



Uwe Prüßmeier

E/A-Baukasten sicher erweitert

Basierend auf dem Profisafe-Standard hat Beckhoff eine eigene Lösung für die sicherheitsgerichtete Automation entwickelt. Bei einfachen Anforderungen kommt dieses Konzept ohne eine spezielle Sicherheitssteuerung aus und auch der Wechsel auf andere Bussysteme ist prinzipiell möglich.

Die Verdrahtung von Not-Aus-Schaltern, Lichtschranken und weiteren Komponenten zur Gewährleistung der Maschinensicherheit beansprucht inzwischen einen großen Teil des in den Kabelkanälen und Schaltschränken zur Verfügung stehenden Platzes. Platz, der sich sparen lässt, wenn auch zur Übertragung der sicherheitsrelevanten Signale die Vorteile der Feldbus-Technologie genutzt werden. Technisch ist das schon lange möglich. Bis vor Kurzem fehlte allerdings eine herstellerübergreifende offene Schnittstelle mit einem Zertifikat, das die ausreichende Sicherheit für ein System garantiert, welches auf nur einem Buskabel die Übertragung von Standard- und sicherheitsgerichteten Signalen

realisiert. Mit Profisafe der Profibus Nutzerorganisation hat ein solches Konzept mittlerweile Marktreife erlangt. Beckhoff hat dieses Konzept aufgegriffen und basierend auf dem Profisafe-Protokoll eine Lösung entwickelt, bei der sicherheitstechnische Funktionen in die E/A-Klemmen integriert sind und bei der sich die „sicheren“ Signale mit den Standard-Signalen beliebig mischen lassen. Das spart Projektierungsaufwand, Montage und Material. Die Wartung wird durch schnellere Diagnose und leichten Austausch nur weniger Komponenten vereinfacht.

Was steckt nun im Detail hinter der Twinsafe-Lösung?

In den Twinsafe-Busklemmen sind lediglich drei Grundfunktionalitäten

enthalten: digitale Eingänge (KL19xx), digitale Ausgänge (KL29xx) und die Verknüpfungseinheit (KL6900). Damit sind alle gängigen Sicherheits-Sensoren und -Aktoren anschließbar: zum Beispiel Not-Aus-Taster, Sicherheitsschloss, Positionsschalter, Zweihandschalter, Seilzugschalter, Lichtvorhang, Lichtschranke oder Laserscanner sowie Aktoren wie Schütze, Schutztürschalter mit Zuhaltung, Signalleuchten oder Servoverstärker.

In kleinen bis mittleren Anwendungen lassen sich die sicheren Ein- und Ausgänge an einer „nicht sicheren“ Steuerung allein über die Logik-Busklemme KL6900 betreiben. Letztere fungiert als Verknüpfungseinheit zwischen den Sicherheits-Eingangs- und Ausgangsklem-

(Bilder: Beckhoff)

men. Die hierzu notwendigen logischen Sicherheitsfunktionen sind als Funktionsbaustein implementiert und werden anwendungsspezifisch parametrierbar. Die Aufgaben einer kleinen Fail-Safe-SPS sind damit bei kleinen Aufbauten innerhalb des Busklemmensystems durchführbar. Der zusätzliche Aufwand für die Schnittstelle zur übergeordneten Steuerung entfällt, alle Zustände der „sicheren Steuerung“ stehen allgemein zur Verfügung. Diese Sicherheitslösung rein über die Verknüpfungseinheit ist geeignet für Anwendungen bis SIL3 (Safety Integrity Level) nach IEC 61508 beziehungsweise EN 954 Kat. 4 und DIN V 19251 AK6. Als übergeordnete Steuerung kann eine beliebige SPS, ein Embedded-PC wie der Beckhoff-eigene CX1000 beziehungsweise ein entsprechender Busklemmen-Controller fungieren.

Mehr als ein Relais, weniger als eine sichere SPS

Die Verwendung der KL6900-Verknüpfungseinheit ist auf ein Maximum von insgesamt 64 Kanäle begrenzt, um die Kosten in kleinen und einfachen dezentralen Anwendungen gering zu halten. Durch die Kombination mehrerer dieser Logik-Busklemmen kann die Anzahl der Kanäle auf

1024 erhöht werden. Komplexe Signalverarbeitung und Reaktionszeiten unter 50 ms bleiben Aufgaben, die nach wie vor eine sichere SPS erfordern. Für diese Applikationen ist prinzipiell jede Profisafe-kompatible Sicherheitssteuerung einsetzbar. Da eine solche Komponente im Produktprogramm von Beckhoff bis dato fehlt, ist in einem weiteren Schritt die Entwicklung einer sicheren SPS vorgesehen. Die angestrebte Leistungsgrenze dieses Systems liegt bei einer Reaktionszeit von 2 ms und einer Verknüpfungszeit von 100 µs für 1 kbyte Befehle. Die sichere SPS wird es zum einen als Piggyback zum Aufstecken auf eine PC-Feldbus-Karte oder als Feldbus-Master in der Embedded-PC Familie CX1000 geben, jeweils programmierbar nach IEC 61131-3. Die Verbindung zum „nicht sicheren“ Teil der SPS wird dabei automatisch vom System durchgeführt. Für den Anwender sind die sicheren Signale nur „sichere Variablen“, die an jeder Stelle im Programm eingebunden werden können.

Die Twinsafe-Logik wird einfach über den Buskoppler oder den Feldbus parametrierbar. Als Werkzeug steht für den

PC der Twincat-System-Manager zur Verfügung. Unabhängig von der Twincat-Automatisierungssoftware lässt sich die Twinsafe-Verknüpfungseinheit mittels einer speziellen Konfigurationssoftware auch über den Buskoppler parametrieren. Die einmal gewählten Parameter werden spannungsausfall- und verfälschungssicher in der Klemme gespeichert. Der Zugriff ist passwortgeschützt. Der Betrieb ist nur im gesicherten und nicht manipulierten Zustand möglich.

Nicht auf Profibus beschränkt

Die von Profisafe genutzten Mechanismen sichern die Daten in einem Datenrahmen vor möglichen Einflüssen der Übertragungsstrecke. Diese Strecke kann neben Profibus auch jedes beliebige andere Übertragungssystem sein. Aus der Sicht eines Bussystems ist Profisafe ein kleiner Datenblock, der zusammenhängend und fehlerfrei transportiert werden muss – also keine besonders schwierige Aufgabe für einen Feldbus.

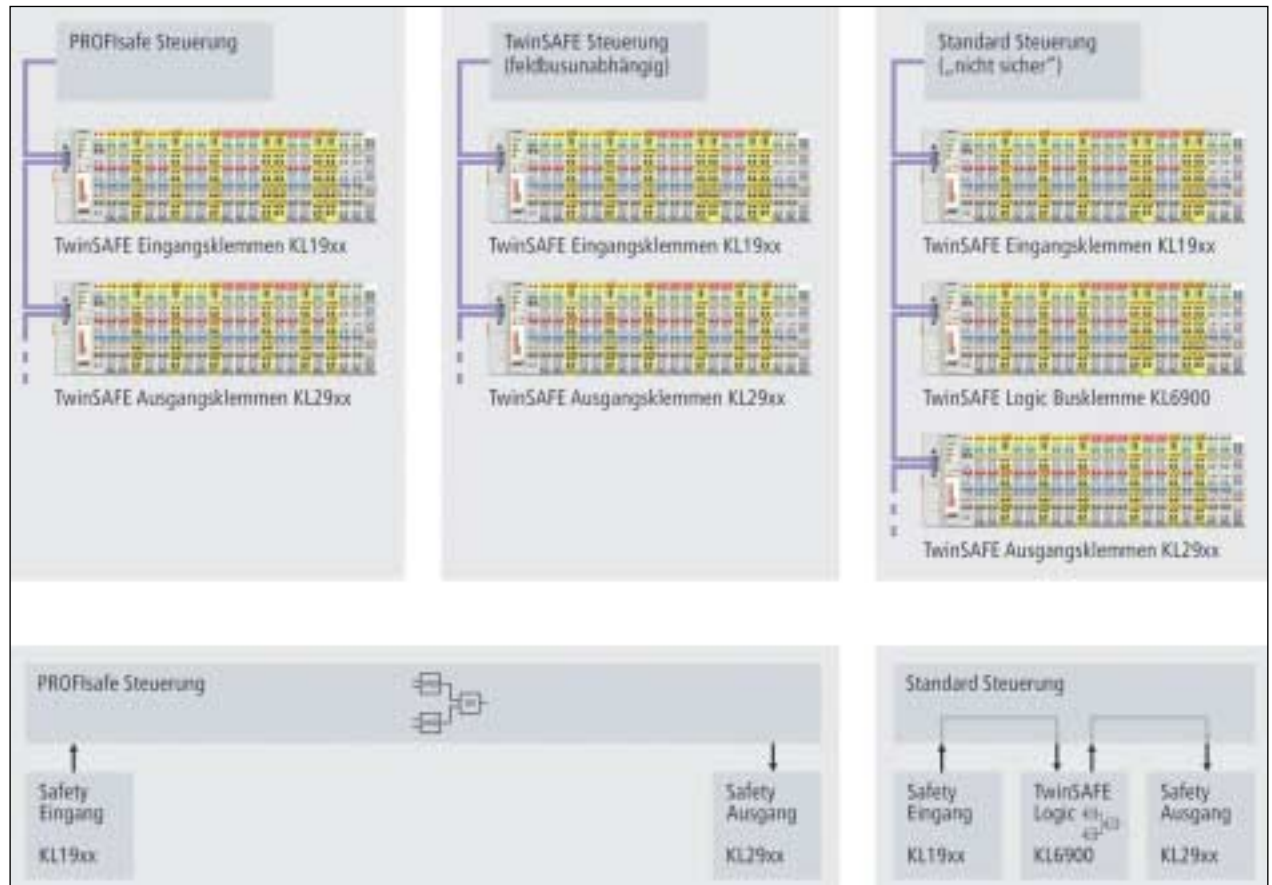
DAS PROFISAFE-KONZEPT

Die Profibus Nutzerorganisation (PNO) hat mit Profisafe ein „Profil“ zur sicheren Datenübertragung erstellt, das den Betrieb von Sicherheitsgeräten im Profibus-Netzwerk ermöglicht. Hierzu sind keine Veränderungen an der RS-485-Busleitung oder der Verdrahtung notwendig; es wird nur ein Feldbus-System für sicherheitsgerichtete und nicht-sicherheitsgerichtete Automatisierungsaufgaben implementiert. Profisafe ist für Aufgaben bis SIL3 IEC 61508, Kat. 4 EN 954 oder DIN V 19251 AK 6 einsetzbar. Zur Sicherung der Daten wurden Mechanismen gegen folgende Fehlerarten geschaffen: Wiederholung, Verlust, Einfügung, falsche Abfolge, Verfälschung der Nutzdaten, Verzögerung, Kopplung sicherheitsrelevanter und nicht-sicherheitsrelevanter Daten und Falschadressierung.

Profisafe verfügt über eine fortlaufende Nummerierung der Sicherheitstelegramme. Die Kommunikation wird im Master und im Slave zeitüberwacht und passwortgeschützt. Zur Sicherung der Datenintegrität wird eine 16/32 bit CRC (Cyclic Redundancy Check) verwendet. Pro Telegramm können maximal 12 byte (bei 16 bit CRC) beziehungsweise 122 byte (bei 32 bit CRC) fehlersichere Daten übertragen werden.

Der Profisafe-Teilnehmer überträgt in dem gesicherten Telegramm nicht nur seine Nutzdaten sondern auch ein Status-/Control-Byte. Mit dem Lebenszähler (Sequenz Number) wird der Zustand des Kommunikationspartners und der Übertragungsstrecke bei jedem Telegramm überprüft.

Einsatzmöglichkeit der Twinsafe-Busklemmen an einer Profisafe-kompatiblen Steuerung oder mit der Twin-safe-Logic-Busklemme an einer (nicht sicheren) Standard-Steuerung.



Mit der Realisierung der sicheren Verpackung der Daten in einer Busklemme stehen die gesicherten Daten prinzipiell für jeden Feldbus zur Verfügung. Einzige Voraussetzung ist das Vorhandensein eines entsprechenden Buskopplers für das Bussystem. Damit besteht auch die Möglichkeit, die Profisafe-Daten über

mehrere unterschiedliche Bussysteme zur gleichen Zeit zu übertragen und „Sichere Daten“ auf diese Weise über die Grenzen unterschiedlicher Steuerungen und Systeme hinweg auszutauschen. Die sicheren Daten können „Feldbus-unabhängig“ über den jeweiligen Bus eingesammelt werden. Eine gesonderte Verdrahtung eines spe-

ziellen Sicherheitsbusses entfällt.

In der Praxis kommt diese Art von „multikulturellen Feldbus-Anschaltung“ häufiger zum Einsatz. Beispielsweise setzt Müller Weingarten bei seinen hydraulischen Tryout-Multicurve-Pressen den Lightbus zur Kommunikation zwischen Rechner und Sensorik, Sercos Interface für die elektrischen Antriebe und Profibus-DP für die Ankopplung der übergeordneten Anlagenteile ein.

Die Markteinführung der sicheren Busklemmen ist für das vierte Quartal geplant, die Logik-Busklemme wird voraussichtlich im ersten Quartal 2004 in den Markt eingeführt. *gh*

Nähere Informationen:
info@beckhoff.de

STANDARD- UND SICHERHEITS-I/OS IN EINEM SYSTEM

Die Twinsafe-Klemmen lassen sich beliebig mit Standard-E/A-Klemmen in einem Block mischen. Insgesamt stehen drei Arten von „sicheren“ Klemmen zur Verfügung:

- ▷ Die Busklemmen KL1904 und KL1908 sind digitale Eingangsklemmen mit vier oder acht fehlersicheren Kanälen. Die Klemmen entsprechen bei zweikanaligem Anschluss den Anforderungen der IEC 61508 SIL3 und EN 954 Kat. 4 beziehungsweise der DIN V 19251 AK6.
- ▷ Dieselben Standards erfüllt die Busklemme KL2904, eine digitale Ausgangsklemme mit vier Kanälen. Sie schaltet Aktoren mit 24 V(DC) bis 2 A. Bei Fehlererkennung schaltet die Klemme selbsttätig ab (Fail-Stop).

- ▷ Die Busklemme KL2901 ist eine Potential-Einspeiseklemme mit integrierter Abschaltung der Einspeisung. Die Einspeiseklemme lässt sich an einer beliebigen Stelle zwischen den Ein- und Ausgangsklemmen einer Busklemmenstation platzieren. Das Potential wird über die Power-Kontakte an die nachfolgende Busklemme weitergeleitet. Dadurch ist es möglich, getrennte Potentialgruppen an einer Busstation zu realisieren. Die Potential-Einspeiseklemme kommuniziert mit der Sicherheitssteuerung über das Profisafe-Protokoll und kann von einer übergeordneten Sicherheitssteuerung abgeschaltet werden. Erkennt die Klemme einen internen Fehler, wird ebenfalls abgeschaltet (Fail-Stop).



Uwe Prüßmeier

ist Produktmanager für Feldbus-Systeme bei Beckhoff.