Sicherheit auf Ethernetbasis

Das Ethernet ermöglicht Sicherheitsanwendungen, ohne das Standardprotokoll zu modifizieren.

Ethernet ermöglicht einen definierten Durchgriff auf allen Netzwerkebenen und damit Diagnoseinformationen innerhalb eines durchgängigen Netzwerkes. Diese Eigenschaften prädestiniert das Ethernet für Sicherheitsanwendungen, zumal ein Sicherheitslayer eingebunden werden kann, ohne das Standardprotokoll anzutasten.

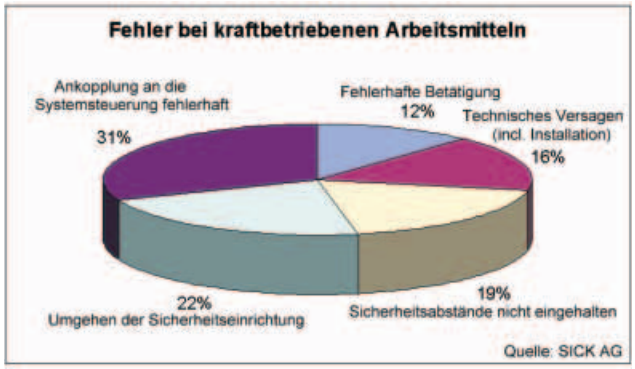

Bild 1: 41% der Fehler haben mit den Sicherheitsvorkehrungen selbst zu tun. Eine gute Sicherheitsarchitektur kann somit auch die Verfügbarkeit erhöhen.

Man kennt die Situation nur zu gut: Während der Nachtschicht wird die Produktion durch einen Fehler im Sicherheitskreis der Maschine gestoppt. Irgendetwas an den Türschaltern, der Verkabelung oder an den Notaus-Geräten ist nicht in Ordnung. Eine rasche Fehlersuche beginnt. Man arbeitet an den Symptomen, den wahren Fehler lokalisiert man nicht. Ein mehrfaches Anfahren der Maschine hat stets den gleichen Fehler zur Folge. Um die Produktion aufrechtzuerhalten, entschließt man sich, den Sicherheitskreis zu überbrücken. Danach kann die Produktion fortgesetzt werden. Leider ist die beschriebene Situation damit oftmals nicht ausgestanden. Nicht selten hat die Überbrückung des Sicherheitskreises fatale Folgen. Bei Nichteinhaltung der organisatorischen Maßnahmen können Personen in den Gefahrenbereich gelangen und sich lebensgefährlich verletzten, solange die Sicherheitskreise nicht aktiviert sind. Spätestens an dieser Stelle wird jedem klar, dass Verfügbarkeit viel mit Sicherheit zu tun hat.

Umgang mit Sicherheit

Noch vor einem Jahrzehnt hörte man von einigen Sicherheitsexperten den Spruch: „Eine sichere Maschine ist eine Maschine, die stillsteht!“ Auch heute noch wird bei fast allen Maschinen und Anlagen der Stillstand als „sicherer Zustand“ definiert. Aber man möchte heute diesen „sicheren Zustand“ immer weniger hinnehmen. Eine schlechte Verfügbarkeit animiert zur Manipulation. Und bei einer kurzgeschlossenen Sicherheitstechnik helfen auch noch so gute organisatorische Maßnahmen recht wenig. Wie die Statistik belegt, passieren in der Tat die meisten Unfälle bei Missachtung der Sicherheitseinrichtungen. Auch die größte Anzahl der Mängel im Maschinenbau ist dort zu finden, wo man die Sicherheitstechnik umgehen kann. Wie Bild 1 verdeutlicht, wird bei 22% aller Fehler die Sicherheitstechnik umgangen. Auch das Nichteinhalten der Sicherheitsabstände und eine fehlerhafte oder unerlaubte Betätigung gehen überwiegend auf das Konto eines menschlichen Fehlverhaltens gegenüber den Sicherheitseinrichtungen. In der Summe dürfte damit ungefähr jeder zweite Fehler mit der Missachtung der Sicherheitsfunktion in Zusammenhang stehen. Eine schlechte Verfügbarkeit oder eine unbrauchbare Ergonomie sind die Hauptursachen.

Strategie: Fehlerlokalisierung

Freilich besteht stets die Möglichkeit, eine Maschine oder Anlage resistenter gegenüber allen Störungen auszulegen.

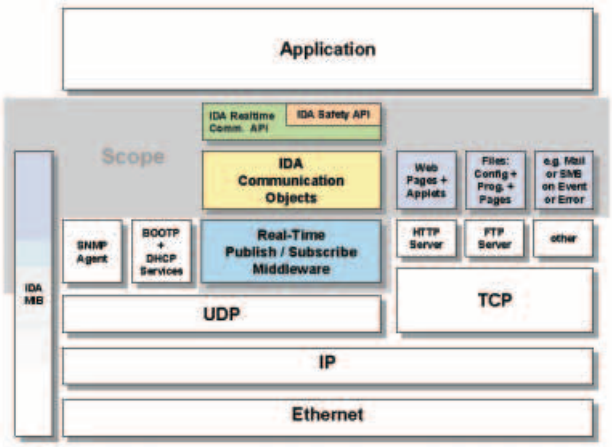

Bild 2: Bei dem Ethernet IDA (Interface for Distributed Automation) wird ein Sicherheitslayer eingefügt, ohne das Standard-Ethernet zu verändern.

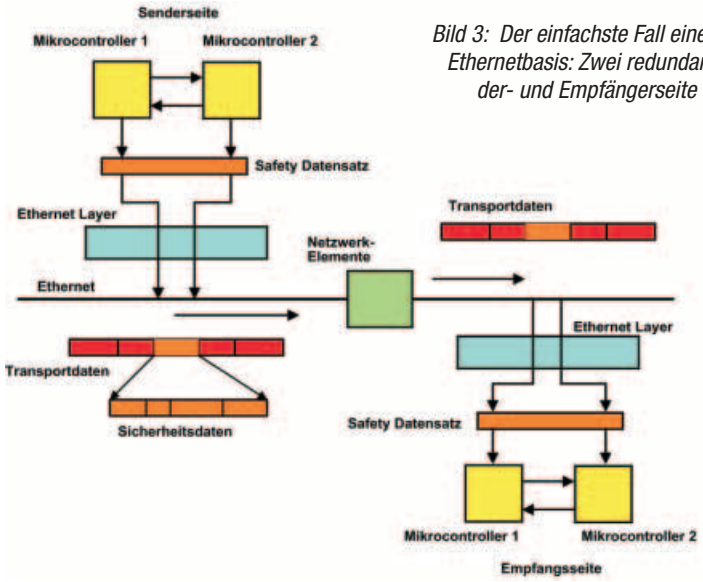

Bild 3: Der einfachste Fall einer Sicherheitsarchitektur auf Ethernetbasis: Zwei redundante Mikrocontroller auf Sender- und Empfängerseite erzeugen eine zweikanalige Sicherheitsverbindung.

Man kann die elektromagnetische Verträglichkeit erhöhen, bessere Sensoren oder Aktuatoren einsetzen. Aber im Endeffekt werden trotzdem Fehler auftreten, die sich nicht gänzlich eliminieren lassen. Viel effektiver fährt man mit der Strategie, mit dem Fehler zu leben, diesen aber sofort zu erkennen und ihn schnellstens zu beheben. Natürlich ist das nur möglich, wenn man von vorne herein nicht zu viele Fehler zulässt und damit eine bereits recht hohe Grundverfügbarkeit garantiert. Zur Strategie der Fehlerlokalisierung tragen Netzwerke ganz besonders bei. Sie verbinden nicht nur Sensoren und Aktuatoren und übertragen Steuerungsdaten, sondern sind auch in der Lage, alle Diagnoseinformationen an eine übergeordnete Leitstelle zu übertragen. Und das führen sie extrem schnell ohne jeglichen Zusatzaufwand durch. Von allen installierten Netzwerken innerhalb der Automatisierungstechnik bringt Ethernet die meisten Vorteile mit sich. Ethernet ermöglicht eine kurze Reaktionszeit, den Anschluss von zahlreichen Teilnehmern und ist oftmals bereits installiert. Eine ganz besondere Eigenschaft von Ethernet besteht jedoch darin, dass man einen definierten Durchgriff von der Automatisierungs- oder Visualisierungsebene bis zum Sensor oder Aktuator hat. Diagnoseinformationen müssen nicht erst über zusätzliche Feldbusse transportiert oder innerhalb von Gateways interpretiert werden. Ethernet stellt damit eine logische Punkt-zu-Punkt-Verbindung zwischen zwei beliebigen Teilnehmern dar. Diese besondere Eigenschaft wirkt sich beim Auftreten eines Fehlerfalls aus. Man erkennt den defekten Teilnehmer oder erhält eine Diagnoseinformation über die aufgetretene Fehlfunktion. Es besteht sogar die Möglichkeit, eine vorkehrende Wartung durchzuführen, da intelligente Teilnehmer auch Daten über Alterung, Schaltzustand, Signalpegel, Verdrahtung der externen Kontakte usw. übertragen. Zudem ersetzt Ethernet (wie jedes andere Netzwerk) alle diskreten Verdrahtungen. Die im Bild 1 angegebenen Fehlerfälle einer falschen Ankopplung an das Steuerungssystem (31%) entfallen damit. In realen Systemen dürften sich damit mehr als drei Viertel aller Fehler durch den konsequenten Einsatz von Ethernet vermeiden lassen.

Ethernet

In den letzten Jahren ist man bei den Ethernet-Anwendungen immer mehr dazu übergegangen, direkt sicherheitsgerichtete Netzwerke zu verwenden. Beispiele hierzu sind: IDA, TTControl, AFDX und andere. Der Einsatz sicherheitsgerichteter Techniken ermöglicht die einfache Integration von allen Sicherheitsgeräten, die man in Maschinen und Anlagen findet (z.B. Notaus-Geräte, Türkontakte, Zweihandschaltungen, sichere Antriebe). Das verwendete Verfahren der Sicherheitsintegration ist nahezu immer gleich: Man fügt in die bekannten Layer des Schichtenmodells einen Sicherheitslayer ein, der alle noch zu unterstellenden Fehlerfälle aus den „normalen“ Applikationen mit hoher Wahrscheinlichkeit erkennt. Die damit noch verbleibende Fehlerrate ist derart gering, dass man mehr als 1 Million Jahre lang Daten übertragen muss, bevor man eine einzige fehlerhafte Nachricht nicht aufdeckt. Am Beispiel des sicheren Ethernets IDA (Interface for Distributed Automation) ist die Einfügung des Sicherheitslayers in Bild 2 dargestellt. Wie das Bild verdeutlicht, wird die Struktur des Standard-Ethernets überhaupt nicht verändert. Der normale TCP/IP-Transfer (Transmission Control Protocoll/Internet Protokoll) bleibt vollkommen unangetastet. Lediglich im UDP-Transfer (User Datagram Protokoll) laufen sicherheitsgerichtete Daten über diesen Sicherheitslayer. Der gesamte Standard-Datenaustausch nimmt in keiner Weise Notiz von der integrierten Sicherheitsfunktion. Damit herrscht eine vollkommene Kompatibilität zum Standard. Die Sicherheitsdaten sind auch nur Bestandteil einer normalen Datenkette, die Teilnehmer miteinander austauschen.

Funktionsweise

Bei der Kommunikation zwischen zwei sicheren Teilnehmern wird auf beiden Seiten der Sicherheitslayer aktiviert und prüft den sicheren Datensatz auf Konsistenz. Die Integration einer sicherheitsgerichteten Information in einem Ethernet-Datensatz hängt von der Applikation ab. Im einfachsten Fall verwendet man zwei

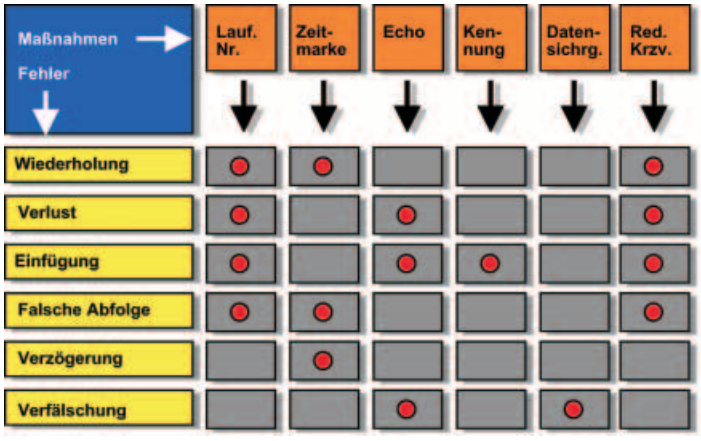

Bild 4: Maßnahmenkatalog für die Fehlererkennung in Netzwerken.

redundante Mikrocontroller, die in ihrem Zusammenspiel den gesamten Sicherheitsdatensatz erzeugen, diesen in den normalen Ethernet-Frame einbinden und auf der Empfängerseite wieder entpacken. Wie in Bild 3 gezeigt wird, erhält man so eine zweikanalige Struktur auf der Sender- und Empfangsseite. Diese beiden Controller sind bei den meisten Anwendungen der Sicherheitstechnik sowieso schon vorhanden, damit man interne Fehler im Interface oder in der externen Schaltung aufdeckt. Die beiden Mikrorechner stellen damit den eigentlichen Sicherheitsteil dar, der auch den Sicherheitsdatensatz verwaltet. Während des Datentransports erscheint nur ein Standard-Datensatz, der innerhalb der Rohdaten diese Sicherheitsinformation enthält. Der sichere Datensatz beinhaltet im Detail viel mehr als nur eine Datensicherung. Über ihn sind zwei Teilnehmer in der Lage, alle zufälligen oder systematischen Fehler aufzudecken. So gibt es eine genaue Zeiterwartung für die Teilnehmer, wann und wie oft sie Nachrichten senden und auf der Empfangsseite erwarten. In der Regel verwendet man hierzu eine laufende Nummer und/oder einen Zeitstempel, mit dessen Hilfe die Reaktionszeit kontrolliert wird. Mittels der laufenden Nummer detektiert man auch Fehler, wenn Nachrichten fehlen oder doppelt verschickt werden. Auch eventuelle Datenvertauschungen werden effektiv erkannt. Wenn sich die verschickten Nummern nicht mehr verändern, so ist das ein sicheres Zeichen, dass der Sender nicht mehr richtig funktioniert (Sender ist eingeschlafen). Ferner enthält der sichere Datensatz auch Informationen über den Sender und den Empfänger, damit man auch Daten sicher erkennen kann, die gar nicht für die einzelnen Teilnehmer bestimmt sind.

Normung

Die speziellen Maßnahmen für sicherheitsgerichtete Netzwerke sind in einem Normenentwurf zusammengefasst (FAET-Entwurf: Fachausschuss Elektrotechnik, Version vom 28.5.2000). Der Entwurf stellt typische Techniken und Verfahren vor, wie man sicherheitsgerichtete Netzwerke entwirft und deren Datensätze zusammenstellt. Neben dem Nachweis der hohen Wahrscheinlichkeit der Fehlererkennung durch spezielle Fehlersicherungsmechanismen enthält der Vorschlag auch einen Maßnahmenkatalog für die sichere Erkennung systematischer Fehler (Bild 4). Für die dargestellt Matrix muss für jede Zeile (Fehlerfall) eine Maßnahme in das Sicherheitsprotokoll integriert werden, damit man die geforderte Sicherheit erreicht. Bild 4 stellt die Maßnahmen für das IDA-Protokoll dar (rote Punkte). Beispielsweise gehören eine laufende Nummer, eine Zeitinformation und eine gute Datensicherung zum Umfang des sicherheitsgerichteten Datensatzes von IDA. ■

www.ida-group.de

Dr. Peter Wratil ist Geschäftsführer der Firma innotec GmbH.