Sicherheitsgerichtete Bussysteme auf der Basis von Ethernet

Ethernet, aber sicher.

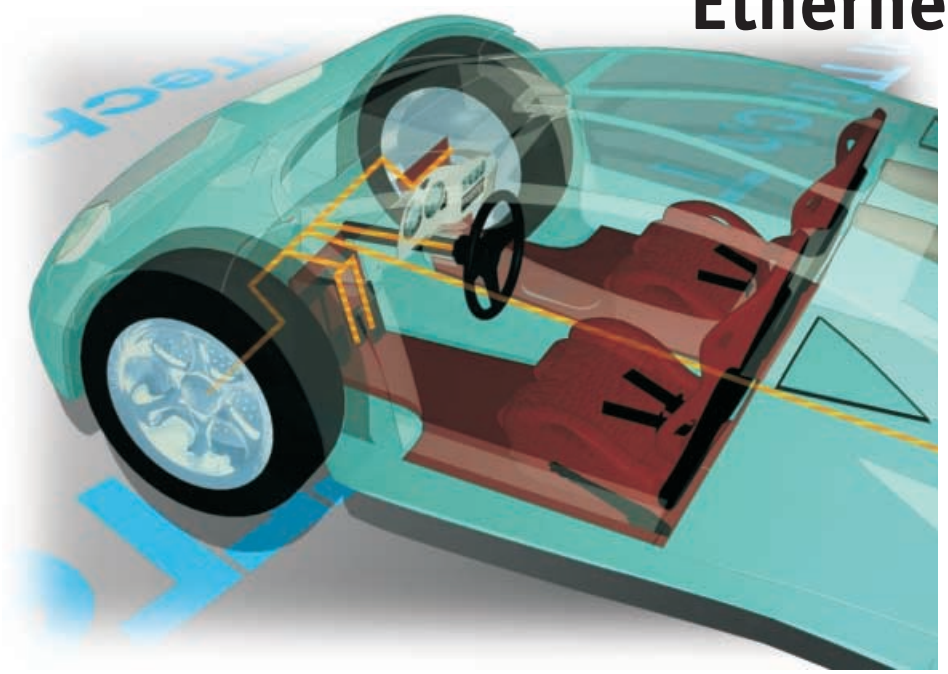

Bild 1 : Fokus auf Sicherheit und zeitkritisches Verhalten: TTP mit Branchenschwerpunkt Maschinenbau und Fahrzeugtechnik.

von Dr. Peter Wratil

Heute ist Sicherheit nicht nur eine Frage der Ergonomie, sondern der IT. Sicherheitsgerichtete Busse müssen sich an bestimmte Richtlinien halten, die auch die Sensor/Aktor-Ebene mit einschließt.

Für ein umfassendes Sicherheitskonzept sind sicherheitsgerichtete Datenverbindungen zur Datenübertragung, Steuerung und Regelung notwendig. Sie garantieren auch dann noch eine sichere Übertragung, wenn einzelne Datenbits oder ganze Datenfolgen gestört sind. Die bekannten Feldbussysteme haben zur Abdeckung dieser Sicherheitsanforderungen neue Profile erhalten, die einen Sicherheitszusatz zum Standard darstellen. Dieser Zusatz ermöglicht einerseits die normale Kommunikation und andererseits den sicherheitsgerichteten Datenverkehr für alle Anwendungen der Datenübertragung, Parametrierung oder Programmierung. Bei einigen aktuellen Bussystemen, die auf der Basis von Ethernet entwickelt wurden, ist man vollkommen anders vorgegangen. Hier hat man die Anforderungen der Sicherheitstechnik von Anfang an integriert. Diese Strategie brachte zahlreiche Vorteile mit sich, die sich sowohl in der Einfachheit, Transparenz, Implementierbarkeit als auch bei allen speziellen Anforderungen innerhalb der Sicherheitstechnik auszahlt. Wie die drei folgenden Beispiele verdeutlichen, bleibt das Anwendungsgebiet dieser modernen Ethernet-Protokolle keineswegs allein auf den Maschinen- oder Anlagenbau beschränkt.

IDA-Lösung

Eines der neuen Ethernet-Netzwerke ist unter dem Namen IDA (Interface for Distributed Automation) bekannt geworden. IDA verwendet Ethernet als Kommunikationsbasis und baut auf dem Standard-Schichtenmodell auf. Damit erfüllt es alle Anforderungen der Kompatibilität zu bestehenden Systemen und Applikationen. Als eine der Grundfunktionen ermöglicht die Kommunikation mittels IDA - neben der Verarbeitung mit Steuerungen - auch die direkte Sensor-Aktor-Kommunikation. Damit gewährleistet IDA auch eine kurze Reaktionszeit und eine einfache Integration. Wie in Bild 2 dargestellt, kann die Architektur und die Topologie an seine spezielle Applikation angepasst werden. Es bleibt dem Anwender überlassen, ob er eine Anzahl von Sensoren direkt mit Aktoren kommunizieren lässt oder ob er lieber eine speicherprogrammierbare Steuerung verwendet. Er kann auch sicherheitsgerichtete Bussysteme ankoppeln und über deren Dienste Daten austauschen Die Fehleraufdeckung ist dabei so zuverlässig, dass Sicherheitsdaten auch über nicht sichere Teilnehmer weitergeleitet werden können, wie z.B. eine normale Bridge oder ein Gateway. Anhand der Datenstruktur kann ein sicherheitsgerichteter Empfänger alle entstandenen Fehler im Datenfluss erkennen, gleichgültig, ob man nur sichere oder auch normale Transport-

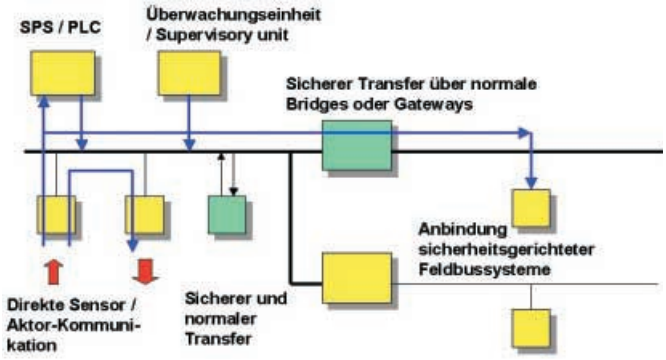

Bild 2: Flexibilität: Architektur und Topologie können an kundenspezifische Applikationen angepasst werden.

medien zur Übertragung verwendet hat. Die gesamte Struktur mit den verfügbaren Diensten ist damit geeignet, die Anforderungen nach SIL 3 (IEC61508) und nach der Kategorie 4 (EN954-1) abzudecken. Mit dieser Datengüte kann IDA für alle bekannten Applikation im Maschinen- und Anlagenbau eingesetzt werden.

Beispiel TTP

Als zweites Beispiel soll das Ethernet mit der Bezeichnung TTP vorgestellt werden. TTP steht für Time-Triggered Protocol und kann überall dort eingesetzt werden, wo extreme Anforderungen an die Echtzeitfähigkeit vorliegen. Anwendungsgebiete von TTP sind beispielsweise die Kontrolle und Steuerung von Antiblockiersystemen oder Antischlupfregelungen. In TTP werden alle Aktivitäten des Kommunikationssystems gemäß eines vordefinierten, systemweit bekannten Ablaufplans abgehandelt. Die dafür notwendige, globale Zeitbasis wird durch die von den TTP-Controllern autonom durchgeführte, fehlertolerante Uhrensynchronisation definiert. Der Buszugriff erfolgt mit einem Zeitschlitzverfahren. Zwischen einem Kommunikationscontroller und dem Host-Prozessor befindet sich eine als CNI (Communication Network Interface) bezeichnete Datenschnittstelle, über die ausschließlich Dateninformationen und keine Steuersignale ausgetauscht werden. Somit kann der Hostprozessor auch im Fehlerfall keinen Einfluss auf das Kommunikationsverhalten des TTP Controllers nehmen. Dieser Schutzmechanismus, der als Temporal-Firewall bezeichnet wird, verhindert die Fortpflanzung von Fehlern und bedingt, dass für alle Echtzeit-Nachrichten im System der Update-Zeitpunkt von vornherein spezifiziert und allen Busteilnehmern bekannt ist. Aus dem zeitgesteuerten Prinzip ergibt sich als Folge eine konstante Buslast, die nur durch den deterministischen Ablaufplan bestimmt wird. Der vom Systemintegrator festzulegende zeitliche Ablauf führt zu genau spezifizierten Schnittstellen im Zeit- und Wertebereich. Das Kommunikationssystem garantiert autonom, dass das zeitliche Verhalten dem Design entspricht, unabhängig davon, ob nur ein Teil des Systems oder alle Knoten aktiv sind. Diese Eigenschaft zielt direkt auf die Komplexitätsproblematik verteilter Systeme ab und ermöglicht die Zusammensetzbarkeit der Komponenten, da sich das Kommunikationsverhalten bei einer Systemintegration nicht verändern kann. Dieser Umstand ist für die Zertifizierung von sicherheitskritischen Anwendungen von großem Vorteil, da Bereiche verschiedener Sicherheitsniveaus definiert und unabhängig zertifiziert werden können. Ein entsprechend konfiguriertes TTP-System erkennt und toleriert jeden Einzelfehler, dessen Folgefehler und darüber hinaus eine Vielzahl an Mehrfachfehlern.

AFDX

Als drittes Beispiel sei ein Ethernet-System vorgestellt, das bei hochsicherheitsrelevanten Applikationen zum Einsatz kommt. Das AFDX (Avionic Full Duplex Switched Ethernet) basiert auf dem IEEE802.3-Standard und wird bei 100Mbit/s betrieben. Durch den Einsatz von Switches kommt ein deterministisches Verhalten zustande. Beispielsweise wird AFDX in der Luftfahrtindustrie (z.B. bei dem neuen Airbus A 380)

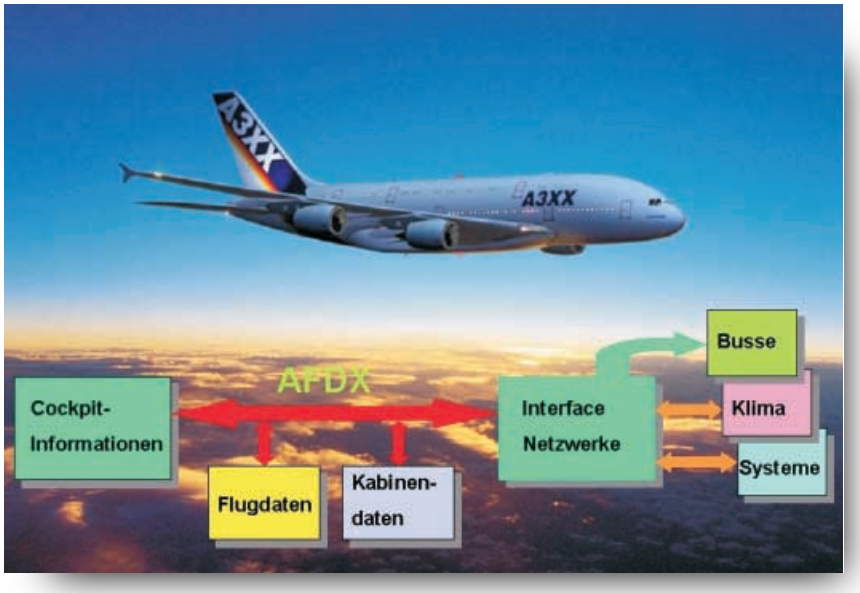

Bild 3: Leitstelle Cockpit: Mittels AFDX werden zahlreiche Informationen über Sicherheitsdaten bereit gestellt.

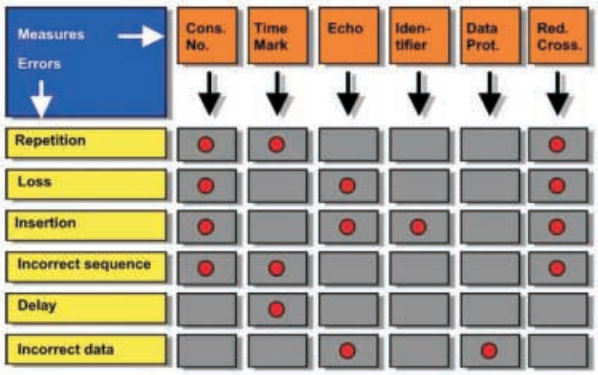

Bild 4: Ein Beispiel für typische Fehler und die entsprechenden Maßnahmen für deren Behebung.

eingesetzt. Das Netzwerk ist aber auch geeignet, sichere Steuerungsfunktionen zu übernehmen. Neben dem normalen Transport der Informationsdaten für das Cockpit werden beim A 380 auch alle Flugdaten und Daten über den Zustand der Kabinen übermittelt. Ferner erfolgt eine Ankopplung an weitere Interface-Systeme die beispielsweise Klimadaten, die Informationen von anderen Systemen oder die Daten unterlagerter Busse übermitteln (Bild 3). Da der Einsatz im Flugzeug keine Umkonfiguration oder Erweiterung im Betrieb zulässt, kann die gesamte Struktur bei der ersten Implementierung festgelegt werden. Das Protokoll und die Dienste entsprechen den höchsten Sicherheitsanforderungen der Luftfahrtindustrie, wobei besonderer Wert auf die Verfügbarkeit gelegt wurde. Die Bussträge sind dabei redundant ausgelegt.

Richtlinien für die Sicherheit

Alle sicherheitsgerichteten Bussysteme müssen sich an gewisse Richtlinien halten, wie sie im Jahr 1999 als Normenentwurf vorgelegt wurden. In dem FAET-Entwurf werden alle denkbaren Fehlerfälle unterstellt, die bei Bussystem bekannt sind. Zu jedem dieser Fehlerfälle stellt der Entwurf ein Bündel an Maßnahmen vor, welche gegen jeden der zu unterstellenden Fehler mit Sicherheit wirkt. Bild 4 zeigt ein Beispiel für typische Fehler beim Datenverkehr und stellt wirksame Mittel vor, die beispielsweise bei dem Profil von sicheren Bussystemen zum Einsatz kamen. Neben der Einhaltung einer geeigneten Maßnahme ist auch noch der Beweis zu erbringen, dass der ebenfalls noch verbleibende Restfehler auf ein erträgliches Maß gesunken ist. Für den Maschinen- und Anlagenbau sollte dabei ein nicht erkannter Fehler höchstens einmal in einer Milliarde Stunden (mehr als 100.000 Jahre) vorkommen. Unter diesen Bedingungen kann man sichere Netzwerke bis zur obersten Sicherheitskategorie der EN 954-1 verwenden. ■

9764

www.innotecsafety.de

Dr. Peter Wratil ist Geschäftsführer des Unternehmens innotec GmbH, Rosengarten.