IDA:
Sicherheitsgerichteter Datenverkehr im Ethernet

von Dr. Peter Wratil

Bild 1: Automatisierungssystem bei der Automobilherstellung

In den letzten Jahren sind immer mehr Bereiche im Maschinenbau und in der Anlagentechnik automatisiert worden. Die Herstellung qualitativ hochwertiger Produkte bei niedrigen Stück- und Herstellungskosten ist ohne den Einsatz moderner Steuerungseinheiten und ohne eine weitreichende Kommunikation nicht mehr möglich. Damit einhergehend steigen natürlich auch die Anforderungen an die Sicherheit.

Produktionsanlagen rentieren sich nur dann, wenn eine hohe Verfügbarkeit garantiert wird. Nicht zuletzt geht es deshalb bei einer automatischen Herstellung darum, den Menschen in den Fertigungsprozess zu integrieren. Er kann Teile optimal platzieren, Fehler im Vorfeld erkennen, Mängel rasch beheben oder sogar Wartungen während des Produktionsablaufs durchführen. Bei jedem Einsatz von Personen muss aber jegliche Gefahr für Leben und Gesundheit aller Beteiligten ausgeschlossen sein. Ein Fehler darf überhaupt nicht vorkommen, oder zumindest sind alle Risiken der Automatisierungseinrichtungen zu eliminieren, bevor eine Gefahr entsteht. Daher müssen die Kommunikationsnetze, die alle Daten der Steuerung, der Sensoren oder der Aktoren übertragen, absolut fehlerfrei arbeiten.

Vergleich zum Standard

Niemand wird behaupten, dass Standard-Bussysteme, wie z.B. Profibus, Interbus, DeviceNet, Modbus usw., unsicher seien. Warum braucht man dann überhaupt sicherheitsgerichtete Bussysteme? Die Beantwortung dieser Frage ist einfach: Normale Bussysteme sind zwar in der Lage, einfache Fehler aufzudecken, hingegen fehlen in der Regel effektive Algorithmen, Mehrfachfehler statistischer oder systematischer Natur eindeutig zu identifizieren und sicher zu beherrschen. Zusätzlich bezieht sich der Standard bei normalen Bussystemen nur auf die Datenübertragung, deren Formate und deren Dienste. Das Interface und dessen Funktion wird dagegen nicht berücksichtigt. Bei sicheren Bussystemen bezieht sich das Fehlermodell nicht nur auf das Bussystem selbst, sondern auch auf die Applikation, die Interfacetechnik, die Versorgung und das Übertragungsmedium. Um den deutlichen Unterschied zwischen normalen und sicherheitsgerichteten Bussystemen zu verdeutlichen, seien zwei Beispiele vorgestellt:

1. Die Sende- und Empfangsfunktion bei standardmäßigen Feldbussen erfolgt fast immer über einen hochintegrierten Spezialbaustein (z.B. Supi beim Interbus). Dieser Baustein kontrolliert den Datenverkehr und detektiert auch mögliche Fehler, indem er eine Datenprüfung über einen ebenfalls integrierten CRC-Tester durchführt (cyclic redundancy check). Die Qualität des Testers ist so hoch, dass ein fehlerhafter Datenstrom auch dann noch als falsch erkannt wird, wenn mehrere Bits ihre Information verloren haben. Dies gilt aber nur solange, bis ein Ausfall des Testers vorliegt. Im Fehlerfall kann somit der Tester auch falsche Daten als richtige vortäuschen. Ein einziger Fehler mit einem weiteren Fehlverhalten kann also verheerende Folgen nach sich ziehen. Schlimmer noch: Der Ausfall des Testers ist kaum erkennbar und kann schon eine Zeitlang zurückliegen, bevor ein weiterer Fehler auftritt.
2. Manche Bussysteme kommunizieren innerhalb ihrer Teilnehmer, indem sie diese über voreingestellte Adressen ansprechen (z.B. beim Profibus). Im Prinzip kann ein Bussystem eine Adresse durch eine Fehleinstellung doppelt beinhalten. Diese doppelte Vergabe einer Adresse kann unbemerkt bleiben, wenn einer der beiden Teilnehmer entweder sehr schwach am Netz erscheint oder sich nur sporadisch zu erkennen gibt. Im schlimmsten Fall kann durch die doppelte Vergabe einer Adresse eine Informati-

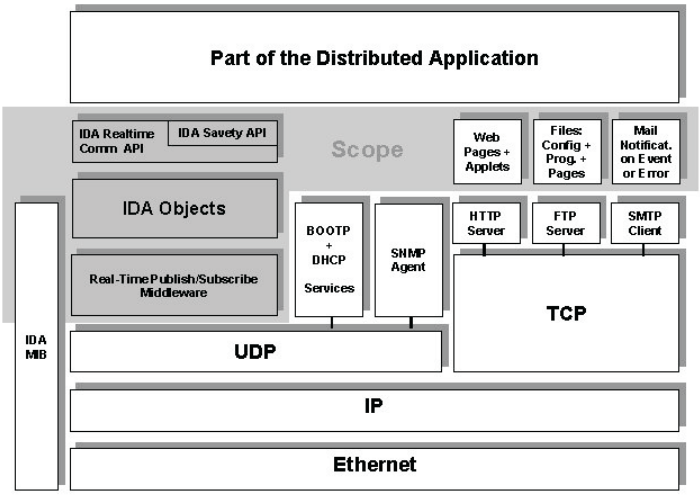

Bild 2: Die interne Struktur des Ethernets für IDA-Anwendungen.

on überschrieben werden, ohne dass jemand Notiz davon nimmt. Wenn man beispielsweise eine sicherheitsgerichtete Information (z.B. Not-Aus) überschreibt, bleibt die gewünschte Reaktion aus. Selbst bei einer raschen Identifikation des Fehlerzustands ist ein normales Netz kaum in der Lage, die richtige Abfolge innerhalb der maximalen Durchlaufzeit herzustellen, und die notwendige Reaktion auf die Sicherheitsanforderung ist zumindest deutlich verzögert.Sicherheitsgerichtete Bussysteme müssen sich daher von normalen Bussystemen dadurch unterscheiden, dass sie alle sporadischen und systematischen Fehler aufdecken. Zusätzlich sind stets Techniken implementiert, die eine Fehlerbeherrschung ermöglichen.

Konzepte

Die Anwendung bestimmt die Güte des verwendeten Bussystems. Nach den heute gültigen Normen (z.B. EN954-1, Maschinenrichtlinie) sind die Anforderungsbereiche in Kategorien eingeteilt. Dabei stellt die Kategorie 4 die höchste Kategorie dar, bei der ein System auch dann noch sicher sein muss, wenn mehrere Fehler gleichzeitig auftreten. In der internationalen Norm (ISO 61508) entspricht diese Kategorie dem Anforderungsbereich nach SIL 3 (safety integrity level). Alle modernen sicherheitsgerichteten Bussysteme entsprechen den Anforderungen nach SIL 3. Hierbei müssen jedoch nicht nur Mehrfachfehler sicher beherrscht werden, sondern es ist auch eine extrem geringe Fehlerrestwahrscheinlichkeit nachzuweisen. Beispielsweise wird bei SIL 3 nur noch ein “nicht identifizierter” Fehler binnen eines Zeitraums von 10^{-7} Stunden (d.h. fehlerfreier Betrieb für mehr als tausend Jahre) akzeptiert. Da diese Fehlerrestwahrscheinlichkeit für das gesamte Automatisierungssystem gilt, darf das Bussystem nur zu einem erheblich geringeren Anteil an einem eventuellen Fehler beteiligt sein. Fehlerrestwahrscheinlichkeiten von 10^{-9} pro Stunde sind dabei durchaus üblich. Neben den hohen Anforderungen an die Fehleraufdeckung sind auch Vorkehrungen zu treffen, eventuelle systematische Fehler zu erkennen. Die Tabelle gibt eine Übersicht der möglichen Fehlerarten und stellt geeignete Maßnahmen vor, diese Fehler zu erkennen. Die Daten-übertragungsqualität wird im Wesentlichen durch Datensicherungsverfahren gewährleistet. Dabei wirkt sowohl ein Echo als auch eine geeignete Datensicherung, z.B. CRC oder Blockprüfung, möglichen Bitfehlern entgegen. Wie viele Bitfehler noch mit Sicherheit erkannt werden, wird auch mit der Hamming-Distanz beschrieben. Hierunter versteht man eine Zahl, die angibt, welche Anzahl von Fehlern man bei einer Datenübertragung an bestimmter Stelle einfügen muss, damit man zu einer Information gelangt, die fälschlicherweise wieder als fehlerfrei erkannt wird. Heutige sicherheitsgerichtete Bussysteme enthalten Sicherheitsalgorithmen zwischen einer Hamming-Distanz von 4 bis 8. In der Tabelle sind auch alle Maßnahmen gegen systematische Fehler vermerkt. So kann beispielsweise das Einfügen einer “laufenden Nummer” sofort anzeigen, ob die richtige Reihenfolge bei der Übertragung eingehalten wurde. Auf diese Weise wird auch der Verlust oder das ungewollte Einfügen von Nachrichten erkannt.

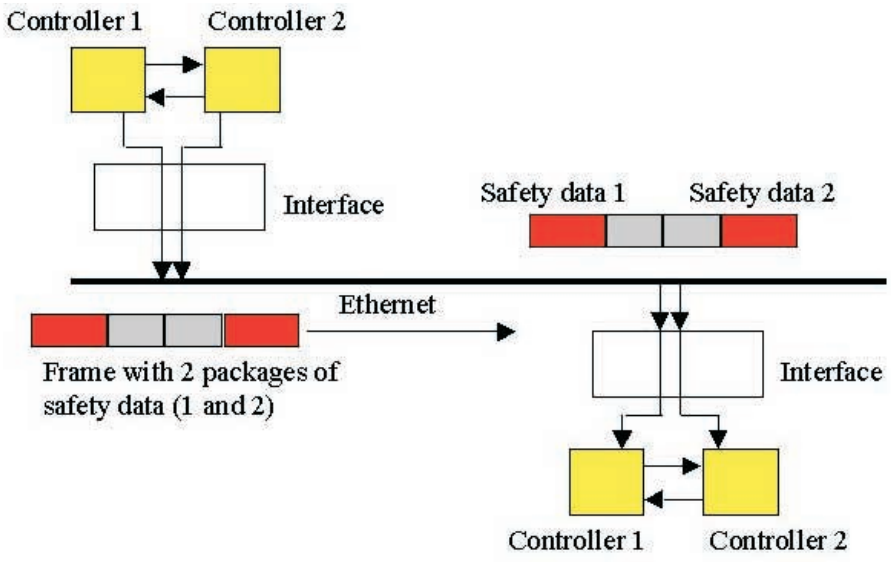

Bild 3: Beispiel eines sicheren Datenverkehrs mit jeweils zwei Mikrocontrollern

Sicherheitsstandard für Ethernet

Im Laufe der nächsten Jahre wird Ethernet die heutigen Feldbussysteme sukzessive ersetzen. Ethernet bringt gegenüber den Standard-Feldbussen den entscheidenden Vorteil mit, dass diese Technik weltweite Verbreitung gefunden hat und mit ihr eine Technologie zur Verfügung steht, die einen umfangreichen Datenverkehr bei hoher Übertragungsgeschwindigkeit zulässt. Darüber hinaus kann man im Ethernet neben den reinen Automatisierungsdaten auch Bilder, Texte oder gar Videos übertragen. Bei einer vollständigen Einhaltung der Kompatibilität stehen ebenso alle Web-Dienste zur Verfügung, damit eine weltweite Parametrierung oder Diagnose sofort gegeben ist. IDA (Interface for destributed automation) verwendet Ethernet zur Kommunikation in Automatisierungseinheiten. Unterstützt werden alle Kommunikationsarchitekturen, wobei die Anwendung von "verteilter Intelligenz" im Vordergrund steht. Der Aufbau einer Sicherheitsstruktur innerhalb des Ethernets zur Abdeckung von verteilten Ressourcen, stellt besondere Anforderungen wie kalkulierbare und niedrige Reaktionszeiten, hohe Datensicherheit, Kompatibilität zur Standard und einfache Implementierung. Freilich sollte sich auch eine große Anzahl von Teilnehmern in einer weiträumig vernetzten Automatisierungslandschaft anschließen lassen. Diese beiden letzten Punkte sind bereits heute hervorstechende Merkmale von Ethernet.

Sicherheitsarchitektur

Bei der Sicherheitsarchitektur wird der gesamte sicherheitsgerichtete Datenverkehr oberhalb der üblichen Ethernet-Layer angeordnet. Hierdurch bleibt die Kompatibilität zu allen normalen Ethernet-Diensten vollständig erhalten. Der sichere Ethernet-Layer hat lediglich die Aufgabe, Daten einem anderen Teilnehmer sicher zur Verfügung zu stellen oder diese von einem Sender entgegenzunehmen. Die Daten sind mit einer Hamming-Distanz von 8 hochwertig abgesichert und garantieren daher eine hohe Fehleraufdeckung. Der TÜV Anlagentechnik (Köln) hat eine positive Konzeptbeurteilung für das verwendete Verfahren ausgesprochen. Damit sind alle Einsatzbereiche bis zur Kategorie 4 (EN954-1) erlaubt.

Datentransfer

Die hohe Datengüte erlaubt nicht nur eine optimale Aufdeckung statischer Fehler (z.B. Bitstörungen), sondern auch eine weitgehende Identifizierung systematischer Fehler. Hierzu wurden verschiedene Techniken implementiert. Je nach Sicherheitsanforderung kann man direkt über dem Sicherheits-Layer eine zweikanalige Systemarchitektur anordnen, die mit dem IDA-Datenformat auch alle systematischen Fehler bei der Verarbeitung der unterlagerten Layer oder Fehler beim Datentransfer innerhalb von Gateways oder Switches mit hoher Sicherheit erkennt. In Bild 3 ist eine mögliche Struktur zu erkennen, bei der zwei unabhängige Mikrocontroller einen gesamten Datensatz für die Übertragung zusammenstellen. Der Datensatz beider Controller wandert durch die Standard-Layer innerhalb des Teilnehmers und wird schließlich über das Ethernet versendet. Auf Empfängerseite erfolgt dann die Rückgewinnung der Dateninformation, wobei ebenfalls zwei Mikrocontroller unabhängig voneinander operieren. Nur bei Erfüllung der Datenprüfung, bei Einhaltung der Reaktionszeit und bei gegenseitiger Kontrolle durch beide Mikrorechner werden die Daten für einwandfrei befunden.

Ausblick

Innerhalb der Automatisierung werden sich sicherheitsgerichtete Datennetze in den nächsten Jahren bei allen Anwendungen etablieren. Sie ersetzen dort recht rasch die Standardnetze oder die Standard-Feldbusse. Um Installationskosten zu sparen, erlangen im ersten Schritt vollkompatible Datennetze besondere Bedeutung, z.B. Profibus Safe ersetzt Profibus oder Interbus Safety ersetzt Interbus. Um Leitungen einzusparen oder lästige Zusatzinstallationen zu vermeiden, dürften sich nur solche Netze durchsetzen, die sowohl sicherheitsgerichtete als auch normale Daten übertragen können. Die Sicherheit versteht sich nicht selten als notwendige Zugabe, ohne dass neue Architekturen oder weitere Kosten notwendig werden. Im Laufe der nächsten Jahre wird Ethernet eine besondere Bedeutung zukommmen, da weltweite Diagnose und Verfügbarkeit eine außerordentliche Rolle spielen. ■

7120

www.innotecSafety.de

Dr. Peter Wratil ist Inhaber der Firma innotec, Rosengarten. Das Unternehmen berät auf dem Gebiet der Sicherheitstechnik. Im Rahmen der IDA-Aktivitäten hat die von Dr. Wratil geleitete Arbeitsgruppe den Sicherheits-Layer für das Ethernet spezifiziert.

Maßnahmen						
Fehler	Laufende Nummer	Zeitmarke	Echo	Kennung	Datensicherung	Redundanz mit Kreuzvergleich
Wiederholung	•	•				•
Verlust	•		•			•
Einfügung	•		•	•		•
Falsche Abfolge	•	•				•
Verzögerung		•				
Verfälschung			•		•	

Mögliche Fehler beim Einsatz von Netzwerken und geeignete Maßnahmen zur Fehlererkennung und -beherrschung.