PROZESSWÄRME

Sonderdruck
05/2020
ISSN 2567-3742

Der Weg zu normenkonform und durchgängig sicher automatisierten Thermoprozessanlagen

von **Ulf Weißhuhn, Hermann Wübbels**

Nach EN 298 zertifizierte Feuerungsautomaten gelten in sich als fehlersicher und sind Voraussetzung, um die Anforderungen der EN 746-2 an industrielle Thermoprozessanlagen zu erfüllen. Was aber ist, wenn mehrere Feuerungsautomaten von einer zentralen Steuerung zu koordinieren sind? Wenn dazu separate Sensorik und damit durchgängig sichere Kommunikation erforderlich ist und die Gesamtanlage einer Sicherheitsbetrachtung nach der EG Maschinenrichtlinie genügen muss? Ist sicher dann wirklich immer sicher?

The path to standard compliant and consistently safe automated thermoprocessing equipment

Automatic burner control systems which are certified according EN 298 are the precondition to fulfil the requirements of the EN 746-2 for industrial thermoprocessing equipment. But what if several automatic burner control systems need to be coordinated by a central controller? If additional sensors, consistent fail-safe communication is required and the complete system needs to fulfil the safety requirements under the EU Machinery Directive. Is safe then really always safe?

Sicherheitsanforderungen an Produkte werden in der Europäischen Gemeinschaft durch EU-Richtlinien geregelt, die Umsetzung dieser EU-Richtlinien sind in spezifischen Normen beschrieben. Diese Normen gliedern sich dabei in (Typ) A-, B- und C-Normen, wobei es sich bei Typ A um Sicherheits-Grundnormen, bei Typ B um Sicherheitsfachgrund- oder Sicherheits-Gruppennormen (z. B. EN 62061 oder ISO 13849-1) und bei Typ C um Maschinensicherheits-Normen (z. B. EN 746-2 oder ISO 13577) handelt.

Für steuerungsbasierte Sicherheitslösungen sind in der EU die EN 62061 und die EN ISO 13849-1 unter der EG Maschinenrichtlinie 2006/42/EG harmonisiert. Dies bedeutet, dass wenn die Sicherheitsfunktionen nach den o. g. B-Normen konzipiert sind, die (CE)-Konformität zu den EU-Richtlinien dadurch nachgewiesen werden kann. Für industrielle Thermoprozessanlagen ist in der EU die C-Norm EN 746 unter der Maschinenrichtlinie harmonisiert. Was wiederum bedeutet, dass die Konformität zu den EU-Richtlinien dadurch nachgewiesen werden sollte, dass die Brennerlösung dieser C-Norm entspricht.

Wie ist nun vorzugehen, wenn sich A-, B- und C-Normen in bestimmten Punkten widersprechen oder gar gegensätzliche Anforderungen an die Produkte stellen? So fordern beispielsweise die EN 62061 und die EN ISO 13849-1, dass die Sicherheit von Sicherheitsfunktionen (beispielsweise eines Flammenwächters) lückenlos vom Sensor über den Controller bis zum Aktor nachzuweisen ist. Und je nach Gefährdungspotenzial einen Safety Integrity Level SIL1 bis SIL3 bzw. einen Performance Level PLa bis PLe erfüllt. Die EN 746-2 besagt dagegen, dass die Sicherheit einer Brennersteuerung nach EN 62061 (oder EN ISO 13849-1) nur für diejenigen Teile nachzuweisen ist, die nicht einer Produktzertifizierung nach Normen für industrielle Thermoprozessanlagen (z. B. nach EN 298) unterliegen. Ein Beispiel für eine solche Komponente wäre eine fehlersichere Steuerung (F-CPU).

In der Praxis führt das zu einem Konflikt: Ist die Anlagensicherheit nun nach EN 62061 bzw. EN ISO 13849-1 oder nach EN 746-2 nachzuweisen?

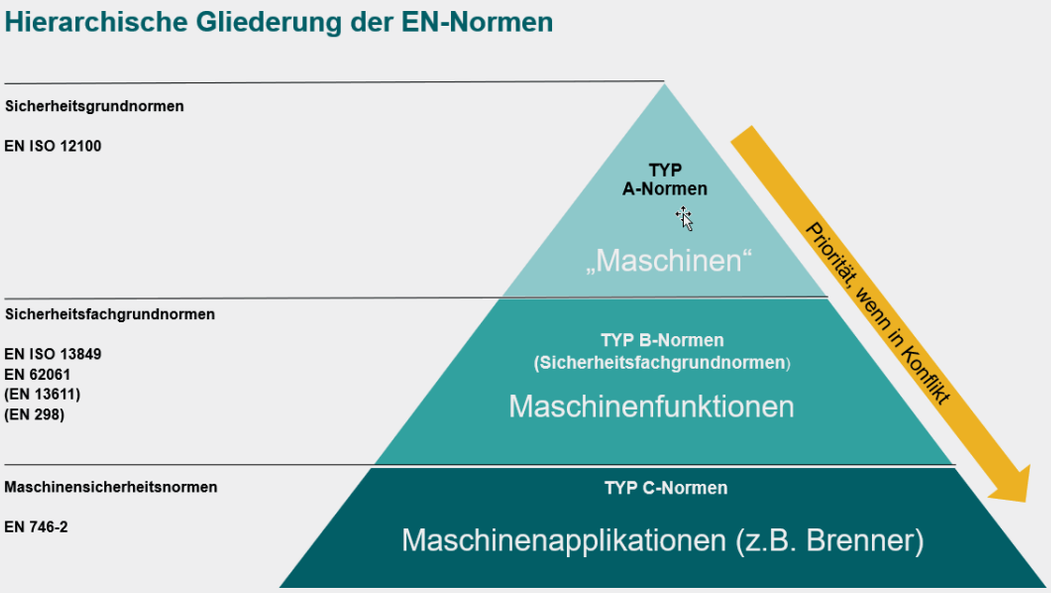

Bild 1: Normenpyramide (Quelle: Siemens AG)

Die Norm, EN 13611, welche die Basis weiterer Normen für industrielle Thermoprozessanlagen ist, wie z. B. die Produktnorm EN 298 stellt eine Verfahrensweise zur Überführung der Bewertung der Hardware in SIL/PL zur Verfügung. Jedoch ist dieser ermittelte SIL/PL trotz derselben normativen Grundlage, wegen der unterschiedlichen Zielsetzungen, nicht gleich.

Der Grund hierfür ist, dass die EN 13611 die Anforderungen an die Hardwareauslegung über eine „Klasse“ definiert, und nicht wie die EN 62061 (oder EN ISO 13849-1), über eine „SIL-Anspruchsgrenze“ (oder einer „Kategorie“). Ein durchgängiger Nachweis lässt sich damit nur sehr schwer führen. Dies führt zu der absurden Situation, dass nach branchenspezifischen Normen entwickelte Produkte mit einem SIL/PL-Level ausgeliefert werden, der aber für den Nachweis der Anlagensicherheit nicht genutzt werden soll.

Es stellt sich aufgrund dieser besonderen Situation also die Frage, wie überhaupt zu verfahren ist?

Eine Antwort darauf gibt die Norm EN ISO 12100, in der die hierarchische Gliederung der Normen geregelt ist

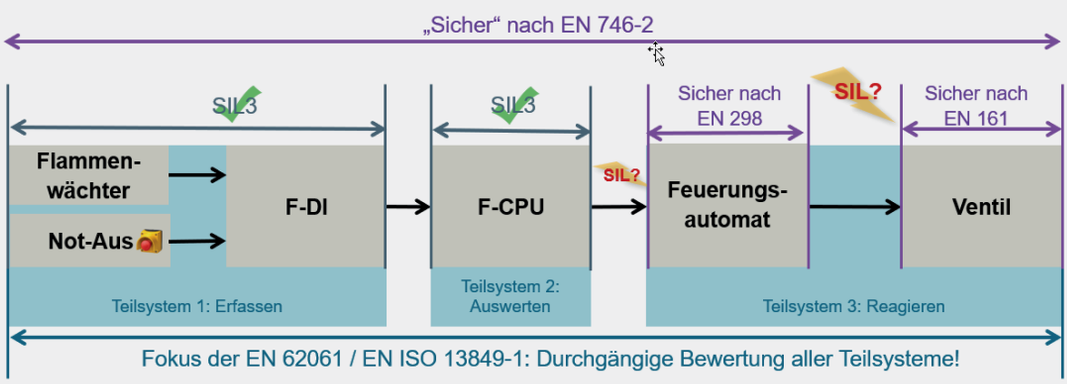

Bild 2: Sicherheitsbetrachtung (Quelle: Siemens AG)

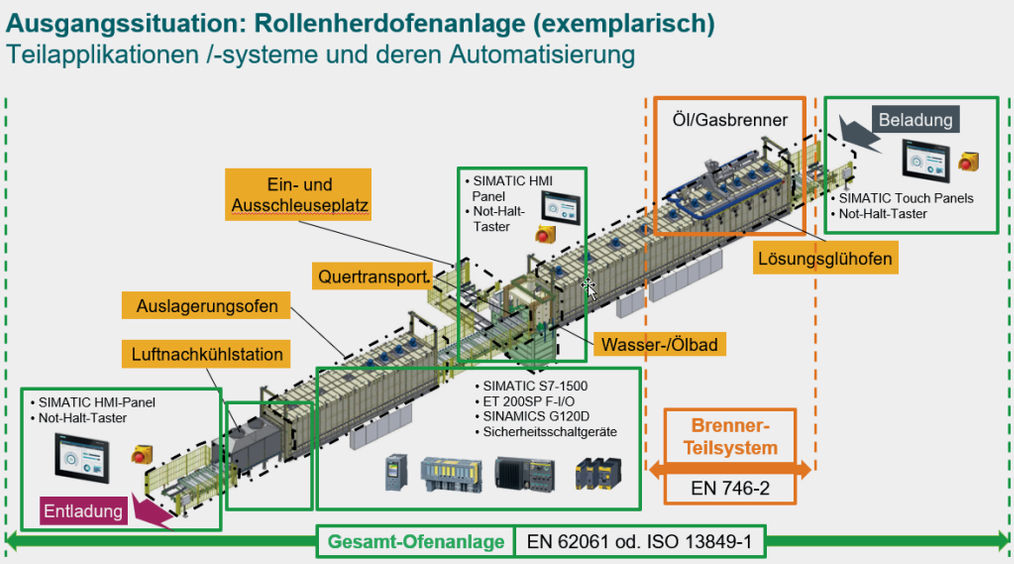

Bild 3: Schematischer Aufbau einer Thermoprozessanlage als Teil einer Maschine (Quelle: Siemens AG)

(Bild 1). Danach sind die Anforderungen an Maschinen und Anlagen umso höher einzustufen, je applikationsbezogener eine Norm ist. Das bedeutet in diesem Fall, dass die Anforderungen der EN 746-2 am höchsten einzustufen sind. Im Detail heißt das, dass bei der Berechnung von PFH und MTTF der Sicherheitsfunktionen nach Produktnormen für industrielle Thermoprozessanlagen zertifizierte Produkte entsprechend den Anforderungen der EN 746-2 nicht betrachtet werden. Das kommt einem Fehlerausschluss gleich – und die Produkte fließen nicht in die Berechnung der Ausfallwahrscheinlichkeit der gesamten Sicherheitsfunktion mit ein (**Bild 2**).

Das ist normenkonform und zulässig – aber sind Thermoprozessanlagen dann in jedem Fall durchgängig sicher?

Die Ausklammerung bestimmter Teilsysteme aus der Sicherheitsbetrachtung hat zur Folge, dass dafür keine Parameter wie Mehrkanaligkeit oder Diagnosefähigkeit berücksichtigt werden.

Und gerade hier liegt das Risikopotenzial der Anforderungen der EN 746-2: Klammert man Teilsysteme der Sicherheitskette aus der Gesamtbetrachtung aus, vernachlässigt man Schnittstellen mit all den daraus folgenden Konsequenzen. Unabhängig von der Frage, welche normativen Anforderungen höher einzustufen sind, ist also viel relevanter, wie die Sicherheit durchgängig bewertet werden kann.

- Was ist beispielsweise zu tun, wenn ein EN 298-konformer Feuerungsautomat zwar für sich genommen als sicher zertifiziert ist, die Signalerfassung aufgrund der Anforderung der EN 746-2 an das Steuerungssystem aber „ausreichend robust“ entsprechend SIL3/PLe ausgeführt werden muss? Wo endet die Anforderung der EN 746-2 – direkt am Feuerungsautomat oder erst an der Eingabebaugruppe der Steuerung?
- Wie weiß die Steuerung mit ausreichender Robustheit, ob ein angesteuerter Feuerungsautomat tatsächlich arbeitet, und ist der Feuerungsautomat mit SIL3/PLe anzusteuern und der Betriebszustand mit SIL3/PLe auszulesen? Wie lässt sich nachweisen, dass mehrere Feuerungsautomaten mit SIL3/PLe zuverlässig koordiniert werden, wenn diese keine ausreichenden Rückmeldungen geben?
- Wie verhält es sich bei einer via Zentralsteuerung ausgeführten Gasdichtheitskontrolle, wenn die dafür notwendigen Ventile von einem lokalen Feuerungsautomaten gesteuert werden? Muss der Feuerungsautomat in diesem Fall SIL3/PLe entsprechend abgeschaltet und erst nach erfolgreicher Dichtheitskontrolle wieder eingeschaltet werden?
- Wie initiiert man eine SIL3/PLe-Störabschaltung einer Ofensteuerung (mit mehreren Einzelbrennern), wenn die überlagerte Steuerung die Temperatur zentral erfasst, die Kontrolle der Sicherheitsabsperrventile jedes einzelnen Brenners aber einem Feuerungsautomaten obliegt?
- Oder generell: Gilt die Zertifizierung eines Flammenwächters nach einschlägigen Produktnormen noch, wenn Teile der sicherheitsgerichteten Funktionalität des Feuerungsautomaten in eine Zentralsteuerung verlagert werden und der Automat nur als deren „verlängerter Arm“ fungiert? Wie kann dies im konkreten Fall auch nachgewiesen werden? Gilt überhaupt die Zertifizierung des Feuerungsautomaten selbst noch?

Wenn auch nur eine dieser Fragen nicht eindeutig positiv beantwortet werden kann, ist wohl ein Teilaspekt des Sicherheitskonzeptes fragwürdig und durchgängige Sicherheit möglicherweise nicht gewährleistet.

Darüber hinaus ergeben sich weitere spezifische und allgemeine Fragen zur technischen, wirtschaftlichen und/oder normenkonformen Machbarkeit bestimmter Dinge.

Durchgängige Sicherheit ist möglich

Sicher bedeutet also NICHT wirklich immer sicher.

Um die genannten Diskrepanzen und Unsicherheiten ausschließen zu können, müssen alle relevanten Systemkomponenten in die Sicherheitsbetrachtung einbezogen werden. Das setzt jedoch durchweg EN 61508-konforme Komponenten mit standardisierten Schnittstellen (z. B. Profisafe) voraus. Eine Alternative wäre die zusätzliche Anbindung per Festverdrahtung, die aber an komplexeren Anlagen sehr aufwändig ist, dazu sehr unflexibel und somit nicht zukunftsgerichtet.

Einfacher, effizienter, komfortabler – ergo kostengünstiger – lässt sich durchgängige Sicherheit durch die Integration der brennerspezifischen Sicherheitsfunktionen in die ohnehin vorhandene fehlersichere Maschinensteuerung realisieren (**Bild 3**). Zusätzlich ist der Aufwand für die Nachweisführung aufgrund der homogenen Normenanforderungen um vieles einfacher. Insbesondere dann, wenn sämtliche Sicherheitsfunktionen

1. standardisiert sind,
2. in dem SPS Softwareprogramm abgebildet und
3. flexibel steuerungsintern umgesetzt werden können.

Wie dies im Detail funktioniert, wird in Teil 2 des Beitrags präsentiert.

AUTOREN

Ulf Weißhuhn
Siemens AG
Digital Industries
Nürnberg
ulf.weisshuhn@siemens.com

Hermann Wübbels
Siemens AG
Digital Industries
Köln
hermann.wuebbels@siemens.com

Sonderdruck

07/2020
ISSN 2567-3742

PROZESSWÄRME

Integrierte Sicherheit für Thermoprozessanlagen

von **Ulf Weißhuhn, Hermann Wübbels**

Wie in Teil 1 unserer zweiteiligen Artikelserie vorgestellt („Der Weg zu normenkonform und durchgängig sicher automatisierten Thermoprozessanlagen", PW 5/2020), kann es bei der Betrachtung der Sicherheit von Thermoprozessanlagen und ihren Teilsystemen zu undefinierten Bereichen in der sicherheitstechnischen Bewertung kommen. Ein Weg zu normenkonform und durchgängig sicher automatisierten Thermoprozessanlagen, der diese Herausforderung löst, ist die Integration der brennerspezifischen Sicherheitsfunktionen in die fehlersichere Maschinensteuerung. Diese Lösung erfüllt nicht nur die Anforderungen gemäß EN 746 und ISO 13577, sondern bietet für Anlagenbauer und -betreiber noch weitere Vorteile.

Integrated safety for thermoprocessing equipment

As presented in part 1 of our two-part article series ("The path to standard compliant and consistently safe automated thermoprocessing equipment", PW 5/2020), the safety assessment of the complete system including the subsystems could result in some undefined areas in regards to the safety evaluation. A way to standard compliant and consistently safe automated thermoprocessing equipment, which solves this challenge, is the integration of burner-specific safety functions into the fail-safe machine control system. This solution not only fulfils the requirements of EN 746 and ISO 13577, but offers even more advantages for plant manufacturers and operators.

Konventionell werden Schutzsysteme von Brenneranlagen mit einer Reihe von Komponenten gesteuert und überwacht, die alle eigenen Produktnormen entsprechen (**Bild 1**): So kann zum Beispiel ein Feuerungsautomat den Anforderungen der EN 298 genügen und ein Sicherheitsabsperrventil kann entsprechend der Norm EN 161 ausgelegt sein. Das Gesamtsystem wiederum muss die Anforderungen der für industrielle Thermoprozessanlagen relevanten Norm EN 746-2 erfüllen. Diese beschreibt einen solchen Aufbau als „Festverdrahtetes System", bei dem alle Komponenten ohne zwischengeschaltete SPS fest miteinander verbunden sind. Die betriebliche Praxis zeigt durchaus, dass solche Konfigurationen sicher sind. Allerdings betrachtet diese Variante nicht die Verwendung einer übergeordneten Steuerung und deren Verdrahtung zu dem Feuerungsautomaten bezüglich der Diagnose im Fehlerfall. Ein weiterer Punkt ist, dass diese Variante nur wenig flexibel im Hinblick auf Änderungen oder die Umsetzung von neuen oder spezifischen Aufgaben ist. Gerade die mangelnde Flexibilität macht sowohl Anlagenbauern als auch Anlagenbetreibern zunehmend zu schaffen: Zum einen ist zu erwarten, dass die Schwankungen in der Zusammensetzung beim Energieträger Erdgas weiter zunehmen. Dies kann gerade für industrielle Brennersysteme im produzierenden Gewerbe und in der Industrie problematisch sein, da sich Schwankungen der Gasbeschaffenheit negativ auf Schadstoffemissionen, Produktqualität, Energieeffizienz und die Lebensdauer von Anlagen oder Komponenten auswirken können. Das allein erhöht bereits den Bedarf nach besser regelbaren Brennersystemen. Zum anderen kommen gesteigerte Anforderungen an die Prozessführung hinzu, wenn z. B. die Anlagen mit unterschiedlichen Temperaturen gefahren werden sollen und der generelle Bedarf der Anlagenbauer steigt, die Bediener- und Wartungsfreundlichkeit ihrer Anlagen zu verbessern.

SPS-basierte, integrierte Sicherheitslösung gemäß EN 746 und EN 62061

Als Alternative zu den klassischen Sicherheitssystemen bietet es sich an, die Safety-/Sicherheitsfunktionen in die

Gegenüberstellung SIL/PL-Bewertung
Safety- und Brenner-Norm: EN 62061 - EN 746-2

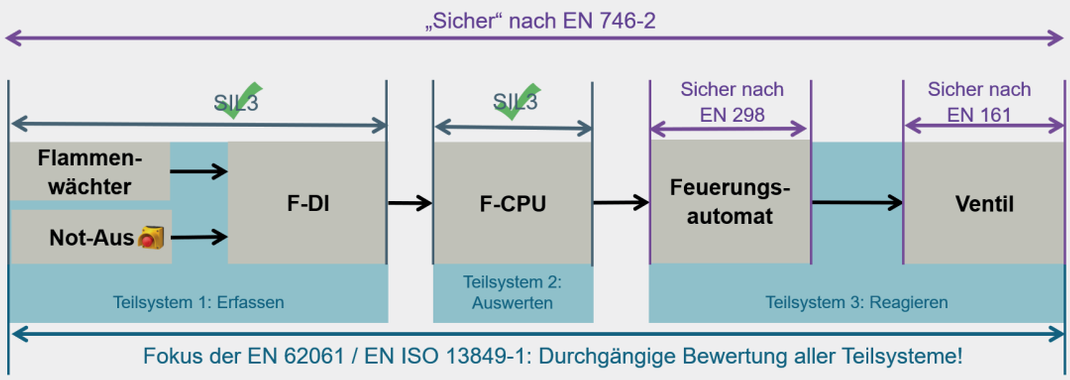

Bild 1: Sicherheitsbetrachtung bei konventionellen Schutzsystemen für Brenneranlagen (Quelle: Siemens AG)

fehlersichere Automatisierung/Steuerung der Anlage zu integrieren. In den allermeisten Fällen sind die Prozessanlagen bereits mit einer entsprechenden übergeordneten Steuerung ausgerüstet, welche Aktoren und Sensoren, wie z. B. Ventile, Druckschalter, Lüfter, sowie die Sicherheitseinrichtungen, wie z. B. einen Not-Halt-Schalter, adressiert. Eine solche SPS-basierte Lösung ist auch nach EN 746-2 zulässig, insofern das System durchgängig SIL3 erfüllt.

Wie eine solche Lösung aussehen kann, zeigt **Bild 2** anhand eines Schutzsystems bei einer Flammenüberwachung. In dieser Konfiguration überwacht der Flammenwächter per Sonde die Flamme und meldet den Zustand zweikanalig an fehlersichere Digitaleingänge (F-DI). Die fehlersichere Steuerung/SPS (F-CPU) wertet das Signal aus und steuert über das fehlersichere digitale Ausgabemodul (F-DO) das Sicherheitsabsperrventil, welches im Falle eines Flammenabrisses die Brennstoffzuführung unterbricht.

Gemäß der Gliederung einer Sicherheitsfunktion nach EN 62061 in die drei Teilsysteme Erfassen, Auswerten und Reagieren stellt sich das System so dar: Die Erfassung des Flammenzustandes geschieht durch die Kombination aus Flammenwächter und F-DI, die Auswertung übernimmt die F-CPU, die Reaktion findet im Zusammenspiel von F-DO und Ventil statt. Um die Sicherheit nach der EN 62061 oder der EN ISO 13849-1 bewerten zu können, muss dement-

Gegenüberstellung SIL/PL-Bewertung
Safety- und Brenner-Norm: EN 62061 - EN 746-2

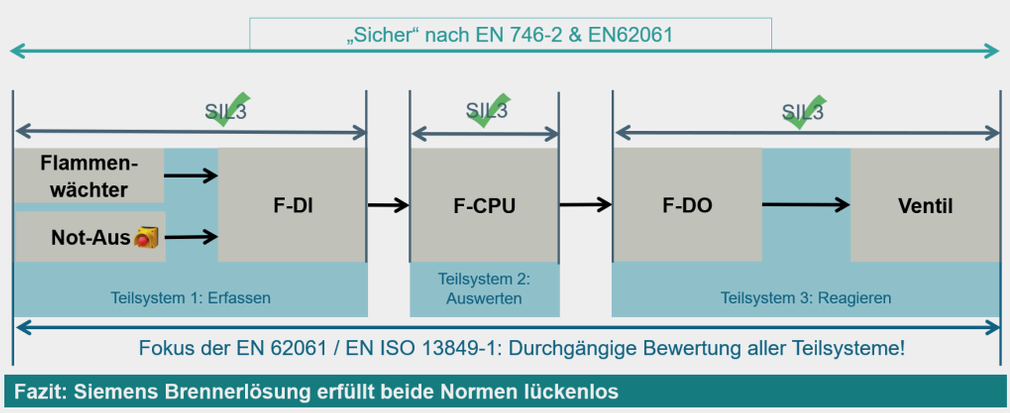

Bild 2: Bewertung einer SPS-basierten Brennerlösung gemäß EN 746 (Quelle: Siemens AG)

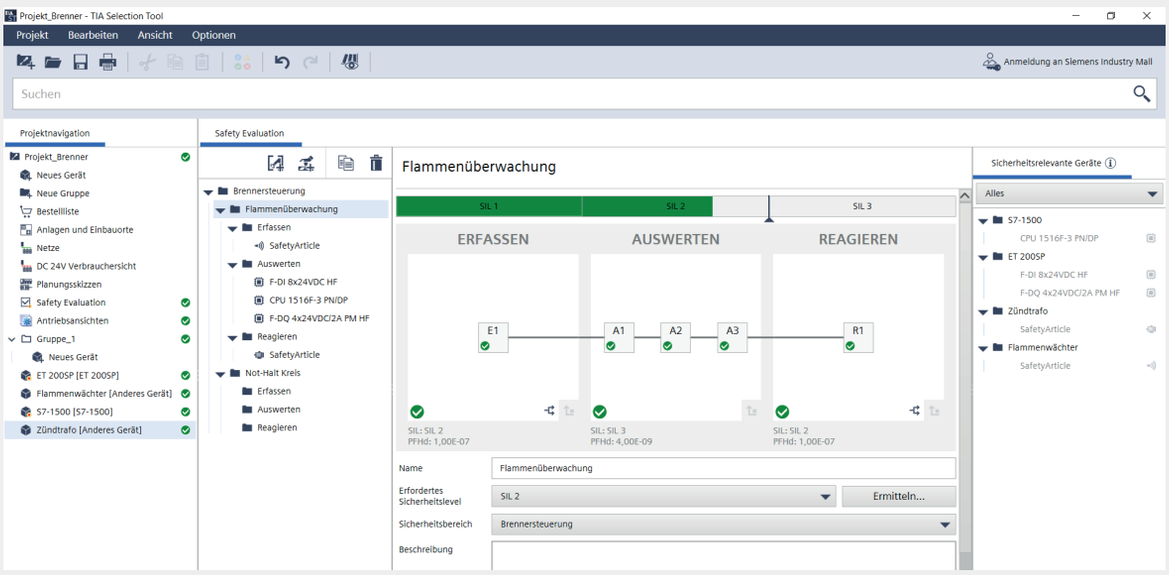

Bild 3: Bewertung einer Sicherheitsfunktion im TIA-Selection-Tool (Quelle: Siemens AG)

sprechend das gesamte System betrachtet werden. Dazu kann man nach Kapitel 5.7.2 Teil d) der EN 746-2 die Vorgaben der EN 62061 bzw. der EN ISO 13849-1 heranziehen.

Siemens unterstützt die darin geforderte Bewertung der Sicherheitsfunktionen des Gesamtsystems mit der Safety Evaluierungs-Funktion im **T**IA **S**election **T**ool (TST) (**www.siemens.de/safety-evaluation**) für die Normen IEC 62061 und ISO 13849-1. Dieses Werkzeug liefert als Ergebnis einen normenkonformen Bericht, der als Sicherheitsnachweis in die Maschinendokumentation integriert werden kann (**Bild 3**). Dadurch können Anlagenbauer einfach nachweisen, dass die SPS-basierte Lösung die EN 62061 erfüllt und damit auch die Anforderungen aus EN 746.

Industriegerechte Komponenten erleichtern den praktischen Einsatz

Bleibt jedoch die Frage, inwieweit sich solche SPS-basierten Lösungen in vorhandene Brennerkonzepte integrieren lassen. Gerade bei Durchlauföfen muss eine Vielzahl von Brennersteuerungen auf sehr beengtem Platz untergebracht werden, sodass die Komponenten der SPS-basierten Lösung entsprechend kompakt sein müssen.

Aufbau Brennersteuerung
Basierend auf SIMATIC S7-1500 und ET 200SP

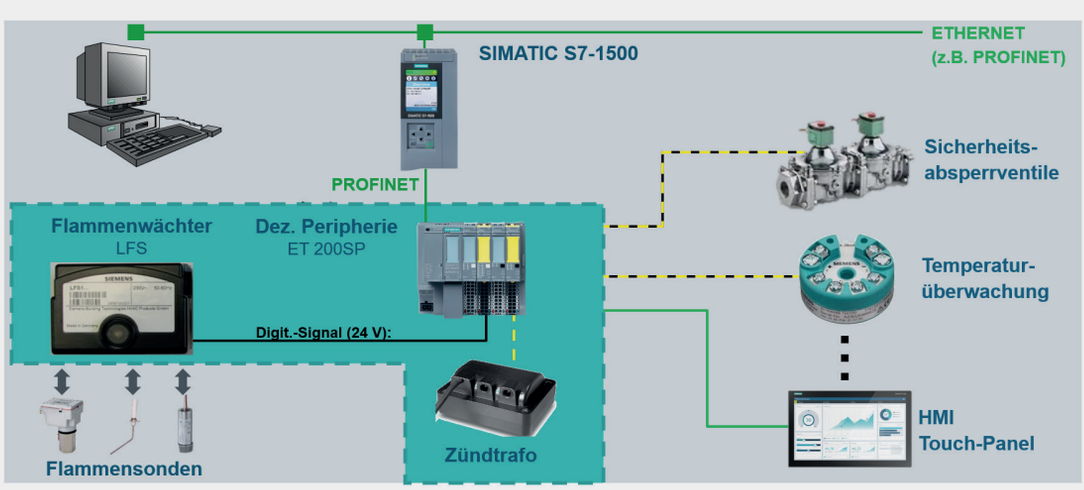

Bild 4: Sicherheitsgerechte Automatisierung einer Brennersteuerung auf SPS-Basis (Quelle: Siemens AG)

Durch die Auswahl geeigneter Komponenten lassen sich diese Herausforderungen jedoch meistern, wie **Bild 4** zeigt. Anstatt der üblichen Feuerungsautomaten, die jeweils nur einen Brennerkopf steuern und überwachen, wird in diesem Beispiel eine dezentrale Simatic ET 200SP-Station zusammen mit entsprechend zertifizierten Flammenwächtern und Zündtransformatoren eingesetzt. Die dezentralen SIMATIC ET 200SP Stationen sind in vielen Varianten verfügbar und benötigen nicht mehr Platz als ein konventioneller Feuerungsautomat, bieten dabei jedoch mehr Funktionalität, da noch weitere Komponenten einfach in die Automatisierung eingebunden werden können. Beispiele sind Sensoren für die Druck- und Temperaturüberwachung. So können mehrere Feuerungszonen und Brenner über eine ET 200SP Station angesteuert werden, was den Hardwareaufwand reduziert.

Weitere Vorteile bringt ein HMI-Bedienpanel. Der Anlagenfahrer kann die Anlage damit lokal überwachen. Aufgrund der durchgängigen Sicherheitslösung ist eine komplette, detaillierte Systemdiagnose angefangen von der Verdrahtung bis hin zu Programmabläufen möglich. Dies unterstützt eine effiziente Wartung und Fehlerbehebung. Die Bedienerfreundlichkeit und die Flexibilität steigen nicht nur durch grafische Oberflächen, sondern auch durch die Möglichkeit Prozessparameter komfortabel und fehlersicher (bis SIL 3) an die fehlersichere SIMATIC-Steuerung über das HMI zu übermitteln, um zum Beispiel eine gewünschte Prozessvariante einzustellen.

Das gesamte System wird durch eine fehlersichere Steuerung gesteuert.

Flexibel durch Software

Um die von der EN 746-2 geforderten Sicherheitsfunktionen in diesem System zu implementieren, stellt Siemens dem Anwender eine Bausteinbibliothek für die Projektierung im Engineering Tool (STEP 7 Professional TIA Portal) zur Verfügung. Diese kostenlose Bausteinbibliothek für Brenner enthält mehrere Bausteine für Funktionen wie Steuerung und Überwachung eines Gas- oder Ölbrenners, die Durchführung von Gasdichtetests und weitere Brenner-Funktionen (**support.industry.siemens.com**, Beitrags-ID 109477036). Die einzelnen Funktionen sind modular aufgebaut und können nach Bedarf verschaltet werden. Auf diese Weise können die Sicherheitsfunktionen für Brenner einfach in der gewohnten Projektierungsumgebung für das Siemens-Automatisierungssystem erstellt werden, wodurch der Engineeringaufwand reduziert und der Umstieg auf eine durchgängige SPS-basierte Sicherheitslösung erleichtert wird.

Ein weiterer Vorteil für den Anlagenbauer ist, dass weitere Funktionen zu einem späteren Zeitpunkt nachgerüstet werden können und kundenspezifische Funktionen umgesetzt werden können. Auch bei der Regelqualität bringt die SPS-basierte Lösung deutliche Vorteile bei der Realisierung folgender Brennerfunktionen:

- Realisierung eines elektronischen Verbundes selbst, z. B. über ein fest definiertes Luft/Brennstoff-Verhältnis
- Temperaturregelung
- Sauerstoffregelung anhand des Restsauerstoffes in den Abgasen.

Insgesamt können dadurch die Brenner besser mit schwankenden Gasbeschaffenheiten umgehen, sodass der Anlagenbetreiber nicht nur zusätzliche Emissionen und Qualitätseinbußen durch Prozessschwankungen vermeidet, sondern auch die Energieeffizienz seiner Anlagen optimieren kann.

Eine SPS-basierte Sicherheitslösung bietet in vielen Fällen Vorteile, da sie oft ohnehin vorhandene Systeme nutzt, wie z. B. eine übergeordnete Steuerung. Durch den Einsatz einer geeigneten Systemkonfiguration können all diese Vorteile genutzt und die lückenlose Anlagensicherheit gewährleistet werden – auch entsprechend der weltweit gültigen Norm ISO 13577.

AUTOREN

Ulf Weißhuhn
Siemens AG
Digital Industries
Nürnberg
ulf.weisshuhn@siemens.com

Hermann Wübbels
Siemens AG
Digital Industries
Köln
hermann.wuebbels@siemens.com