Sichere Netzwerke – Technik und Anwendung

Teil 2: Sichere Datenformate und Nachweis der Sicherheit

Im ersten Teil dieses Beitrags wurden mögliche Fehlerquellen bei der Netzwerk-Kommunikation gezeigt und Gegenstrategien vorgestellt. Im vorliegenden zweiten Teil geht es darum, wie die sichere Kommunikation über ein Übertragungsprotokoll abgewickelt wird und wie sich die Sicherheit nachweisen lässt – damit die Busse das von der IEC-Norm 61508 geforderte Maß an Sicherheit erreichen.

Von Dr. Peter Wratil

Die in Teil 1 dieses Artikels [10] vorgestellten Maßnahmen prägen die Struktur sicherer Datenformate. Nahezu alle Übertragungsformate enthalten eine Kennung, die sich entweder als Sender- oder als Empfängeradresse darstellt. Damit wird sichergestellt, dass keine fremden Daten vom Sender zum Empfänger gelangen, da sich die beiden Busteilnehmer vorher über die Adressierung geeinigt haben. Das Problem der Maskerade ist damit im Wesentlichen beseitigt. Des Weiteren enthält der sichere Datensatz eine laufende Nummer oder einen Zeitstempel. Zusätzlich zu den eigentlichen Nutzdaten erscheint dann auch noch die Datensicherung. *Bild 1* stellt ein typisches Beispiel eines sicherheitsgerichteten Telegramms dar.

Bild 1. Typischer Aufbau eines sicherheitsgerichteten Telegramms mit einer Kennung, dem Zeitstempel, den Daten mit der Längenangabe und einer Sicherung.

Das Telegramm beginnt mit der Adresse, die beispielsweise die Adresse des Senders sein kann. Anhand dieser Adresse erkennt der Empfänger, dass die Nachrichten für ihn bestimmt sind. Er ist ja z.B. an dem Zustand des Not-aus-Tasters interessiert. Danach folgt der Zeitstempel mit der aktuellen Sendezeit des Senders. Eventuell kommt dann eine Längeninformation, die man nur benötigt, wenn man eine variable Anzahl von Daten versenden möchte. Nach der Längenangabe folgen die Nutzdaten selbst. Das gesamte Telegramm inklusive der Adresse, des Zeitstempels, der Längeninformation und der Daten wird über die CRC-Information gesichert. Mit zunehmender Datenlänge und mit anwachsender Störbeeinflussung werden Mehrfachfehler immer wahrscheinlicher. Da ein vierfacher Fehler nicht mehr mit Sicherheit durch die CRC-Information aufgedeckt wird, passieren mit nicht zu vernachlässigbarer Wahrscheinlichkeit fehlerhafte Telegramme die Sicherheitsprüfung und gelten damit als fehlerfrei. In diesen Fällen wendet man einen Trick an, der darin besteht, das gesamte Sicherheitstelegramm zu verdoppeln. Das kostet zwar etwas Übertragungszeit, macht sich aber bei der Sicherheit deutlich bemerkbar. *Bild 2* zeigt ein solches Telegramm, das lediglich aus zwei Telegrammen des Bildes 1 besteht.

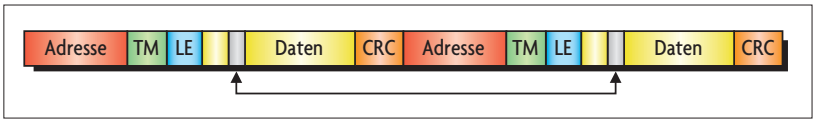

Bild 2. Sicherheitstelegramm mit Verdopplung des Einzeltelegramms zur Erhöhung der Sicherheit.

Das Gesamttelegramm, das aus den beiden Einzeltelegrammen besteht, hat die Eigenschaft, dass nun auch noch alle Fehler aufgedeckt werden, die nicht identische Positionen in beiden Einzeltelegrammen aufweisen. Hierzu vergleicht man nach dem Empfang die beiden Einzeltelegramme Bit für Bit. Ein unentdeckter Fehler kann überhaupt nur existieren, wenn beide Einzeltelegramme an identischer Stelle Fehler aufweisen, die auch zu identischen Bitkombinationen führen (durch den Pfeil verknüpfte Felder in Bild 2). Da jeder CRC für sich mindestens jeden Dreifachfehler aufdeckt, müssen schon sowohl im vorderen als auch im hinteren Einzeltelegramm mindestens vier Fehler vorliegen. Die Gesamtfehlerzahl beträgt damit mindestens acht. Darüber hinaus können die vier Fehler innerhalb der Einzeltelegramme nicht irgendwie verstreut sein, sondern müssen sich zwingend an identischen Positionen befinden. Diese letzte Eigenschaft führt sogar dazu, dass die Fehlerwahrscheinlichkeit mit zunehmender Datenmenge wieder absinkt.

Das Verfahren der Datenverdopplung zeichnet sich auch durch eine hohe Immunität gegenüber Büschelfehlern aus. Diese Art von Störungen tritt in regelmäßig wiederkehrenden Abständen auf und kann mehrere hintereinander liegende Bits verändern. Da die CRC-Sicherung in der Regel nur acht benachbarte gestörte Bits erkennt (bei einem CRC mit einem 8-bit-Polynom), werden größere Fehlerstrukturen nicht mehr sicher aufgedeckt. Wie aus *Bild 3* aber ersichtlich wird, wirkt hier die Wiederholung der Daten ganz besonders. Die Störung im ersten Datensatz muss ja eine identische Störstruktur im zweiten Datensatz hinterlassen, damit ein Vergleich versagt.

Nachweis der Sicherheit

Der Nachweis der Sicherheit gelingt nur mit Hilfe der Wahrscheinlichkeitsrechnung. Das heißt, man kann nur eine statistische Aussage manchen, wie wahrscheinlich ein nicht erkennbarer Fehler ist. Dabei ist es also gleichgültig,

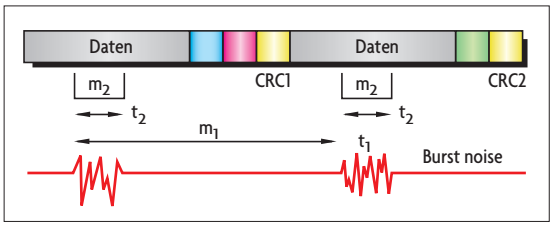

Bild 3. Büschelfehler erscheinen in der Regel mit einer festen Frequenz (t_1). Die Störduaer beträgt t_2. Die Größen m_1 und m_2 dienen zur Berechnung der Fehlerwahrscheinlichkeit.

ob der Fehler in der nächsten Stunde oder erst in einer Million Jahren auftritt. Man ist lediglich an einer mittleren Größe interessiert, die eine hohe Sicherheit bietet. Nach den Anforderungen der IEC 61508 entsprechend SIL 3 sollte die Wahrscheinlichkeit für einen nicht erkennbaren Fehler geringer als 10^{-7} pro Stunde für das Gesamtsystem sein. Aus den vorher genannten Gründen muss die Netzwerkverbindung sogar 100mal besser sein.

Als Basis der Berechnung wird die sog. Binomialverteilung herangezogen [6]. Diese Verteilung führt zu einer statistischen Kalkulation unter der Annahme, dass alle Bits des Telegramms gleichverteilt gestört werden können. In *Bild 4* ist ein Datensatz (8 Bits) mit zwei Fehlstellen gezeigt. Wenn die Wahrscheinlichkeit für die Störung eines Bits genau p ist, dann beträgt die Wahrscheinlichkeit für eine doppelte Störung p × p, also p^2. Voraussetzung ist dabei, dass die Störungen wirklich unabhängig voneinander sind. Für Büschelfehler lässt sich die Berechnung nicht heranziehen. Eine größere Anzahl an Fehlern kann man damit durch die Multiplikation der Einzelwahrscheinlichkeiten beschreiben:

$$p_{sum} = p_1 \cdot p_2 \cdot \ldots \cdot p_x \qquad (1)$$

Wenn ein Datensicherungsverfahren durch eine garantiere Hamming-Distanz e Fehler aufdeckt, so beträgt die Wahrscheinlichkeit für diesen Fehlerfall p^e:

$$p_{sum} = p^e \qquad (2)$$

Wenn die gesamte gesicherte Information aus n Bits besteht, so kann man die Wahrscheinlichkeit angeben, dass alle anderen Bits fehlerfrei sind. Hierzu verwendet man die Gegenwahrscheinlichkeit (n – e Bits sind nicht gestört):

$$p_{sum} = (1-p)^{n-e} \qquad (3)$$

Damit berechnet sich die Wahrscheinlichkeit für das genaue Auftreten von e fehlerhaften Bits zu:

$$p_{sum} = p^e \cdot (1-p)^{(n-e)} \qquad (4)$$

Bis jetzt gibt Gleichung 4 noch die Wahrscheinlichkeit an, dass man die Fehler an genau festgelegten Stellen vermutet. Da aber die bekannten Sicherungsverfahren nur eine feste Anzahl von Fehlern aufdecken, die unabhängig von der festen Position sind, muss man noch einen Faktor vorsehen, der auf die Verteilung der Fehler im Telegramm eingeht. Dieser Faktor ist:

$$A_{n,e} = \binom{n}{e} = \frac{n!}{e!(n-e)!} \qquad (5)$$

Der Faktor $A_{n,e}$ gibt alle möglichen Kombinationen an, e Fehler auf n Stellen im Telegramm zu verteilen. Diese Permutationsformel mag dem einen oder anderen noch aus der Schulmathematik bekannt sein, als es darum ging, für ein Lottospiel die Möglichkeiten von 6 richtigen Positionen unter 49 Möglichkeiten zu finden. Insgesamt berechnet sich damit die Wahrscheinlichkeit, e fehlerhafte Bits auf n Bits zu haben mit:

$$R = A_{n,e} \cdot p^e (1-p)^{(n-e)} \qquad (6)$$

Dabei spielen jetzt die Positionen keine Rolle mehr. Die fehlerhaften Bits können sich überall im Telegramm aufhalten. Bei der Berechnung von n ist es aber wichtig, dass man stets die Bits des CRC mit berücksichtigt, da sich auch hier Fehler verbergen können.

Wenn das verwendete Sicherungsverfahren eine gewisse Hamming-Distanz garantiert, so kann der erste nicht erkennbare Fehlerfall auftreten, wenn die Anzahl der Fehler dieser Hamming-Distanz entspricht. Freilich kann eventuell auch eine größere Fehleranzahl

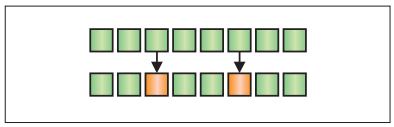

Bild 4. Störung von zwei beliebigen Bits innerhalb eines Datensatzes von 8 Bits.

nicht sicher erkannt werden. Damit muss man alle Fehlerfälle, von der Hamming-Distanz bis zu der Anzahl der Datenbits, im Telegramm berücksichtigen:

$$R_{(p)} = \sum_{e=d}^{n} A_{n,e} \cdot p^e (1-p)^{(n-e)} \qquad (7)$$

Wenn man die Datensicherung mittels eines CRC durchführt, so kann man die Summation auch nur über die gerade Anzahl der Fehlerfälle laufen lassen, da ungerade Fehlerraten sicher erkannt werden (bis zum Grad des Polynoms). Allerdings stellt Gl. (7) einen mehr theoretischen Wert dar, da höhere Fehlerwerte (oberhalb der Hamming-Distanz) mit Wahrscheinlichkeiten auftreten, die um Zehnerpotenzen niedriger sind. Für eine realistische Kalkulation ist daher Gl. (6) fast immer ausreichend.

Wenn man die Datensicherung über CRC durchführt, kann man auch noch einen Reduktionsfaktor hinzufügen, der durch die Aufdeckung aller Fehler zustande kommt, die zwar eine Fehleranzahl enthalten, die größer als die Hamming-Distanz ist, aber dennoch erkennbar sind:

$$R_s = R_p \cdot \left(\frac{1}{2}\right)^r \qquad (8)$$

Bei der Wiederholung des Telegramms kann man noch einen weiteren Faktor einfügen, der die Permutation von Fehlerstellen berücksichtigt, wenn man im vorderen als auch im

Anzahl der Nutzdaten-bytes	Bitfehlerrate p = 0,001 (im Mittel 1 Bit pro 1000 gestört)	Fehlerrestwahr-scheinlichkeit für einen Datenverkehr mit 10 000 Nachrichten pro Sekunde und einer Störrate von 0,001
9	$1{,}964 \cdot 10^{-26}$	$7{,}070 \cdot 10^{-17}$
20	$9{,}853 \cdot 10^{-26}$	$3{,}547 \cdot 10^{-16}$
32	$5{,}339 \cdot 10^{-21}$	$1{,}922 \cdot 10^{-11}$

Fehlerrestwahrscheinlichkeit bei der Übertragung von Ethernet-Powerlink-Safety. Die Technik vermag bis zu 10 000 Telegramme pro Sekunde zu verschicken.

hinteren Datensatz identische Positionen annimmt:

$$B_{m,e} = \binom{m}{e}^{-1} = \left(\frac{m!}{e!(m-e)!}\right)^{-1} \quad (9)$$

Bei dieser Gleichung bezieht sich m auf die zu prüfenden Bits (beispielsweise nur die Datenbits).

Alle bis jetzt vorgestellten Gleichungen gelten für die Wahrscheinlichkeiten eines einzelnen Telegramms. Die Norm IEC 61508 bezieht sich aber auf Fehlerraten innerhalb einer Stunde. Da man bei Datenverkehr zahlreiche Telegramme pro Stunde verschickt, ist die berechnete Wahrscheinlichkeit auf den Fehlerfall innerhalb einer Stunde zu berechnen:

$$\Lambda_s = R \cdot 100 \cdot 3600 \cdot \nu \quad (10)$$

Der so aufgestellte gesamte Wert für die Wahrscheinlichkeit enthält bereits den Faktor 100 für die Fehleraufteilung innerhalb des Gesamtsystems. Der Faktor 3600 gibt die Anzahl der Sekunden in einer Stunde an und ν gibt die Anzahl der Telegramme pro Sekunde wieder (Frequenz). Gl. (10) ist strenggenommen nur dann richtig, wenn zur Datenübertragung nur jeweils ein Telegramm notwendig ist.

Unter Berücksichtigung aller vorher vorgestellten Maßnahmen lassen sich auch bei hohen Frequenzen ganz ausgezeichnete Werte erzielen. Die *Tabelle* gibt als Beispiel die Fehlerrestwahrscheinlichkeit für die Übertragung von Ethernet-Powerlink-Safety wieder. Die Technik vermag bis zu 10 000 Telegramme pro Sekunde (alle 100 µs ein Telegramm) zu verschicken. Durch die Verwendung geeigneter CRC-Polynome und das Verfahren der Datenwiederholung beträgt die Einzelfehlerrate kaum mehr als 10^{-20}. Die gesamte Fehlerrate pro Stunde liegt noch deutlich niedriger als 10^{-10}. Damit werden alle Anforderungen nach SIL 3 bestens erreicht (SIL 3 fordert Werte kleiner als 10^{-7}).

Sichere Netzwerke, die ohne eine Datenwiederholung auskommen, bringen Fehlerrestwahrscheinlichkeiten mit, die pro Telegramm bei 10^{-10} liegen. Um hier eine Eignung nach SIL 3 nachzuweisen, muss entweder die stochastische Störrate reduziert oder die

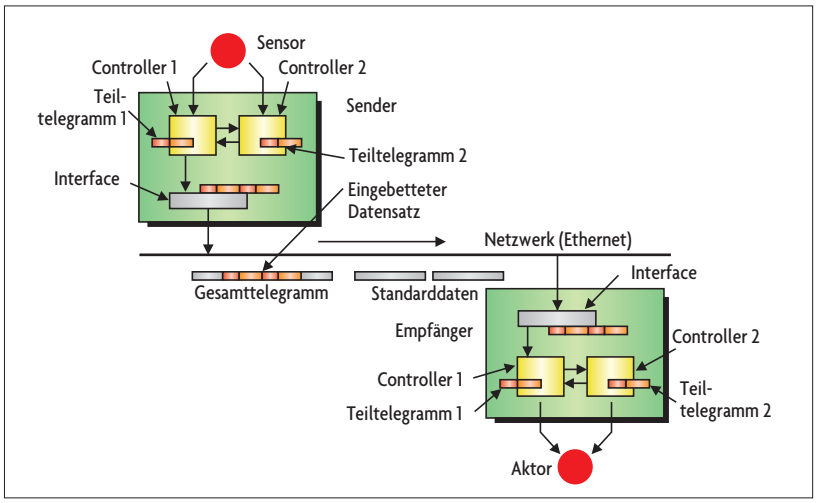

Bild 5. Eine Architektur zur sicheren Erfassung und Übertragung von Sensordaten. Die Struktur ist von der Erfassung bis zur Auswertung zweikanalig.

Anzahl der Telegramme pro Stunde begrenzt werden.

Integration des sicheren Netzwerkes in die Automatisierungsstruktur

Das sichere Netzwerk stellt nur einen zwar wichtigen aber eher kleinen Bestandteil des gesamten Automatisierungssystems dar. Im Prinzip geht es darum, die Sensordaten zu erfassen und deren Zustand zu einem Aktor zu übertragen. Jede Ankopplung des sicheren Netzwerkes zwischen der Sensorgröße und der Aktorgröße kann Probleme mit sich bringen, die dadurch entstehen, dass man mögliche Fehler eventuell nicht erkennt. Je besser die Integration des Netzwerkes in die Automatisierungsapplikation gelingt, desto sicherer wird das gesamte System. Optimal stellt sich eine Lösung dar, bei der das Netzwerk bereits ein fester Bestandteil der Datenerfassung und der Datenauswertung ist. In *Bild 5* ist eine überaus sichere Architektur zu sehen, die das gesamte Sicherheitstelegramm als festen Bestandteil der Applikation nutzt.

Der Sender dient als sichere Verarbeitungseinheit zur Erfassung von Sensordaten. Zur Abdeckung der Anforderungen nach IEC 61508 (SIL 3) kommt nur eine zweikanalige Struktur in Frage. Die beiden Controller 1 und 2 messen unabhängig voneinander die Sensorgrößen. Nach gegenseitiger Funktionskontrolle und internem Vergleich erzeugt jeder Controller jeweils ein Teiltelegramm, das genau die Hälfte des endgültigen Übertragungstelegramms darstellt. Über das Interface werden beide Telegrammhälften zusammengefügt und mit weiteren (nicht sicherheitsrelevanten) Daten versehen. Das so erzeugte Telegramm wird dann mit anderen Telegrammen über das Netzwerk verschickt (z.B. über Ethernet). Der Empfänger ist ebenfalls zweikanalig aufgebaut und geht bei der Verarbeitung des erhaltenen Gesamttelegramms genau in umgekehrter Reihenfolge wie der Sender vor. Das Interface verteilt die beiden Teiltelegramme auf die Controller 1 und 2. Beide Controller prüfen die Fehlerfreiheit der Daten durch Kontrolle der mitgeführten CRC. Zusätzlich werden alle Datenbits zwischen den Controllern verglichen. Erst nach diesen Prüfungen kann der Datensatz als sicher angesehen werden und der Aktor wird entsprechend angesteuert.

Eine derartige Übertragungsstruktur bietet eine hohe Immunität gegenüber allen systematischen und stochastischen Störungen. Sofern man das Telegramm mit einem Zeitstempel versieht, können auch Daten über unbekannte Netzwerkkomponenten sicher übermittelt werden.

Selbst in proprietären Netzwerken einsetzbar

Sicherheitsgerichtete Datenstrukturen beruhen stets auf ähnlichen Prinzipien. Je nach Anforderung lassen sich geringste Fehlerrestwahrscheinlichkeiten erreichen. Hierzu stehen zahlreiche Techniken zur Verfügung. Unkomplizierte Methoden erlauben es sogar, die Verfahren bei proprietären Netzwerken einzusetzen. Je weiter man die Prinzipien der sicheren Netzwerktechnik in die Architektur der Automatisierung integriert, desto besser werden alle Fehlerfälle aufgedeckt. *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

Literatur

[1] 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.

[10] *Wratil, P.:* Sichere Netzwerke – Technik und Anwendung; Teil 1: Fehlerarten und Korrekturstrategien. *Elektronik* 2005, H. 21, S. 72ff.