Sichere Bussysteme in der Automatisierung

Während Bussysteme in der industriellen Automatisierung und auch in der Gebäudetechnik längst auf dem Vormarsch sind, ist ist die Sicherheitstechnik häufig noch konventionell verdrahtet. Vielfältig ist das Bestreben, auch die sicherheitsgerichteten Teile busbasiert auszuführen. Einige Lösungen und Ansätze dieser sicheren Kommunikation sind im Folgenden dargestellt.

1 Weniger Verdrahtung durch Datenkommunikation

Im Vergleich zur übersichtlichen Bustechnik erhöht die herkömmliche Einzelverdrahtung von Sicherheitskomponenten die Komplexität von Anlagen erheblich. Denn zumeist werden die sicherheitsbezogenen Teile in einem 1:1-Verhältnis verdrahtet, bei dem jeder einzelne Kontakt auf Anschaltbaugruppen vor Ort oder zum Schaltschrank geführt ist, um die Signale von dort aus – zum Teil logisch verknüpft – der betriebsmäßigen Steuerung zuzuführen. Bei den Bussytemen hingegen sind alle Komponenten an einer einzigen Datenleitung angeschlossen, über die die gesamte Signalübertragung erfolgt. Per Software ist es möglich, die angekoppelten Geräte zu parametrieren, funktional zu verknüpfen und den betriebsmäßigen Ablauf der Gesamtanlage zu programmieren. Neben einer deutlichen Reduzierung des Verdrahtungsaufwandes verringert eine solche Lösung den Planungs- und Projektierungsaufwand, senkt die Installations- und Inbetriebnahmekosten und vereinfacht Wartung, Service und Instandhaltung.

Es liegt nahe, auch die sicherheisgerichteten Teile einer Maschine, einer Anlage oder auch eines Gebäudes busbasiert auszuführen. In Betracht kommen prinzipiell zwei Möglichkeiten:

1. Die Sicherheitstechnik wird unmittelbar in das vorhandene, betriebsmäßige Datennetz eingebunden. Damit verbunden sind Änderungen an der vorhandenen Bus- und Protokollstruktur, um zu gewährleisten, dass wichtige sicherheitsrelevante Daten auch tatsächlich mit höchster Priorität bearbeitet werden. So ist vor allem im industriellen Bereich definitiv sicherzustellen, dass eine Steuerung innerhalb einer eindeutig festgelegten Zeit reagiert: Greift beispielsweise ein Arbeiter in eine durch ein Lichtgitter gesicherte Stanze, so muss diese unabhängig vom Datenaufkommen auf dem Bus sofort zum Stillstand kommen. Bei dieser homogenen Lösung mit nur einem Bussystem für sichere und nichtsichere Aufgaben kann zumeist mit den bekannten Parametrierwerkzeugen gearbeitet werden. Ein kompliziertes Einarbeiten in völlig neue Strukturen und Tools entfällt dann.

2. Als zweite Möglichkeit bietet sich an, die sicherheitsgerichteten Signale erst separat über einen eigens für diese Aufgaben entwickelten und optimierten Sicherheitsbus zu führen, der dann über ein so genanntes Gateway mit der betriebsmäßigen Bus-Steuerung kommuniziert und sicherheitsrelevante Ausgänge ggf. selbst aktiviert. Die Konsequenz sind zwei parallel verlaufende Datenleitungen. Die strikte Trennung hat aber den Vorteil, dass sich Modifikationen im betriebsmäßigen Segment einer Anlage oftmals leichter durchführen lassen, ohne dabei die Sicherheitstechnik zu beeinflussen. Darüber hinaus kann ein bestehendes Sicherheitskonzept oftmals nur durch einen Wechsel des Gateways an verschiedenen Standardbussen betrieben werden.

2 Der Weg zu busbasierten Sicherheitssystemen

Die konventionelle Verdrahtung vieler Sicherheitssysteme ist maßgeblich auf die bis zum Jahre 2000 gültige Normenregelung auf deutscher und internationaler Ebene zurückzuführen. So war in der EN 60204, Stand November 1998, noch aufgeführt, dass sicherheitstechnische Signale weder logisch verknüpft verarbeitet noch über ein Datenübertragungssystem geleitet werden dürfen. Erst die Einführung der Maschinenrichtlinie und die Neufassung der EN 60204 ließen in der Sicherheitstechnik auch andere als die bis dahin üblichen „kontaktbehafteten“ Lösungen zu. Allerdings hatten namhafte Hersteller auch schon vor diesem Zeitpunkt programmierbare Sicherheitssysteme auf den Markt gebracht. Heute sind längst sicherheitsgerichtete, busbasierte Systeme mit Zulassung nach Kategorie 4 der EN 954-1 bzw. SIL 3 nach IEC 61508 im Einsatz. Allen Lösungen gemein sind dabei Maßnahmen, die Wahrscheinlichkeit einer fehlerhaften Datenübertragung auf dem Bus bis auf ein tolerables Restrisiko zu minimieren.

3 AS-Interface

Vorgestellt wurde das Konzept von AS-Interface hinsichtlich sicherheitsgerichteter Funktionen erstmals auf der Hannover Messe 1999. Im Normalbetrieb kommunizieren in einem AS-i-System bis zu 124 Sensoren und Aktoren über 31 Slaves (ab Version 2.1 der Spezifikation: 62 Slaves) an einer Zweidraht-Leitung mit einem Master, der den Informationsaustausch steuert und seinerseits alle relevanten Daten mit einem Host austauscht. Bei diesem Host handelt es sich zumeist um eine SPS, einen Industrie-PC oder einen Koppler zum übergeordneten Bussystem. Auch in der Sicherheitstechnik ist AS-Interface in erster Linie auf binär schaltende Komponenten ausgelegt. Zusätzlich zu den üblichen Buselementen ist ein Sicherheitsmonitor vorhanden, der – ähnlich einem Schaltgerät in konventioneller Technik – die über den Bus übertragenen Informationen der einzelnen Sicherheitsgeräte überwacht, sammelt und verarbeitet. Der Monitor ist als eigenständiges Gerät ausgeführt und enthält als nachgeschaltetes Element eine Einheit, die die Verknüpfung der Daten durchführt und über Relais in konventionell aufgebaute sichere Steuerkreise eingreift. Er übernimmt so die Aufgabe einer Schnittstelle zwischen busbasierter und konventioneller Sicherheitstechnik, sodass sich auch herkömmliche Installationen vergleichsweise



❶ **EU-Normen zur Sicherheit** Foto: Interbusclub

einfach mit AS-i kombinieren lassen. Das Übertragungsverfahren ist so ausgelegt, dass Anwendungen bis zur Sicherheitskategorie 4 nach EN 954-1 realisiert werden können.

4 CAN

Am Anfang der Entwicklung des CAN-Busses (Controller Area Network) Mitte der 80er Jahre stand die Verwendung im Automobilbereich. Vor diesem Hintergrund entstand ein Bussystem mit zahlreichen Fehlererkennungsmechanismen, das auch in rauen Umgebungen eingesetzt werden kann. CAN ist ein Multimaster-System, in dem jeder Teilnehmer den gesamten Datenverkehr abhört und anhand des Absenders entscheidet, ob die jeweilige Nachricht für ihn relevant ist oder nicht. In der Grundstruktur der Kommunikation ist die Priorität eines Datenpaketes bereits berücksichtigt, sodass dringende Informationen auch als erstes versendet werden. So entstand ein sicheres Übertragungsprotokoll, mit dem sich neben den betriebsmäßigen Daten auch sicherheitsgerichtete Informationen über den gleichen Bus leiten lassen. Kernstück dieser Struktur sind mehrfach vorhandene Hardware-Komponenten, deren Signale durch übergeordnete Mikrocontroller gegeneinander verglichen werden (Kreuzvergleich). Die eigenständigen Sicherheitsbusse Safetybus p von Pilz und Esalan von Elan basieren beide auf den Mechanismen des Controller Area Networks.

5 Safetybus p

Safetybus p arbeitet parallet zum betriebsmäßigen Bussystem. Sensoren und Aktoren werden über dezentrale I/O-Module an die Sicherheitssteuerung angebunden. In der Anwendung können logisch zusammenhängende Komponenten als Gruppen konfiguriert und im Störfall separat abgeschaltet werden. Das Konzept verfolgt dabei drei Prämissen:

- die Dezentralisierung von Sicherheitssteuerungen über dezentrale I/O-Module,
- die Direktanbindung sicherheitsgerichteter Sensoren und Aktoren an den Bus und
- die sicherheitsgerichtete Kopplung mehrerer Sicherheitssteuerungen.

Alle drei Aspekte können in einem Safetybus-Netzwerk verwirklicht sein. So werden beispielsweise Not-Aus-Taster für gewöhnlich über dezentrale I/O-Module, komplexere Feldbusmodule wie Lichtgitter dagegen direkt an den Bus angeschlossen. Eine oder mehrere so gekoppelte Sicherheitssteuerungen übernehmen die Datenverarbeitung.
Der Sicherheitsbus arbeitet ereignisorientiert, d. h. Nachrichten werden nur dann gesendet, wenn sich der Zustand an den zentralen bzw. dezentralen I/O oder an den Busteilnehmern geändert hat. Aus diesem Grund eignet sich das System besonders gut zur Vernetzung von Anlagen mit unterschiedlich ausgeprägter Meldehäufigkeit und hohen Anforderungen an die Reaktionszeit. Das Applikationsspektrum bei Sicherheitsanwendungen reicht durch Abnahme bis einschließlich Kategorie 4 nach EN 954-1 und AK 6 DIN V 19250. Derzeit sind über 20 000 Safetybus-Geräte im Einsatz.

6 Esalan

Esalan steht für „Elan Safety Local Area Network“. Hier steht ein Ablaufsteuerprogramm im Vordergrund, das durch spezielle Parametrier- und Programmiermasken festgelegt wird. Dies sind funktionsorientierte, strukturierte Masken für gängige Schutzeinrichtungen. Hinzu kommen Programmiermenüs mit Masken für logische Verknüpfungen. Das Programieren und Parametrieren des Systems erfolgt via PC oder Laptop, wobei auch Funktionen für Service- oder Diagnosezwecke zur Verfügung stehen. Hardwaremäßig ist das System aus 64 Schaltschrank- oder Feldstationen aufgebaut. Die Stationen können über eine Länge von 400 m (max. 2 km) verteilt werden. Jede Station hat 8 Eingänge, 8 Ausgänge oder Kombinationen von 6 Ein- und 2 Ausgängen oder 4 Ein- und 4 Ausgängen. Der Einsatz der Feldstationen kann auch vollständig entfallen und Esalan übernimmt die Funktion einer Sicherheits-Mini-SPS oder einer multifunktionalen Relais-Sicherheitkombination mit frei paramentrierbaren Ein- und Ausgängen.
Die Feldstationen kommen hingegen dann zum Tragen, wenn es um die sicherheitsgerichtete Verkettung von mehreren dezentral angeordneten Maschinen oder Maschinenteilen geht und ein Sicherheits-Netzwerk aufgebaut werden muss. Weitere Einsatzmöglichkeiten bei NC- oder CNC-gesteuerten Maschinen eröffnet ein Sicherheits-Controller, bei dem zwei voneinander unabhängig arbeitende Einheiten das Überwachen von numerisch gesteuerten Antrieben übernehmen.

7 Profisafe

Zur Entwicklung von Profisafe, wie die sicherheitsgerichtete Lösung in Profibus-Systemen genannt wird, gehörte die Forderung, vorhandene Komponenten wie Leitungen, ASIC oder DP-Protokolle unverändert weiterbetreiben zu können. Die Sicherheitsapplikationen arbeiten gemeinsam mit den Standardanwendungen auf dem gleichen Bus. Darüber hinaus wurde angestrebt, die Lösung in Form eines Profils, also über ein spezielles Datenformat in den Nutzdaten, zu erreichen. Zahlreiche Unternehmen aus dem Sicherheitssektor haben an der Erstellung der Richtlinie mitgewirkt. Die sichere Lösung bietet die volle Freizügigkeit eines Baukastensystems, d. h. die definierten Schnittstellen und Verfahren erlauben das Nutzen einer stetig wachsenden Zahl von Sicherheitsgeräten (F-Hosts und F-Slaves) und Systemen in fast beliebiger Konstellation. Es bleibt dem Anwender überlassen, Sicherheits- und Standardfunktionen auf zwei Profibus-Stränge zu verteilen, wenn dies zweckmäßig erscheint. Genutzt werden Funktionen aus dem Standard-Kommunikations-Verfahren, die zur Erhöhung der Übertragungssicherheit beitragen. Ansonsten sind die Sicherheitsmaßnahmen in den Kommunikationsendteilnehmern gekapselt. Diese Kapselung führt dazu, dass die „Nutzlast“ von Standard-Profibus-Telegrammen um einige Bytes Information erweitert wird, die die Sicherheit der Kommunikation gewährleisten. Grundsätzlich bestehen keine Einschränkungen hinsichtlich Übertragungsrate, Zahl der Busteilnehmer oder der Übertragungstechnik, sofern die geforderten Reaktionszeiten dies jeweils zulassen.

8 Interbus

Die Sicherheitstechnik bei Interbus basiert darauf, dass eine zusätzliche Überwachungseinheit in das Bussystem eingebaut wird, die jeglichen Busverkehr mithören kann und die korrekte Arbeitsweise der Steuerungen überwacht. Ausgangspunkt der Lösung ist die Tatsache, dass Standard-Steuerungssysteme in der Regel korrekt arbeiten. Die Sicherheitsinformationen werden als Bitstrom über Interbus übertragen und in den sicherheitsgerichteten Teilnehmern verarbeitet. Da sich der Sicherheitsmonitor direkt nach dem Bus-Master an exponierter Stelle im System befindet, passieren ihn alle für die Teilnehmer bestimmten Daten. Umgekehrt kann er auf der Datenleitung, die vom letzten Teilnehmer zum Master zurückführt, die Eingangsinformationen aller angeschlossenen Teilnehmer mitlesen. Die Überwachungseinheit erzeugt aus den ihr vorliegenden Eingangsdaten ihr sicherheitsgerichtetes Prozessausgangsabbild. Die so ermittelten Daten vergleicht der Monitor mit den Ausgangsdaten, die die SPS oder der Bus-Master an die sicherheitsgerichteten Ausgangskomponenten übertragen will. Für den Fall, dass eine Sicherheitsbedingung erfüllt war, verweigert die Überwachungseinheit ihre Zustimmung, schaltet einzelne Ausgänge oder Segmente ab ab oder verhindert deren Zuschaltung. Das Interbus-Protokoll bleibt in dieser Lösung unangetastet.