Sichere Netzwerke – Technik und Anwendung

Teil 1: Fehlerarten und Korrekturstrategien

Im letzten Jahrzehnt haben sicherheitsgerichtete Netzwerke diskrete Verkabelungen zunehmend ersetzt. Sie sorgen für eine fehlerfreie Übertragung und garantieren ein Höchstmaß an Sicherheit bei deutlich verbesserter Verfügbarkeit. Entsprechend diesem Trend haben nahezu alle bekannten Feldbusse Sicherheitslayer erhalten, wodurch sowohl Standarddatenverkehr als auch eine sichere Kommunikation über ein einziges Netzwerk abgewickelt werden. Die Technik derartiger Netzwerke ist recht einfach und lässt sich auch auf beliebige Kommunikationsverbindungen anwenden.

Von Dr. Peter Wratil

Bis zum Beginn der neunziger Jahre hatten Netzwerke bei der Erfassung von Sicherheitsdaten oder der Verarbeitung von sicheren Messwerten nichts zu suchen. Gab es doch immer wieder sporadische Fehlerzustände, die man entweder auf fehlerhafte Übertragungen oder falsche Dienste der Bussysteme zurückführen konnte. Netzwerke waren überall dort willkommen, wo es darum ging, Verkabelungskosten einzusparen; aber die sichere Abschaltung durch einen Not-Aus-Taster wollte man den Netzwerken nicht überlassen.

Diese Ansicht hat sich drastisch geändert, nachdem man erkannt hat, dass gerade diskrete Verkabelungen oftmals fehlerträchtig waren und eine nur geringe Diagnosefähigkeit zuließen. Nach und nach wuchs das Vertrauen in Busverbindungen, ohne dass man konkrete Vorgehensweisen oder Techniken vorsah. Im ersten Schritt folgte man der Strategie, die Busverbindungen redundant auszulegen, nach der Devise: Zwei Netzwerke sind sicherer als ein Netzwerk. Dieses Verfahren half auch, die am häufigsten bekannten Fehler zu erkennen, die durch Bitfehler oder Störungen zustande kamen. Allerdings wurden systematische Fehler nur unzureichend aufgedeckt und stochastische Störungen mit nicht hinreichender Wahrscheinlichkeit erkannt.

Seitens der Zulassungsstellen (TÜV, BG) sah man sich alsbald mit dem Problem konfrontiert, dass die Automatisierungstechnik rapide zunahm und manche Anlagen ohne Netzwerke überhaupt nicht zu betreiben waren. So wurde Mitte der neunziger Jahre ein

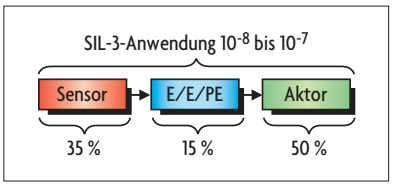

Bild 1. Verteilung der Fehlerfälle innerhalb einer automatisierten Anlage nach Safety Integrity Level 3. Die Netzwerke tragen in ihrer Fehlerträchtigkeit höchstes zu 1% an allen Fehlern bei. Die Angaben nach SIL 3 lassen höchstens einen unerkannten Fehler innerhalb von 10^7 bis 10^8 Stunden zu.

erstes Konzeptpapier entwickelt, das die Grundprinzipien der Technik sicherer Datenübertragungen beschrieb. Dieses FAET-Papier (FAET: Fachausschuss Elektrotechnik) stellt bis zum heutigen Tage die Grundlage für alle sicheren Netzwerke dar [1]. Es basiert auf der internationalen Norm IEC 61508 und formuliert nicht nur Anforderungen, sondern stellt auch Lösungen vor [2]. Dabei werden nur Prinzipien erwähnt, die je nach Anwendung zu ganz verschiedenen Ausprägungen innerhalb der Netzwerkverbindung führen können. Mittlerweile gibt es kaum noch Sicherheitsanforderungen, die nicht mit dem Einsatz von Netzwerken lösbar wären. Ganz besonders tragen sichere Netzwerke dazu bei, Fehler rasch zu entdecken, um damit geeignet reagieren zu können. Man findet die Anwendung dieser neuen Technologie daher nicht nur bei Maschinen und Anlagen, sondern auch ganz besonders bei Transportsystemen wie Flugzeugen oder Bahnanlagen.

Fehler zuverlässig erkennen

Warum sind normale Busverbindungen unsicher? Was unterscheidet eigentlich sichere Netzwerke von Standarddatenverbindungen? Diese beiden Fragen lassen sich nur dann beantworten, wenn man die Ursachen für fehlerhafte Übertragungen kennt und konkrete Maßnahmen vorsieht, diese zu eliminieren. Alle bei Netzwerken bekannten Fehler lassen sich in zwei Kategorien einteilen: in systematische und stochastische Fehler. Zu den systematischen Fehlern gehören beispielsweise Fehler bei der Übertragung, die durch Interface-Einheiten oder Netzwerkkomponenten entstehen. Hier seien als Beispiele die Datenverzögerung oder der Datenverlust in einem Gateway oder einem Ethernet-Switch genannt. Stochastische Fehler machen sich in der Regel durch Bitfehler bemerkbar, die durch EMV-Einflüsse (Elektromagnetische Verträglichkeit) zustande kommen. Zusätzlich wird eine Eignung nach den höchsten Sicherheitsanforderungen nur dann erreicht, wenn sowohl Einzelfehler oder gar Mehrfachfehler nicht zum Versagen der Sicherheitsfunktion führen. So kann beispielsweise ein fehlerhafter CRC-Prüfer (CRC: Cyclic Redundancy Check) innerhalb eines Interface nicht geprüft werden und bei einer fehlerhaften Nachricht auch nicht mehr geeignet reagieren. Sicherheitsgerichtete Datenverbindungen müssen für alle denkbaren Fehlerfälle geeignete Maßnahmen bereithalten, die zumindest eine Fehlererkennung erlauben. Dabei schreibt

die Norm (IEC 61508) eine extrem niedrige Fehlerrestwahrscheinlichkeit vor, die höchstens einen unerkannten Fehler in einem Zeitraum von mehr als 100 000 Jahren zulässt (SIL 3, SIL: Safety Integrity Level).

Netzwerke sind weit mehr als nur das Protokoll der Datenübertragung. Zu den Komponenten des Netzwerks gehören auch alle Interface-Einheiten, die das Netzwerk nachweislich beeinflussen. Hier sind insbesondere auch die Versorgungsgeräte – also die Netzteile – zu beachten, deren Fehler sich auf die Kommunikationsarchitekturen auswirken können. Freilich muss man auch die Einflüsse der Verbindungsstrukturen berücksichtigen, die ganze Datensätze verfälschen können. Eine besonders kritische Anforderung wird an die sicheren Netzwerke durch die Anwendung der Norm gestellt. Hier gilt aus Erfahrung eine Aufteilung der Fehlerfälle innerhalb einer automatisierten Anlage. Wie *Bild 1* zeigt, entfallen in der Regel 35 % aller Fehler auf die Sensorik, 15 % auf die Steuerung und 50 % auf die Aktorik. Die Netzwerke tragen in ihrer Fehlerträchtigkeit höchstes zu 1% an allen Fehlern bei. Entsprechend müssen Netzwerke 100-mal zuverlässiger sein als der Rest des Automatisierungssystems.

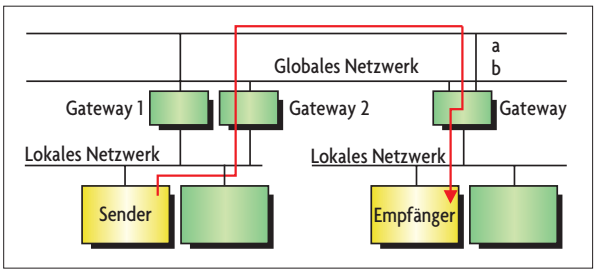

Bild 2. Datentransfer zwischen einem Sender und einem Empfänger unter Verwendung einer Standard-Netzwerkarchitektur.

Systematische Fehler

Die Architektur aller beteiligen Netzwerkkomponenten bestimmt den gesamten Ablauf der Kommunikation. Bereits bei der wohl einfachsten Aufgabe, ein Telegramm von einem Sender zu einem Empfänger zu schicken, gibt es zahlreiche mögliche Fehler. So können Nachrichten verschwinden, eventuell sogar doppelt versendet werden oder durch eine Zerstückelung in kleine Pakete aufgeteilt werden, die dann während der Übertragung in falscher Reihenfolge vorliegen.

Moderne Netzwerke erlauben dazu auch noch den gleichzeitigen Datenverkehr von Standard-Telegrammen, die Sicherheitstelegramme nachhaltig zu stören vermögen. Gerade bei der Verwendung des Ethernet als Kommunikationsmedium bettet man die Sicherheitstelegramme in den Standard-Datenverkehr ein. Damit treten bei der Kommunikation alle Fehler auf, die beim normalen Datenverkehr auch vorkommen. Dieser Standard-Datenverkehr wird oftmals als „Grauer Kanal“ bezeichnet, der für die sicheren Daten „Gelber Kanal“ als Transportvehikel fungiert. *Bild 2* stellt eine derartige Kommunikationsverbindung zwischen einem Sender und einem Empfänger dar. Der Sender überträgt seine Daten zu einem bestimmten Empfänger und verwendet hierzu die vorhandene Netzwerkarchitektur. In dem Beispiel geschieht das im ersten Schritt über das angeschlossene lokale Netzwerk, dessen Daten von einem Gateway zum globalen Netzwerk übertragen werden. Im zweiten Schritt nimmt ein anderes Gateway diese Daten auf und sendet sie zum lokalen Netzwerk der Empfängerseite. Letztlich gelangen dann die Daten von diesem lokalen Netzwerk zum gewünschten Empfänger.

Innerhalb dieser recht einfachen Struktur können mannigfaltige Fehler zustande kommen, die eine sichere Datenübertragung beeinflussen:

- Ein Gateway nimmt zwar die Daten auf, unterlässt aber den Weitertransport. Eventuell erfolgt auch der Weitertransport, aber die Daten werden über das falsche Netzwerk weitergeleitet. In jedem Fall kommen die gewünschten Daten nicht beim Empfänger an.
- Die beiden Gateways 1 und 2 nehmen jeweils die Daten auf und versenden sie getrennt über die globalen Netzwerke a und b. Damit liegen die Daten doppelt im Empfänger vor.
- Das gesamte Datentelegramm ist wegen einer zu großen Länge nicht auf einmal zu übertragen. Also wird es in einzelne Pakete zerlegt, die nach und nach über die beiden Gateways 1 und 2 über die Netzwerke a und b transportiert werden. Hierbei kann man die Reihenfolge leicht vertauschen, so dass der Empfänger das Gesamttelegramm nicht mehr richtig erhält.

Bei genauer Analyse der Kommunikationsstruktur und der Eigenschaften der verwendeten Komponenten lassen sich noch weitere Fehler unterstellen, die in *Bild 3* dargestellt sind. Ein Antrieb führt innerhalb einer Maschine eine gefährliche Funktion aus. Sobald eine Gefahr für eine Person entsteht (z.B. Zutritt in den gefahrvollen Bereich), muss der Antrieb über einen Not-Aus-Taster sicher abgeschaltet werden. Diese recht einfache Aufgabe kann durch vielerlei Fehlfunktionen scheitern:

- Das Gateway 2 überträgt zwar die Daten vom Not-Aus zum Antrieb, allerdings enthält dieses Gateway bereits intelligente Komponenten, die Nachrichten speichern und verzögert herausgeben. In ungünstigen Fällen kann das Gateway bis zu 100 000 Nachrichten enthalten, die erst nach und nach zum Empfänger oder zu anderen Teilnehmern gelangen. Die Not-Aus-Anforderung gelangt zwar sofort zum Gateway, dieses sendet aber noch alle anderen Nachrichten aus, und es dauert viel zu lang, bis die Abschaltanforderung zum Antrieb gelangt.
- Bei der gleichzeitigen Übertragung von Standarddaten über die verwendeten Netzwerke sind auch weitere Fehler zu unterstellen, die aufgrund der

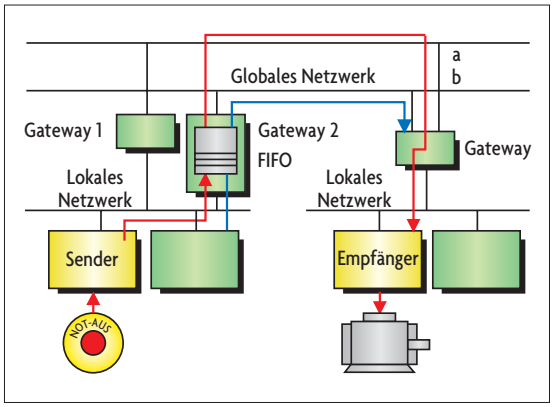

Bild 3. Not-Aus-Abschaltung eines Antriebs über ein Netzwerk mit unterschiedlichen Netzwerkkomponenten.

Überlastung der Gateways oder der Netzverbindung entstehen.

● Geradezu bösartig sind Probleme, die ihre Ursache in der Maskerade von Standarddaten haben. Dabei stellen sich die „normalen Daten“ eines Teilnehmers als „sichere Daten“ dar, die den Antrieb zu einer Fehlfunktion anleiten.

Maßnahmen zur Erkennung systematischer Fehler

Gegen alle genannten systematischen Fehlerfälle gibt es bestimmte Maßnahmen, die jeden zu unterstellenden Fehlerfall aufdecken [3, 4]. Ein wesentliches Prinzip muss bei sicheren Netzwerken unbedingt eingehalten werden: Jeder Sender hat sich regelmäßig bei seinem Empfänger zu melden. Damit muss der Not-Aus-Taster seinem angeschlossenen Antrieb nicht nur dann etwas mitteilen, wenn er gerade betätigt wird, sondern er sendet dem Antrieb auch laufend Nachrichten, wenn sich nichts verändert hat. Er meldet damit in festen zyklischen Abständen: „Ich bin nicht betätigt – ich bin nicht betätigt – ...“. Nur so kann der Empfänger feststellen, dass etwas nicht stimmt, wenn längere Zeit Nachrichten von seinem Sender ausbleiben. Kabelunterbrechungen oder fehlgeleitete Telegramme sind damit sofort erkennbar.

Unterbleibt die Datenübertragung für einen längeren Zeitraum, so muss der Empfänger eine Sicherheitsreaktion durchführen. Im Falle der Ansteuerung eines Antriebs kann das beispielsweise ein sofortiger Notstopp sein. Der Empfänger enthält daher immer eine Uhr, die auf eine maximale Reaktionszeit programmiert ist und von jeder gültigen Nachricht zurückgesetzt wird. Wenn die Uhr ohne das Erkennen einer gültigen Nachricht abläuft, so erfolgt die Sicherheitsreaktion. Allerdings wird hier bereits deutlich, dass der Datenverkehr sicherheitsgerichteter Netzwerke erheblich größer ist, als der von normalen Netzwerken. Sichere Netzwerke müssen alle Empfänger laufend bedienen, auch wenn es nicht Neues gibt. Alle Maßnahmen, die wirkungsvoll gegen systematische und sporadische Fehler helfen, sind in der Matrix in *Bild 4* dargestellt.

Die Matrix ist derart angelegt, dass zu jedem möglichen Fehlerfall genau eine Zeile gehört. In den Spalten stehen die Maßnahmen, die zur Aufdeckung der Fehlerfälle herangezogen werden können. Eine wirkungsvolle Maßnahme ist innerhalb der grauen Felder mit einem roten Punkt gekennzeichnet. Beim Aufbau sicherheitsgerichteter Netzwerke ist daher stets darauf zu achten, dass man für jede Zeile zumindest eine Maßnahme ergreift, damit man alle vorkommenden Fehler mit Sicherheit erkennt.

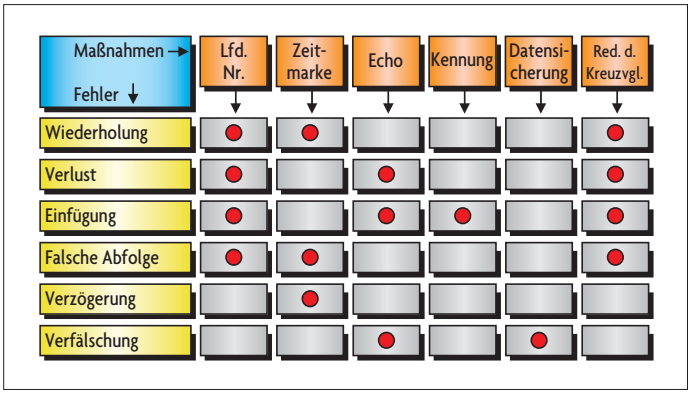

Bild 4. Diese Matrix stellt alle zu unterstellenden Fehler bei der Nachrichtenübertragung dar. Die möglichen Fehler sind gelb gekennzeichnet. Zur Aufdeckung jeder dieser Fehlerfälle gibt es eine oder mehrere Maßnahmen, die in den orangefarbenen Fehlern eingefügt sind. Die roten Punkte in den entsprechenden Matrixfeldern geben an, ob die Maßnahme wirkungsvoll ist. (Red. d. Kreuzvgl. = Redundanz durch Kreuzvergleich)

Jede Maßnahme führt zu ganz spezifischen Ausprägungen innerhalb des Datenaufbaus sicherer Nachrichten. Eine der besonders wichtigen Maßnahmen besteht darin, den Daten eine laufende Nummer mitzugeben. Hierdurch werden gleich vier Fehler mit Sicherheit aufgedeckt. Verlust, Einfügung, Wiederholung oder falsche Abfolge fallen sofort auf, wenn der Empfänger die ankommenden Nummern in ihrer Reihenfolge überprüft. Wenn es sich um einfache Netzwerke handelt, die keine verzögernden Netzwerkgeräte enthalten, so benötigt man neben dem Einfügen einer laufenden Nummer nur noch eine zuverlässige Datensicherung. Diese Methode ist weit verbreitet und findet bei zahlreichen sicheren Bussystemen Anwendung, sofern die Datenverbindung über einfache Leitungen realisiert ist.

Wenn die Netzwerkverbindung sich allerdings als komplexer oder gar als unbekannt herausstellt, so muss die Laufzeit einer Nachricht kontrolliert werden. Das gelingt entweder durch das Zurücksenden einer Antwort in Form einer Bestätigung oder durch das Einfügen einer Zeitmarke. Bei der Verwendung einer Zeitmarke wird eine Quittierung überflüssig. Jedem Datensatz wird die Sendezeit aufgeprägt. Man spricht daher auch von einem Zeitstempel. Beim Erhalt der Nachricht durch den Empfänger prüft dieser die Laufzeit und entscheidet, ob die Nachricht aktuell oder veraltet ist. Grundlage einer solchen Netzwerkstruktur ist allerdings, dass alle Teilnehmer über Uhren verfügen, die sie irgendwann miteinander verglichen haben. Dieser Uhrenvergleich mag recht schwierig klingen, er bringt allerdings den enormen Vorteil, dass man sich alle Quittierungen sparen kann. Die Buslast (Anzahl der Nachrichten pro Zeiteinheit) wird nahezu halbiert. Die typischen Funktionen innerhalb der Automatisierungstechnik, die darin bestehen, dass Ausgänge durch die Funktionen der Eingänge verändert werden, sind für den Datenverkehr mit Zeitstempel geradezu prädestiniert. Hier spielen in der Regel verlorene oder eingefügte Nachrichten keine Rolle, sofern eine gültige Nachricht innerhalb der Reaktionszeit erscheint. Die letzte Nachricht ist die aktuellste und damit die beste. Der Empfänger braucht somit nur die Gültigkeit einer erhaltenen Nachricht prüfen und den Zeitstempel abfragen. Wenn der Zeitstempel jünger als der letzte ist, so wird der Zustand entsprechend der neueren Nachricht aufgefrischt. *Bild 5* stellt ein Prüfungsverfahren für einen Empfänger dar, der die Laufzeit kontrolliert.

In Abhängigkeit der Genauigkeit der internen Uhren zwischen Sender und Empfänger müssen die Uhren regelmäßig verglichen werden. Die im Bild 5 vorgestellte Methode ist dabei nur eine von vielen [7, 8]. Zum Vergleich der Uhrzeit sendet der Empfänger eine Anfrage an den Sender. Dieser liest seine interne Uhr aus und überträgt den Wert an den Empfänger.

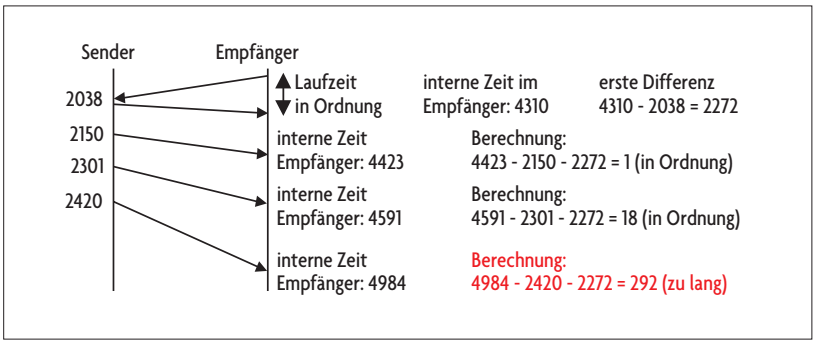

Bild 5. Verfahren zum Uhrenvergleich und zur Kontrolle der Laufzeit zwischen einem Sender und einem Empfänger.

Wenn die gesamte Laufzeit von der Anfrage bis zum Erhalt der Nachricht recht klein ist, so kann der Empfänger aus der Kenntnis seiner eigenen Uhrzeit und dem erhaltenen Wert die Differenz der beiden Uhren hinreichend genau bestimmen. Beispielsweise können sich die beiden Teilnehmer auf eine Taktrate von 10 µs geeinigt haben. Durch die erste Berechnung ermittelt der Empfänger eine Uhrendifferenz zwischen ihm und seinem Sender von ca. 23 ms (4310 – 2038 = 2272, zu je 10 µs-Einheiten ergibt 22,72 ms). Jede weitere Nachricht versieht der Sender nun mit seiner Uhrzeit. Der Empfänger kann jeweils durch eine Subtraktion des ersten Wertes und des Empfangswertes von seiner aktuellen Zeit die Laufzeit ermitteln. Beispielsweise beträgt die Laufzeit bei der ersten Nachricht 10 µs und bei der zweiten Nachricht 180 µs. Wenn die maximale tolerierbare Reaktionszeit etwa bei 1 ms liegt, so kommt die 3. Nachricht zu spät, da sie eine Laufzeit von 2,92 ms hatte.

Sporadische Fehler

Bereits im Bild 4 sind schon Maßnahmen zur Erkennung sporadischer Fehler dargestellt. Dabei hat das Verfahren, ein Echo zu schicken, nur theoretische Bedeutung. Beim Echo sendet der Empfänger die erhaltene Nachricht zurück und der Sender kann nun prüfen, ob der Inhalt richtig ist. Das Verfahren belastet den Busverkehr stark und ist mit zwei wesentlichen Nachteilen behaftet. Einerseits erhält nur der Sender die Information, ob die Nachricht richtig oder falsch war. Da aber nicht vom Sender, sondern vom Empfänger in der Regel die gefahrvolle Funktion ausgeht, muss dieser erst über eine eventuell falsche Nachricht in Kenntnis gesetzt werden. Andererseits kann ein möglicher Fehler in der einen Datenrichtung genau durch die Rücksendung in die andere Datenrichtung eliminiert werden. Dieser Doppelfehler würde nicht erkannt und führt zum eventuellen Versagen der Sicherheitsfunktion. Daher haben sich Datensicherungsverfahren eher durchgesetzt, die kein Echo benötigen und anhand einer Datensicherung funktionieren [6, 9].

Zur Absicherung der Dateninformation (gemeint ist eigentlich der gesamte Datensatz) verwendet man daher Verfahren, bei denen zusätzliche Bits in Form von Codierungen eingefügt werden, anhand derer man auf die Richtigkeit der Gesamtinformation schließen kann. Diese zusätzlichen Bits werden auch als Redundanz bezeichnet. Die wohl einfachste Form einer solchen Redundanz ist das Hinzufügen eines Paritätsbits. Hierbei wird der eigentlichen Information (Nutzdaten) ein Bit hinzugefügt, das je nach der Anzahl der Nullen oder Einsen entweder selbst den Wert Null oder Eins annehmen kann. Beispielsweise kann man die Anzahl der Einsen in einem Telegramm zählen und dann bei einer ungeraden Anzahl ein Paritätsbit mit dem Wert 1 hinzufügen (*Bild 6*).

Wenn ein Telegramm aus einer Anzahl von Einsen und Nullen besteht (grün unterlegt im Bild 6), so fügt man ein einzelnes Paritätsbit (rot) hinzu. Ein einzelner Fehler wird durch diese Maßnahme mit Sicherheit erkannt, da sich in jedem Fall entweder die Parität im Datensatz oder das Paritätsbit selbst verändert. Zur Abschätzung der Güte eines Sicherungsverfahrens wird oftmals der Begriff der Hamming-Distanz verwendet. Dabei gibt die Hamming-Distanz an, wie viele Bits sich mindestens verändern müssen, damit eine neue Nachricht entsteht, die nicht mehr als fehlerhaft erkennbar ist. Das Verfahren der Paritätssicherung hat da-

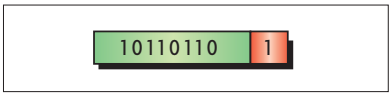

Bild 6. Durch Hinzufügung eines Paritätsbits (rot unterlegt) kann ein Fehler erkannt werden.

Bit 0	1	0	0	1	1	1	1	0	1
Bit 1	0	1	1	1	0	0	0	0	1
Bit 2	1	1	0	0	0	0	0	1	1
Bit 3	0	0	0	1	1	1	1	1	1
Bit 4	1	0	1	1	0	0	1	1	1
Bit 5	1	1	0	0	0	0	1	0	1
Bit 6	1	1	0	1	0	1	0	1	1
Bit 7	0	0	1	1	1	1	0	0	0
Parität	1	0	1	0	1	0	0	0	1

Bild 7. Erzeugung einer Kreuzsicherung für 8 Byte Nutzdaten.

Bit 0	1	0	0	1	1	1	1	0	1
Bit 1	0	0	1	1	0	0	0	1	1
Bit 2	1	1	0	0	0	0	0	1	1
Bit 3	0	0	0	1	1	1	1	1	1
Bit 4	1	0	1	1	0	0	1	1	1
Bit 5	1	0	0	0	0	0	1	1	1
Bit 6	1	1	0	1	0	1	0	1	1
Bit 7	0	0	1	1	1	1	0	0	0
Parität	1	0	1	0	1	0	0	0	1

Bild 8. Vier Fehler innerhalb der Kreuzsicherung führen zum Versagen der Fehlererkennung.

Bit 0	1	0	0	1	1	1	1	0	1
Bit 1	0	0	1	1	0	0	0	1	1
Bit 2	1	1	0	0	0	0	0	1	1
Bit 3	0	0	0	1	1	1	1	1	1
Bit 4	1	0	1	1	0	0	1	1	1
Bit 5	1	1	0	0	0	0	1	0	1
Bit 6	0	1	0	1	0	1	0	0	1
Bit 7	0	0	1	1	1	1	0	0	0
Parität	1	0	1	0	1	0	0	0	1

Bild 9. Je nach Position der Fehler im Datenfeld lassen sich auch vier oder gar mehrere Fehler mit Sicherheit erkennen. Gelbes Feld: Fehler wird erkannt.

mit eine Hamming-Distanz von 2, da bereits 2 Fehler nicht mehr erkennbar sind.

Da Netzwerke nicht selten stark gestört werden, ist eine Sicherung mittels einer Parität oftmals unzureichend. Ein wesentlich besseres Sicherungsverfahren besteht in der Kreuzsicherung. Hierbei werden die übertragenen Datenbytes in Form einer Matrix angeordnet. Zu jedem Byte erzeugt man die Parität und am Schluss wird nochmals die Gesamtparität über alle Bitpositionen der Bytes bestimmt. Die so ermittelten Einzelparitäten und die Gesamtparitäten werden mit den Daten übertragen. *Bild 7* zeigt das Verfahren für die Übertragung von 8 Bytes.

Aus der Anordnung der Daten mit den entsprechenden Paritätsbits wird sofort klar, dass hier eine Hamming-Distanz von 4 erreicht wird. Wie *Bild 8* zu entnehmen ist, müssen schon mindestens vier Fehler auftreten, damit man eine Nachricht erhält, deren fehlerhafter Inhalt unentdeckt bleibt. Wie Bild 8 aber schon deutlich zeigt, müssen sich die vier unentdeckbaren Fehler an speziellen Positionen befinden. Sie bilden quasi ein Rechteck im Datenfeld. Damit gibt es zahlreiche Kombinationsmöglichkeiten, vier oder gar mehr Fehler im Datenfeld zu verteilen, die mit Sicherheit erkannt werden, obwohl die Hamming-Distanz nur 4 ist. *Bild 9* stellt eine Kombination von Fehlern dar, die aufzudecken ist.

Checksumme: zuverlässige Fehlererkennung

Neben dem soeben vorgestellten Verfahren der Kreuzsicherung wird bei sicheren Datenverbindungen auch die Datensicherung über CRC (Cyclic Redundancy Check) verwendet. Das Sicherungsverfahren besteht darin, dass zu jedem Dateninhalt ein Sicherungsanteil hinzugefügt wird, der durch eine mathematische Operation erzeugt wird. CRC-Sicherungen weisen gegenüber den Kreuzsicherungsverfahren einige Vorteile auf, die darin bestehen, dass einerseits die Anzahl der Sicherungsbits nicht mit der Anzahl der Daten ansteigt, denn CRC-Sicherungen garantieren eine feste Hamming-Distanz bis zu einer gewissen Anzahl von Nutzdaten (beispielsweise 4 oder 6); andererseits dass CRC-Sicherungen auch Büschelfehler zu erkennen vermögen, die sich innerhalb eines kleinen Bereichs der Daten aufhalten, auch wenn hier gar fünf oder mehr Fehler verborgen sind. Bei der Verwendung von CRC-Sicherungen wird jedem Datensatz eine Codierung angehängt, die für die Bitkombination des Datensatzes einzigartig ist.

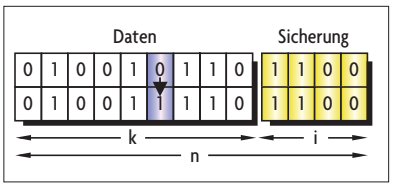

Bild 10. Dem zu übertragenden Datensatz wird eine Codierung angehängt, die nur in diesem Datensatz vorkommt. Ein Fehler ist sofort erkennbar, da er in der Gesamtinformation zu einer Kennung führt, die nicht vorkommen darf.

Bild 10 stellt ein Beispiel für ein Datum mit einer Codierung dar. Der Einfachheit halber wurde hier ein Datenbyte mit 8 bit und eine Sicherung mit 4 bit gewählt. Die gesamte übertragene Information beträgt damit 12 bit (k + i = n). Ein möglicher Fehler während der Übertragung führt zu einer Informationskette, die nicht erlaubt ist. Daher wird diese vom Empfänger sofort als falsch identifiziert.

Geschickterweise wählt man die Sicherungscodierungen (in Bild 10 gelb hinterlegt) derart, dass jeweils mehrere Bits verändert werden müssen, damit eine neue mögliche Nachricht entsteht. Damit gibt die Wahl dieser Codierung bereits die Hamming-Distanz vor. Sofern zu jedem Datensatz eine geeignete Codierung gefunden wird, geht aus Bild 10 bereits hervor, dass ein Großteil aller möglichen Fehler immer aufgedeckt wird. Wie das Bild zeigt, gibt es ja nur k Felder für die Kombinationen der Daten (hier also $2^k = 256$ Kombinationen). Dem gegenüber stehen n Möglichkeiten (also 2^n Kombinationsmöglichkeiten, in diesem Fall also 4096 Möglichkeiten). 4096 Möglichkeiten stehen somit nur 256 zugelassenen Kombinationen gegenüber. Die Wahrscheinlichkeit, einen Fehler nicht zu erkennen, beträgt damit 256/4096 = 1/16. Damit ist die noch übersehbare Fehlerrate stets in dem Bereich der Anzahl der Bits aus den Sicherungsdaten ($2^i = 16$).

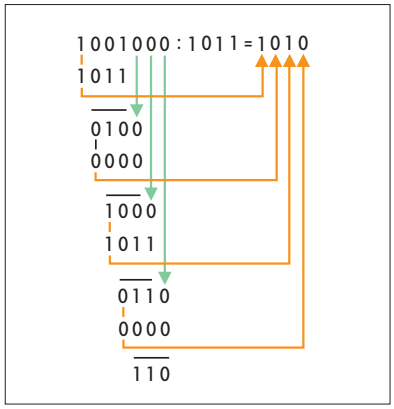

Bild 11. Erzeugung des Rests für die Übertragung einer CRC-Sicherung.

Die Sicherung über CRC basiert auf einem mathematischen Verfahren, bei dem sich Sender und Empfänger auf ein gewisses Generatorpolynom einigen. Die Wahl dieses Polynoms

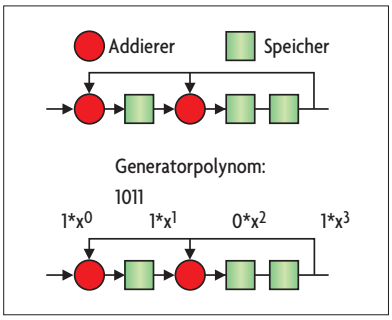

Bild 12. Aufbau eines Schieberegisters zur Berechung der Division mit dem Generatorpolynom 1011.

hängt von der Güte der Fehlererkennung und von der Länge der zu übertragenden Daten ab. Zur Erzeugung der Datensicherung multipliziert der Sender zuerst die gesamte Dateninformation mit dem Grad des Generatorpolynoms (also beispielsweise mit 4). Danach dividiert er diesen Wert durch das Generatorpolynom und versendet die Daten unter Anhängung des Restes aus der Division. *Bild 11* stellt den Vorgang für das Generatorpolynom (1011) dar.

Die Dateninformation besteht aus der Bitkombination 1001000. Bei der Division wird wie beim schriftlichen Dividieren vorgegangen, wobei man allerdings beachten muss, dass als Operation nicht die bekannte Division (aus der Schulmathematik) herangezogen wird, sondern eine exklusive Oder-Operation zugrunde liegt (ungleiche Werte führen zum Wert 1, gleiche Werte führen zum Wert 0). Rechner können derartige Operationen in extrem kurzer Zeit durchführen. Auch der Empfänger hat nicht viel Arbeit, die Richtigkeit der empfangenen Information zu prüfen. Er entnimmt den empfangenen Wert und dividiert diesen durch das bekannte Generatorpolynom. Wenn hierbei kein Rest übrig bleibt, war die Nachricht richtig (sofern nicht eine höhere Anzahl an Fehlern als die garantierte Hamming-Distanz vorliegt).

Die Division kann man auch mit einem Schieberegister nachbilden, das in seiner Struktur bereits die Form des Generatorpolynoms enthält. *Bild 12* stellt ein Schieberegister dar, welches dem Generatorpolynom 1011 entspricht. Die zu dividierende Funktion (hier 1001000) wird bitweise in das Schieberegister eingefügt. An den Addiererstellen erfolgt die logische Verknüpfung des exklusiven Oders (*Bild 13*). Nach dem vollständigen Durchlauf der gesamten Nachrichtenkette verbleibt der Rest (110) im Schieberegister.

Neben den vorgestellten Verfahren der Datensicherung gibt es noch einige weitere, die jedoch nur untergeordnete Bedeutung haben. Ein Großteil der bekannten sicherheitsgerichteten Netzwerke verwendet CRC-Sicherungen, da sie besondere Eigenschaften aufweisen:

- Je nach Wahl des Polynoms wird eine Hamming-Distanz von 4 erreicht.
- Alle ungeradzahligen Fehler werden bis zur Größe des Exponenten eines Generatorpolynoms erkannt.
- Büschelfehler, die sich innerhalb eines Bereichs aufhalten, der kleiner ist als der Exponent des Generatorpolynoms, werden ebenfalls erkannt.
- CRC-Generatorpolynome sind bestens bewährt und in der Literatur aufgeführt.

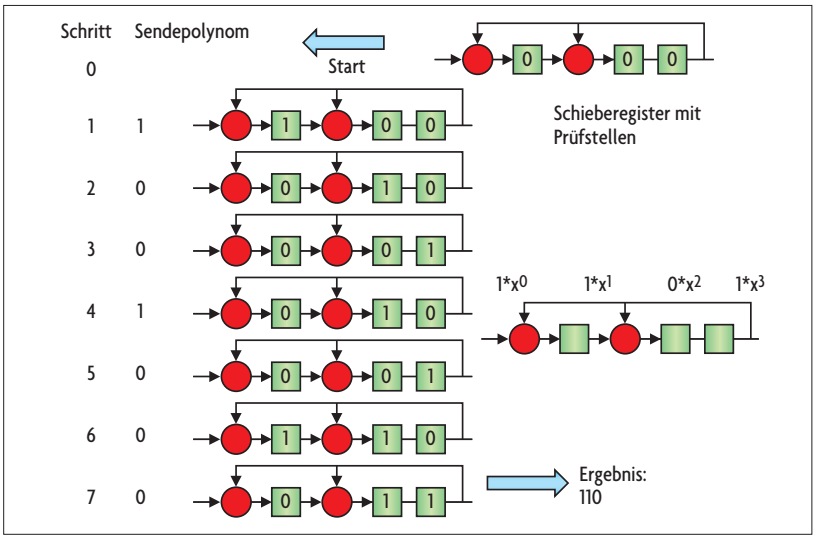

Bild 13. Bildung des Restes aus der Division durch das Generatorpolynom mittels eines Schieberegisters.

Bei der Überprüfung der Sicherungsdaten einer Übertragung sollte man nicht auf die integrierte Hardware des Empfangsbausteins zurückgreifen, da diese ausgefallen sein könnte. Eine defekte Hardware fällt in der Regel nur auf, wenn man sie testen kann. *jk*

Dr. Peter Wratil

studierte in Köln Physik und war Hauptabteilungsleiter für Automatisierungs- und Sicherungstechnik bei Klöckner-Moeller in Bonn. Eine weitere Station führte ihn als Bereichsleiter zur Körber AG in Hamburg, bis er 1998 die Innotec GmbH gründete, die sich mit Sicherheit im Maschinen- und Anlagenbau beschäftigt.

E-Mail: peter.wratil@innotecsafety.de

Der zweite und letzte Teil dieses Beitrags beschreibt sichere Datenformate und den Nachweis der Sicherheit. Er erscheint in einer der nächsten Ausgaben der Elektronik.

Literatur

[1] *Fachausschuss Elektrotechnik (Hrg.):* Grundsatz für die Prüfung und Zulassung von „Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten". Fachausschuss Elektrotechnik, Gustav-Heinemann-Ufer 130, 50698 Köln, Version Mai 2002.

[2] IEC 61508: Functional safety of electric/electronic/programmable electronic safety-related systems, IEC part 1-7.

[3] *Schaefer, M.:* New concepts for safety-related bus systems. BIA St. Augustin.

[4] *Schaefer, M; Reinert. D.:* Bus-Software mit Feuermelder. Hüthig-Verlag, IEE Heft 8/1998.

[5] *Gall, H,; Steffens, T.; Kemp, K.:* Anwendung der Bussysteme in der Anlagensicherheit der Chemie-Industrie. TÜV Anlagentechnik GmbH.

[6] *Lochmann, D.:* Digitale Nachrichtentechnik. Signale, Codierungen, Übertragungssysteme, Netze. Berlin, 1995.

[7] *Wratil, P.:* Sicherheitsgerichteter Datenverkehr im Ethernet. SPS-Magazin, Ausgabe 7/2001.

[8] *Wratil, P.:* Safety über Ethernet. Computer & Automation, Ausgabe 10/2001.

[9] *Wratil, P.:* Speicherprogrammierbare Steuerungen in der Automatisierungstechnik. Vogel-Verlag, Würzburg 1989.