Bibliografie

Zeitschrift	arbeitssicherheits.journal
Autor	Guido Matthes
Rubrik	arbeitssicherheit.titel
Referenz	Arbeitssicherheitsjournal 2009, 12 - 13 (Heft 2)
Verlag	Carl Heymanns Verlag

Matthes, Arbeitssicherheitsjournal 2009, 12
Sicherheitstrends in der Automatisierungstechnik

Guido Matthes

Matthes: Sicherheitstrends in der Automatisierungstechnik - Arbeitssicherheitsjournal 2009 Heft 2 - 12 >>

Die Technik hilft uns in vielen Bereichen, sie muss aber auch sicher und beherrschbar sein. Dafür stellt die A+A 2009 ein breites Spektrum an Sicherheitslösungen aus vielen Bereichen vor – einer davon ist die Sicherheit in der Automatisierungsindustrie. Hier wird Safety heutzutage oft über das Datenkommunikationsnetz der Produktionsanlage realisiert.

Höhere Produktivität, bessere Integration, höherer Bedienkomfort – das sind keine leeren Schlagworte, sondern vielmehr berechtigte Forderungen an Maschinen und deren Sicherheitsfunktionen. Doch wohin geht der Trend? Ist es besser für die Sicherheitsfunktionen, das Datennetz der Maschine zu nutzen, oder ist es sinnvoller, auf einfache, mechanische Lösungen zurückzugreifen?

Unabhängig von Trends ist in der Sicherheitstechnik der Begriff SIL wichtig und spielt eine tragende Rolle. Um nämlich „Sicherheit“ zu definieren bzw. in Kategorien einzuteilen, gibt es die Sicherheitsanforderungsstufen SIL (Safety Integrity Level) mit einer Skala von 1 bis 4. Diese sind ein Maß für die notwendige bzw. erreichte risikomindernde Wirksamkeit der Sicherheitsfunktionen, wobei SIL 1 die geringsten Anforderungen hat. SIL dient also als Maß für die Wirksamkeit von Sicherheitsfunktionen. Den notwendigen SIL ermitteln die Fachleute über eine Gefahren- und Risikoanalyse.

Informieren und kommunizieren

Ein Kunstbegriff in diesem Zusammenhang ist die Sicherheitsintegrität. Eine Sicherheitsfunktion muss zwei Hauptaufgaben erfüllen. 1. Im Gefährdungsfall muss sie zuverlässig funktionieren (Maschine abschalten/Personen schützen). 2. Sie muss das gefahrverursachende System (muss nicht die eigentliche Maschine sein) im Fall der Fälle unmittelbar abschalten (auch wenn keine direkte Gefahrensituation vorhanden ist, z.B. „nur“ ein System- oder Softwarefehler). Deshalb sollte man nicht von der Zuverlässigkeit einer Sicherheitsfunktion sprechen, sondern von der „Sicherheitsintegrität“.

In der Automatisierungstechnik stehen komplexe Sicherheitssysteme in Konkurrenz zu einfachen Lösungen, die schneller montiert und konfiguriert sind und deshalb weniger fehlerträchtig erscheinen. Häufig haben Anlagen aber verschiedene Fertigungszellen mit unterschiedlichen Kommunikations- und Steuerungssystemen. Zwar lassen sich hier Hierarchieebenen einrichten, aber je komplexer ein System, umso schwieriger ist es zu konfigurieren und umso anfälliger wird es gegen Störungen. Hier ist weniger manchmal mehr.

Durch leistungsfähige Informationstechnik besteht die Möglichkeit, Maschinensicherungen in Systeme zu integrieren. Hier gibt es drei grundsätzliche Arten, die Sicherheitsfunktionen über die Daten-Kommunikationsnetzwerke zu realisieren.

1. Integrierte Safety über den CAN-Bus

Der CAN-Bus (Controller Area Network): Eine Anlage hat viele unterschiedliche Feldgeräte, die alle angesteuert werden müssen. Dazu gibt es grundsätzlich zwei Arten. a) Jeder Sensor/Aktor wird mit je einem Kabel verbunden, daraus entsteht eine parallele Verkabelung und b) das Kabel wird bei jedem Sensor/Aktor vorbeigeführt (serielle Verdrahtung). Bei vielen Anlagen wäre der Verkabelungsaufwand bei paralleler Verdrahtung aufgrund der größeren Anzahl der Sensoren/Aktoren viel zu hoch. Deshalb gibt es die serielle Verkabelung = CAN-Bus.

2. Safety auf Ethernet-Basis

Der Einsatz des Ethernets ermöglicht es, die normalen Steuerungsaufgaben und die sicherheitsgerichteten Aufgaben in einem System durchzuführen. Zu den Vorzügen des Ethernets zählt, dass auf eine ganze Reihe bewährter, standardisierter Verfahren zurückgegriffen werden kann, wobei praktisch für alle Medien (Koaxialleitung, verdrillte Kupferpaare und Lichtwellenleiter) Treiberbausteine zur Verfügung stehen. Varianten der „Safety“ auf Ethernet-Basis sind z.B. Safety-over-Ether-CAT3 und ähnliche.

3. AS-Interface mit „Safety at Work“

Das AS-Interface ist eine intelligente „Verkabelung“, die in der Sensor-/Aktor-Ebene, sozusagen „ganz unten an der Maschine“, den Aufbau einfacher und kostengünstiger Systeme ermöglicht. Es sind dafür zwar spezielle Chips, aber auch weniger Verkabelungsaufwand erforderlich. Die erforderliche Sicherheit wird durch eine zusätzliche Signalübertragung erreicht.

Gegen den Trend, Sicherheitseinrichtungen in die Maschinensteuerungstechnik zu integrieren und die Netzwerke für die sicherheitsgerichtete Kommunikation zu nutzen, stellen mehrere Hersteller einfachere Systeme vor. Diese kleinen Safety-Steuerungen können dabei in Fertigungszellen Aufgaben übernehmen, die über die bloße Notabschaltung hinausgehen. So gibt es z.B. modulare Steuerungen, die Not-Aus-Taster, Schutztüren und Lichtgitter überwachen. Die Module kommunizieren über eine Bus-Verbindung miteinander. Das System konfiguriert sich nach dem Zusammenstecken selbst, dabei bleibt die Zulassung nach der Sicherheitskategorie SIL 3 erhalten. Die verschiedenen Funktionen und Verknüpfungen werden nur durch die Anordnung der Module realisiert.

Von modular bis High-End – Lösungen für jede Anwendung

Andere Systeme vereinen die Zugangs- und Steuerungstechnik in einem System. Der wichtigste Punkt: Das Netzwerk konfiguriert sich auch hier selbst. Das Einsatzfeld sind übliche Torschalter, mit denen der Zugang zu den Maschinen gesichert wird. Dabei kommen weder ein zusätzlicher Torschalter noch ein Steuergerät mehr zum Einsatz. Das ganze System wird auf herkömmliche Aluminiumstranggussprofile aufgeschraubt und zusammengesteckt. Die Schalter lassen sich dann an Schiebe- oder Scharniertüren anbringen. Ganz oben an der Spitze der Sicherheitsskala stehen Systeme, die dreifach redundant aufgebaut

Matthes: Sicherheitstrends in der Automatisierungstechnik - Arbeitssicherheitsjournal 2009 Heft 2 - 13 <<

sind. Dabei steuern drei voneinander isolierte, parallel arbeitende Rechner das System. Bei Abweichungen der Rechner voneinander wird so verfahren, wie es die Mehrheit der Geräte für richtig hält, zwei Rechner „überstimmen“ also den dritten, eventuell fehlerhaften. Durch die dreifache Redundanz kann das Versagen einer Komponente die Funktion des Systems nicht beeinträchtigen: Es gibt keinen „single point of failure“.

Neue Technologien liegen im Bereich Safety im Trend – nicht zuletzt durch die Anforderungen der neuen Maschinenrichtlinie 2006/42/EG, die bis zum 29.12.2009 umgesetzt werden muss (siehe Bericht in dieser Ausgabe). Dadurch wird die alte Sicherheitsnorm EN 954-1 durch die neue Norm EN ISO 13849 abgelöst. Ob man dann ein dreifach redundantes System, eine Standard-SPS (Speicher Programmierbare Steuerung) mit integrierter Sicherheits-SPS oder „nur“ eine modulare Steuerung, die die Not-Aus-Taster, Schutztüren und Lichtgitter überwacht, einsetzt, muss sich nach dem jeweiligen Anwendungsfall richten.