichen, ist es derzeit kaum möglich, SIL 3/PL e technisch zu realisieren. Differenzdruckmessumformer zur Durchflussmessung über einer Blende sind zwar in der Regel einkanalig mit SIL 2/PL d oder zweikanalig mit SIL 3/PL e erhältlich, jedoch wird in den entsprechenden Zertifikaten häufig nur ein PFD-Wert für den Low Demand Mode anstelle eines PFH_D-Wertes für den High Demand Mode ausgewiesen. Der Umstand, dass gemäß EN 62061 (siehe oben) der Low Demand Mode für Maschinen und somit für Thermoprozessanlagen als nicht relevant betrachtet wird und deshalb Geräte für den High Demand Mode eingesetzt werden sollen, erschwert die Problematik zusätzlich. Letztendlich kann man sagen, dass hier Hersteller von Geräten und Hersteller von Thermoprozessanlagen noch gemeinsam Lösungen entwickeln müssen, welche auf der einen Seite zu dem gewünschten hohen sicherheitstechnischen Niveau führen, auf der anderen Seite unter wirtschaftlicher Betrachtung bezahlbar sein sollen.

Die Hochtemperatur-Grenzwertüberwachung, welche an Thermoprozessanlagen in Abhängigkeit der Prozesstemperatur zur Umschaltung der Flammenüberwachung auf Temperaturüberwachung verwendet wird, ist eindeutig SIL 3/PL e zuzuordnen, da hier die gleichen Anforderungen wie bei der Sicherheitsfunktion Flammenüberwachung bestehen. Auch hier wiederum Übereinstimmung mit der EN 746-2.

Die Sicherheitsfunktion Not-Halt/Not-Aus wird üblicherweise in SIL 2/PL d oder SIL 3/PL e eingestuft. Gelegentlich kann hier auch SIL 1/PL c in Abhängigkeit der jeweiligen Anlagenbeschaffenheit ausreichend sein.

Die erforderlichen SIL/PL-Level für Sicherheitsfunktionen des Schutzsystems können im Einzelfall abweichen, eine Risikobeurteilung ist wie beschrieben generell durchzuführen.

Fazit

Grundsätzlich kann man an der Tabelle 1 sehen, dass es für die meisten Sicherheitsfunktionen des Schutzsystems einer Thermoprozessanlage machbar ist, die von den Normen zur funktionalen Sicherheit geforderten Anforderungen zu ermitteln und auch umzusetzen. Es gibt zwar hier und da noch Schwierigkeiten, grundsätzlich ist die Branche aber auf einem guten Weg.

Für die Berechnung der SIL/PL-Level werden von Geräteherstellern sowie der IFA (BGIA) entsprechende Tools angeboten, alternativ kann die Berechnung aber auch gemäß der Beschreibung in den Normen IEC 62061 oder ISO 13849 vorgenommen werden.

Es ist zu erwarten, dass von Seiten der Gerätehersteller mehr und mehr Geräte mit SIL/PL-Zertifizierung angeboten werden, und dass bei Herstellern von Thermoprozessanlagen die neuen Anforderungen nach und nach in den Konstruktionsalltag einbezogen werden. Hilfreich sind hier nicht zuletzt die alternativ anwendbaren Ausführungen A – D des Schutzsystems gemäß EN 746-2.

Zusammenstellung relevanter EG-Richtlinien und Normen

Maschinenrichtlinie 2006/42/EG

RICHTLINIE 2006/42/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung)

Niederspannungsrichtlinie 2006/95/EG

RICHTLINIE 2006/95/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 12. Dezember 2006 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten betreffend elektrische Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen (kodifizierte Fassung)

EMV Richtlinie 2004/108/EG

RICHTLINIE 2004/108/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 15. Dezember 2004 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit und zur Aufhebung der Richtlinie 89/336/EWG

Richtlinie über Gasverbrauchseinrichtungen 2009/142/EG

RICHTLINIE 2009/142/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 30. November 2009 über Gasverbrauchseinrichtungen (kodifizierte Fassung)

GPSG

Gesetz über technische Arbeitsmittel und Verbraucherprodukte

(Geräte- und Produktsicherheitsgesetz – GPSG) Ausfertigungsdatum: 06.01.2004

EN ISO 12100:2010

Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung (ISO 12100:2010); Deutsche Fassung EN ISO 12100:2010

DIN EN ISO 12100 – 1, April 2004 (darf noch bis 2013-11-01 angewendet werden)

Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze

Teil 1: Grundsätzliche Terminologie, Methodologie

DIN EN ISO 12100 – 2, April 2004 (darf noch bis 2013-11-01 angewendet werden)

Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze

Teil 2: Technische Leitsätze

EN ISO 14121-1:2007

Sicherheit von Maschinen – Risikobeurteilung – Teil 1: Leitsätze (ISO 14121-1:2007);

Deutsche Fassung EN ISO 14121-1:2007

TECHNICAL REPORT ISO/TR 14121-2

Safety of machinery – Risk assessment – Part 2: Practical guidance and examples of methods

EN 61508-1:2010

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010);

Deutsche Fassung EN 61508-1:2010

EN 61508-2:2010

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010);

Deutsche Fassung EN 61508-2:2010

EN 61508-3:2010

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:2010);

Deutsche Fassung EN 61508-3:2010

EN 61508-4:2010

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010);

Deutsche Fassung EN 61508-4:2010

EN 61508-5:2010

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:2010);

Deutsche Fassung EN 61508-5:2010

EN 61508-6:2010

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2010);

Deutsche Fassung EN 61508-6:2010

EN 61508-7:2010

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 7: Überblick über Verfahren und Maßnahmen (IEC 61508-7:2010);

Deutsche Fassung EN 61508-7:2010

EN 60204-1:2006

Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen (IEC 60204-1:2005, modifiziert); Deutsche Fassung EN 60204-1:2006

EN 61511-1:2004

Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware (IEC 61511-1:2003 + Corrigendum 2004); Deutsche Fassung EN 61511-1:2004

EN 50156-1:2004

Elektrische Ausrüstung von Feuerungsanlagen - Teil 1: Bestimmungen für die Anwendungsplanung und Errichtung; Deutsche Fassung EN 50156-1:2004

EN 62061:2005

Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme (IEC 62061:2005);

Deutsche Fassung EN 62061:2005

EN ISO 13849-1:2008

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2006); Deutsche Fassung EN ISO 13849-1:2008

EN ISO 13849-2:2008

Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (ISO 13849-2:2003); Deutsche Fassung EN ISO 13849-2:2008, Berichtigung zu DIN EN ISO 13849-2:2008-09

EN 61439-1:2009

Niederspannungs-Schaltgerätekombinationen – Teil 1: Allgemeine Festlegungen

(IEC 61439-1:2009, modifiziert); Deutsche Fassung EN 61439-1:2009

EN 61439-2:2009

Niederspannungs-Schaltgerätekombinationen – Teil 2: Energie-Schaltgerätekombinationen

(IEC 61439-2:2009); Deutsche Fassung EN 61439-2:2009

DIN EN 746-1:2010-02

Industrielle Thermoprozessanlagen – Teil 1: Allgemeine Sicherheitsanforderungen an industrielle Thermoprozessanlagen; Deutsche Fassung EN 746-1:1997+A1:2009/DIN EN 746-1:2010-02

DIN EN 746-2:2011-02

Industrielle Thermoprozessanlagen - Teil 2: Sicherheitsanforderungen an Feuerungen und Brennstoffführungssysteme; Deutsche Fassung EN 746-2:2010 / DIN EN 746-2:2011-02

DIN EN 746-3:2010-02

Industrielle Thermoprozessanlagen – Teil 3: Sicherheitsanforderungen für die Erzeugung und Anwendung von Schutz- und Reaktionsgasen;

Deutsche Fassung EN 746-3:1997+A1:2009 / DIN EN 746-3:2010-02

EN 746-4:1999

Industrielle Thermoprozessanlagen - Teil 4: Besondere Sicherheitsanforderungen an Feuerverzinkungsanlagen; Deutsche Fassung EN 746-4:1999

EN 746-5:2000

Industrielle Thermoprozessanlagen - Teil 5: Besondere Sicherheitsanforderungen an Salzbad-Wärmebehandlungseinrichtungen und -anlagen; Deutsche Fassung EN 746-5:2000

EN 746-8:2000

Industrielle Thermoprozessanlagen - Teil 8: Besondere Sicherheitsanforderungen an Abschreckanlagen; Deutsche Fassung EN 746-8:2000

EN 13611:2007

Sicherheits-, Regel- und Steuereinrichtungen für Gasbrenner und Gasgeräte - Allgemeine Anforderungen; Deutsche Fassung EN 13611:2007

DIN EN 298:2004-01

Feuerungsautomaten für Gasbrenner und Gasgeräte mit oder ohne Gebläse;

Deutsche Fassung EN 298:2003 / DIN EN 298:2004-01

EN 1643:2000

Ventilüberwachungssysteme für automatische Absperrventile für Gasbrenner und Gasgeräte; Deutsche Fassung EN 1643:2000

EN 1854:2010

Druckwächter für Gasbrenner und Gasgeräte; Deutsche Fassung EN 1854:2010

EN 161:2007

Automatische Absperrventile für Gasbrenner und Gasgeräte;

Deutsche Fassung EN 161:2007

EN 12067-2:2004

Gas-Luft-Verbundregeleinrichtungen für Gasbrenner und Gasgeräte –

Teil 2: Elektronische Ausführung; Deutsche Fassung EN 12067-2:2004

BGIA – Report 2/2008

Funktionale Sicherheit von Maschinensteuerungen

- Anwendung der EN ISO 13849 - ■

Klaus Kroner
Elster GmbH, Geschäftssegment Systeme, Osnabrück/Lotte (Büren)

Tel.: 0541/1214-360
klaus.kroner@elster.com