



Kompromisslose Sicherheit

Anwender zögern bei der Einführung von Leitsystemen mit integrierter Sicherheitstechnik

Ein System für alles oder strikte Trennung? Die Stimmung in der Sicherheitstechnik ist nicht leicht wiederzugeben. Während die einen Anwender auf autarke Systeme setzen, vertrauen andere auf Prozessleitsysteme mit integrierten Sicherheitsfunktionen.

DIPL.-ING. SABINE MÜHLENKAMP

Bei der Sicherheitstechnik kennen die Automatisierer keine Kompromisse, bewährte Systeme ändern die Prozessleittechniker nur in dringenden Fällen. Mittlerweile erweitert sich jedoch das Spektrum. Viele Industrieanwender beobachten und diskutieren besonders Leitsysteme mit integrierten Sicherheitsfunktionen, deren Integration unterschiedlich weit fortgeschritten ist. Während bei einem Hersteller ein einziger Controller sowohl nicht-sicherheitsrelevante wie sicherheitsgerichtete Aufgaben übernimmt, verwenden andere für diese Aufgaben unterschiedliche Baugruppen, die jedoch in einem Leitsystem integriert sind (siehe Tabelle). Ein anderer Weg ist die strikte – also auch räumliche – Trennung der Systeme. Ebenfalls realistisch, wenn auch in der Prozessindustrie noch in den Anfängen, ist der Einsatz eines Feldbussystems mit sicherheitsgerichteten Funktionen, z.B. Profisafe oder FF-SIF.

Kompromisslose Sicherheit wünscht sich jeder Anlagenbetreiber. Aber nicht überall ist es gewünscht Prozessleitsystem und sicherheitsgerichtete Funktionen zu koppeln. Bei BP in Gelsenkirchen trennt man zwischen Beidem.

Leichtere Handhabung

Für Siemens hält der Trend zur integrierten Lösung unvermindert an. Treiber hierbei ist nach Aussage von Thomas Bartsch, Marketing Manager Simatic PCS7&Process Safety der Siemens-Division Industry Automation, der heutige Kostendruck, der sich sowohl bei der Planung als auch im Betrieb der Anlage zeigt. Hierbei gilt es, verschiedene Stufen der Integration zu unterscheiden. „Die Integration des Sicherheitssystems in das Engineering des Leitsystems ist heute als Standard zu betrachten“, so Bartsch. Siemens ermöglicht den Ablauf sicherer und nicht sicherer Funktionen in einem Controller, was insbesondere bei kleineren Applikationen ein Vorteil ist.

Auch die Zunahme von Komplexitäten der Anlagen mündet laut ABB zunehmend in der Forderung eines in das Prozessleitsystem vollständig integrierten Sicherheitssystems. Die Abbildung von Prozessabläufen und die Bedienung wird einfacher und der Engineeringaufwand geringer. „Sei es das Anfahren, Produktionsänderungen oder Wartungsarbeiten – die Sicherheitsparameter lassen sich automatisch an die verschiedenen Automatisierungsphasen anpassen. Die Automatisierungsanwendung kann Parameter in der Sicherheitsanwendung in Echtzeit lesen und so zur optimierten Steuerung der Sicherheitsabstände beitragen“, erklärt Gregor Kilian, Manager Sales & Marketing Control Systems, ABB Automation, und nennt als Beispiel die dynamische Anpassung an eine oder mehrere Sicherheitsgrenzen. Auch lassen sich die gleichen Geräte sowohl in Sicherheits- als auch in einfachen Automatisierungsanwendungen verwenden.

„Der Anwender hält sich in der ihm bekannten Software-Umgebung auf, sodass er auch bei der Konfiguration von sicherheitsgerichteten Funktionen auf sein Wissen aus der PLS-Konfiguration zurückgreifen kann“, nennt Fatih Denizer, Sales Support Engineer bei Process Systems & Solutions, Emerson Process Management, einen weiteren Vorteil.

Autarke Systeme

Das Interesse an den integrierten Systemen ist auch bei den Anwendern vorhanden.

Die Autorin arbeitet als freie Redakteurin bei PROCESS.
E-Mail-Kontakt: info@muehlenkamp.net



Bild: BP



„Mittlerweile ist höchste Verfügbarkeit ohne Kompromisse hinsichtlich der Sicherheit gefordert – das kann nicht nur mit Redundanzen erzielt werden.“

Rolf Hafner, Hima Paul Hildebrandt



„Der Trend zur integrierten Lösung hält an. Die Integration des Sicherheitssystems in das Engineering des Leitsystems ist heute als Standard zu betrachten.“

Thomas Bartsch, Siemens-Division Industry Automation

Dennoch lassen sich nicht alle Bedenken zerstreuen. So ist eine Sorge der Betreiber, dass der Servicetechniker eventuell nicht genau zwischen sicherheitsgerichtetem und nicht gefährdetem Bereich unterscheiden kann. Zudem bewegt sich ein Techniker bei der Wartung immer in einem sicherheitsrelevanten Aufgabengebiet. Ein anderer Weg liegt daher in einem autarken System, wie es Hima anbietet. Deren Sicherheitssysteme erfüllen uneingeschränkt die für die Prozesstechnik höchste Sicherheitsstufe SIL 3. „Unser Engagement zielt darauf ab, Lösungen zu entwickeln, die maximale Sicherheit und maximale Verfügbarkeit bieten“, erklärt Rolf Hafner, Leiter Produktmanagement bei Hima Paul Hildebrandt. Die Hima-Sicherheitstechnik lässt sich in eine Automatisierungslösung integrieren, sie bleibt aber stets ein autarkes System, das frei ist von jeglicher Rückwirkung aus den allgemeinen Betriebseinrichtung und ist somit eine vollwertige zusätzliche Schutzebene im Rahmen der Layer of Protection Analysis.

Für Hafner beruht Anlagensicherheit auf der Grundlage von verschiedenen Schutzebenen, den so genannten „Independent Protection Layers“. Das beginnt bei organisatorischen Maßnahmen (z.B. Notfallmanage-

ment), über bauliche Maßnahmen (z.B. Schutzwand), über den Einsatz von Sicherheitssystemen (SSPS) und endet (meist) mit einem Bedien- und Beobachtungssystem (z.B. Prozessleitsystem). Die IEC 61511 fordert eine ausreichende Unabhängigkeit der genannten Schutzebenen untereinander. Der Verzicht auf eine oder mehrere Schutzebene(n) erhöht grundsätzlich das Risiko. Daher gewährleistet seiner Meinung nach eine strikte Trennung zwischen dem Leitsystem und dem Sicherheitssystem den Erhalt der Schutzebenen und regelt nebenbei die strikte Zuständigkeit für das Sicherheitssystem. „Trennung bringt Rechtssicherheit, denn sie entspricht dem Status „Good Engineering Practice“, so Hafner. Für ihn ist die optimale Lösung hinsichtlich der Wirksamkeit der Schutzschichten dann gegeben, wenn Leitsystem und Sicherheitssystem sogar von unterschiedlichen Firmen und somit auf unterschiedlichen Plattformen entwickelt wurden.

„Eine Integration sicherheitsgerichteter Funktionen in das Prozessleitsystem ist aus Gründen der zentralen Bedienung und Handhabung von Interesse“, erklärt Andreas Meyne, Safety Solutions Consultant bei Honeywell Process Solutions. Allerdings setzt man auch bei Honeywell auf die Entwicklung separater

PROCESS PLUS

- Magazin** • In PROCESS 12 beschäftigt sich ein großes Special mit dem Thema Ex-Schutz.
- Online** • Auf process.de finden Sie ein Whitepaper zum Thema Gaswarngeräte mit SIL-Standard. Mehr zum Beitrag über InfoClick **2316798**
- Events** • Die Namur-Hauptversammlung zum Thema findet am 11. und 12.11.2010 in Bad Neuenahr statt. Besuchen Sie auch den SIL-Tag bei der Dechema am 25.11.2010.
- Services** • Details zur NE 97 gibt es auf der Seite der Namur. Die Fieldbus Foundation bietet einen Download zu FF-SIF. Auch der ARZ hält ein Whitepaper zum Thema bereit.

und für diese Aufgabe speziell ausgelegter Hard- und Softwaremodule durch spezifische Entwicklungsbereiche. „Dies schließt das Risiko des 'common cause failures' aus“, verweist Meyne. „Mögliche Fehler oder Störungen in Teilen des Basisleitsystems beeinflussen die Sicherheitsfunktionen nicht.“

Aus der Praxis

In der Praxis wird der Einsatz ganz unterschiedlich gehandhabt. So wendet die BASF in Ludwigshafen derzeit integrierte Sicherheitssysteme im Rahmen von Pilotprojekten an. Das Ziel ist es, Erfahrungen zu sammeln und sie mit bewährten Lösungen zu vergleichen. Derzeit nutzt das Unternehmen jedoch separate Sicherheitssteuerungen, die unabhängig vom PLS sind. Der Grund liegt vor allem darin, dass integrierte Sicherheitssysteme heute im (Sicherheits-)Engineering noch sehr komplex sind. Das stellt im gesamten

Lebenszyklus hohe Anforderungen an die Mitarbeiter in der Projektierung und Wartung. Auch das Thema Verfügbarkeit sieht man kritisch: Bedien- oder Hantierungsfehler im nicht sicherheitsrelevanten Teil eines solchen Systems – z.B. bei Wartung und/oder beim Laden von Änderungen – können zu ungewollten Abschaltungen der Schutzfunktionen führen (z.B. aufgrund einer Hardwareänderung in RUN). Insbesondere bei umfangreichen Installationen mit wöchentlichen Änderungen im nicht sicherheitsgerichteten Teil, steigt das Risiko ungewollter Abschaltungen aufgrund möglicher Hantierungsfehler.

Bei BP in Gelsenkirchen mit vielen Anlagen, die unter die Störfallverordnung §4 fallen, trennt man streng zwischen Prozessleitsystem und einem System für sicherheitsgerichtete Funktionen. „Zum einen gibt es hier eine ganz klare Verordnung, die wir

selbstverständlich einhalten müssen, zum anderen ist das Handling einfach leichter“, erklärt Björg Otte, zuständig für EMR Instandhaltung Mineralöl Horst am Standort Gelsenkirchen. Derzeit werden schon Überwachungsfunktionen an ein Leitsystem übertragen. Dabei vertraut Otte den Leitsystemen und hält es durchaus für denkbar, dass man Anwendungen unter SIL1 in das Leitsystem integriert. „Die Leitsysteme verfügen heute über eine so hohe Verfügbarkeit, dass ich keine Bedenken habe.“ Dennoch fehlt es seiner Meinung nach an Erfahrungen und einer gesicherten Datenbasis für Sicherheitsberechnungen, um integrierte Systeme einzusetzen.

Evonik setzt sowohl Leitsysteme mit integrierten Sicherheitssteuerungen unterschiedlicher Lieferanten, als auch Leitsysteme mit separaten sicherheitsgerichteten Steuerungen weltweit ein. Michael Kartenberg, Leiter

Wie weit sind die Unternehmen in Sachen Integration?

Unternehmen	Status quo der Integration	Wie funktioniert es?
ABB	Das System 800xA bietet ein komplettes Safety Instrumented System (SIS). Dazu gehören eine einheitliche, High-Integrity-Systemarchitektur, eine umfassende SIL-kompatible SIS-Lösung, eine Engineering-Umgebung für den gesamten Safety-Lebenszyklus sowie personalisierte Arbeitsplätze für das gesamte Safety-Personal, ein Information-Management für Safety und die Optimierung von Safety-Assets sowie Safety-Services.	Der AC 800M High Integrity Controller bietet eine SIL-3-TÜV zertifizierte Automatisierungsumgebung, die Safety- und die geschäftskritische Prozessautomatisierungen innerhalb eines Controllers kombiniert, ohne dabei die Integrität der Sicherheit zu gefährden. Der AC 800M HI Controller wird durch eine Kombination des Prozessormoduls und des Co-Prozessors realisiert. Die SIL-Auswahl aktiviert die entsprechenden Einschränkungen und Begrenzungen, sodass zum Beispiel nur als SIL gekennzeichnete Elemente in SIL-Applikationen verwendet werden.
Emerson	Das DeltaV SIS ist soweit in das DeltaV Leitsystem integriert, dass keine zusätzlichen Schnittstellen benötigt werden. Die Uhrzeit zwischen PLS und SIS ist synchron, und Ereignisse beider Systeme werden gemeinsam erfasst.	Alle sicherheitsgerichteten Funktionen werden mit entsprechend zertifizierten Funktionsbausteinen erstellt und in den SIS Logic Solvern abgearbeitet, so dass eine Trennung zwischen PLS und SIS gemäß IEC 61511 gewährleistet ist. Durch die Integration werden gemeinsame Engineering-Werkzeuge für PLS und SIS bereitgestellt.
Honeywell	Das System Experion PKS koppelt die eigene Sicherheitssteuerung, den Safety Manager, in das leitsystemeigene FTE-Netzwerk (Fehlertolerantes Ethernet) an. Die Integration bezieht sich allerdings lediglich auf die Einbindung in eine zentrale Datenbasis und damit die gemeinsame Anzeige- und Bedienebene.	Die eigentlichen Sicherheitsfunktionen sind sowohl aus Sicht der Hardware als auch der Funktionssoftware separiert und laufen auf einer eigenen, für diese Sicherheitsaufgaben zertifizierten CPU. Diese Separierung gilt konsequent auch für die Entwicklung der jeweiligen Komponenten einschließlich der Ein-/Ausgangsmodule und schließt somit gemeinsame Fehlentwicklungen aus (common cause failures). Als Teil der Integration ist es aber möglich, Daten der Sicherheitssteuerung direkt über einen Peer-to-peer-Mechanismus in den Messstellen der prozessnahen Komponenten des Basissystems zu verwenden.
Siemens	Mit Safety Integrated for Process Automation verfügt Simatic PCS 7 über ein umfassendes Produktspektrum für sicherheitsgerichtete Anwendungen. Hardware wie Software sind in das Leitsystem integriert und bis einschließlich SIL 3 einsetzbar. Engineering, Alarmierung und Bedienung sind integraler Bestandteil des Systems.	Die sicheren Simatic S7-400F/FH Controller können sowohl für sicherheitsgerichtete Funktionen als auch für Regelungs- und Steuerungsaufgaben eingesetzt werden, wobei die sicheren Funktionen in einer eigenen, getrennten Task unabhängig von den Regelungs- und Steuerungsaufgaben ablaufen. Für den sicherheitsgerichteten Einsatz verfügt das System über eine Bibliothek mit sicheren Funktionsbausteinen. Auf der EA-Ebene kommen speziell entwickelte sichere EA-Baugruppen zum Einsatz. Über FMR (Flexible Modular Redundancy) ist ein modularer und flexibler Aufbau mit unterschiedlichen Redundanzen in allen Ebenen möglich.
Yokogawa	Die sicherheitsgerichteten Funktionen sind integriert aber separat im Produktionsleitsystem. Die sicherheitsgerichteten Steuerungen übernehmen die Sicherheitsfunktionen und die prozessnahen Komponenten (PNK) die Steuer- und Regelungsfunktionen, und zwar unabhängig voneinander. Die Integration ist auf die Informationstransparenz begrenzt.	Die Sicherheitskommunikation zwischen den sicherheitsgerichteten Komponenten über das Vnet/IP-Netzwerk ist so aufgebaut, dass sie logisch von der Prozesskommunikation unabhängig ist und dadurch von der normalen Kommunikation geschützt ist. Sie unterstützt auch einen Broadcast-Modus für die gleichzeitige Kommunikation zu allen sicherheitsgerichteten Steuerungen. Sie verfügt über eine duale Architektur, die auf einer separaten Plattform zur PNK bearbeitet wird und ist modular aufgebaut. Die Module selbst können in einer zweikanalig redundanten Konfiguration installiert werden. Diese wird durch die S-SPS gesteuert und ist für den Anwender völlig transparent.



„Ich bin überzeugt davon, dass Profisafe bzw. FF-SIF, sollte diese Technologie erst einmal in einigen Anlagen sicher laufen, ein Selbstläufer wird.“

Thomas Kasten, Pepperl+Fuchs

Automation & Process Management bei Evonik sieht das Thema pragmatisch „Unsere Untersuchungen des letzten Jahres zu dieser Thematik zeigen, dass die projekt-/einsatzspezifischen Randbedingungen den entscheidenden Ausschlag für die eine oder die andere Variante ergeben. Eine von diesen Randbedingungen unabhängige Empfehlung hat sich für uns nicht ergeben.“

Feldbus mit integrierter Sicherheit

Prinzipiell kann auch ein Feldbus sicherheitsgerichtete Funktionen übernehmen. Wie dieser auszusehen hat, wurde schon 1993 in der Namur-Empfehlung NE 97 ‚Feldbusse für Sicherheitsaufgaben‘ beschrieben. Dennoch üben die Anwender vorsichtige Zurückhaltung, wobei an der prinzipiellen Eignung kaum jemand zweifelt. „Die Anwender fürchten bei einem integrierten System bei einem Netzwerkausfall sofort einen Totalausfall. Das sind aber Anfangsbedenken gegenüber einer neuen Technologie“, ist der Vorsitzende des deutschen Foundation Fieldbus Komitees, Thomas Kasten von Pepperl+Fuchs, überzeugt. „Schließlich ist die Anlage so aufgebaut, dass sie dann wie bei einem konventionellen Sicherheitssystem in den sicheren Zustand fährt.“

Die BASF steht Profisafe bzw. FF-SIF abgeschlossen gegenüber und erwartet keine sicherheitstechnischen Probleme. Allerdings müsse die zugrunde liegende Feldbustechnologie erst einmal vollständig ausgereift und ausreichend robust sein. Hier stehe neben der Sicherheit insbesondere eine stabile Installation und damit eine hohe Anlagenverfügbarkeit an erster Stelle.

Bei Evonik steht man dagegen einem Einsatz im Feldbusbereich eher skeptisch gegenüber. „Unsere Philosophie ist die Benutzung betriebsbewährter Gerätetechnik im Feldbereich“, erklärt Kartenberg und meint damit eine Gerätetechnik, die sowohl in betrieblichen als auch in sicherheitsgerichteten Anwendungen einsetzbar ist. „Beim Einsatz von Profisafe bzw. FF-SIF würde unsere Philosophie durchbrochen, da aus unserer Sicht momentan die verfügbare Gerätetechnik (Sensorik/Aktorik mit zertifiziertem Proto-

kollstack) eine spezialisierte Technik darstellt“, so Kartenberg .

Dabei gibt es einige Pilotprojekte. So waren nach Aussage von Emerson die Rückmeldungen von den Betreibern der vier FF-SIF-Testanlagen (BP, Shell, Chevron und Saudi Aramco) so positiv, dass FF-SIF in Zukunft auch zum Einsatz kommen wird. Shell Project & Technology (früher Shell Global Solutions) und Saudi Aramco kündigten bereits eine Fortführung der Projekte an. Shell hat FF-SIF für das Niederlande Aardolie Maatschappij-Projekt in den Niederlanden spezifiziert. In Saudi Arabien soll Ende 2010 ein Initialprojekt in der Juaymant Gasanlage in Saudi Arabien starten. Waren damals noch Prototypen bei den Testanlagen eingebaut, fordern die Betreiber die Gerätehersteller nun auf, geeignete Feldgeräte auf den Markt zu bringen. „Ich bin überzeugt davon, dass Profisafe bzw. FF-SIF – sollte diese Technologie erst einmal in einigen Anlagen sicher laufen – ein Selbstläufer wird“, so Kasten und verweist auf die Treiber im Nahen Osten und Asien, wo derzeit ein Großteil der Neuanlagen mit Feldbussen ausgestattet werden.

Ausblick

Für welche Lösung sich der Anwender auch entscheidet: Zu den wichtigsten Trends gehört der Wunsch nach mehr Produktivität. „Nicht warten bis ein Gerät ausfällt, sondern die präventive Wartung soll den Ausfall verhindern“, so der Hima-Sicherheitsexperte Hafner. Dazu müssen zusätzliche Informationen von Feldgeräten für den Operator sinnvoll aufbereitet werden. Die Aufgabe der Sicherheitssysteme wird es dabei sein, diese Informationen zu unterstützen.

Schließlich ist die Aufgabe der Sicherheitssysteme nicht mit der Erfüllung der sicheren Abschaltung erledigt. „Mittlerweile ist höchste Verfügbarkeit ohne Kompromisse hinsichtlich der Sicherheit gefordert, das kann nicht nur mit Redundanzen erzielt werden“, macht Hafner deutlich. So muss seiner Meinung nach ein Betriebssystem-Upgrade oder die Durchführung einer Wiederholungsprüfung auch ohne Anlagenstillstand möglich sein. ●