Landesumweltamt Nordrhein-Westfalen

Forschungsvorhaben 35/00

Anwendung der Bussysteme in der Anlagensicherheit der Chemie-Industrie

von

Dipl.-Ing. Heinz Gall

Dipl.-Ing. Thomas Steffens

Dipl.-Ing. Klaus Kemp

TÜV Anlagentechnik GmbH
Automation, Software und Informationstechnologie (ASI)

Inhaltsverzeichnis **Seite**

Tabellenverzeichnis

Seite

Abbildungsverzeichnis

Bussysteme in der Anlagensicherheit

1 Einleitung

In der heutigen industriellen Landschaft haben Rechner- und Mikroprozessorsysteme einen nicht mehr wegzudenkenden bzw. zu vernachlässigenden Stellenwert eingenommen. So hängt häufig das Leben und die Gesundheit von Personen bzw. die Unversehrtheit von Umwelt oder auch die Erhaltung von hohen Sachwerten von der ordnungsgemäßen Funktion solcher Systeme ab.

Darüber hinaus nimmt die Menge der Informationen, die in komplexen industriellen Steuerungen benötigt und verarbeitet werden, stetig zu. Um diesen Kommunikationsumfang bewältigen zu können, werden in zunehmendem Maße Feldbussysteme für Prozessleitsysteme und prozessnahe Komponenten eingesetzt.

Zusätzlich zu den Prozessdaten müssen auch Daten verarbeitet werden, die in sicherheitsgerichtete Funktionen eingebunden sind. Die Übertragung der sicherheitsgerichteten Daten erfolgt in der Regel immer noch durch eine direkte Punkt-zu-Punkt Verdrahtung der Sicherheitskomponenten mit einer speicherprogrammierbaren Steuerung (SPS) und dem notwendigerweise damit verbundenen hohen Verdrahtungsaufwand.

Moderne Sensoren und Aktoren bieten bereits heute mit ihren umfangreichen Parametriermöglichkeiten und den Diagnosefunktionen komfortable Möglichkeiten für den Betrieb, wobei aber in den meisten Fällen eine effiziente und den Anforderungen der Sicherheitstechnik entsprechende Kommunikation über ein Feldbussystem noch nicht realisiert ist.

Durch den mittlerweile hohen Verbreitungsgrad von Feldbussystemen in der gesamten Industrie und den damit verbundenen Vorteilen stellt sich zunehmend die Frage, ob und unter welchen Bedingungen diese Feldbussysteme auch für die anfallenden sicherheitsgerichteten Aufgaben in der Verfahrenstechnik - wie in der VDI/VDE 2180 beschrieben - eingesetzt werden können.

Der wesentliche Zweck dieses Forschungsvorhabens ist die Beantwortung der Frage: Ist bei dem gegenwärtig fortgeschrittenen Stand der Signalübertragungstechnik die Übertragung von Signalen einer Schutzeinrichtung mittels eines Bussystems **gemeinsam** mit den Signalen der Betriebs- und Überwachungseinrichtungen ohne Verlust von Zuverlässigkeit, Verfügbarkeit und Funktionalität und ohne Zunahme des Risikos, d. h. auf mindestens gleichem sicherheitstechnischen Niveau wie bei Punkt-zu-Punkt verdrahteten Sicherheitskomponenten bei SSPS Einsatz, in der Verfahrenstechnik möglich.

Diese Studie wendet sich an Anlagenbetreiber und Anlagenerrichter, die beabsichtigen, ein Feldbussystem für sicherheitsrelevante Aufgaben im Sinne der 12. BImSchV (Störfall-Verordnung) zukünftig einzusetzen sowie an Behörden oder Institutionen, die solche Systeme prüfen, genehmigen bzw. abnehmen.

Neben einer grundlegenden Sicherheitsbetrachtung aus Sicht der Normen werden die theoretischen Grundlagen der verschiedenen Feldbussysteme sowie ihre Vor- und Nachteile in Bezug auf die Sicherheitstechnik behandelt.

Ferner wird auf die Problematik, ob und unter welchen Randbedingungen die verfügbaren Feldbussysteme möglicherweise schon heute in der Sicherheitstechnik eingesetzt werden können, eingegangen. Hierzu werden neben den Anforderungen aus der Normung auch Einflussfaktoren wie Verfügbarkeit und die sichere Parametrierung der Busteilnehmer untersucht.

2 Normung

Die heute in der Industrie eingesetzten gängigen Feldbussysteme sind in verschiedenen Normen erfasst. Hierbei sind nur jeweils einzelne Teilbereiche der Feldbussysteme in der Norm beschrieben. Diese Normungen orientieren sich an dem ISO-OSI-Schichtenmodell, wobei fast durchgängig bei allen Feldbussystemen die Schichten 1 und 2 spezifiziert sind.

Die Schicht 1 legt die physikalische Realisierung, wie z. B. Spannungspegel und Medium für die Übertragung fest. In der Schicht 2 werden Festlegungen bezüglich des Buszugriffes und der Telegrammstruktur getroffen. Darüber hinaus wird bei einigen Feldbussystemen auch die Schicht 7 behandelt. In ihr wird die Generierung und Interpretation von Nachrichten einheitlich geregelt. Dies hat den Vorteil, dass sich Geräte verschiedener Hersteller problemlos über den Feldbus verständigen können.

In diesen gängigen Feldbusnormen sind Maßnahmen zur Sicherung der Datenübertragung festgelegt. Hierbei stellt sich die Frage, ob diese Maßnahmen ausreichend sind, um diese Feldbussysteme für sicherheitsrelevante Aufgaben einzusetzen. Eine Aussage darüber existiert zur Zeit in der Normung über Feldbussysteme nicht.

Die Maßnahmen, die für eine sichere Datenübertragung erforderlich sind, werden in der übergeordneten Norm IEC 61508 „Functional safety of electrical/electronic/programmable electronic safety-related systems“ behandelt.

Diese Norm muss auch bei der sicherheitstechnischen Betrachtung von Feldbussystemen Anwendung finden, da diese in der Regel auch aus programmierbaren Komponenten bestehen und mit Mikrocontrollern bestückt sind. In diesem Zusammenhang ist auch die DIN V VDE 0801 „Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben“ zu betrachten.

3 Grundlegende Sicherheitsbetrachtung

Wird beabsichtigt, Feldbussysteme für sicherheitsrelevante Anwendungen einzusetzen, sind sie wie rechnergestützte, programmierbare Systeme zu behandeln, und es sind die Anforderungen aus den dafür gültigen Normen (IEC 61508/DIN V VDE 0801) zu berücksichtigen.

Zum besseren Verständnis dieser Thematik wird im weiteren Verlauf kurz auf die Grundlagen der Sicherheitsbetrachtung der Normen IEC 61508 und DIN V VDE 0801 eingegangen.

Im allgemeinen sind die sicherheitstechnischen Anforderungen an Rechner bzw. Feldbussysteme anwendungsunabhängig. Die Höhe der Anforderungen richtet sich nach dem Risiko und dem Gefährdungspotential, das von der jeweiligen Anwendung ausgeht.

Die Fachgremien für „Funktionale Sicherheit“ haben Anforderungen an Rechner, Rechnersysteme bzw. Steuerungssysteme allgemein in Anforderungsklassen (AK) bzw. Safety Integrity Levels: (SIL) eingeteilt. Dadurch sind die anwendungsorientierten Fachgremien in der Lage, den in ihrem Bereich vorhandenen Gefährdungspotentialen die entsprechende AK bzw. SIL zuzuordnen und damit die Anforderungen an die Steuerungen und Rechner zu bestimmen.

Das in der Normung zur funktionalen Sicherheit gewählte Verfahren zu einer anwendungsunabhängigen Klassenbildung basiert auf einer grundsätzlichen Risikobetrachtung, wie sie in der DIN V19250 beschrieben ist und aus der Abbildung 3-1 hervorgeht.

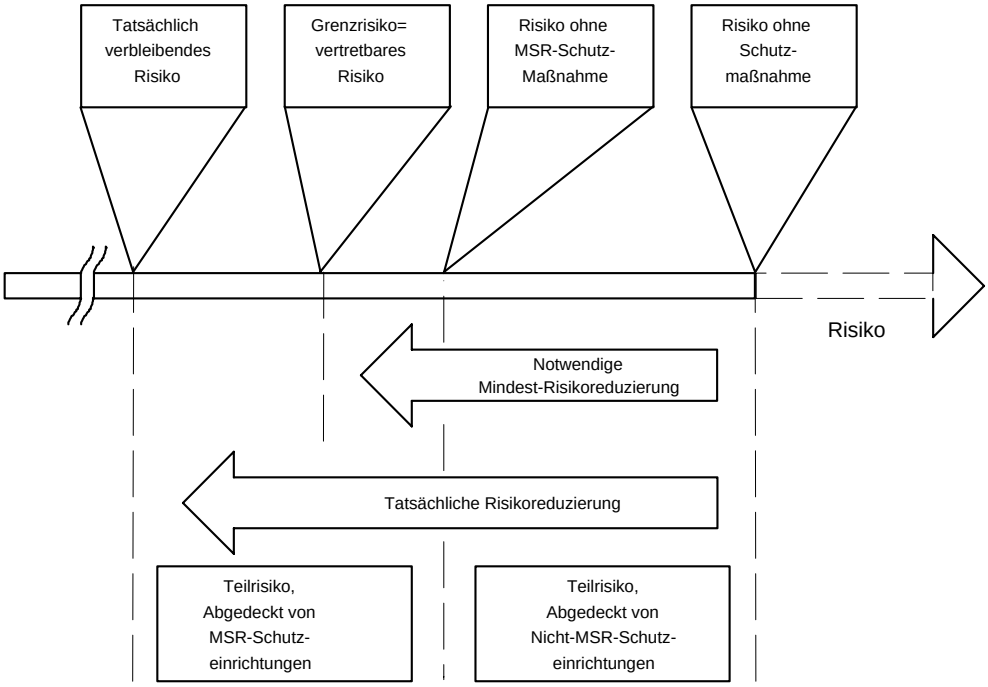


Abbildung 3-1 Risikoreduzierung nach DIN V 19250

Die gleiche Beschreibung der Risikoreduzierung wird auch in dem internationalen Standard IEC 61508 verwendet, um die Anforderungen zu definieren, bzw. eine Klasseneinteilung vorzunehmen.

Diese nachfolgend beschriebene neutrale Risikobetrachtung muss von den anwendungsorientierten Fachgremien mit Fakten „belegt“ werden. Daraus folgt eine Zuordnung zu einer Anforderungsklasse bzw. zu einem SIL als Richtschnur für Betreiber, Entwickler und Prüfinstitute.

Das Risiko (R) ist definiert als eine Größe, die die zu erwartende Häufigkeit (H) des Eintritts eines Schadens und das zu erwartende Schadensausmaß (S) nach der folgenden Berechnung berücksichtigt:

$$\mathbf{R = H \times S} \qquad (3.1)$$

Risiko ist folglich eine Größe, die sich aus der Kombination der Häufigkeit und des Schadensausmaßes ergibt.

Diese Größe stellt das objektiv vorhandene Risiko dar und nicht das von der Gesellschaft oder dem Einzelnen (z. B. bezüglich Auto- oder Eisenbahnverkehr) empfundene Risiko. Dieses von der Gesellschaft bzw. dem Einzelnen empfundene Risiko wird als Risikoakzeptanz bezeichnet.

Um nun eine Abstufung unterschiedlicher Anforderungsklassen bzw. SIL abhängig vom Risiko durchführen zu können, ist es erforderlich, ein Verfahren zur Bestimmung des wirklich vorhandenen Risikos einzuführen. Es bieten sich mehrere Möglichkeiten an. Eine Möglichkeit ist die Quantifizierung des Risikos, die hier nicht weiter betrachtet wird, da eine Quantifizierung des Risikos in den meisten Anwendungsfällen nicht möglich ist.

Ein vereinfachter Weg ist die Verwendung von Risikoparametern, um eine qualitative Abschätzung des Risikos durchzuführen (siehe [DIN V 19250] und [IEC 61508]). Dabei ist darauf zu achten, dass die Risikoparameter nur auf das von der gesamten Sicherheitseinrichtung einschließlich der Kommunikationsverbindungen abzudeckende Risiko angewendet werden. Wie aus Abbildung 3-2 hervorgeht, können Risiken, die von einer Anwendung ausgehen, auch durch andere technische und nicht technische Maßnahmen, wie z. B. seltener Aufenthalt im Gefahrenbereich, reduziert werden.

Während sich das Schadensausmaß (S) noch relativ leicht abschätzen lässt, werden zur Abschätzung der Häufigkeit (H) Hilfsgrößen benutzt, die leichter als H abzuschätzen sind.

Dies sind:

- **A:** zeitlicher Aufenthalt von Personen im Gefahrenbereich,
- **G:** die Möglichkeit einer Gefahrenabwendung,
- **W:** die Wahrscheinlichkeit des unerwünschten Ereignisses ohne Vorhandensein der MSR-Schutzeinrichtung.

Mit den Größen S, A, G und W, die als Risikoparameter verwendet werden, ergibt sich der folgende angegebene Zusammenhang:

$$\mathbf{R = f\,(S, A, G, W)} \qquad (3.2)$$

Die Risikoparameter S, A, G und W werden nun in einige wenige, sinnvolle Bereiche abgestuft:

Schadensausmaß S: (hier nur Personenschäden aufgeführt, Umwelt und Sachschäden auch möglich)

- **S1:** Leichte Verletzung
- **S2:** Schwere, irreversible Verletzung von einer oder mehreren Personen, Tod einer Person
- **S3:** Tod mehrerer Personen
- **S4:** Katastrophale Auswirkung, sehr viele Tote

Aufenthaltsdauer A:

- **A1:** Seltener bis häufiger Aufenthalt im Gefahrenbereich
- **A2:** Häufiger bis dauernder Aufenthalt im Gefahrenbereich

Gefahrabwendung G:

G1: Möglich unter bestimmten Bedingungen

G2: Kaum möglich

Eintrittswahrscheinlichkeit des unerwünschten Ereignisses W:

W1: Sehr geringe Wahrscheinlichkeit des unerwünschten Ereignisses

W2: Geringe Wahrscheinlichkeit des unerwünschten Ereignisses

W3: Relativ hohe Wahrscheinlichkeit des unerwünschten Ereignisses

In der DIN V 19250 ist vorgegeben, wie die Risikoparameter in der in Abbildung 3-2 angegebenen Weise in einem sogenannten Risikographen zueinander in Bezug zu setzen sind. Aus dem Graphen ergibt sich die Zuordnung von der Anforderungsklasse zu den angegebenen Risikoparametern entsprechend dem vorher analysierten Risiko.

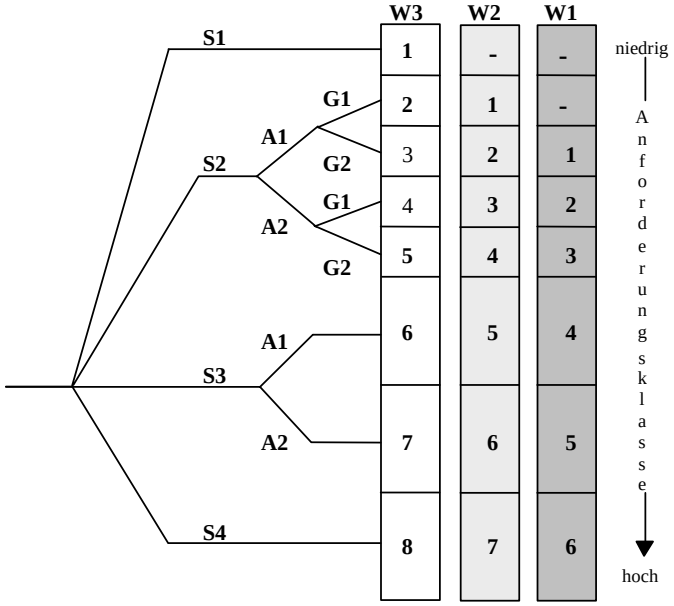


Abbildung 3-2 Risikograph und Anforderungsklassen nach DIN V 19250

Damit ergibt sich die Möglichkeit, dem im Einzelfall vorhandenen Risiko- bzw. Gefährdungspotential acht Anforderungsklassen gegenüberzustellen.

In der IEC 61508 ist der oben gezeigte Risikograph als ein Beispiel zur Ermittlung von Safety integrity level dargestellt. Die Risikographen in der IEC 61508 führen im Endergebnis zu vier Klassen, die dort als "Safety integrity level" (SIL) bezeichnet sind. Diese vier “Safety integrity level“ können unter bestimmten Voraussetzungen den acht Anforderungsklassen gegenübergestellt werden, wie in der folgenden Tabelle 3-1 dargestellt.

Tabelle 3-1 Gegenüberstellung von Anforderungsklassen, Risikobereich und Safety Integrity Level

Risikobereich (NE31/ VDI/VDE2180)	Anforderungsklasse (DIN V 19250)	Safety integrity level (IEC 61508)
I	**1**	Keine Sicherheitsanforderungen
	2, 3	**1**
	4	**2**
II	**5, 6**	**3**
--	**7**	**4**
	8	Ein einzelnes System ist nicht ausreichend zur Erfüllung der Sicherheitsanforderungen

Neben den Anforderungsklassen und den Safety integrity Level gibt es im Bereich der NAMUR-Empfehlungen eine weitere Einteilung in zwei Risikobereiche.

Der Risikobereich I findet Anwendung bei geringem Risiko, d. h. das Risiko ohne PLT-Schutzeinrichtung liegt nur wenig oberhalb des Grenzrisikos. Bei einem höheren Risiko gilt der Risikobereich II und die entsprechenden Maßnahmen [NE31].

Bei der Gegenüberstellung der Anforderungsklassen nach DIN V 19250 und DIN V VDE 0801 mit den Safety integrity level nach IEC 61508 sind die folgenden Aspekte besonders zu berücksichtigen.

In der DIN V VDE 0801 ist ein Rechnersystem als Sicherheitssystem definiert. Es wird dort das Rechnersystem vom Eingang des Systems bis zu dessen Ausgang betrachtet. Im Prinzip werden nur Anforderungen an das Rechnersystem gestellt. Die weiteren Komponenten zur Anschaltung an die Anlage oder den Prozess (Feldinstrumentierung) werden nicht betrachtet.

Die IEC 61508 betrachtet dagegen jeweils die sicherheitsrelevante Funktion, das heißt es wird immer eine gesamte Funktionskette, z. B. Sensor - Rechner (logische/programmierbare Einheit) - Aktor, betrachtet. Die unterschiedlichen Zuordnungen zeigt die nachfolgende Abbildung 3-3.

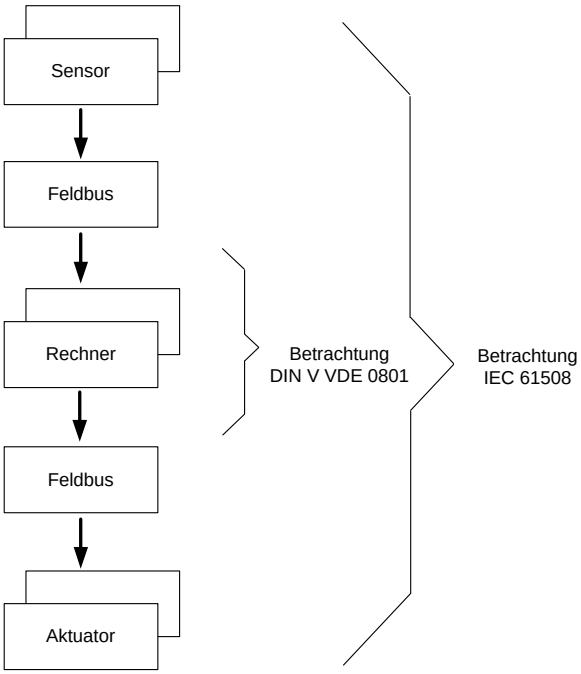


Abbildung 3-3 Vergleich der Sicherheitsbetrachtungen nach DIN V VDE 0801 und IEC 61508

Die dargestellte Funktionskette muss nach IEC 61508 insgesamt die Anforderungen des jeweiligen safety integrity levels erfüllen. Somit sind auch die Feldbussysteme mit in die Betrachtung einzubeziehen.

Mit der Festlegung des safety integrity levels ergeben sich Umfang und Wirksamkeit, der zu realisierenden sicherheitstechnischen Maßnahmen. Welcher Umfang und welche Wirksamkeit die einzelnen fehlervermeidenden und fehlerbeherrschenden Maßnahmen haben müssen ist in der anwendungsunabhängigen Norm IEC 61508 festgelegt.

Weiterhin fordert die IEC 61508, dass eine zu betrachtende sicherheitsgerichtete Funktion eine definierte gefährliche Versagenswahrscheinlichkeit der Hardware unterschreiten muss. Dabei werden sicherheitsgerichtete Systeme in zwei Kategorien unterteilt.

1. Systeme die nur auf Anforderung reagieren (low demand)

Per Definition wird an diese Systeme max. eine Anforderung pro Jahr gestellt. Die geforderte Versagenswahrscheinlichkeit bei Anforderung für die einzelnen safety integrity level kann der folgenden Tabelle entnommen werden.

Tabelle 3-2 Versagenswahrscheinlichkeit, Systeme im Anforderungsmode

Safety integrity level	**Anforderungsmode, niedrige Rate Mittlere Versagenswahrscheinlichkeit bei Anforderung**
4	$\leq 10^{-5}$ bis $\leq 10^{-4}$
3	$\leq 10^{-4}$ bis $\leq 10^{-3}$
2	$\leq 10^{-3}$ bis $\leq 10^{-2}$
1	$\leq 10^{-2}$ bis $\leq 10^{-1}$

2. Systeme mit hoher Anforderungsrate oder dauerndem Eingriff

Per Definition werden an diese Systeme mehr Anforderungen gestellt als eine Anforderung pro Jahr, bzw. sind diese Systeme dauernd im Eingriff um die sicherheitsgerichtete Funktion aufrecht zu erhalten. Die geforderte Wahrscheinlichkeit eines gefährlichen Fehlers pro Stunde kann der folgenden Tabelle entnommen werden.

Tabelle 3-3 Wahrscheinlichkeit eines gefährlichen Fehlers, Systeme im Anforderungsmode hohe Rate, dauernder Eingriff

Safety integrity level	**Anforderungsmode, hohe Rate Dauernder Eingriff Wahrscheinlichkeit eines gefährlichen Fehlers pro Stunde**
4	$\leq 10^{-9}$ bis $\leq 10^{-8}$
3	$\leq 10^{-8}$ bis $\leq 10^{-7}$
2	$\leq 10^{-7}$ bis $\leq 10^{-6}$
1	$\leq 10^{-6}$ bis $\leq 10^{-5}$

Für die zu betrachtenden Feldbussysteme müssen in der Regel die mittleren Versagenswahrscheinlichkeiten aus der Tabelle 3-2 betrachtet werden, da die hier zu betrachtenden Feldbussysteme in Schutzsystemen eingesetzt werden.
Eine rechnerische Abschätzung für ein Bussystem wird in einem späteren Kapitel behandelt.

Diese geforderten quantitativen Werte können nur für den Hardwareteil eines Systems berechnet werden, das bedeutet, dass eine Quantifizierung nur möglich ist in Bezug auf Ausfälle in der Hardware.

Die möglichen Fehler in der Software und Hardware werden auf ihre Art, ihre grundsätzlichen Ursachen, ihre möglichen Auswirkungen und ihren Entstehungszeitpunkt hin betrachtet. Hierbei werden Fehler unterschieden, die entstehen bis einschließlich der Inbetriebnahme und Fehler die nach der Inbetriebnahme entstehen. Im ersten Fall handelt es sich ausschließlich um systematische Fehler und im anderen im wesentlichen um zufällige Fehler.

Um Fehler zu vermeiden bzw. zu beherrschen, genügt meistens eine Maßnahme alleine nicht, sondern es ist immer ein Zusammenwirken mehrere Maßnahmen aus einem Maßnahmenkatalog notwendig.

Diese Maßnahmen zur Fehlervermeidung und Fehlerbeherrschung müssen so zusammengestellt werden, dass sie sich in ihrer Wirkung ergänzen und das Risiko auf ein vertretbares Maß reduzieren (siehe DIN V 19250, Grenzrisiko).

Es stehen eine ganze Reihe von Maßnahmen zur Verfügung, um Fehler, die im Entwicklungs- und Fertigungsprozess entstehen können, zu vermeiden.

Beispiele für solche systematische Fehler im Entwicklungs- und Fertigungsprozess sind:

- Spezifikationsfehler,
- Fehler bei der Programmierung,
- falsche Bauteildimensionierung und
- Fertigungsfehler.

Dort, wo die ergriffenen Maßnahmen zur Vermeidung nicht ausreichen, müssen die Fehler im Betrieb beherrscht werden.

Im Betrieb können noch folgende Fehler auftreten:

- systematische Fehler in der Hard- und Software,
- zufällige Fehler in der Hardware und
- Fehler, die durch eine falsche Nutzung, Instandhaltung oder durch nachträgliche Änderung entstehen,
- Störungen durch Umgebungsbedingungen und
- Bedienungsfehler.

Ausgehend von einem Fehlermodell werden die Fehler in Fehlerarten eingeteilt. Diese Fehlerarten werden im wesentlichen bezüglich der Art und Weise ihrer Entstehung (Ursachen) und der möglichen Maßnahmenart (Vermeidung oder/und Beherrschung), mit denen diesen Fehlerarten begegnet werden kann, abgegrenzt.

Folgende Fehlerarten müssen insgesamt betrachtet werden:

1. Systematische Fehler

- Systematische Fehler in der Spezifikation
- Systematische Fehler in der Hardware
- Systematische Fehler in der Software

2. Zufällige Fehler in der Hardware (Ausfälle)

3. Handhabungsfehler

- Unbeabsichtigte Handhabungsfehler
- Fehler durch Manipulation
- Instandhaltungsfehler

4. Fehler durch Betriebs- und Umgebungseinflüsse

- Störungen (EMV)
- Zerstörungen

Im Betrieb kann man mit Maßnahmen zur Fehlerbeherrschung erreichen, dass beim Auftreten von Fehlern keine gefährliche Situation auftritt.

Diese Maßnahmen müssen schon bei der Entwicklung berücksichtigt werden. Voraussetzung für die Beherrschung von Fehlern ist deren Erkennung. Dafür gibt es zwei unterschiedliche Methoden:

- Strukturelle Maßnahmen auf Systemebene mit Vergleich von Ergebnissen (Redundanz...) und

- Testverfahren zur gezielten Fehlererkennung.

Sofern Feldbussysteme in Sicherheitssystemen integriert sind, muss der Entwickler auch in einem sicheren Bussystem diese Maßnahmen vereinen, das heißt, er muss eine passende Struktur ermitteln, die im wesentlichen vom Verhalten des Prozesses (sicherer Zustand, erforderlicher Fehleraufdeckungsgrad, Fehlertoleranzzeit) im Fehlerfall abhängig ist.

Zusätzlich müssen Tests eingebunden werden, wenn Fehler durch die Struktur nicht in ausreichendem Maße erkannt werden.

Die Maßnahmen und Maßnahmenkombinationen müssen nun den Anforderungsklassen bzw. den safety integrity level zugeordnet werden. Merkmal für die Maßnahmen, die in der jeweiligen Anforderungsklasse bzw. dem safety integrity level anzuwenden sind, sind die anzunehmenden Fehlerarten, gegen die die Maßnahmen wirken müssen. Maßnahmen und Maßnahmenkombinationen werden somit nach zwei abgestuften Kriterien für die jeweilige Anforderungsklasse bzw. safety integrity level ausgewählt:

- Anzunehmende Fehlerarten und
- Maßnahmen zur Aufdeckung der unterstellten Fehler mit entsprechender Wirksamkeit.

Die folgende Tabelle gibt einen Überblick über die Fehlerarten und die anzuwendenden Maßnahmen.

Tabelle 3-4 Wirksamkeit der zu treffenden Maßnahmen, Tabelle 1 aus der DIN V VDE 0801

Versagen bedingt durch	Anforderungsklassen nach DIN V 19250							
	1	2	3	4	5	6	7	8
Zufallsfehler in der **Hardware**	Maßnahmen zur Fehler**beherrschung**							
1 Einfachfehler								
2 Mehrfachfehler								
3 **Systematische** Fehler in der **Hardware**	Maßnahmen zur Fehler**vermeidung**							
	Maßnahmen zur Fehler**beherrschung**							
4 **Systematische** Fehler in der **Software**	Maßnahmen zur Fehler**vermeidung**							
	Maßnahmen zur Fehler**beherrschung**							
5 Handhabungs- und Bedienfehler, Manipulation	Maßnahmen zur Fehler**vermeidung**							
	Maßnahmen zur Fehler**beherrschung**							
6 Fehler durch Betriebs- und Umgebungseinflüsse	Maßnahmen zur Fehler**vermeidung**							
	Maßnahmen zur Fehler**beherrschung**							

Geforderte Wirksamkeit der sicherheitstechnischen Maßnahmen:

Basis	Einfach	Mittel	Hoch

In dieser Tabelle sind die im vorherigen Absatz aufgeführten Fehlerursachen aufgelistet. Maßnahmen zur Fehlervermeidung und -beherrschung sind entsprechend ihrer Wirksamkeit den Anforderungsklassen bzw. SIL als Mindestanforderungen zugeordnet.

Aus der Tabelle 3-4 lässt sich entnehmen, ob fehlervermeidende und (oder) fehlerbeherrschende Maßnahmen zu treffen sind. Hierbei muss die Kombinationen der fehlervermeidenden und fehlerbeherrschenden Maßnahmen entsprechend der Anforderungsklasse bzw. dem SIL so gewählt werden, dass die Wahrscheinlichkeit eines gefährlichen Versagens hinreichend klein wird.

4 Hierarchisches Sicherheitskonzept in der Verfahrenstechnik

Die Ausrüstung von Industrieanlagen ist bezüglich Umweltschutz und Sicherheit gegen Schäden an Personen und Sachen hierarchisch gegliedert, wie die folgende Abbildung 4-1 zeigt.

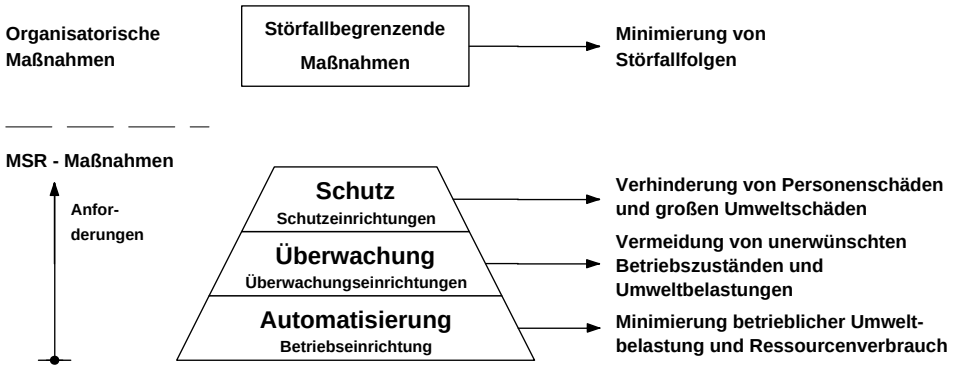


Abbildung 4-1 Hierarchisches Sicherheitskonzept

Das Bundes-Immissionsschutzgesetz (BImSchV) mit seiner Störfallverordnung (12.BImSchV) und den Verwaltungsvorschriften bzw. den Erkenntnisquellen fordert Maßnahmen gegen Störungen des bestimmungsgemäßen Betriebes. Eine Störung des bestimmungsgemäßen Betriebes ist jede, auch eine bewusst herbeigeführte, sicherheitstechnisch bedeutsame Abweichung vom bestimmungsgemäßen Betrieb. Hierzu zählt das Eintreten von Ereignissen, die größere Emissionen, größere Brände oder größere Explosionen zur Folge haben.

4.1 Automatisierung

Die unterste Ebene dient der Automatisierung des Prozesses und wird mit MSR-Betriebseinrichtungen realisiert. Diese Einrichtungen haben die Aufgabe durch Nutzung fortschrittlicher Prozessführungstechnologien und Einhaltung enger Regeltoleranzen den Prozess so zu optimieren, dass dadurch die betriebliche Einrichtung die Umweltbelastung und den Ressourcenverbrauch minimiert und das Produkt in genügender Qualität und Quantität hergestellt werden kann.

Hier werden speicherprogrammierbare Steuerungen und Rechner mit komplexen Regelalgorithmen und Ablaufsteuerungen eingesetzt, die teilweise über intelligente, automatische Optimierungsstrategien verfügen. Die MSR-Betriebseinrichtungen erfassen und verarbeiten eine Vielzahl von Prozessdaten und sind ständig im Eingriff, so dass sich ein Ausfall einer Systemkomponente in der Regel schnell bemerkbar macht.

Die Prozessabläufe haben jedoch oft eine derart hohe Komplexität erlangt, dass das Betriebspersonal Ausfälle von Systemkomponenten durch Plausibilitätskontrollen nicht mehr schnell und eindeutig erkennen kann. Diese Aufgabe übernimmt die nächste Ebene "Überwachung" mittels geeigneter MSR-Überwachungseinrichtungen.

4.2 Überwachung

Die MSR-Überwachungseinrichtungen sprechen an, wenn Prozessgrößen den Gutbereich verlassen und in den zulässigen Fehlbereich übergehen und beeinflussen den Prozess so, dass dieser möglichst wieder in den Gutbereich gelangt, zumindest jedoch die durch Vorschriften festgelegten Grenzwerte nicht überschreitet.

Die MSR-Überwachungseinrichtungen sorgen also dafür, dass die Anlage im bestimmungsgemäßen Betrieb fortgeführt werden kann. MSR-Überwachungseinrichtungen sprechen bei gut beherrschten Prozessen selten an. Funktionsstörungen können daher nur bei regelmäßigen Prüfungen erkannt werden.

Die Überwachung von Anlagen wird gegenüber der Automatisierung schon erheblich einfacher konzipiert. Auf automatische Optimierungsalgorithmen wird zu Gunsten der Überschaubarkeit verzichtet.

In der Regel wird die Überwachung mit den gleichen mikroelektronischen Komponenten aufgebaut wie die Automatisierung. Die Fehlererkennung insbesondere passiver Fehler, sollte jedoch in dieser Ebene durch automatische, regelmäßige Prüfungen verstärkt erfolgen.

4.3 Schutz

Liegen die Parameter des Prozessen über oder unter den zulässigen Grenzwerten, so spricht der Schutz an und löst die vorgesehene Schutzfunktion aus. Für einen großen Teil der Anlagen ist die Schutzfunktion die Not-Aus-Funktion. Der Schutz mit seinen Schutzeinrichtungen muss so konzipiert sein, dass Ausfälle von Bauelementen in den Schutzeinrichtungen die Wirksamkeit des Schutzes nicht beeinflussen. Deshalb muss der Schutz insgesamt oder jede Schutzeinrichtung fehlertolerant oder fail-safe aufgebaut sein. Der Schutz sollte von der Struktur her so einfach und geradlinig wie möglich aufgebaut sein, damit die Wahrscheinlichkeit von Entwurfs und Projektierungsfehlern gering ist.

Die Wahrscheinlichkeit eines Störfalles (H), d. h. des Versagens der Automatisierung, der Überwachung und des Schutzes muss so gering sein, dass in Kombination mit den Störfallauswirkungen (S) das Risiko geringer ist als das zulässige Grenzrisiko.

Das verbleibende, tolerierte Restrisiko muss durch störfallbegrenzende Maßnahmen abgefangen werden.

4.4 Störfallbegrenzende Maßnahmen

Die störfallbegrenzenden Maßnahmen, wie z. B. Feuerwehr und Katastrophenschutz sind notwendig für die hinreichend seltenen Störfälle, für die der Schutz nicht ausgelegt ist. Im Rahmen der störfallbegrenzenden Maßnahmen wird die Mikroelektronik vornehmlich für die Messwerterfassung, die Alarmgabe und die Telekommunikation eingesetzt.

4.5 Anforderungen zur Verhinderungen von Störfällen

Im Anhang der zweiten allgemeinen Verwaltungsvorschrift zur Störfall-Verordnung (2. StörfallVwV), die seit 02.04.2000 nicht mehr aktuell ist, aber als Erkenntnisquelle durchaus berücksichtigt werden kann, sind die Anforderungen zur Verhinderung von Störfällen beschrieben.

Gemäß §4 der Verordnung hat der Betreiber die zur Verhinderung von Störfällen erforderlichen Vorkehrungen zu treffen. Im einzelnen können folgende Gesichtspunkte von Bedeutung sein:

- Auslegungsbeanspruchungen;
- Brand- und Explosionsschutz;

- Warn-, Alarm- und Sicherheitseinrichtungen;
- Mess-, Steuer- und Regeleinrichtungen (MSR).

Im Abschnitt Mess-, Steuer- und Regeleinrichtungen sind Forderungen bezüglich der Art und Auslegung, sowie der Zuverlässigkeit der MSR-Einrichtungen gestellt.

In diesem Abschnitt werden Punkte genannt, die prinzipiell die Zuverlässigkeit einer MSR-Einrichtung erhöhen können. Hierzu gehören zum Beispiel:

- Verwendung geeigneter Geräte, deren Zuverlässigkeit nachgewiesen ist;
- Verwendung fehlersicherer oder selbstüberwachender Geräte;
- redundante Auslegung von MSR-Einrichtungen;
- entmaschte Auslegung von MSR-Einrichtungen;
- diversitäre Auslegung von MSR-Einrichtungen;
- regelmäßige Funktionsprüfungen in geeigneten Prüfintervallen.

Zu beachten ist, dass hier keinerlei Aussage gemacht wird, ob Einzelmaßnahmen oder nur eine Kombination dieser Maßnahmen für die Erreichung der geforderten Zuverlässigkeit notwendig ist. Eine Aussage über den Umfang der zu treffenden Maßnahmen kann nach Risiko-Ermittlung und SIL oder AK-Festlegung aus den anwendungsunabhängigen Normen DIN V VDE 0801 und IEC 61508 abgeleitet werden.

5 Prinzipielle Funktionsweise heutiger Bussysteme

Ein Feldbussystem besteht mindestens aus zwei Teilnehmern, die Daten untereinander austauschen können. Jeder der Teilnehmer besitzt dafür einen Buskoppler, der für den Datentransfer zwischen den Anwendungen und dem eigentlichen Bus (Übertragungsmedium) zuständig ist.

Der Buskoppler packt die Daten der Anwendung entsprechend dem busspezifischen Telegrammformat ein und regelt die Adressierung, organisiert den Buszugriff und realisiert die eigentliche Übertragung der Daten und packt empfangene Daten aus und gibt sie an die Anwendung weiter. Die folgende Abbildung 5-1 zeigt das Modell eines Feldbussystems.

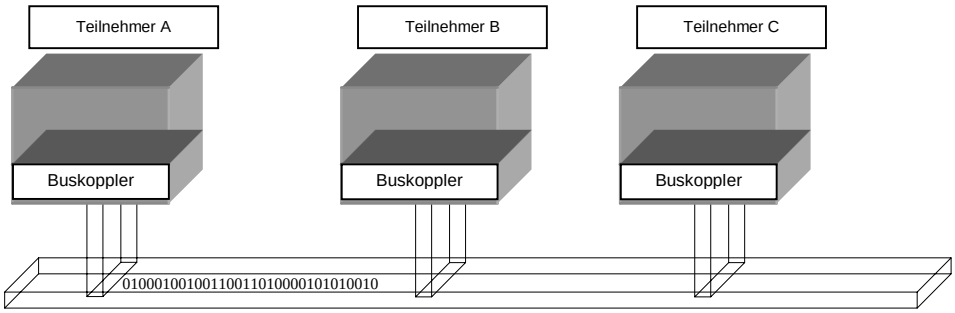


Abbildung 5-1 Modell eines Feldbussystems

Die Art und Weise, wonach der Buszugriff, die Datensicherung und die Datenübertragung ausgeführt werden, kann von Feldbussystem zu Feldbussystem variieren. Welche Verfahren und welche technologischen Unterschiede bei den heute eingesetzten Feldbussystemen bestehen zeigt die folgende Tabelle 5-1.

Tabelle 5-1 Feldbussysteme im Überblick

	CAN	Profibus PA	Profibus DP	ASI	Foundation-Feldbus	Ethernet	WorldFIP	Interbus-S
Physikalische Struktur	Zweidraht, verdrillt, geschirmt	Zweidraht, verdrillt, geschirmt oder ungeschirmt	Zweidraht, verdrillt	Zweidraht, verdrillt, ungeschirmt	Zweidraht, verdrillt, geschirmt oder ungeschirmt	Koaxialkabel mit doppelter Schirmung	Zweidraht, verdrillt, geschirmt oder ungeschirmt	5-adrig, paarweise verdrillt
Topologie	Linie	Linien, Baum	Linien, Baum	Linien	Linien, Baum	Linien, Baum	Linien, Baum	Kombinierte Ring- und
Zugriffsverfahren	CSMA/CA	Token-Passing/ Master Slave	Token-Passing/ Master Slave	Master-Slave	Arbitrator-Producer-Consumer	CSMA/CD	Arbitrator-Producer-Consumer	Summenrahmen
Netzausdehnung	Bis 1000 m	Bis 1900 m	Bis 1200 m	Bis 100 m	Bis 1900 m	Bis 500 m	Bis 1900 m	Bis 1200 m
Übertragungsrate	Max. 1Mbit/s	Max. 31,25 kbit/s	Max. 12 Mbit/s	Max. 167 kbit/s	Max. 31,25 kbit/s	Max. 10 Mbit/s	Max. 2,5 Mbit/s	Max. 500 kbit/s
Max. Datenlänge	8 Bytes	246 Bytes	64 Bytes	4 Bit		1500 Bytes		100 Bytes
Standard	ISO11898/ ISO 11519	IEC 1158-2/ DIN 19245	EN 50170/ DIN 19245		EN 50170	IEEE 802	EN 50170	DIN 19258
Übertragungs-standard	RS 485	IEC 1158-2	RS 485		IEC 1158-2	IEEE 802.3	IEC 1158-2	RS 485
Hamming-Distanz	6	4	4	2			4	4
Datensicherung	CRC	CRC	Paritybit plus Prüfsumme	Paritybit	CRC	CRC	CRC	CRC
Hauptanwendungs-gebiet	Fahrzeug-technik	Prozeßauto-matisierung	Fertigungs-auto-matisierung	Fertigungs-auto-matisierung	Prozeß-auto-matisierung	Büronetz , offener und ge-schlossener Systembus	Fertigungs-automatisierung, Prozeß-automatisierung	Fertigungs-automatisierung

5.1 ISO-OSI-Schichtenmodell

Das ISO-OSI-Schichtenmodell wurde von der ISO (International Standard Organisation) entwickelt und veröffentlicht, um einen Standard für die Datenkommunikation zwischen zwei oder mehreren Teilnehmern zu setzen. Das Modell ist ein Referenzmodell für herstellerunabhängige Kommunikationssysteme. Es standardisiert und spezifiziert die verschiedenen für die Netzwerkkommunikation erforderlichen Protokolle. Die bei einer Kommunikation zwischen zwei Partnern notwendigen Operationen werden in sieben Ebenen (Schichten) mit unterschiedlicher Funktionalität eingeteilt, wie in der folgenden Abbildung 5-2 gezeigt.

7	Anwendungsschicht (Application Layer)
6	Darstellungsschicht (Presentation Layer)
5	Sitzungsschicht (Session Layer)
4	Transportschicht (Transport Layer)
3	Vermittlungsschicht (Network Layer)
2	Sicherungsschicht (Data Link Layer)
1	Bitübertragungsschicht (Physical Layer)

Abbildung 5-2 ISO-OSI-Schichtenmodell

Das Schichtenmodell unterscheidet zwischen Diensten, die die Aufgabe der Schicht definieren, Schnittstellen, die den Zugriff auf den Dienst beschreiben und Protokollen, die die Implementierung des Dienstes regeln.

Jede Schicht bietet der darüberliegenden Schicht definierte Dienste an und nutzt ihrerseits die Dienste der darunterliegenden Schicht.

Da die Schichteneinteilung mit definierten Schnittstellen erfolgt können die einzelnen Schichten ohne große Gesamtsystemänderungen ausgetauscht und angepasst werden. Die Schichten 1... 4 sind die transportorientierten Schichten und regeln den physikalischen Datentransport. Die Schichten 5... 7 sind die anwendungsorientierten Schichten. Das Übertragungsmedium ist in diesem Modell nicht festgelegt.

Wenn ein Busteilnehmer Daten an einen anderen Busteilnehmer senden will, so benutzt dieser einen Dienst der Schicht 7, der Anwendungsschicht. Die Daten werden dann im Teilnehmer A Schicht für Schicht bis zur Schicht 1 (Physikalische Schicht) durchgereicht. Jede Schicht bearbeitet dabei die Daten entsprechend ihrer Aufgabe und gibt sie dann an die darunterliegende Schicht weiter. Nach der Übertragung durchlaufen die Daten die Schichten des Teilnehmers B in umgekehrter Reihenfolge bis zur Anwendungsschicht, die dann die Daten an die Anwendung übergibt. Die folgende Abbildung 5-3 zeigt das Prinzip der Kommunikation zwischen zwei Teilnehmern.

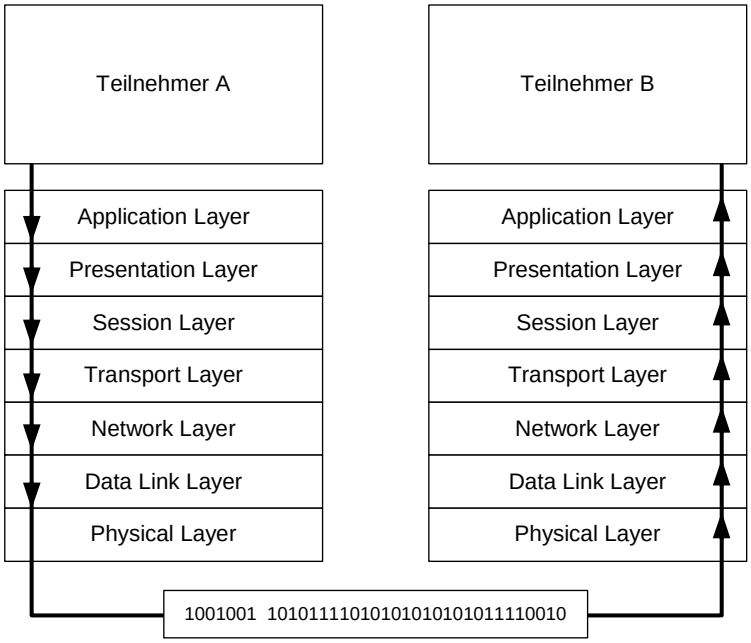


Abbildung 5-3 Datenübertragung nach ISO-OSI Schichtenmodell

Im folgenden sollen die Aufgaben und Funktionen der einzelnen Schichten genauer betrachtet werden.

Die 1. Schicht des Schichtenmodells, Physical Layer, stellt die physikalische Schicht dar und ist verantwortlich für die Realisierung der physikalischen Übertragung der digitalen Informationen. Es werden die mechanischen Komponenten, wie Kabel, Stecker und deren PIN-Belegung festgelegt. Darüber hinaus regelt sie die elektrischen Eigenschaften bezüglich der Datenübertragung, wie Signalpegel usw.

Die 2. Schicht, Data Link Layer, ist zuständig für den unverfälschten Datentransport. Sie überwacht die vollständige und richtige Übertragung der Daten von den darüberliegenden Schichten. In der 2. Schicht wird zum einen der Buszugriff festgelegt, damit sichergestellt wird, das nicht zwei Teilnehmer gleichzeitig senden und sich gegenseitig ihre Telegramme zerstören. Zum anderen versieht die zweite Schicht die zu verschickenden Daten mit einem dem Bus eigenen Rahmen. Hierbei werden die Daten in ein Paket verpackt, welches mit einer Startkennung beginnt und einer Endekennung aufhört. Zwischen diesen beiden Bereichen befinden sich in der Regel das Adressfeld, die Controlbits, das Datenfeld und die Prüfbits.

Die darüberliegende Schicht 3 (Network Layer) ist die Vermittlungsschicht. Sie ist zuständig für die Überbrückung geografischer Entfernungen zwischen den einzelnen Teilnehmern. Sie überprüft die Zieladressen der eingehenden Datenpakete und leitet sie, wenn sie für diese Vermittlungsstation bestimmt sind, an die oberen Schichten weiter. Die ausgehenden Datenpakete werden mit Ziel- und Quelladresse versehen und es wird der Weg von der Quelle bis zum Ziel festgelegt.

Die Schicht 4, Transport Layer, bildet die Verbindungsschicht zu den anwendungsorientierten Schichten, sie ist zuständig für die Erweiterung von Verbindungen zwischen den Endsystemen und den Teilnehmerverbindungen.

Die Schicht 5, Session Layer, regelt den geordneten Ablauf des Dialoges zwischen den Endsystemen und verwaltet die Berechtigungsmarken für die Kommunikation.

Die Schicht 6, Presentation Layer, ist zuständig für den gemeinsamen Zeichensatz und die gemeinsame Syntax. In dieser Schicht erfolgt die Umwandlung der lokalen Syntax in die für den Transport festgelegte Syntax und umgekehrt. Die Schichten 3 bis 6 finden ihre Anwendung weniger in Feldbussystemen als in Büronetzen, den sogenannten LAN‘s (Local Area Network).

Die Schicht 7, Application Layer, stellt einer Anwendung die Verbindung zu den anderen Teilnehmern und deren Anwendungen zur Verfügung. Sie übernimmt die Anpassung an die jeweilige Anwendung und ist zuständig für die Steuerung der untergeordneten Schichten. In der Schicht 7 erfolgt die Zuordnung und Interpretation der empfangenen Daten.

Es ist zwar möglich, alleine mit der Schicht 1 und 2 eine Datenkommunikation aufzubauen und mit entsprechenden Befehlen Daten von einem Teilnehmer zum anderen zu verschicken, aber die Bedeutung dieser Daten können in diesen Schichten nicht offenbart werden. Die zusätzlichen Daten hinsichtlich der Bedeutung der unterschiedlichen Bytes werden im Datenfeld des Telegramms untergebracht. Hierfür wird von der Schicht 7 ein entsprechender Rahmen gebildet, der die eigentlichen Daten einrahmt. Die Aufteilung der Rahmenpakete geht aus der folgenden Abbildung hervor.

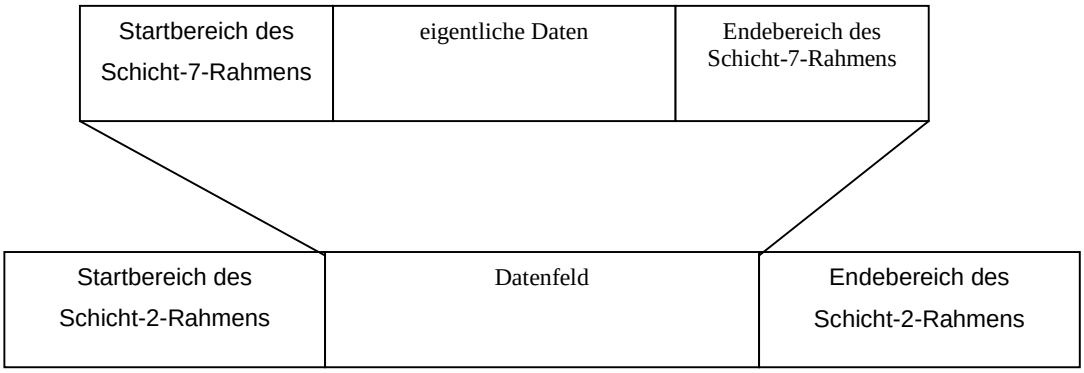


Abbildung 5-4 Einbindung der Rahmen in einem Telegramm

5.2 Netzcharakteristiken

5.2.1 Netzkonfiguration

Feldbussysteme lassen sich in unterschiedlichen Strukturen (Topologien) realisieren. Hierbei unterscheidet man Ring-, Linien-, Baum- oder Sternstrukturen.

Die verschiedenen Strukturen können zum Teil einem Feldbussystem fest zugeordnet werden. So besteht beispielsweise der Interbus-S immer aus einer Ringstruktur. Dies hängt in der Regel mit dem Zugriffsverfahren des Feldbusses zusammen. In einer Interbus-S Ringstruktur werden die Informationen von Teilnehmer zu Teilnehmer weitergereicht. Fällt einer der Teilnehmer aus, so steht der gesamte Feldbus. Aufgrund dieser Problematik legt man die Ringstruktur häufig redundant aus. Damit ist man in der Lage die funktionsfähigen Teilnehmer durch Umschaltung auf den zweiten Ring weiterhin zu betreiben und gleichzeitig den defekten Busteilnehmer zu isolieren.

Durch den festgelegten Durchlauf der Daten von Teilnehmer zu Teilnehmer verfügt diese Struktur über eine, in gewissen Grenzen, definierte maximale Telegrammlaufzeit. Abhängig von der Anzahl der Busteilnehmer können dadurch feste Reaktionszeiten definiert werden. Eine Kommunikation der einzelnen Teilnehmer untereinander ist nur über den Master möglich. Die folgende Abbildung 5-5 zeigt symbolisch die Ringstruktur.

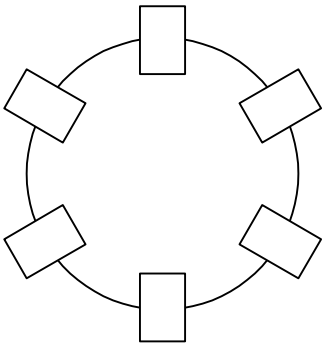


Abbildung 5-5 Ringstruktur

Eine weitere sehr stark verbreitete Struktur ist die Linienstruktur. In der reinen Linienstruktur gibt es keine Knoten und ein Master ist nicht erforderlich, wie es in der Sternstruktur der Fall ist.

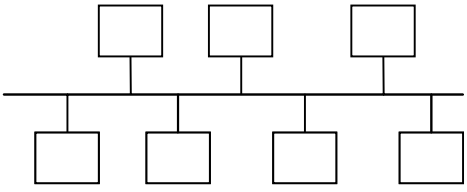


Abbildung 5-6 Linienstruktur

Alle Teilnehmer nutzen den gleichen Übertragungsweg und es kann immer nur eine Nachricht über den Feldbus übertragen werden. Fällt ein Teilnehmer aus, so ist der restliche Feldbus weiter in Funktion. Jeder Teilnehmer in dieser Struktur hört am Feldbus mit und wirkt somit im elektrotechnischen Sinne als Last für die sendende Station. Aus diesem Grund ist die Anzahl der anzuschließenden Stationen begrenzt.

Die Effektivität dieser Struktur ist im großem Maße abhängig von dem verwendeten Zugriffsverfahren. Wird zum Beispiel ein Zugriffsverfahren ohne Kollisionserkennung verwendet, so kann es bei einer starken Busauslastung zu starken Signalverzögerungen kommen, welche zu sicherheitstechnisch nicht akzeptablen Reaktionszeiten führen kann. Jedes Feldbussystem welches für eine Linienstruktur geeignet ist kann meist auch mit einer Baumstruktur betrieben werden. Bei einer Baumstruktur hängen mehrere kurze Stichleitungen mit Busteilnehmern an einer Leitung. Genau wie bei der Linienstruktur ist auch bei der Baumstruktur eine direkte Kommunikation der Teilnehmer untereinander möglich.

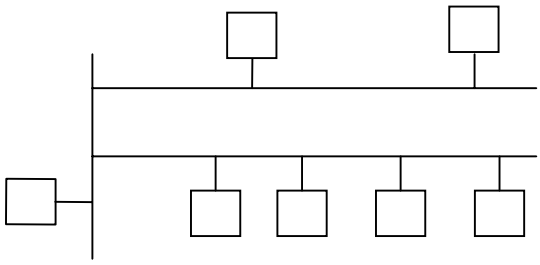


Abbildung 5-7 Baumstruktur

Eine weitere Struktur ist die Sternstruktur (s. Abbildung 5-8). Bei der Sternstruktur erfolgt die gesamte Kommunikation zentralistisch, d. h. die einzelnen Teilnehmer können nur über den Master miteinander kommunizieren. Fällt ein Teilnehmer aus, so hat dies keinen Einfluss auf den übrigen Feldbus. Beim Ausfall des Masters steht der gesamte Feldbus. Ein großer Nachteil dieser Struktur ist der für Feldbussysteme untypisch hohe Verdrahtungsaufwand. Da jeder Teilnehmer seine eigene Verbindung zum Master hat ist diese Struktur echtzeitfähig. Die Signallaufzeit ist abhängig von der Leistung des Masters.

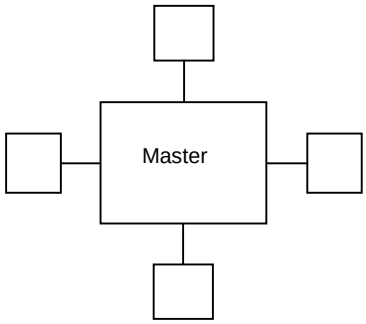


Abbildung 5-8 Sternstruktur

5.2.2 Bandbreite

Die Bandbreite ist der Frequenzbereich, in dem elektrische Signale mit einem Amplitudenabfall von bis zu 3 dB übertragen werden können. Je größer die Bandbreite, desto mehr Informationen können theoretisch in einer Zeiteinheit übertragen werden. Bei analogen Systemen wird die Bandbreite in Hertz (Hz), bzw. kHz oder MHz angegeben. Auch bei der Übertragung digitaler Signale wird oft als synonym der Begriff Bandbreite verwendet, obwohl in der Regel die Übertragungsrate gemeint ist.

Es gibt allerdings einen unmittelbaren Zusammenhang zwischen der verfügbaren Bandbreite und der Übertragungsrate, da bei der Datenübertragung die erreichbare Übertragungsrate direkt von der Bandbreite des Netzwerkes abhängt. Die maximale Bandbreiten-Ausnutzung beträgt für binäre Signale 2 Bit pro Hertz Bandbreite.

5.2.3 Bitfehlerrate

Bei jeglicher Art der Übertragung von Daten werden die Signale durch physikalische Größen wie beispielsweise Amplitude, Frequenz oder Impulsdauer übertragen. Da alle physikalischen Größen mit gewissen Toleranzen behaftet sind kann es bei jeder Übertragung dieser Größen zu Toleranzüberschreitungen beim Sender und insbesondere auch beim Empfänger der Daten kommen.

Alle elektronischen Bauteile arbeiten in gewissen Grenzen. Beispielsweise erkennt eine TTL-Logik eine logische 0 im Toleranzbereich von 0 bis 0.7 Volt und eine logische 1 zwischen 2.0 und 5 Volt. Für einen Empfänger von Daten heißt das, dass ein Pegel zwischen 0.7 und 2.0 Volt als undefiniert einzustufen ist und in diesem Fall einen Übertragungsfehler angenommen wird. Solche Übertragungsfehler können durch ein ungünstiges Signal-Rausch-Verhältnis (thermisches Rauschen) oder beispielsweise durch Reflexionen auf den Leitungen hervorgerufen werden.

Darüber hinaus kann es auch zu einer Bitverfälschung kommen, d. h. eine logische 1 wird während der Übertragung so gestört, dass das Bit beim Empfänger als logische 0 ankommt. Solche Arten von Störungen können z. B. durch EMI (electromagnetic interference) , unzulässige Leitungswiderstände und Reflexionen auf den Leitungen verursacht werden.

Ein Maß für die Qualität einer Übertragung von Daten ist die sogenannte Bitfehlerrate p (engl. Bit error rate (BER)).

$$p = \frac{n_f}{N_g} \tag{5.1}$$

mit

n_f = Anzahl der fehlerhaften Bits
N_g = Anzahl der übertragenen Bits

Diese Bitfehlerrate gibt also das Verhältnis der binären Signalelemente, die bei der Übertragung verfälscht werden zur Gesamtzahl der übertragenen binären Signalelemente an.

Die Bitfehlerrate einer Übertragungsstrecke kann entweder messtechnisch bestimmt oder durch vereinfachte Modelle näherungsweise berechnet werden.

Liegt kein Nachweis über die tatsächliche Bitfehlerrate der Übertragungsstrecke vor, sollte man eine Bitfehlerrate von $p = 10^{-2}$ bis $p = 10^{-3}$ annehmen.

5.3 Verfahren der Datenübertragung

Um den unterschiedlichen Anforderungen hinsichtlich der Netzstruktur, Leitungslänge und Übertragungsrate gerecht zu werden sind für den Physical Layer und das Übertragungsmedium in der Norm unterschiedliche Übertragungstechniken beschrieben.

Durch die gewählte Übertragungstechnik wird im Großen und Ganzen die Busstruktur, die Anzahl der Teilnehmer, die Übertragungsrate, das Übertragungsmedium sowie der Busanschluss festgelegt. Im folgenden sollen kurz die Übertragungstechniken nach RS 485, IEC 1158-2, Lichtwellenleiter und IEEE 802.3 beschrieben werden. Eine Koppelung der unterschiedlichen Übertragungstechniken ist mittels Bussegmentkoppler möglich.

5.3.1 Übertragung nach RS 485

Die Übertragungstechnik nach RS 485 basiert auf dem amerikanischen Standard EIA RS 485 und entspricht der symmetrischen Datenübertragung mit NRZ-Bitcodierung (NRZ: Non Return to Zero). Derzeit ist nur die Version 1 durch die Profibus-Norm spezifiziert. Die Version 1 beschreibt eine aufwandarme potentialgebundene oder potentialgetrennte Übertragung auf abgeschlossener Linie. Die RS 485 Übertragungstechnik ist für universelle Anwendungen in der Fertigungstechnik geeignet.

Der Standard RS 485 sieht als Übertragungsmedium eine geschirmte, verdrillte Zweidrahtleitung vor, die an ihren Enden mit dem Wellenwiderstand der Leitung abgeschlossen ist. Über diese Zweidrahtleitung können Übertragungsraten von 9.6 kbit/s bis 12 Mbit/s bei Leitungslängen bis 1200 m realisiert werden. Mit zunehmender Leitungslänge nimmt die Übertragungsrate ab, da die Dämpfung zunimmt. Der Zusammenhang zwischen Leitungslänge und Übertragungsrate wird im amerikanischen Standard EIA RS422 beschrieben.

Aufgrund elektrischer Eigenschaften der Schnittstelle ist die Anzahl der Busteilnehmer an einem Bussegment auf 32 begrenzt.

Durch die Verwendung von Repeatern kann die Teilnehmerzahl auf max. 127 Teilnehmer erhöht werden.

Die Teilnehmerzahl von 127 Teilnehmer ist bedingt durch die logischen Eigenschaften der Übertragungsschicht 2, welche nur in der Lage ist, maximal 127 Teilnehmer zu adressieren.

5.3.2 Übertragung nach IEC 1158-2

Die synchrone Übertragungstechnik mit einer festgelegten Übertragungsrate von 31,25 kbit/s findet besonders ihre Anwendung in der Prozessautomatisierung. Sie erfüllt wichtige Anforderungen der chemischen Industrie zur Eigensicherheit und Busspeisung in Zweileitertechnik. Die Datenübertragung erfolgt bitsynchron in Manchester Codierung mit einer gleichspannungsfreien Datenübertragungsrate von 31,25 kbit/s.

Bei Varianten ohne Eigensicherheit sind Übertragungsraten von bis 2.5 Mbits/s möglich. Durch entsprechende Segmentkoppler ist es möglich, auch schnellere Übertragungstechniken mit dieser Übertragungstechnik zu verbinden.

Eine Fernspeisung der Busteilnehmer über die Signaladern ist optional möglich. Die Busstruktur ist realisierbar in Baum- und Linienstruktur. Es ist eine Ankoppelung von bis zu 32 Busteilnehmern pro Leitungssegment möglich. Die Anzahl ist erweiterbar auf bis zu 126 Teilnehmer durch die Verwendung von maximal 4 Repeatern.

5.3.3 Übertragung nach IEC 1158-2 und FISCO-Modell

Für den Einsatz in explosionsgefährdeten Bereichen wird zusätzlich zu der Übertragungstechnik nach IEC 1158-2 das FISCO-Modell hinzugezogen, welches von der PTB Braunschweig entwickelt wurde und heute international als Basismodell für den Betrieb von Feldbussen in Ex-Bereichen anerkannt wird.

Die Übertragung nach IEC 1158-2 und FISCO-Modell erfolgt nach folgenden Grundsätzen:

- Beim Senden durch einen Teilnehmer wird keine Leistung in den Bus eingespeist;
- in jedem Segment gibt es nur eine einspeisende Quelle, das Speisegerät;
- jedes Feldgerät nimmt im eingeschwungenen Zustand einen konstanten Grundstrom auf;
- die Feldgeräte wirken als passive Stromsenke;
- der passive Leitungsabschluss erfolgt an beiden Enden der Bushauptleitung;
- es sind Netze in Linien-, Baum- und Sterntopologie möglich.

Wie angegeben nimmt in der Regel jeder Busteilnehmer im eingeschwungenen Zustand einen konstanten Grundstrom auf. Dieser Strom dient bei Buspeisung der Energieversorgung des Feldgerätes. Anhand dieses Grundstromes lässt sich für das Bussystem die maximale Teilnehmerzahl bestimmen, die sich aufgrund der Forderung des maximal zulässigen Speisestromes im explosionsgefährdeten Bereich ergibt.

5.3.4 Übertragung nach IEEE 802.3

Bei der Übertragung nach IEEE 802.3 sind Netztopologien in Linien- und Baumstruktur möglich. Das verwendete Zugriffsverfahren ist das CSMA/CD-Verfahren, welches im weiteren Verlauf noch näher erläutert wird. Diese Übertragungsart wird weitestgehend im LAN (Ethernet) verwendet. Die Signalcodierung erfolgt nach dem Manchesterverfahren einer NRZ-Codierung. Das Manchesterverfahren hat die Eigenschaft, dass die Taktinformation in der Codierung enthalten ist. Die maximale Ausbaustufe ist 1024 Teilnehmer, wobei nur jeweils 100 Teilnehmer pro Leitungssegment realisiert werden können. Die maximale Ausdehnung pro Segment beträgt 500 m. Mit dieser Übertragungsart lassen sich hohe Übertragungsraten realisieren.

5.3.5 Übertragung mit Lichtwellenleiter

Die Datenübertragung mit Lichtwellenleiter (LWL) hat den entscheidenden Vorteil, dass sie aufgrund des Mediums Licht gegenüber elektromagnetischen Einwirkungen unempfindlich ist. Aufwendige Entstörungsmaßnahmen, wie Leitungsabschirmung, können entfallen.

Da der Lichtwellenleiter elektrisch als Isolator zwischen den einzelnen Busteilnehmern wirkt, sind störende Ausgleichströme über das Übertragungsmedium nicht möglich. Aufgrund der extrem geringen Energie der optischen Übertragung eignet sich die LWL-Technik als ideales Übertragungsmedium in explosionsgefährdeter Umgebung.

Allerdings stellt der Einsatz von LWL-Technik eine erhöhte Anforderung an den physikalischen Aufbau des Netzwerkes. Beim Einsatz von LWL-Leitungen ist eine bidirektionale Datenübertragung im LWL-Netzwerk nur über zwei unidirektionale LWL-Strecken, je eine für jede Datenrichtung, möglich.
Mit der LWL-Technik ist es möglich, große Reichweiten zu realisieren, welche aber stark abhängig vom verwendeten Fasertyp ist.

5.3.6 HART-Kommunikation

Die HART-Kommunikation (HART: Highway Adressable Remote Transducer) stellt eine Übergangslösung von herkömmlicher Verdrahtungstechnologie zur Ansteuerung von prozessnahen Komponenten (PNK) zu den heute üblichen Feldbussystemen dar. Bei dieser Kommunikationsart besteht weiterhin das analoge 4 bis 20 mA Signal für die Messgröße, nur zusätzlich wird diesem Signal mittels FM-Technologie (FM: Frequenzmodulation) zum bidirektionalen Datenaustausch ein weiteres digitales Signal aufmoduliert. So können in herkömmlich verdrahteten Systemen einzelne intelligente Feldgeräte genutzt werden. Diese Kommunikationsmethode ist abwärtskompatibel. Wenn eine Prozesskomponente kein HART-Protokoll versteht, kann immer noch auf den analogen Wert zurückgegriffen werden. Bei Verwendung dieses Verfahren geht es darum, bestehende Infrastruktur entsprechend mit intelligenter Technologie zu ertüchtigen, ohne eine Anlage komplett neu zu konzipieren.

5.4 Buszugriffsverfahren

Das verwendete Buszugriffsverfahren ist ein wesentliches Kriterium bei der sicherheitstechnischen Betrachtung eines Feldbussystems und ist in der Schicht 2 gemäß dem ISO-OSI-Schichtenmodell realisiert.

Es hat entscheidenden Einfluss darauf wie aufwendig das Businterface sein muss, welche Übertragungsraten und welche Leitungslängen realisiert werden können. Weiterhin entscheidet das gewählte Buszugriffsverfahren darüber, ob der Feldbus über Echtzeitfähigkeit verfügt oder nicht und welche garantierten Reaktionszeiten möglich sind.

Im weiteren Verlauf werden die unterschiedlichen Buszugriffsverfahren erläutert und auf wichtige Eigenheiten bezüglich der sicherheitstechnischen Betrachtung wird eingegangen.

Grundsätzlich wird zwischen zwei verschiedenen Buszugriffsverfahren unterschieden, welche im weiteren Verlauf als **„Buszugriff nach Zuteilung“** und **„Buszugriff nach Bedarf“** bezeichnet werden.

5.4.1 Buszugriff nach Zuteilung

Beim Buszugriff nach Zuteilung fungiert ein Teilnehmer als Master über die anderen Teilnehmer. Dieser teilt den einzelnen Busteilnehmern den Feldbus zum Senden von Nachrichten für einen definierte Zeit zu. In der Regel erfolgt die Zuteilung zyklisch bzw. nahezu deterministisch, da schon bei der Buskonfiguration weitgehend festgelegt wird in welcher Reihenfolge die einzelnen Teilnehmer senden dürfen.

5.4.1.1 Master-Slave-Verfahren

Ein einziger Teilnehmer ist bei diesem Verfahren der Master, welcher selbst über das Senderecht verfügt und den anderen Teilnehmern (Slaves) das Senderecht erteilen kann. Diese Teilnehmer senden nur auf Anforderung durch den Master ein Telegramm an den Master. Hierbei kann der Master dem Slave eine Nachricht zusenden und fordert gleichzeitig die Empfangsbestätigung ein oder fordert den Slave auf eine Nachricht zu senden. Eine weitere Möglichkeit besteht darin, dass der Master eine Nachricht an den Slave versendet und im Anschluss der Slave eine Statusmeldung zurückgibt. Das Ansprechen der einzelnen Busteilnehmer erfolgt streng zyklisch. Die folgende Abbildung 5-9 zeigt die prinzipielle Funktionsweise des Master-Slave-Verfahrens.

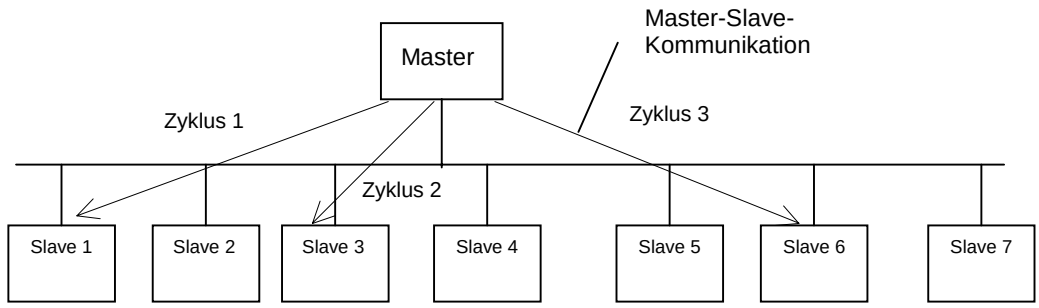


Abbildung 5-9 Master-Slave-Verfahren

Der Master sendet die Daten zu den einzelnen Teilnehmern und holt Daten von den einzelnen Teilnehmern. Die Businterfaces der Slaves können sehr einfach ausgeführt werden, da die Intelligenz im Master konzentriert ist. Dadurch ist ein Anschließen von einfachen Aktoren und Sensoren möglich.

Dieses Verfahren ist echtzeitfähig, da jeder Teilnehmer in vorher festgelegter Weise den Zugriff zum Bus bekommt. Dadurch dass in der Regel der Master nur einmal vorhanden ist, fällt beim Defekt des Master die gesamte Buskommunikation aus. Eine Kommunikation der Slaves untereinander ist nur über den Master möglich.

5.4.1.2 Token-passing-Verfahren

Beim Token-passing-Verfahren (s. Abbildung 5-10) wird in einem „Obermaster“ eine Buszugriffsberechtigung in Form eines Token (ein spezielles Kurztelegramm) erzeugt, und reihum an die einzelnen Teilnehmer weitergereicht. Jeder Teilnehmer, der dann im Besitz des Token ist übernimmt für einen definierten Zeitraum die Masterfunktion.

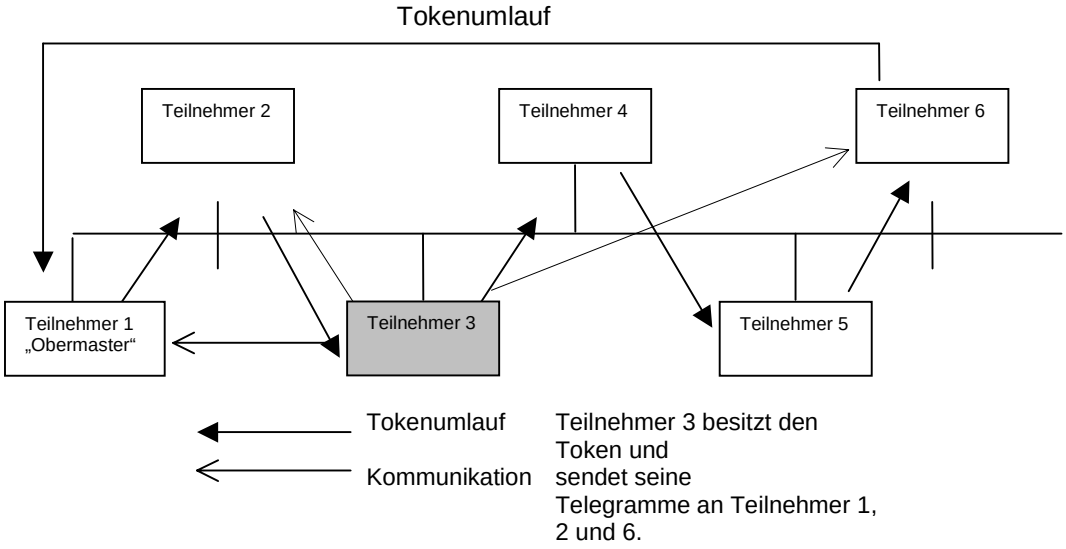


Abbildung 5-10 Token-Passing-Verfahren

Über diesen Zeitraum ist der Teilnehmer (in der Abbildung 5-10 zur Verdeutlichung grau unterlegt) berechtigt, den Feldbus als Master zu verwalten. Er kann in diesem Zeitraum auf den Feldbus zugreifen und Telegramme versenden.

Ist dieser Zeitraum abgelaufen, reicht er den Token weiter an den nächsten Teilnehmer. Hat ein Teilnehmer nichts zu senden, so kann er den Token auch gleich an den nächsten Teilnehmer weiterreichen, welcher dann eine größere Zeit, nämlich die des Vorgängers und seine eigene, zur Verfügung hat.

Geht ein Token durch einen Fehler verloren oder werden fälschlicherweise zwei Token erzeugt, so ist der Obermaster in der Lage, den Feldbus zurückzusetzen und einen neuen Token zu erzeugen. Da die maximale Tokenumlaufzeit garantiert ist handelt es sich hier um ein Feldbussystem mit definierter maximaler Reaktionszeit.

Ein großer Vorteil besteht darin, dass die einzelnen Teilnehmer miteinander kommunizieren können, ohne dass ein dritter dazwischengeschaltet ist. Die Master überwachen sich gegenseitig und wenn ein Teilnehmer ausfällt wird dieser vom Tokenumlauf ausgeschlossen und der Feldbus kann weiter betrieben werden.

Nachteile sind, dass die Verwaltung des Feldbusses recht kompliziert ist und die Businterfaces relativ aufwendig sind. Mit wachsender Teilnehmerzahl nimmt die maximale Tokenumlaufzeit zu. Bei einer Erweiterung oder Reduzierung der Teilnehmer muss jedes Mal der Feldbus neu konfiguriert werden, welches für bestimmte Anwendungsfälle problematisch sein kann.

Beim Profibus wird das Token-passing-Verfahren kombiniert mit dem Master-Slave-Verfahren eingesetzt (s. Abbildung 5-11). Hierbei wird der Token unter Masterstationen weitergereicht. Diese kommunizieren dann mit ihren zugehörigen Slaves oder mit den anderen Masterstationen. Nach Ablauf einer vorher definierten Zeit wird der Token an die nächste Masterstation weitergereicht. Somit ist hier eine Master-Master-Kommunikation und eine Master-Slave-Kommunikation möglich.

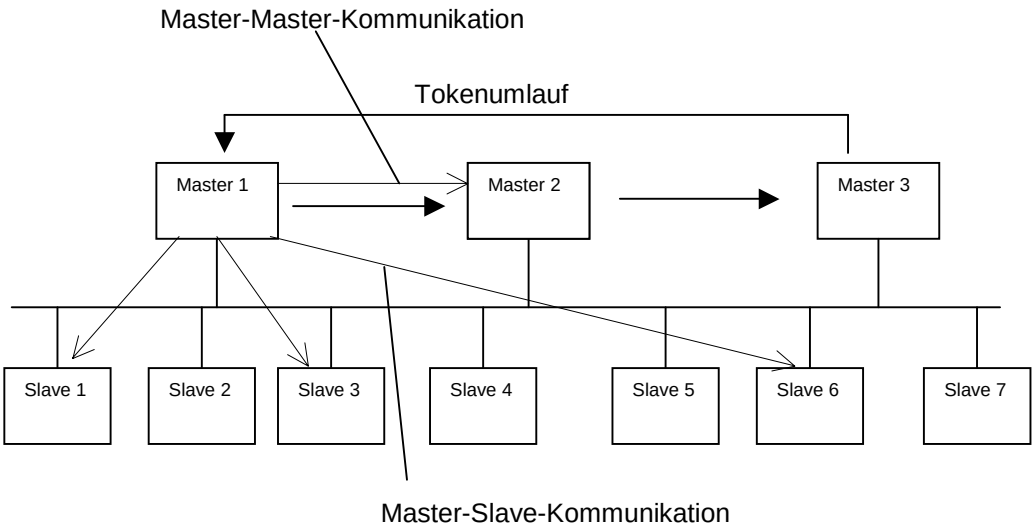


Abbildung 5-11 Kombination Token-Passing-Verfahren mit Master-Slave

5.4.1.3 Arbitrator-Producer-Consumer-Verfahren

Bei diesem Verfahren hat ein sogenannter Vermittler, der Arbitrator, die Aufgabe den Buszugriff zu verwalten. Er fordert die einzelnen Busteilnehmer zyklisch reihum auf ein Telegramm zu verschicken. Mit der Aufforderung durch den Arbitrator wird der entsprechende Busteilnehmer zum „Producer“.

Die anderen Teilnehmer, auch „Consumer“ genannt, hören permanent am Feldbus mit und erfahren dadurch, ob diese Information für sie relevant ist oder nicht. Besteht ein Interesse an diesem Telegramm, so schalten sie auf Empfang. Hat der Producer sein Telegramm abgegeben, so stößt der Arbitrator den nächsten Teilnehmer an. Die Reihenfolge in der die Teilnehmer angestoßen werden erfolgt nach einer vorher bei der Konfiguration des Feldbusses festgelegten Tabelle.

Auch der Arbitrator hört stets am Feldbus mit und erfährt dadurch, ob ein Producer zusätzliche Übertragungswünsche hat, welche über den zyklischen Datenaustausch hinausgehen.

Der Arbitrator notiert diesen Wunsch in seine Tabelle und erteilt dem Producer das Senderecht, wenn zwischen dem zyklischen Datenaustausch Zeit dafür ist. Das Mithören des Arbitrators am Feldbus dient auch der Kontrolle der Teilnehmer. Für die zyklische Datenübertragung kann eine maximale Zeit angegeben werden, so dass es sich hier um ein echtzeitfähiges Feldbussystem handelt.

Daten, welche als zeitkritisch angesehen werden, wie Reaktionszeiten bei Ausführung einer sicherheitsgerichteten Funktion, müssen in die zyklischen Datenübertragung eingebunden werden. Beim Datenaustausch, welcher über den zyklischen Betrieb hinausgeht erhält der Teilnehmer nur den Feldbus, wenn er ihn braucht und wenn er frei ist. Bei diesem Verfahren kann jeder Teilnehmer mit jedem anderen oder mehreren kommunizieren, ohne dass die Information über einen Dritten laufen muss.

Der Nachteil dieses Buszugriffsverfahrens besteht darin, dass der Feldbus steht, wenn der Arbitrator ausfällt. In der WorldFIP-Norm (Factory Instrumentation Protocol) gibt es eine Forderung, dass es mehr als einen Arbitrator im Feldbus geben muss. Dieser redundante Arbitrator überwacht nur die Arbeit des aktiven Arbitrators und springt ein, wenn dieser ausfällt.

5.4.1.4 Summenrahmen-Verfahren

Beim Summenrahmen-Verfahren ist der Feldbus ringförmig aufgebaut. Die prozessnahe Komponente übernimmt die Masterfunktion. Sie sendet ein Telegramm an die Busteilnehmer (Slaves) in Form eines Summenrahmens. Die Telegrammübertragung ist vergleichbar mit einem Schieberegister, welches kontinuierlich Byte für Byte durch den Feldbus schiebt. Für jedes Byte, welches der Master auf der einen Seite hinausschiebt erhält er auf der anderen Seite ein neues. Das Verfahren ist prinzipiell in der Abbildung 5-12 dargestellt.

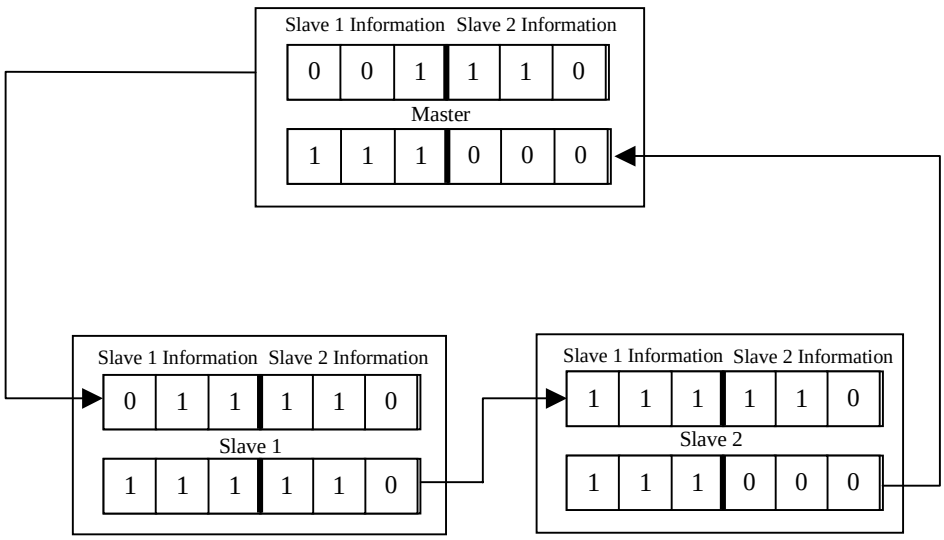


Abbildung 5-12 Summenrahmen-Verfahren

Die Anzahl der Bytes, welche jedem Slave zustehen ist von der Anwendung abhängig. Für jeden Slave ist ein Datenbereich mit vorgegebener Länge im Summenrahmen vorhanden. Während der Master in jedem Schiebeschritt ein Byte herauslesen und hineinschreiben kann, können die Slaves diesen Austausch nur zu einem bestimmten Zeitpunkt vollziehen. Nach einer festen Umlaufzeit ist der Summenrahmen einmal durch den kompletten Feldbus geschoben und jeder Teilnehmer wurde bedient. Damit handelt es sich um ein echtzeitfähiges Buszugriffsverfahren. Fällt der Master aus, so steht der gesamte Feldbus. Üblicherweise ist eine Kommunikation zwischen den einzelnen Busteilnehmern nicht möglich. Es gibt einige modifizierte Summenrahmen-Verfahren, die diesen Nachteil nicht besitzen

Bei der Übertragung hoher Datenmengen für einen Teilnehmer müssen mehrere Umläufe des Summenrahmen stattfinden, welches wiederum auf Kosten geforderter Reaktionszeiten gehen kann. Wenn schnelle Teilprozesse mit langsamen Prozessen gekoppelt werden, so muss der Feldbus über die erforderliche Datenübertragungsrate für den schnellen Prozesses verfügen. Somit werden bei dieser Kombinationen für die langsamen Prozesse viele nicht benötigte Daten übertragen, welches auf Kosten der Effizienz geht.

5.4.2 Buszugriff nach Bedarf

Beim Buszugriff bei Bedarf sind alle Teilnehmer gleichberechtigt. Sobald ein Teilnehmer ein Telegramm absetzen möchte, wartet dieser solange bis gerade kein anderer Teilnehmer den Feldbus belegt, und sendet dann sein Telegramm. Problematisch kann es hier sein, dass diesen Bedarf zwei Teilnehmer gleichzeitig haben können und es dann zu einer Kollision der beiden Telegramme kommt, welche dabei zerstört werden.

Folglich müssen die Teilnehmer das Senden dieser Telegramme wiederholen. Bei starker Auslastung des Feldbusses kann es hierbei häufiger zu Kollisionen kommen und es kann nicht genau gesagt werden wie groß die Übertragungszeiten für diese Telegramme sind.

5.4.2.1 CSMA/CD-Verfahren

Dieses Verfahren arbeitet mit einer Kollisionserkennung. Senden zwei Teilnehmer ihr Telegramm zur gleichen Zeit wird eine Kollision erkannt und beide Teilnehmer brechen sofort ihre Übertragung ab und geben den Feldbus wieder frei. Die Teilnehmer versuchen nach einer zufällig bestimmten Zeit ihr Telegramm wiederholt zu senden. Das Prinzip geht aus der Abbildung 5-13 hervor.

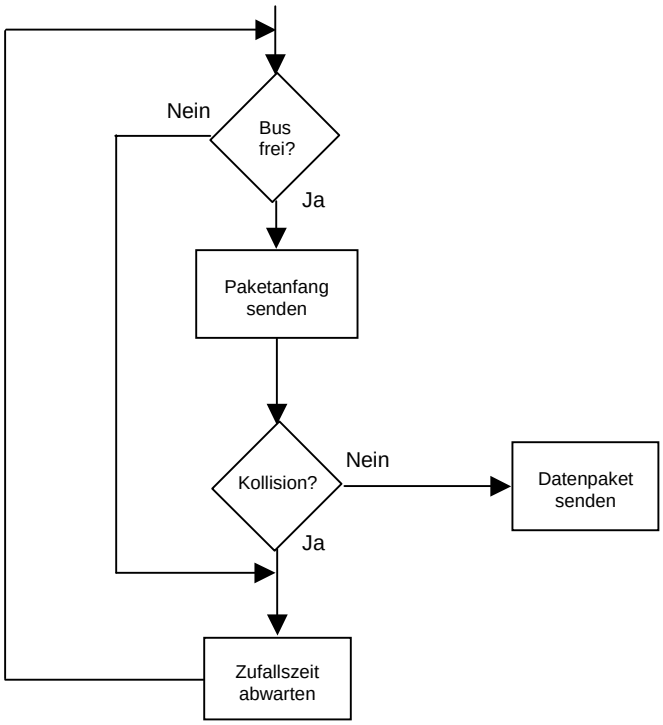


Abbildung 5-13 Prinzip des Buszugriffes beim CSMA/CD-Verfahren

Dieses Verfahren findet seine Anwendung in Ethernetnetzwerken mit ausgedehnter Netzstruktur und großen Leitungslängen und daraus resultierenden langen Signallaufzeiten. Damit hier Kollisionen auch wirklich erkannt werden, müssen die Telegramme über eine Mindestlänge verfügen. Im Ethernet besteht ein Telegramm aus mindesten 72 Bytes mit 46 Datenbytes. Der Vorteil dieses Zugriffsverfahren ist, dass hier sehr viele Teilnehmer angeschlossen werden können und das Teilnehmer entfernt und hinzugefügt werden können ohne den Feldbus rekonfigurieren zu müssen.

Aus der großen Teilnehmerzahl ergibt sich gleichzeitig ein Nachteil, wenn diese Teilnehmer nämlich ein hohes Mitteilungsbedürfnis haben. In diesem Fall sinkt die Effizienz des Feldbusses sehr stark, da immer mehr Telegramme kollidieren. Zwischen dem Abbruch eines Telegramms und dem erneuten Versuch des Sendens vergeht immer wieder eine zufällige Zeit und es kann nicht garantiert werden, dass der nächste Versuch zum Erfolg führt. Dadurch verfügt ein Feldbussystem mit diesem Zugriffsverfahren über keine Echtzeitfähigkeit und eine maximale Signallaufzeit kann nicht ohne weiteres angegeben werden.

5.4.2.2 CSMA-Verfahren bei LON

Hierbei handelt es sich um ein modifiziertes CSMA-Verfahren mit dem Ziel die Echtzeitfähigkeit zu verbessern. Die Ausdehnung des LON-Busses liegt in der Größenordnung von 1000 Teilnehmern und wird weitestgehend in der Gebäudetechnik eingesetzt.

Bei diesem Verfahren wird versucht, Kollisionen der Telegramme zu vermeiden, indem der Busteilnehmer nachdem er festgestellt hat, dass der Feldbus frei ist, nicht sofort sendet, sondern ein ganzzahliges Vielfaches einer Basiszeit wartet und dann das Telegramm verschickt. Das ganzzahlige Vielfache der Basiszeit wird hier Slot genannt. Die Ermittlung der Slots unterliegt festen Regeln und wird der Busbelastung angepasst, so dass Kollisionen größtenteils verhindert werden können.

Es ist hier auch möglich, die Wartezeit über die Vergabe von Prioritäten für einzelne Teilnehmer zu bestimmen, das heißt der Teilnehmer mit der höchsten Priorität und dadurch mit dem kleinsten ganzzahligen Vielfachen der Basiszeit darf zuerst senden, da seine Wartezeit zuerst abgelaufen ist.

Werden die Prioritäten bei diesem Verfahren ungünstig vergeben, d. h. sie unterscheiden sich nur geringfügig, so kann es vorkommen, dass die Telegramme dieser Teilnehmer oft miteinander kollidieren, da die Wartezeiten fast immer gleich sind.

Beide Methoden können mit und ohne Kollisionserkennung arbeiten. Mit Kollisionserkennung wird bei Erkennung einer Kollision der aktuelle Sendezyklus sofort abgebrochen und wenn der Feldbus wieder frei ist ein erneuter Versuch durchgeführt. Ohne Kollisionserkennung wird der Misserfolg erst nach dem Ausbleiben einer Bestätigung des Empfängers bemerkt.

Trotz der Verbesserung der Kollisionsvermeidung in diesem modifizierten CSMA-Verfahren kann man aufgrund der vielfältigen Einflussmöglichkeiten auf die Signallaufzeit nicht von einem echtzeitfähigen Verfahren sprechen.

5.4.2.3 CSMA/CA-Verfahren

Bei diesem Verfahren steht das CA für Collision Avoidance (Kollisionsvermeidung). Das Zugriffsverfahren wird beim CAN-Bus verwendet und ist so modifiziert, dass der binäre Zustand „0“ dominant ist. Wenn zwei Teilnehmer feststellen, dass der Feldbus frei ist beginnen sie mit dem Senden ihres Startbits, welches immer dominant ist. Als nächstes folgt die Adressinformation. Hier setzt sich, wenn beide Adressinformationen aufeinandertreffen immer die binäre „0“ durch, mit anderen Worten setzt sich der Teilnehmer mit der niedrigsten Adresse durch und der unterlegene Teilnehmer bricht daraufhin sein Telegramm ab und unternimmt einen weiteren Versuch, wenn der Feldbus wieder frei ist. Dadurch, dass die Teilnehmer mit niedrigen Adressen eine größere Erfolgschance haben ihr Telegramm beim ersten Versuch zu übertragen, ist es hier möglich, über die Adressierung eine Art von Prioritäten zu vergeben.

Bei Verwendung dieses Verfahrens können, wie bei jedem anderen CSMA-Verfahren, viele Teilnehmer angeschlossen werden. Teilnehmer können entfernt und angehängt werden ohne das eine Rekonfigurierung des Feldbusses notwendig ist.

5.5 Telegrammaufbau

Der Telegrammaufbau wird in Feldbussystemen in der Schicht 2 des ISO-OSI-Schichtenmodells geregelt. Das Telegramm besteht aus einer Startkennung und einer Endekennung. Zwischen diesen beiden Segmenten liegen in der Regel das Adressfeld, die Controlbits, das Datenfeld und die Prüfbits, wie in Abbildung 5-14 gezeigt.

	Startkennung	Adressfeld	Controlbits	Datenfeld	Prüfbits	Endekennung	

Abbildung 5-14 Prinzipieller Telegrammaufbau

Das Adressfeld beinhaltet zum Beispiel die Adresse des Empfängers sowie des Senders. Dadurch kann eine eindeutige Telegrammzuordnung im Feldbus erfolgen. Es hören zwar alle Teilnehmer am Feldbus mit, aber nur der Teilnehmer mit der vorher im Adressfeld definierten Adresse wird dieses Telegramm entgegennehmen. Durch die im Adressfeld abgelegte Senderadresse kann der Empfänger je nach Konfiguration dieses Telegramm quittieren oder die angeforderte Information zurücksenden. Die Controlbits kennzeichnen den Telegrammtyp, wie Aufruf-, Quittungs- oder Antwort-Telegramm.

Zusätzlich können die Controlbits Informationen zu den Übertragungsfunktionen sowie Steuerinformationen enthalten.

Den Controlbits schließt sich das Datenfeld an, welches die eigentliche Informationen enthält. Die folgenden Prüfbits dienen der Datensicherung. Die Schicht 2 hat also nur die Aufgabe die Daten mit einem entsprechenden Rahmen zu versehen und so das gesamte Telegramm aufzubauen und versandfertig zu machen. Die jeweilige Bedeutung der zu versendenden Daten ist in der Schicht 2 nicht relevant, hier interessiert nur die Länge des Datenfeldes. Der Aufbau des Datenfeldes wird in der Schicht 7 geregelt.

5.6 Verfahren der Datensicherung

Bei Feldbussystemen muss der Datenverkehr zwischen den einzelnen Busteilnehmern durch geeignete Maßnahmen gegen Datenverfälschung ausreichend gesichert werden. Die Datensicherung wird in der Schicht 2 des ISO-OSI-Schichtenmodells geregelt. Ursachen für Datenverfälschungen sind im Abschnitt 5.2.3 beschrieben. Feldbussysteme werden i. A. anfälliger je höher die Übertragungsrate und je ausgedehnter das Feldbussystem ist.

Bei allen im industriellen Bereich eingesetzten Feldbussystemen sind Verfahren zur Erkennung von Datenverfälschungen implementiert.

Es haben sich im wesentlichen drei Methoden zur Fehlererkennung bei der Übertragung von Daten etabliert:

- Paritybit;
- Prüfsumme;
- Cyclic Redundancy Check (CRC).

Alle drei Methoden beruhen darauf, dass dem Telegramm zusätzliche redundante Informationen für die Zeit der Übertragung hinzugefügt werden. Hierbei kann es sich um ein Bit oder mehreren Bits handeln. Je größer die redundante Information ist, desto größer ist i. a. der Fehleraufdeckungsgrad. Den Grad der Fehleraufdeckung beschreibt die Hamming-Distanz d. Hat ein Code eine Hammingdistanz von d, so unterscheidet sich jedes Binärwort in diesem Code um mindestens d Bits. Die Hammingdistanz d subtrahiert mit 1 ergibt die Anzahl der möglichen sicher detektierbaren Fehler in diesem Code.

Neben der Erkennung von Datenverfälschungen besteht auch die Möglichkeit mit den redundanten Informationen eine Fehlerkorrektur vorzunehmen. Mit zunehmender Größe der redundanten Informationen nimmt aber auch die Übertragungseffizienz ab, da zu den eigentlichen Nutzdaten auch die redundanten Informationen übertragen werden müssen. Die drei genannten Methoden zur Datensicherung sollen im folgenden erläutert werden.

5.6.1 Paritybit

Eine sehr einfache Form der Datensicherung ist die Sicherung durch ein zusätzliches Paritybit, welche vorwiegend bei asynchroner Datenübertragung eingesetzt wird. Hierbei wird beispielsweise zu den acht Bits eines Datenbytes ein neuntes Bit, das Paritybit, hinzugefügt. Dieses Bit wird beispielsweise so hinzugefügt, dass die Anzahl der Einsen innerhalb der neun Bits gerade ist (gerades Parity). Wird nun ein Bit verfälscht, so ist die Anzahl der Einsen nicht mehr gerade und der Empfänger kann bei seiner Parityprüfung diesen Fehler erkennen.

Die Schwäche dieser Datensicherung wird sofort deutlich. Werden zwei Bits verfälscht, so ist eine Fehlererkennung mit dem Paritybit nicht mehr möglich. Die Datensicherung mit Paritybit ist nur in der Lage eine ungerade Anzahl von Fehlern in einem Datenbyte sicher zu erkennen.

Die Ermittlung des Paritätsbits erfolgt mittels einer Modulo-2-Addition der Datenbits. Dies bedeutet, dass bei jeder Addition zweier Bits der Übertrag mit der Wertigkeit 2 ignoriert wird. Diese Art der Addition entspricht einer bitweisen Exklusiv-Oder-Verknüpfung wie sie andeutungsweise in der Abbildung 5-15 dargestellt ist.

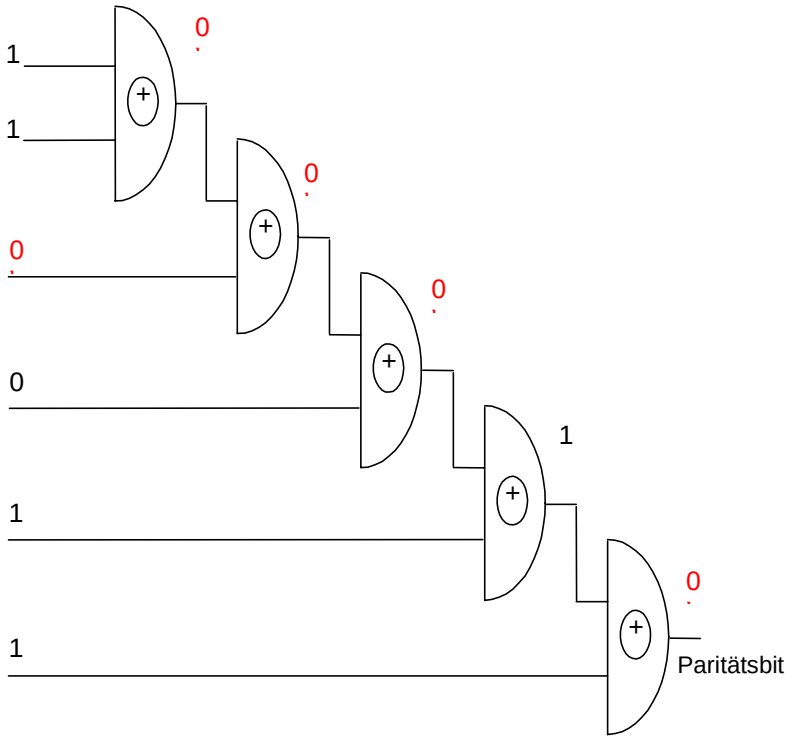


Abbildung 5-15 Exklusiv-Oder Verknüpfung für Paritätsbitermittlung

Dieses Verfahren zur Fehlererkennung hat eine Hamming-Distanz d = 2 und ist somit in der Lage Einzelfehler (ein verfälschtes Datenbit) sicher zu erkennen.

Die Unzulänglichkeit dieser Fehlererkennungsmaßnahme soll anhand eines Beispieles verdeutlicht werden.

Die Dezimalzahl 229 wird als Binärcode **11**10 0101 vom Sender auf dem Bus gelegt. Für diese Binärzahl ergibt sich ein Paritätsbit von „1“. Wird dieser Binärcode derart bei der Übertragung verfälscht, dass der Empfänger die Information **00**10 0101 erhält, so ist das Paritätsbit ebenfalls „1“, aber die Information Dezimal 37.

5.6.2 Prüfsumme

Bei der Datensicherung mittels einer Prüfsumme werden alle Datenbytes des Senders modulo-256 aufsummiert. Eine Modulo-256-Addition bedeutet, dass bei der Addition der Bytes der Übertrag mit der Wertigkeit 256 ignoriert wird.

Bei Art der Aufsummierung der Datenbytes entsteht eine 8 Bit lange Prüfsumme, die dem Telegramm hinzugefügt wird. Der Empfänger führt diese Addition mit den empfangenen Datenbytes ebenfalls durch und vergleicht die daraus resultierende Prüfsumme mit der vom Sender gesendeten Prüfsumme. Stimmen die Prüfsummen nicht überein, so wird dieses Telegramm als fehlerhaft verworfen und es muss erneut gesendet werden.

Ein Vertauschen, Weglassen oder Hinzufügen, sowie eine Veränderung des Telegramms werden bei ungünstigen Konstellationen nicht erkannt.
So kann ein Telegramm mit identischer Prüfsumme unterschiedliche Informationen enthalten.
In den folgenden Beispielen ergibt sich bei allen Telegrammen die gleiche Prüfsumme, aber die Information dieser Telegramme ist unterschiedlich.

Originaltelegramm 1001 0101 0011 1000

	Datenbits	Dezimalzahl
Datenbyte1	1001 0101	149
Datenbyte2	0011 1000	56
Prüfsumme	1100 1101	205

Verfälschtes Telegramm 0101 0101 0111 1000

	Datenbits	Dezimalzahl
Datenbyte1	**01**01 0101	85
Datenbyte2	0**1**11 1000	120
Prüfsumme	1100 1101	205

Verfälschtes Telegramm 0011 1000 1001 0101

	Datenbits	Dezimalzahl
Datenbyte1	**0**0**1**1 **10**0**0**	56
Datenbyte2	**1**0**0**1 **01**0**1**	149
Prüfsumme	1100 1101	205

Diese Methode der Datensicherung wird meist in Verbindung mit dem Paritybitverfahren verwendet, um einen höheren Fehleraufdeckungsgrad zu erhalten.

Jeder Einzelfehler innerhalb eines Bytes und jede ungerade Anzahl von Fehlern in einem Byte werden durch das Paritybitverfahren erkannt.

Im Folgenden wird die Effizienz dieser Erweiterung gezeigt. Hierfür wird das vorher verwendete Beispiel mit dem Parityverfahren erweitert.

Originaltelegramm 1001 0101 0011 1000

	Datenbits	Parity	Dezimalzahl
Datenbyte1	1001 0101	0	149
Datenbyte2	0011 1000	1	56
Prüfsumme	1100 1101	1	205

Verfälschtes Telegramm 0101 0101 0111 1000

	Datenbits	Parity	Dezimalzahl
Datenbyte1	0101 0101	0	85
Datenbyte2	0111 1000	**0**	120
Prüfsumme	1100 1101	1	205

Verfälschtes Telegramm 0011 1000 1001 0101

	Datenbits	Parity	Dezimalzahl
Datenbyte1	0011 1000	**1**	56
Datenbyte2	1001 0101	**0**	149
Prüfsumme	1100 1101	1	205

Die fehlerhaften Telegramme werden durch das Hinzufügen eines Paritybits erkannt.

Unterzieht man dieses Verfahren einer genaueren Betrachtung hinsichtlich der Hamming-Distanz (d), so ergibt sich diese zu d = 4, womit bis zu 3 Fehler im Telegramm sicher erkannt werden können.

Bei vier Fehlern ist die Aussage der sicheren Fehlererkennung nicht mehr gegeben. Es ist zwar möglich, dass auch vier Fehler durch dieses kombinierte Verfahren erkannt werden, aber es kann nicht mehr garantiert werden, wie am folgenden Beispiel zu erkennen ist.

Originaltelegramm 1001 0101 0011 1000

	Datenbits	Parity	Dezimalzahl
Datenbyte1	0011 **10**01	0	57
Datenbyte2	1111 **01**00	1	244
Prüfsumme	0010 1101	0	45

Verfälschtes Telegramm 1001 0101 0011 1000

	Datenbits	Parity	Dezimalzahl
Datenbyte1	0011 **01**01	0	53
Datenbyte2	1111 **10**00	1	248
Prüfsumme	0010 1101	0	45

5.6.3 CRC

Das CRC-Verfahren (Cyclic Redundancy Check) hat im Vergleich zu den vorher betrachteten Verfahren eine höhere Effizienz bei der Fehlererkennung. Die folgende Abbildung 5-16 verdeutlicht das Übertragungsprinzip mit CRC-Verfahren.

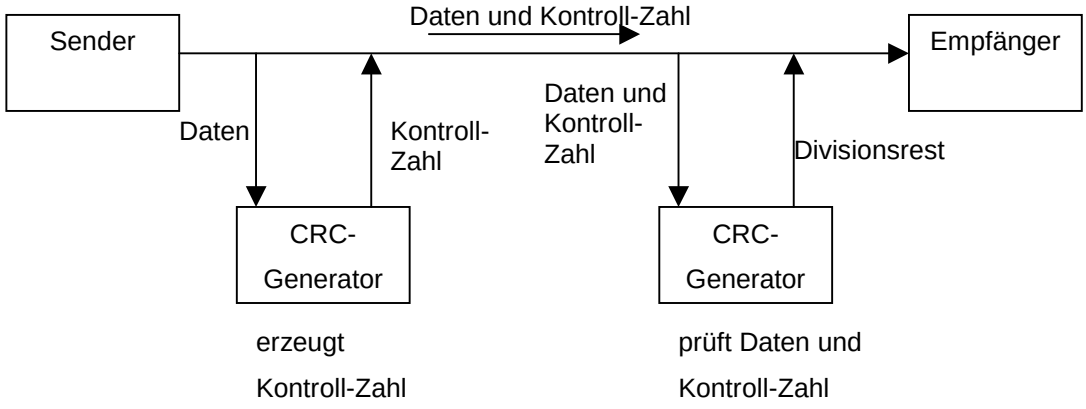


Abbildung 5-16 CRC-Verfahren

Beim CRC-Verfahren werden die gesamten Daten eines Telegramms als serieller Bitstrom betrachtet. Alle Bits dieses Bitstroms werden an einen CRC-Generator übergegeben. Dieser dividiert den Bitstrom durch ein Generatorpolynom und erzeugt daraus eine Kontroll-Zahl.

Die aus der Division entstandene Kontroll-Zahl entspricht dem Rest der Division und wird dem Bitstrom angehängt. Nach der Übertragung des Bitstromes wird dieser wiederum in einem CRC-Generator im Empfänger durch das dem Bus fest zugeordnete Generatorpolynom dividiert. Ist der Divisionsrest gleich null, so hat keine Verfälschung stattgefunden.

Bei dem Verfahren wird das Telegramm um die CRC-Kontrollzahl, also um die Anzahl der Prüfbits erweitert. Die Anzahl der Prüfbits ergibt sich aus der Länge des Generatorpolynoms. Sollen n Prüfbits bei der Division entstehen, so muss das Generatorpolynom n+1 Bit lang sein.

Allgemein lässt sich ein Generatorpolynom beschreiben als:

$$G_{(n)} = g_n * u^n + g_{n-1} * u^{n-1} + ... + g_1 * u^1 + g_0 * u^0 \qquad (5.2)$$

Der Grad des Generatorpolynoms ist n. Somit besitzt das Generatorpolynom

$$g = x^4 + x^1 + 1 \qquad (5.3)$$

den Grad 4.

Generell ist man mit einem Generatorpolynom n-ten Grades in der Lage folgende Bitfehler zu erkennen:

- alle einfach Bitfehler
- alle zweifach Bitfehler
- alle ungeraden Bitfehler
- alle zusammenhängende Bitfehler (Burst-Fehler) die kleiner als n sind
- die „meisten“ zusammenhängende Bitfehler die größer als n sind

Die große Kunst bei der Wahl eines Generatorpolynoms besteht darin, dass das Generatorpolynoms eine große Anzahl von zusammenhängenden Bitfehlern, die größer als n sind, erkennen kann.

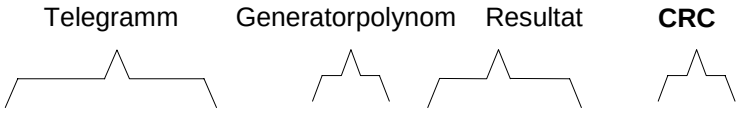
Von den verschiedenen Standardisierungsorganisationen werden verschiedene Generatorpolynome empfohlen, wie z. B.

CRC-12:	$x^{12}+x^{11}+x^3+x^2+x+1$
CRC-16 (IBM):	$x^{16}+x^{15}+x^3+1$
CRC-CCITT:	$x^{16}+x^{12}+x^5+1$
	→ Interbus-S/Profibus-PA/LON
CRC-32:	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$
	→ Ethernet
CRC-15:	$x^{15}+x^{14}+x^{10}+x^8+x^7+x^4+x^3+x$
	→ CAN

Diese Generatorpolynome sind so optimiert, dass sie einen großen Bereich von Burst-Fehlern oberhalb n aufdecken können. Eine weiterführende Betrachtung findet man in [SWO73].

Anhand eines Beispieles mit einem zufällig gewählten Generatorpolynom soll das Prinzip des CRC verdeutlicht werden.

Das Telegramm mit der Binärzahl **1101011011** soll mit dem CRC-Verfahren gesichert werden. Die Länge der CRC-Kontrollzahl soll vier Bit betragen. Hierfür muss das Generatorpolynom aus fünf Bit bestehen. Für dieses Beispiel wird ein Generatorpolynom **10011** ($g = x^4 + x^1 + 1$) vorgegeben. Das Telegramm wird vor der Division um die Länge der Kontrollzahl erweitert zu **11010110110000**.

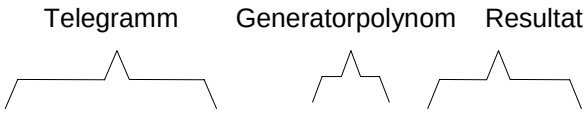


11010110110000 : 10011 = **1100001010 Rest 1110**

10011
10011 (1 = **11010** xor **10011**, Rest=> 1001)
10011
00001 (1 = **10011** xor **10011**, Rest=> 0000)
00000
00010 (0 = **00001** xor **00000**, Rest=> 0001)
00000
00101 (0 = **00010** xor **00000**, Rest=> 0010)
00000
01011 (0 = **00101** xor **00000**, Rest=> 0101)
00000
10110 (0 = **01011** xor **00000**, Rest=> 1011)
10011
01010 (1 = **10110** xor **10011**, Rest=> 0101)
00000
10100 (0 = **01010** xor **00000**, Rest=> 1010)
10011
01110 (1 = **10100** xor **10011**, Rest=> 0111)
00000
CRC⟶ 1110 (0 = **01110** xor **00000**, Rest=> 1110)

Vom Sender wird nun ein Telegramm mit der Information **11010110111110** übertragen.

Im Empfänger erfolgt wiederum eine Division des gesamten empfangenen Telegramms durch das Generatorpolynom. Bei unverfälschtem Telegramm ergibt sich:



11010110111110 XOR **10011** = **1100001010**

10011
10011 (1 = **11010** xor **10011**, Rest=> 1001)
10011
00001 (1 = **10011** xor **10011**, Rest=> 0000)
00000
00010 (0 = **00001** xor **00000**, Rest=> 0001)
00000
00101 (0 = **00010** xor **00000**, Rest=> 0010)
00000
01011 (0 = **00101** xor **00000**, Rest=> 0101)
00000
10111 (0 = **01011** xor **00000**, Rest=> 1011)
10011
01001 (1 = **10111** xor **10011**, Rest=> 0100)
00000
10011 (0 = **01001** xor **00000**, Rest=> 1001)
10011
00000 (1 = **10011** xor **10011**, Rest=> 0000)
00000
0000 (0 = **00000** xor **00000**, Rest=> 0000)

Wären nun ein oder mehrere Bits im Telegramm verfälscht worden, so würde die Division in der Regel nicht ohne Rest aufgehen und das Telegramm könnte als falsch identifiziert werden.

6 Sichere Feldbussysteme in der chemischen Industrie

Ein Feldbussystem kann als ein sicheres Feldbussystem bezeichnet werden, wenn es aufgrund der vorliegenden Merkmale und der getroffenen Maßnahmen zur Fehlervermeidung und zur Fehlerbeherrschung als Bestandteil eines Gesamtsystems für Sicherheitsanwendungen geeignet ist.

Das Feldbussystem selbst besteht dabei aus dem Übertragungsmedium und den Buskopplern, die ihrerseits Schnittstellen zu den übergeordneten Komponenten des Gesamtsystems aufweisen. Eine entsprechende Anordnung geht prinzipiell aus der folgenden Abbildung hervor.

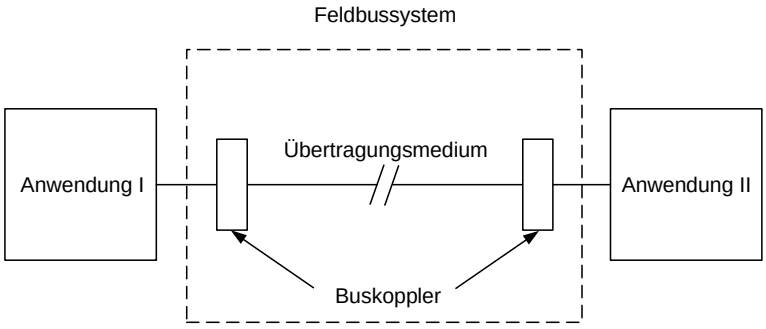


Abbildung 6-1 Vereinfachte Darstellung eines Feldbussystems

Die Eignung eines solchen Feldbussystems ist abhängig davon in welcher Sicherheitsanwendung es eingesetzt werden soll und ob es die sich daraus ergebenden Anforderungen der anzuwendenden Sicherheitsstandards erfüllt. Die Anforderungen aus den Sicherheitsstandards, die für das Gesamtsystem gelten, gelten auch gleichermaßen für das im System eingebundene Feldbussystem, da dieses eine Komponente des Sicherheitssystems darstellt.

Eine Aussage, ob eine Eignung für den geforderten Sicherheitsstandard vorliegt oder nicht, ist nur möglich, wenn die sicherheitstechnischen Kenngrößen für dieses System bzw. für die Komponenten zugänglich oder berechenbar sind.

Sind diese Kenngrößen für das Feldbussystem nicht im ausreichenden Maße verfügbar oder auch nicht ausreichend berechenbar, so muss dieses Feldbussystem als unsicher, d. h. als nicht geeignet betrachtet werden. Möglichkeiten ein solches unsicheres Feldbussystem evtl. durch zusätzliche Maßnahmen zu einem sicheren Feldbussystem zu ertüchtigen, werden im späteren Verlauf (Kapitel 6.3) näher untersucht.

Welche Anforderungen an sichere Feldbussysteme gestellt werden, ergibt sich, wie für die anderen Komponenten eines Sicherheitssystems, immer aus der jeweiligen Anwendungsnorm und dem übergeordneten anwendungsunabhängigen Standard IEC 61508, wenn das System elektronische und programmierbare Komponenten beinhaltet. Ebenso verweist die VDI/VDE-Richtlinie 2180 „Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik“ in ihrem Teil 5 auf diesen Standard, wenn es um die sicherheitstechnische Bewertung von programmierbaren Systemen geht. Auch die IEC 61511 „Functional Safety: Safety Instrumented Systems for the Process Industry“ Teil 1 lehnt sich an die IEC 61508 an.

Im Folgenden sollen schwerpunktmäßig Feldbussysteme betrachtet werden, die in Schutzsystemen eingesetzt werden sollen. Auf Feldbussysteme mit einem Einsatz in Continuous-Run-Systemen wird nur der Vollständigkeit halber zum besseren Verständnis der Problematik kurz eingegangen.

Unabhängig davon, ob das Feldbussystem in einem Schutzsystem oder in einem Continuous-Run-System eingesetzt werden soll, müssen diesbezüglich alle sicherheitstechnischen Anforderungen der zugrundegelegten Standards erfüllt werden.

In den folgenden Abschnitten sollen die sicherheitstechnischen Anforderungen an sichere Feldbussysteme anhand der relevanten Standards ermittelt werden und anschließend wird die Frage behandelt, ob die Standardfeldbussysteme prinzipiell in der chemischen Industrie als Bestandteil einer Sicherheitseinrichtung eingesetzt werden können und welche Randbedingungen gegebenenfalls zu beachten sind.
Weiterhin wird untersucht, ob ein Standardfeldbussystem für die gleichzeitige Übertragung von sicherheitsrelevanten und nicht sicherheitsrelevanten Daten eingesetzt werden kann.

6.1 Funktionale Sicherheit

Die „Funktionale Sicherheit“ ist die Eigenschaft eines Sicherheitssystems, seine bestimmungsmäßige Funktion, die Sicherheitsfunktion, auch unter definierten Fehlerbedingungen bzw. mit einer definierten hohen Wahrscheinlichkeit auszuführen.

Die Sicherheitsfunktion muss vorher eindeutig definiert werden, um eine Beurteilung gemäß IEC 61508 „Functional safety of electrical/electronic /programmable electronic safety-related systems“ durchführen zu können. Zur Aufrechterhaltung dieser Sicherheitsfunktion fordert die IEC 61508 abhängig vom geforderten SIL abgestufte fehlerbeherrschende, sowie fehlervermeidende Maßnahmen.

Die Sicherheitsfunktion besteht bei Schutzsystemen darin, die Anlage bei Bedarf in den sicheren Zustand zu überführen (z. B. Abschalten).

Um die Wirksamkeit der getroffenen fehlerbeherrschenden Maßnahmen zu beurteilen, müssen alle Komponenten einer Sicherheitsfunktion einer Wahrscheinlichkeitsbetrachtung unterzogen werden, wobei bei Schutzsystemen die gefährliche Versagenswahrscheinlichkeit PFD (Probability of failure of demand) ermittelt wird. Die PFD darf abhängig vom SIL bestimmte Werte nicht überschreiten.

Abhängig vom SIL fordert die Norm zudem für das Sicherheitssystem eine bestimmte Hardwarefehlertoleranz (HFT) in Verbindung mit einer Safe Failure Fraction (SFF), Verhältnis der sicheren Fehleranteile zu allen Fehleranteilen).
Diese Forderung gilt für das gesamte Sicherheitssystem und alle seine Komponenten und somit auch für ein in das Sicherheitssystem integriertes Feldbussystem.

Bei der weiteren Betrachtung wird angenommen, das es sich bei dem Sicherheitssystem um ein Schutzsystem handelt, d. h. die Sicherheitsfunktion wird nur bei Anforderungen (Demand) benötigt, wie z. B. bei Betätigung eines Not-Aus-Tasters oder bei Überschreitung eines Grenzwertes.

6.1.1 Fehlerbeherrschende Maßnahmen

In dem internationalen Standard IEC 61508-2 Kapitel 7.4.8 wird die Forderung aufgestellt, dass für eine sicherheitsgerichtete Datenkommunikation, zusätzlich zu den anderen fehlerbeherrschenden Maßnahmen, Maßnahmen für die Beherrschung von Fehlern während der Datenkommunikation zu treffen sind und dass ein Nachweis über die Wirksamkeit jeder getroffenen Maßnahme zu führen ist.

Innerhalb einer sicherheitsgerichteten Datenkommunikation müssen nach IEC 61508 Übertragungsfehler, Wiederholung, Verlust, Einfügung, falsche Abfolge, Nachrichtenverfälschung, zeitliche Verzögerung und Maskierung angenommen werden und durch entsprechende Maßnahmen beherrscht werden.
Im folgenden werden die anzunehmenden Fehler, die während der Datenkommunikation auftreten können näher erläutert.

Übertragungsfehler

Während der Übertragung wird die Nachricht, z. B. durch EMV, verfälscht.

Wiederholung

Eine Wiederholung liegt dann vor, wenn eine bereits gesendete Nachricht zu einem späteren Zeitpunkt fälschlich wiederholt wird.

Verlust

Die Nachricht wird durch einen Fehler komplett gelöscht. Dabei ist es unerheblich ob die Nachricht im Sender nicht abgeschickt wird oder im Empfänger durch einen Fehler nicht mehr an die Applikation weitergegeben wird oder ob überhaupt keine Busverbindung mehr besteht.

Einfügung

Unter Einfügen wird eine unerlaubte Erweiterung der Nutzdaten in einer Nachricht verstanden. Wird beispielsweise eine Nachricht von Busteilnehmer zu Busteilnehmer weitergereicht, so könnte auf dem Weg von einem Sender über mehrere Busteilnehmer zum eigentlichen Empfänger eine Nachricht unzulässig durch Einfügung verändert werden.

Falsche Abfolge

Durch einen Fehler wird die Reihenfolge von Nachrichten so manipuliert, dass eine ältere Nachricht nach der zeitlich aktuellen Nachricht beim Empfänger eintrifft.

Nachrichtenverfälschung

Durch einen Fehler wird eine Nachricht, noch bevor sie mit einem Sicherungsmechanismus im Buskontroller versehen wird bzw. nachdem sie durch einen Sicherungsmechanismus im Buskontroller geprüft worden ist, unzulässig verfälscht.

Verzögerung

Durch einen Fehler oder eine Überlastung des Busses trifft eine Nachricht zeitlich verzögert beim Empfänger ein mit der Folge, dass Sicherheitsfunktionen nicht innerhalb der Reaktionszeiten ausgeführt werden können.

Maskierung (fehlerhafte Adressierung)

Ein beliebiger sicherer Busteilnehmer wird durch eine Adressverfälschung als ein anderer Busteilnehmer in der Anwendung identifiziert. Bei der Verwendung von „sicheren“ und „nicht sicheren“ Teilnehmern innerhalb eines Feldbussystems kann durch einen Fehler eine Nachricht eines nicht-sicheren Teilnehmers durch eine inkorrekte Identifizierung (z. B. durch eine fehlerhafte Adressdekodierung beim Empfänger oder durch eine falsch geführte Liste über die sicheren Busteilnehmer auf der Empfängerseite) als eine Nachricht eines sicheren Busteilnehmers gewertet werden.

Bei den angegebenen Fehlern kann es sich um temporär auftretende Fehler, die nicht auf dauerhaften Hardwareausfällen beruhen handeln. Die Fehler können jedoch auch aufgrund von Hardware-Ausfällen in den Buskomponenten entstehen und werden dann in der Regel dauerhaft auftreten.

Darüber hinaus müssen für Schutzsysteme übergeordneten Sicherheitsprinzipien eingehalten werden, insbesondere das Ruhestromprinzip, welches auch eine Forderung der VDI/VDE 2180 Blatt 2 „Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT)“ ist.

Die Erfüllung der übergeordneten Forderung nach dem Ruhestromprinzip kann bei Datenübertragungen sinngemäß erreicht werden durch eine Dynamisierung des Feldbusses, dass heißt es muss durch einen permanenten Datenverkehr aller sicherheitsgerichteter Busteilnehmer sichergestellt werden, dass bei einer Unterbrechung der Busverbindung eine Überführung in den sicheren Zustand (Abschaltung) erfolgt.

Gegen alle zuvor genannten Fehlerarten der Datenkommunikation sind Maßnahmen zu treffen. In den heutigen Standardfeldbussystemen sind Maßnahmen gegen die genannten Fehlerarten nur teilweise implementiert.

Für jedes Feldbussystem, das innerhalb einer Sicherheitskette eingesetzt werden soll, muss daher im Einzelnen untersucht werden welche fehlerbeherrschenden Maßnahmen bereits in Standardfeldbussystemen implementiert und ausreichend sind und welche Maßnahmen zur Fehlerbeherrschung noch zusätzlich hinzugefügt werden müssen.

Zusätzlich zu der Bewertung der einzelnen Maßnahmen zur Fehlerbeherrschung fordert die IEC 61508 die Berechnung der gefährlichen Versagenswahrscheinlichkeit, wobei die im Feldbus implementierten Maßnahmen bei der Berechnung zu berücksichtigen sind.

6.1.2 Gefährliche Versagenswahrscheinlichkeit

Die Wahrscheinlichkeit, dass ein Schutzsystem im Falle einer Anforderung fehlerhaft ist, so dass die Schutzfunktion nicht mehr korrekt ausgeführt werden kann, wird als gefährliche Versagenswahrscheinlichkeit (Probability of failure of demand, PFD) bezeichnet.

Die PFD ist in der Regel zeitabhängig. Mit PFD_{AV} wird der Mittelwert der gefährlichen Versagenswahrscheinlichkeit bezeichnet.

Für jedes elektronische und programmierbare System muss gemäß IEC 61508 abhängig vom SIL ein PFD_{AV} eingehalten werden (s. Kapitel 3, Tabellen 3-2 und 3-3).

Zur Ermittlung der PFD ist es erforderlich, eine FMEA bezogen auf Einzelausfälle von Komponenten durchzuführen und aufgrund der Auswirkungen sichere Ausfallraten (λ_S) und gefährliche Ausfallraten (λ_D) zusammenzufassen, so dass die Gesamtausfallrate sich ergibt zu:

$$\lambda = \lambda_S + \lambda_D \tag{6.1}$$

Bei den gefährlichen Ausfallraten ist weiterhin zwischen durch Diagnose aufgedeckten (λ_{DD}) und nicht erkannten (λ_{DU}) zu unterscheiden, so dass sich ergibt:

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \tag{6.2}$$

Mit diesen Werten, die bei mehrkanaligen Systemen für alle Kanäle zu ermitteln sind, wird PFD bzw. PFD_{AV} entsprechend der sicherheitstechnischen Struktur und dem Einfluss von periodisch ausgeführten Funktionstests berechnet, wie in der IEC 61508 ausführlich angegeben ist.

Ist nun ein Feldbussystem in das Sicherheitssystem integriert; müssen selbstverständlich alle Einzelfehler der Buskomponenten mitbetrachtet und die entsprechenden λ_D-Werte der Buskomponenten in die Berechnung der gefährlichen Versagenswahrscheinlichkeit aufgrund von Hardwareausfällen eingehen.

Damit ist aber das gefährliche Versagen des Systems aufgrund von fehlerhaften Datenübertragungen aufgrund temporärer Störungen noch nicht berücksichtigt. Die Berücksichtigung erfolgt durch Ermittlung der gefährlichen Versagenswahrscheinlichkeit aufgrund von Übertragungsfehlern. Hierbei handelt es sich im Gegensatz zu Hardwareausfällen um temporäre Fehler.

Beide Anteile zusammen bilden die gefährliche Versagenswahrscheinlichkeit des gesamten Schutzsystems mit integriertem Feldbus. Mittels der gefährlichen Versagenswahrscheinlichkeit lässt sich nun auf einen entsprechenden SIL (Safety Integrity Level) schließen, der der Tabelle 3.2 im Kapitel 3 oder der IEC 61508 entnommen werden kann.

Die Ermittlung der gefährlichen Versagenswahrscheinlichkeit aufgrund von Übertragungsfehlern ist Gegenstand der folgenden Betrachtung.

6.1.2.1 Versagenswahrscheinlichkeit aufgrund von Übertragungsfehlern

Die Vorgehensweise der Ermittlung der gefährlichen Versagenswahrscheinlichkeit bei der Datenkommunikation soll anhand von einfachen Beispielen prinzipiell erläutert werden.

Beispiel 1:

Betrachtet wird ein Feldbus für ausschließlichen Einsatz zur Übertragung sicherheitsgerichteter Daten auf Anforderung. Das Schutzsystem besteht aus einem Sensor, einem Feldbus mit einem Sender und Empfänger, sowie einer Abschaltvorrichtung.

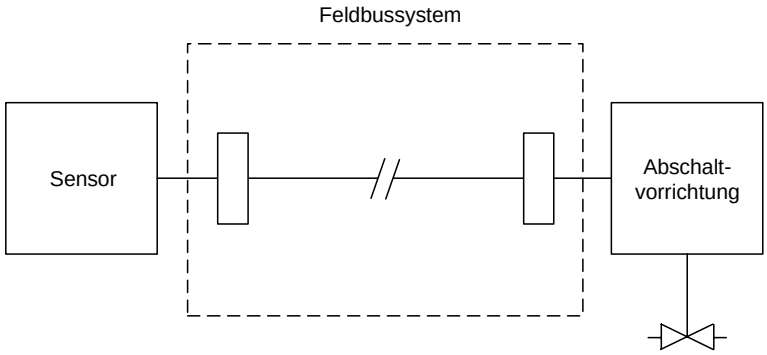


Abbildung 6-2 Sicherheitssystem mit Feldbus

Die Sicherheitsfunktion des Feldbusses im System besteht darin, das ein bestimmtes Telegramm bei Anforderung der Sicherheitsfunktion zum Empfänger übertragen wird, welches den Informationsgehalt „Abschalten“ hat. Ist dieses bestimmte Telegramm in irgendeiner Weise verfälscht ist die Sicherheitsfunktion nicht mehr gegeben.

Um nun eine Aussage über die gefährliche Versagenswahrscheinlichkeit aufgrund von Datenverfälschung zu machen müssen für diesen fiktiven Feldbus noch einige Annahmen getroffen werden.

Anhand dieser Annahmen wird deutlich, dass dieses Beispiel nur der Verdeutlichung dient und es sich um keinen realistischen Einsatz eines Feldbusses handelt:

1. Annahme: Datensicherungsmaßnahmen sind nicht existent

2. Annahme: Die Bitfehlerrate p (Kapitel 5.3.3) ist bekannt oder angenommen, z. B.

$p = 10^{-2}$

Daraus ergibt sich die Wahrscheinlichkeit PB, das in einem Telegramm ein bestimmtes Bit verfälscht wird (Bitfehlerwahrscheinlichkeit) zu

$PB = p = 10^{-2}$.

Die Wahrscheinlichkeit PT einer Telegrammverfälschung bei einer Telegrammlänge von n Bits ergibt sich in erster Annährung zu

$$PT = n \cdot p \tag{6.3}$$

unter der Vorraussetzung p<<1 und PT<<1. Dies würde bedeuten, dass ein Telegramm mit einer Länge von 100 Bit statistisch gesehen immer fehlerhaft wäre.
In diesem Beispiel wäre PT die gefährliche Versagenswahrscheinlichkeit der Sicherheitsfunktion aufgrund von Datenverfälschung.

Dadurch, dass die Sicherheitsfunktion derart definiert ist, dass die Telegrammübertragung nur auf Anforderung erfolgt, würde beispielsweise eine Unterbrechung des Übertragungsmediums nie erkannt werden. Dieser Fehler wäre bei der Ermittlung der gefährlichen Versagenswahrscheinlichkeit aufgrund von HW-Ausfällen als gefährlich anzunehmen.

Beispiel 2:

In dem zweitem Beispiel soll ein Feldbus betrachtet werden, der strukturell so aufgebaut ist wie im ersten Beispiel beschrieben, auch über keine Datensicherungsmaßnahmen verfügt, aber im Gegensatz zum ersten Beispiel das dynamische Prinzip aufweist, d. h. die Telegramme werden permanent wiederholt und enthalten die Telegramminformation „Abschalten“ oder „Nicht-Abschalten“.

Die Sicherheitsfunktion wird dahingehend erweitert, das beim Ausbleiben eines Telegramms innerhalb einer definierten Zeit es zur Abschaltung kommt, d. h. zur Ausführung der Sicherheitsfunktion. Hier ist, wie im ersten Beispiel, die Wahrscheinlichkeit, dass ein Telegramm das die Information „Abschalten“ enthält verfälscht ist, womit die Sicherheitsfunktion im Anforderungsfall nicht ausgeführt werden kann,

$$PT = n \cdot p\,. \tag{6.4}$$

Da hier die Telegramme zyklisch gesendet werden, wäre es möglich, durch mehrmaliges Senden eines Telegramms innerhalb der zulässigen Reaktionszeit Redundanz zu schaffen.

Werden zum Beispiel durch eine mehrfache Übertragung zwei identische Telegramme, die beide die Abschaltinformation enthalten, übertragen, so ist die Wahrscheinlichkeit dafür, dass beide verfälscht sind in erster Annährung

$$(PT)^2 = n^2 \cdot p^2\,. \tag{6.5}$$

Diese Aussage ist nur gültig, wenn vorrausgesetzt wird, dass die Bitfehler stochastisch auftreten.

Da es nicht ausgeschlossen werden kann, dass durch eine Störung beide Telegramme verfälscht werden, müssen bei Redundanz durch Mehrfachübertragung, wie auch bei jedem anderen redundanten System, Common-Cause-Fehler angenommen werden. Ein entsprechendes Vorgehen kann analog zur Betrachtung von Hardwareausfällen, wie in der IEC 61508 beschrieben, angesetzt werden.

Die gefährliche Versagenswahrscheinlichkeit durch Hardwareausfälle der Buskomponenten wird in diesem Beispiel reduziert aufgrund der Anwendung des dynamische Prinzips. Dies hängt damit zusammen, dass durch die Dynamisierung ein Teil der gefährlichen Ausfälle (beispielsweise die Unterbrechung des Übertragungsmediums) erkannt wird und zur Abschaltung führt und somit als sicher angesetzt werden kann.

Beispiel 3:

Abschließend soll ein praxisnäheres Beispiel betrachtet werden. Das zu betrachtende Schutzsystem beinhaltet einen Feldbus, welcher vom Prinzip her dem im Beispiel 2 entspricht, mit dem entscheidenden Unterschied, dass nun angenommen wird, dass Datensicherungsmaßnahmen mit einer bestimmte Hamming-Distanz, wie im Kapitel 5.6 beschrieben, implementiert sind.

Die Sicherheitsfunktion wird ausgeführt, wenn

- innerhalb einer festgelegten Zeit das zu erwartende Telegramm ausbleibt,
- eine Anforderung erfolgt oder
- ein Telegramm als fehlerhaft erkannt wird.

Aufgrund der Datensicherungsmaßnahmen wird nun eine großer Teil der fehlerhaften Datenübertragungen erkannt, was dazu führt, dass das Schutzsystem die Sicherheitsfunktion ausführt (abschaltet). Damit setzt sich die Gesamtwahrscheinlichkeit der fehlerhaften Telegramme aus einem Anteil der erkannt wird und einem Anteil der nicht erkannt wird zusammen.

$$PT = PT_{erkannt} + PT_{nicht\ erkannt} \tag{6.6}$$

Die Wahrscheinlichkeit $PT_{nichterkannt}$, dass ein Telegramm fehlerhaft ist und der Fehler nicht erkannt wird, obwohl Datensicherungsmaßnahmen implementiert sind, wird durch die Restfehlerwahrscheinlichkeit angegeben.

$$R = f(p,d,n) = PT_{nichterkannt} \tag{6.7}$$

mit

p = Bitfehlerrate
d = Hamming-Distanz
n = Nachrichtenlänge

Der Berechnung von R können verschiedene Modelle zugrunde gelegt werden, wie nachfolgend noch gezeigt wird.

Unter den angegebenen Vorraussetzungen können sich nur die nicht erkannten fehlerhaften Telegramme gefährlich auswirken. Die Wahrscheinlichkeit, dass ein Telegramm mit der Anforderung zur Ausführung der Sicherheitsfunktion verfälscht wird, so dass die Sicherheitsfunktion nicht ausgeführt werden kann, ist folglich identisch mit der Restfehlerwahrscheinlichkeit und stellt somit die gefährliche Versagenswahrscheinlichkeit aufgrund von Übertragungsfehlern dar.

In der Praxis werden Feldbusse nicht nur zur Übertragung sicherheitsrelevanter Daten verwendet, sie bestehen auch nicht nur aus einem Sender und einem Empfänger, sondern die gesamte Struktur solcher Systeme ist bei weitem komplexer als in den vorangegangenen Beispielen beschrieben.
Feldbussysteme bestehen in der Regel aus mehreren Busteilnehmern und können einen gemischten Telegrammverkehr enthalten, d. h. zusätzlich zu den sicherheitsrelevanten werden auch nicht sicherheitsrelevante Daten übertragen.

Daher müssen in jedem konkreten Anwendungsfall sehr sorgfältige und teils umfangreiche Untersuchungen durchgeführt werden, um die genaue Sicherheitsfunktion des Feldbusses für das Schutzsystem zu definieren. Alle Informationen, die für die Berechnung der gefährlichen Versagenswahrscheinlichkeit notwendig sind, müssen zur Verfügung stehen.

Ist ein Quantifizieren der Einflüsse nicht möglich und sind die notwendigen Daten hierfür nicht ausreichend zugänglich, so sind gegebenenfalls zusätzliche Maßnahmen zur Ertüchtigung erforderlich.

Sollen Feldbusse in Continuous-Run-Systemen ohne sicheren Zustand eingesetzt werden, so sind diese grundsätzlich, entsprechend dem Anwendungsfall, anders zu betrachten. Sie sind mit den zuvor behandelten Feldbussen in Schutzsystemen nicht zu vergleichen.

Solche Systeme sind dadurch gekennzeichnet, dass beim Auftreten eines Fehlers nicht abgeschaltet werden darf, d. h. sie müssen zur Aufrechterhaltung der Sicherheitsfunktion permanent aktiv sein.

Für Continuous-Run-Systeme wird in der IEC 61508 anstelle der gefährlichen Versagenswahrscheinlichkeit bei Anforderung (PFD) abhängig vom SIL die Einhaltung einer gefährlichen Versagenswahrscheinlichkeit pro Stunde, also eine gefährliche Versagensrate, gefordert. Die maximal zulässigen Werte für die gefährliche Versagensrate können in Abhängigkeit des geforderten SIL der Tabelle 3. im Kapitel 3 oder der IEC 61508 entnommen werden.

Wie in den vorangegangenen Beispielen gezeigt, kann auch hier die Wahrscheinlichkeit ermittelt werden, dass ein Telegramm fehlerhaft ist (PT) bzw. unerkannt fehlerhaft ist (z. B. $R = f(p,d,n)$).

Mit Hilfe der Telegrammrate W [1/s]

$$W = \frac{Anzahl\,Telegramme}{Zeiteinheit} = \frac{1}{Übertragungszeit\ für\,1 Telegramm} = \frac{\nu}{n} \qquad (6.8)$$

mit

ν = Übertragungsrate [Bit/s]
n = Anzahl der Bits pro Telegramm

lässt sich nun eine Rate Λ für fehlerhafte Telegramme oder eine Rate Λ_U für unerkannt fehlerhafte Telegramme ermitteln.

Die Rate für fehlerhafte Telegramme ergibt sich zu

$$\Lambda = PT \cdot W \qquad (6.9)$$

und die Rate für unerkannt fehlerhafte Telegramme berechnet sich aus

$$\Lambda_U = R(p, d, n) \cdot W \qquad (6.10)$$

Zur kompletten Bewertung eines solchen Systems muss wiederum die Versagensrate aufgrund von Datenverfälschungen der gefährlichen Versagensrate aufgrund von Hardwareausfällen hinzugefügt werden, ähnlich wie es bei der Betrachtung von Schutzsystemen dargestellt wurde.

Bei Continous-Run-Systemen ohne sicheren Zustand sind Datensicherungsmaßnahmen ohne zusätzliche Maßnahmen in der Regel nicht ausreichend, da im Falle fehlerhafter Telegramme nicht abgeschaltet werden darf.

Insofern sind in diesem Falle alle Telegrammverfälschungen als gefährlich einzustufen und λ als gefährliche Versagensrate aufgrund von Übertragungsfehlern anzusetzen.

Sind Zusatzmaßnahmen implementiert, die bei erkannten Telegrammverfälschungen geeignet reagieren, wie beispielsweise Telegrammwiederholung oder Umschaltung auf einen anderen Kanal, kann ggf. die Rate λ_U bzw. die Restfehlerwahrscheinlichkeit R für die gefährliche Versagensrate aufgrund von Übertragungsfehlern angesetzt werden.

Aus den zuvor gemachten Ausführungen geht hervor, dass im Zusammenhang mit der gefährlichen Versagenswahrscheinlichkeit aufgrund von Übertragungsfehlern der Restfehlerwahrscheinlichkeit bei der Bewertung eines Feldbussystems besondere Bedeutung zukommt. Daher soll im Folgenden auf die Restfehlerwahrscheinlichkeit etwas näher eingegangen werden.

6.1.2.2 Restfehlerwahrscheinlichkeit

Die Berechnungsmethode für die Bestimmung der Restfehlerwahrscheinlich ist abhängig von der angenommenen Störstruktur, welche auf der Übertragungsstrecke im üblichen industriellen Einsatz auftreten kann.

Hierbei wird unterschieden zwischen:

- Gaußstörung (z. B. Rauschen und Übersprechen),
- Burststörungen (z. B. EMV),
- gleichverteilte Fehlermuster.

Eine Gaußstörung ist ein idealisierter Störungstyp, der statistisch gleichverteilte und unabhängige Fehlermuster verursacht.

Burststörungen sind elektromagnetische Störungen die auf die Übertragungsstrecke einwirken. Ursachen für eine elektromagnetische Störung können technische Anlagen mit elektrischen Antrieben und deren Leistungselektronik, Transformatoren oder auch moderne Kommunikationstechniken sein.

Bei einem gleichverteilten Fehlermuster wird angenommen, dass alle möglichen Einfachfehler, Zweifachfehler bis zum n-Fachfehler, wobei n die Telegrammlänge ist, gleichwahrscheinlich sind.

Im weiteren Verlauf soll untersucht werden, wie sich die Störstrukturen „Gaußstörung“ und „Burststörung“ auf die Restfehlerwahrscheinlichkeit der Datenübertragung auswirken. Weitergehende Informationen bezüglich anderer Störstrukturen kann der entsprechenden Literatur, wie z. B. [LOC97], entnommen werden.

Die Restfehlerwahrscheinlichkeit bei **Gaußstörung** ergibt sich mit Hilfe der Bernoulli-Verteilung zu:

$$R(n,d,p)=\sum_{i=d}^{n} A_{n,i}\, p^{i}(1-p)^{(n-i)} \tag{6.11}$$

$$\text{mit } A_{n,i}=\binom{n}{i}=\frac{n!}{i!(n-i)!} \tag{6.12}$$

und p = Bitfehlerrate
d = Hamming-Distanz
n = Nachrichtenlänge

Betrachtet man die **Burststörung**, die in der Praxis wohl am häufigsten anzutreffen ist, kann man die Restfehlerwahrscheinlichkeit beispielsweise mit der NTA-Verteilung näherungsweise bestimmen [Loc97].

$$R(p,d,n,m_1) = \sum_{i=d}^{n} (e^{-m1} \frac{m_2^d}{d!} \sum_{k=0}^{\infty} \frac{z^k}{k!} k^d) \tag{6.13}$$

mit

$z = m_1 e^{-m_2}$

$m_1 = Anzahl\ Bursts\ in\ einem\ Telegramm$

$$m_2 = Anzahl\ Bitfehler\ im\ \ einem\ Burst = \frac{n \cdot p}{m_1} \tag{6.14}$$

$k = Zählzahl\ \ für\ die\ unendliche\ Summe$

Anhand von Beispielen soll untersucht werden, inwieweit sich die Ergebnisse bei beiden mathematischen Ansätze zur Berechnung der Restfehlerwahrscheinlichkeit unterscheiden.

Beispiel 1:

Für die Übertragungsstrecke sollen folgende Parameter und Eigenschaften angenommen werden:

Geschirmtes und verdrilltes Kabel mit einer Bitfehlerrate p = 10^{-3}

Nachrichtenlänge n = 80 Bits

Hamming-Distanz = 6

Ein Burst pro Telegramm m_1 = 1

Für die Restfehlerwahrscheinlichkeit bei Gaußstörung ergibt sich dann:

$$R(p,n,d) = 2{,}8 \cdot 10^{-10}$$

Wird die Burststörung zugrundegelegt, so ergibt sich für die Restfehlerwahrscheinlichkeit

$$R(p,n,d,m_1) = 5{,}5 \cdot 10^{-8}$$

Die nachfolgende Abbildung 6-3 zeigt für unterschiedliche Telegrammlängen die berechnete Restfehlerwahrscheinlichkeit einer Gauß- bzw. einer Burststörung bei einer Hamming-Distanz von 6 und einer angenommenen Bitfehlerrate von $p = 10^{-3}$.

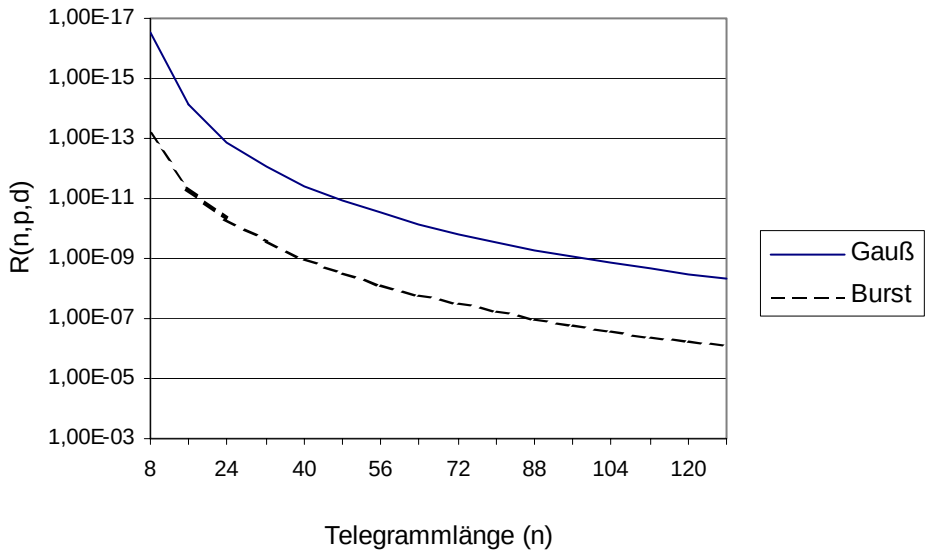


Abbildung 6-3 Restfehlerwahrscheinlichkeit in Abhängigkeit zur Telegrammlänge

Aus dem dargestellten Diagramm ist ersichtlich, dass die Restfehlerwahrscheinlichkeit bei einer Burststörung mindestens um den Faktor 100 schlechter ist als bei der Annahme einer Gaußstörung.

Die folgende Abbildung 6-4 zeigt die Restfehlerwahrscheinlichkeit in Abhängigkeit von der Hamming-Distanz bei konstanter Telegrammlänge n = 80 Bits und einer angenommenen Bitfehlerrate von 10^{-3}.

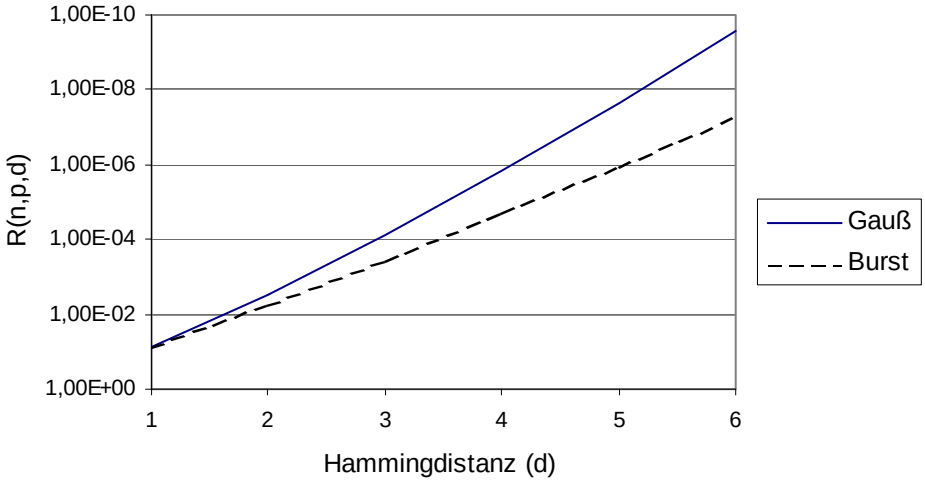


Abbildung 6-4 Restfehlerwahrscheinlichkeit in Abhängigkeit zur Hamming-Distanz

Es lässt sich klar erkennen, dass die Werte der Restfehlerwahrscheinlichkeit der beiden angenommenen Störstrukturen mit zunehmender Hamming-Distanz auseinanderlaufen.

Anhand dieser Beispiele wird deutlich, dass die Burststörung als angenommene Störstruktur zu schlechteren Werten bei der Berechnung der Restfehlerwahrscheinlichkeit führt.

Wenn die Sicherheitsfunktion darin besteht, kontinuierlich sicherheitsrelevante Daten zu übertragen, so kann wie vorher bereits ausgeführt eine gefährliche Versagensrate aufgrund fehlerhafter Datenübertragung ermittelt werden.

Die gefährliche Versagensrate Λ_U ergibt sich aus der Restfehlerwahrscheinlichkeit, der Telegrammlänge und der Übertragungsrate zu:

$$\Lambda_U = \frac{R(p,n,d) * v}{n} \tag{6.15}$$

mit

n = Anzahl der Bits pro Telegramm
v = Übertragungsrate [Bit/s]

Die gefährliche Versagensrate pro Stunde ergibt sich für ein Continuous-Run-System durch die folgende Zahlenwertgleichung:

$$\Lambda_U = \frac{R(p) * v * 3600}{n} \tag{6.16}$$

mit

n = Anzahl der Bits pro Telegramm
v = Übertragungsrate [Bit/s]

Zur Verdeutlichung soll beispielhaft die gefährliche Versagensrate pro Stunde für eine CRC-15 Datensicherung mit einer Hamming-Distanz von 6 sowie für eine einfache CRC Datensicherung mit einer Hamming-Distanz von 3 bestimmt werden.

Beispiel CRC-15:

Geschirmtes und verdrilltes Kabel mit einer Bitfehlerrate $p = 10^{-4}$

Nachrichtenlänge n = 80 Bits, einschließlich der 15 CRC-Bits

Hamming-Distanz d = 6

Übertragungsrate v = 500 kBit/s

Für die Restfehlerwahrscheinlichkeit bei einer unterstellten Gaußstörung ergibt sich dann:

$$R(p,n,d) = 3 \cdot 10^{-16}$$

und bei einer Burststörung

$$R(p,n,d) = 7 \cdot 10^{-14}$$

Bei einer Übertragungsrate von 500 kBit/s und einer Telegrammlänge von 80 Nutzbits einschließlich 15 CRC-Bits ergibt sich eine theoretische Nachrichtenanzahl von ungefähr 6000 Nachrichten/s.

Somit ergibt sich für die gefährliche Versagensrate pro Stunde und einer angenommenen Busauslastung von 100 %:

$\Lambda_U = 6{,}9 \cdot 10^{-9} \frac{1}{h}$ für die Annahme einer Gaußstörung

$\Lambda_U = 1{,}6 \cdot 10^{-6} \frac{1}{h}$ für die Annahme einer Burststörung

oder ungefähr 0,014 nicht entdeckte Fehler pro Jahr bei täglich 24 h Betrieb unter der Annahme das Burststörungen vorliegen.

Beispiel CRC-5:

Geschirmtes und verdrilltes Kabel mit einer Bitfehlerrate p = 10^{-4}

Nachrichtenlänge n = 80 Bits einschließlich 5 CRC-Bits

Hamming-Distanz d = 3

Übertragungsrate v = 500 kBit/s

Für die Restfehlerwahrscheinlichkeit ergibt sich dann:

$R(p, n, d) = 8{,}2 \cdot 10^{-8}$

bei der Annahme einer Gaußstörung und

$R(p, n, d) = 4{,}2 \cdot 10^{-7}$

bei einer Burststörung.

Somit ergibt sich für die Übertragungsstrecke eine gefährliche Versagensrate pro Stunde von:

$\Lambda_U = 1{,}8\frac{1}{h}$ für die Annahme einer Gaußstörung

$\Lambda_U = 10\frac{1}{h}$ für die Annahme einer Bursttörung

Bei dieser Art der Sicherung werden im Mittel etwa zwei bzw. zehn falsche Telegramme pro Stunde unentdeckt bleiben.

An dieser Stelle ist noch anzumerken, dass bei dieser Abschätzung nur die reine Übertragungsstrecke, also ohne die Buskoppler und deren Elektronik, betrachtet wurde.

Die nachfolgende Abbildung 6-5 verdeutlicht den Einfluss der Restfehlerwahrscheinlichkeit auf die mittlere Zeit zwischen zwei unentdeckten Fehlern bei einer Nachrichtenlänge n = 80 Bits und einer max. Übertragungsrate v = 500 kBits/s.

Mit $\Lambda = \frac{1}{T}$ ergibt sich die mittlere Zeit zwischen zwei unerkannt fehlerhaften Telegrammen zu:

$$T = \frac{n}{v \cdot R(p, n, d)} \tag{6.17}$$

Restfehlerwahrscheinlichkeit R	Mittlere Zeit zwischen unerkannten Fehlern
10^{-6}	160 s
10^{-10}	18 Tage
10^{-12}	5 Jahre

Abbildung 6-5 Zeiten zwischen zwei unerkannten Fehlern

Zusammengefasst kann folgendes festgehalten werden:

Für die Bewertung einer Datensicherungsmaßnahme ist ihr Einfluss auf die gefährliche Versagenswahrscheinlichkeit zu betrachten. Dabei bildet die gefährliche Versagenswahrscheinlichkeit aufgrund von Übertragungsfehlern die entsprechende Kenngröße. Abhängig vom zu bewertenden Sicherheitssystem sind die entscheidenden Parameter die Bitfehlerrate, die Telegrammlänge, die Übertragungsrate und die Hamming-Distanz.

6.1.3 Hardwarefehlertoleranz HFT und Safe Failure Fraction SFF

Zusätzlich zur Einhaltung einer gefährlichen Versagenswahrscheinlichkeit fordert die IEC 61508 je nach SIL eine bestimmte Hardwarefehlertoleranz (HFT) in Verbindung mit der Safe Failure Fraction (SFF).
Die Hardwarefehlertoleranz ist die Eigenschaft eines Systems, trotz des Vorliegens eines oder mehrerer Hardwarefehler, die geforderte Sicherheitsfunktion ausführen zu können.

Eine Hardwarefehlertoleranz von N bedeutet das N Einzelfehler nicht dazu führen, dass die Sicherheitsfunktion gefährlich versagt. Dies bedeutet, dass Systemarchitekturen wie 1 aus 2 (1oo2) oder 2 aus 3 (2oo3) eine Hardwarefehlertoleranz von 1 besitzen, weil sie bei Auftreten eines gefährlichen Fehlers bei Anforderung die Sicherheitsfunktion ausführen können und erst bei dem zweiten Einzelfehler gefährlich versagen können.

Die Safe Failure Fraction SFF eines Systems ist definiert als das Verhältnis der Rate der sicheren Fehler plus der Rate der gefährlichen detektierten Fehler zur gesamten Ausfallrate des Systems.

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda} = \frac{\lambda - \lambda_{DU}}{\lambda} \tag{6.18}$$

und

$$\lambda = \lambda_D + \lambda_S \tag{6.19}$$

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \tag{6.20}$$

Gemäß der IEC 61508 wird der maximal erreichbare SIL eines Systems beschränkt durch die Hardwarefehlertoleranz und die Safe Failure Fraction des Systems. Die IEC 61508 unterscheidet hierbei noch, ob es sich bei dem System um ein High-Complex-System (Typ B) oder Low-Complex-System (Typ A) handelt.

Die erreichbaren SIL, abhängig von HFT und SFF, sind in den folgenden der IEC 61508 entnommenen Tabellen 6-1 und 6-2 dargestellt.

Da die Feldbussysteme dem Typ B zu geordnet werden müssen ist für eine Bewertung der Feldbussysteme die Tabelle 6-2 heranzuziehen.

Tabelle 6-1 Hardware safety integrity: architectural constraints on type A safety-related subsystems [IEC 61508]

Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4

Tabelle 6-2 Hardware safety integrity: architectural constraints on type B safety-related subsystems [IEC 61508]

Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60 %	not allowed	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

Betrachtet man nun ein Feldbussystem mit einer Übertragungsstrecke ohne Redundanz, so muss von einer HFT von 0 ausgegangen werden, d. h. jeder beliebige Hardwarefehler im Feldbussystem kann zum Versagen der Sicherheitsfunktion führen.

Bezüglich der SFF liefert ein in einem Sicherheitssystem integrierter Feldbus im allgemeinen Anteile zu sicheren und gefährlichen Ausfallraten wie jede andere Komponente des Sicherheitssystems.

6.1.4 Fehlervermeidende Maßnahmen

Systematische Fehler in der Spezifikation, in der Hardware und in der Software, Instandhaltungsfehler und Nutzungsfehler des Sicherheitssystems müssen so weit wie möglich vermieden werden.

Hierfür schreibt die IEC 61508 eine Reihe von fehlervermeidenden Maßnahmen vor, die je nach angestrebtem SIL durchgeführt werden müssen. Die fehlervermeidenden Maßnahmen müssen den gesamten Lebenszyklus des Sicherheitssystems, von der Konzeptphase bis zur Außerbetriebnahme, begleiten und gelten selbstverständlich auch für die Feldbussysteme.

Die Maßnahmen orientieren sich am Ablauf der Entwicklung eines Systems. Es werden Maßnahmen zur Fehlervermeidung den einzelnen Phasen der Entwicklung zugeordnet. Einzelne Maßnahmen können dabei in mehreren Phasen wirksam sein.

Die einzelnen Phasen können im wesentlichen wie folgt aufgeteilt werden:

- Entwicklung
    - Beachtung der zutreffenden technischen Regeln
    - Definition übergeordneter Sicherheitsanforderungen
    - Konzept, Spezifikation
    - Gefahren- und Risikoanalyse
    - Festlegen der sicherheitstechnischen Anforderungen
    - Entwicklung Hardware
    - Entwicklung Software
    - Verifikation und Validation
    - Fertigungsvorbereitung, Fertigung

- Betrieb
    - Installation
    - Betrieb und Wartung
    - Änderungen

- Außerbetriebnahme

Zu diesen Phasen müssen im einzelnen Maßnahmen angeführt werden, die dazu geeignet sind, Fehler zu vermeiden.

Zu den Phasen Konzept und Entwicklung Hardware/Software sind im folgenden beispielhaft Maßnahmen aufgeführt:

Konzept

- Verwenden einer verbindlichen Systemspezifikation
- Verwendung von rechnergestützten Entwurfswerkzeuge
- Strukturierter Entwurf
- Verwendung von Checklisten
- Inspektionen/Verifikation der Spezifikation

Entwicklung Hardware/Software

Bei der Entwicklung von Systemen mit Sicherheitsaufgaben müssen zahlreiche einzelne Maßnahmen durchgeführt werden. Für eine bessere Übersicht werden sie folgendermaßen eingeteilt:

a) Organisatorische Maßnahmen

- Projektorganisation
- Organisation der Qualitätssicherung
- Dokumentation

b) Technische Maßnahmen

Die technischen Maßnahmen betreffen die Verfahren der Entwicklung, die Bereitstellung von Hilfsmitteln, die Qualitätssicherung, die Prüfung von Hard- und Software.

Sie bilden den Kern der Maßnahmen und werden in zwei Gruppen unterteilt, die sich grundsätzlich unterscheiden.

- Man ergreift während der Entwicklung konstruktive Maßnahmen, um von vornherein Fehler zu vermeiden.

- Man ergreift analytische Maßnahmen, um Fehler aufzudecken.

Die Maßnahmen haben jeweils für sich gesehen eine eingeschränkte Mächtigkeit. Keine Maßnahme ist so mächtig, dass man sich auf sie alleine verlassen kann.
Es dürfen auch nicht Maßnahmen der einen Gruppe gegenüber der anderen vernachlässigt werden. Die Wirksamkeit wird insbesondere durch gezielte Kombination von Maßnahmen erhöht.

Die folgende Liste stellt einen Auszug von Maßnahmen dar:

Konstruktive Maßnahmen bei der Hardware-Entwicklung

- Beachtung der zutreffenden technischen Regeln
- Verwendung rechnergestützter Konstruktions- und Entwicklungssysteme
- strukturierter Entwurf der Hardware
- Spezifikation von hoher Qualität
- Baueinheitenauswahl

Analytische Maßnahmen bei der Hardware-Entwicklung

- Entwurfsprüfung durch Inspektion
- statische Analyse

- Funktionsanalyse
- Simulation
- Ausfalleffektanalyse
- Funktionstest

Konstruktive Maßnahmen bei der Software-Entwicklung

- Einhaltung von Richtlinien zur Erstellung von Software
- Verwendung rechnergestützter Entwurfs- und Software-Produktionssysteme
- Spezifikation von hoher Qualität
- strukturierter Entwurf
- Modularisierung
- Verwendung höherer Programmiersprachen
- strukturierte Programmierung
- Verzicht auf Optimierungen
- Überwachungsmaßnahmen

Analytische Maßnahmen bei der Software-Entwicklung

- Inspektion
- Walk-through
- statische Analyse
- Korrektheitsbeweis (formale Verifikation)
- systematischer Test
    - Black-box-Test
    - White-box-Test
- statistischer Test

Funktionsprüfung des Vormusters bzw. Prototyps

- Prüfung der Funktion
- Prüfung der Störfestigkeit
- Prüfung der Zerstörfestigkeit
- Prüfung der Verträglichkeit gegenüber Umgebungsbedingungen

Organisatorische Maßnahmen

- Projektorganisation
- Dokumentation

Soll ein bestehendes Feldbussystem für die sicherheitstechnische Eignung nachträglich geprüft werden, so sind alle erforderlichen fehlervermeidenden Maßnahmen gemäß IEC 61508 zu betrachten. Da im Allgemeinen die Unterlagen über den kompletten Entwicklungszyklus nicht verfügbar sind und somit die fehlervermeidenden Maßnahmen, die während der Entwicklung durchgeführt wurden, nicht vollständig überprüft werden können, kommt dieser Ansatz im Allgemeinen für die nachträgliche Qualifizierung nicht in Betracht. Ein alternativer Nachweis über die Wirksamkeit der fehlervermeidenden Maßnahmen könnte der Nachweis über eine Betriebsbewährung [Fb888] sein, da Feldbussysteme im Allgemeinen in sehr großen Stückzahlen im Einsatz sind. Diese Möglichkeit kommt allerdings nur für die unveränderte Standardhardware und Standardsoftware in Betracht und nicht für die sicherheitstechnische Erweiterung des Feldbussystems.

Bei der Ertüchtigung eines bestehenden Feldbussystems sind selbstverständlich alle zuvor genannten Entwicklungsschritte durchzuführen und fehlervermeidende Maßnahmen gemäß der IEC 61508 zu treffen und zu dokumentieren.

Die Sicherheit eines Systems, hängt nicht nur davon ab, ob es spezifikationsgemäß funktioniert und das ausreichende fehlerbeherrschende Maßnahmen implementiert sind, sondern auch davon, ob das System einfach und sicher zu handhaben ist. Daher sind fehlervermeidende Maßnahme zur Bedienerfreundlichkeit und Handhabungsfreundlichkeit des Systems zusätzlich zu fordern.

Bezieht man diese Forderung auf ein Feldbussystem, so sind hiermit im wesentlichen die „Parametrierung und Programmierung“ und die „Instandhaltung und Wartung“ von Feldbussystemen gemeint.

6.1.4.1 Parametrierung und Programmierung von Feldbussystemen

Für die Parametrierung und Programmierung müssen Dokumente zur Verfügung gestellt werden, welche alle relevanten Schritte und Sicherheitshinweise beinhalten, die für die korrekte Durchführung der Konfiguration notwendig sind.

Für eine fehlerfreie Inbetriebnahme müssen dem Anwender mindesten eine technische Beschreibung des Feldbussystems sowie ein Installations- und Bedienerhandbuch zur Verfügung gestellt werden.

In diesen Unterlagen müssen alle Informationen für die mechanische und elektrische Installation, Inbetriebnahme, Instandhaltung und Wartung beschrieben sein. Die folgenden Inhalte müssen Bestandteil dieser Dokumente sein:

- Mechanische Abmessungen
- Hinweise für die richtige Installation
- Verschiedene Betriebsarten und Betriebsbedingungen
- Anwendungsbeispiele
- Notwendige Bedienungshinweise
- Beschreibung von Status- und Fehlermeldungen
- Hinweise zur Diagnose
- Technische Daten
- Anforderungen an einen sicheren Betrieb, Sicherheitshinweise
- Anschlussbelegungen der Verbindungen
- Anwendungsprogrammierung und Konfiguration
- Einstellungen von Hardwarekonfiguration (z. B. Adresse des Busteilnehmers)
- Zubehör und Ersatzteile

Zusätzlich müssen vor der Inbetriebnahme und Konfiguration Dokumente erstellt werden, aus denen klar hervorgeht, welche Teilnehmer in dem Sicherheitssystem, mit welchen Adressen und Parametern, sicherheitsrelevant und welche nicht sicherheitsrelevant sind. Darüber hinaus muss die jeweilige Funktion der einzelnen Busteilnehmer in diesem Sicherheitssystem aus den Unterlagen eindeutig hervorgehen.

Durchgeführte Änderungen im System müssen entsprechend IEC 61508 dokumentiert werden und nachvollziehbar sein. Der Anwender muss gemäß IEC 61508 entsprechend seiner Aufgabe ausreichend geschult sein, um Fehler aufgrund mangelnder Kenntnisse zu vermeiden.

Die zur Programmierung und Parametrierung verwendeten Tools müssen zuvor auf ihre Eignung zur Programmierung von Feldbussen für sicherheitsgerichtete Aufgaben untersucht und zertifiziert werden, wie für jedes andere Subsystem des Sicherheitssystems auch.

Die verwendeten Tools müssen sicherstellen, dass durch eine bedienerfreundliche Gestaltung der Oberflächen beim Eingeben, Speichern und Übertragen der Daten keine Fehler auftreten können. Zusätzlich muss die Eingabe von sicherheitsrelevanten Daten auf ihre Plausibilität überprüft werden und die vom Tool gespeicherten Daten müsse zusätzlich mit einem Datensicherungsmechanismus versehen werden.

Die Parametrierung und Programmierung mit dem Tool darf nur autorisierten Anwendern über eine Zugangskontrolle möglich sein, so dass widerrechtliche Veränderung im Sicherheitssystem unterbunden werden.

Weitere Maßnahmen, die zu einer Vermeidung von Fehlern bei Parametrierung und Programmierung beitragen sind:

- Verfahrensanweisung für die Parametrierung und Programmierung erstellen,
- Default Parameter müssen immer in die sichere Richtung weisen,
- Anwendung des Vier-Augen-Prinzips, d. h. zwei unabhängigen Personen kontrollieren die Richtigkeit der Parameter,
- Plausibilitätskontrolle nach der Parametrierung, d. h. Auslesen der Parameter aus den einzelnen Busteilnehmern und vergleichen mit den im Tool gespeicherten Daten,
- alle Kontrollmöglichkeiten, die das Tool bietet, nutzen.

Weitere Maßnahmen zur Fehlervermeidung befinden sich in den Anhängen der IEC 61508 und VDE 0801.

6.1.4.2 Instandhaltung und Wartung

Die Instandhaltungs- und Wartungsintervalle in einem nach IEC 61508 betrachteten Schutzsystems werden durch die zeitabhängige gefährliche Versagenswahrscheinlichkeit mit bestimmt.

In Folge nicht durch Diagnose aufgedeckter gefährlicher Fehler steigt die gefährliche Versagenswahrscheinlichkeit an. Durch periodische Funktionstests, z. B. im Rahmen durchgeführter Wartungsintervallen, lässt sich der Zeitverlauf der PFD i. a. so beeinflussen, dass der zulässige Mittelwert der PFD, in einem bestimmten Zeitrahmen, eingehalten wird.

Wenn ein vollständiger Funktionstest innerhalb eines Wartungsintervalls nicht möglich ist, steigt der Wert PFD im Laufe der Zeit so an, dass der zulässige Wert überschritten wird, mit der Folge, dass dann die Komponenten ersetzt werden müssen.

Weiterhin sind die Anforderungen an die fehlervermeidenden Maßnahmen bezüglich der Wartung die Gleichen, wie sie bei der Parametrierung und Programmierung von Busteilnehmern beschrieben worden sind. Die erforderlichen Wartungsintervalle müssen gemäß den Anforderungen der IEC 61508 dokumentiert und eingehalten werden.

Soll die Wartung und Diagnose eines Feldbussystems durch allgemeine Kommunikationskanäle (Internet, DFÜ...) erfolgen ist sicherzustellen, dass keinerlei Funktionen ausgeführt werden können, die die Sicherheitsfunktionen beeinträchtigen können.

6.2 Eignung bestehender Feldbussysteme

Bereits heute sind in einem Sicherheitssystem die Komponenten (Sensoren, Logikeinheiten und Aktoren) für den sicherheitstechnischen Einsatz in der chemischen Industrie entsprechend den heranzuziehenden Standards zertifiziert. Dies bezieht sich jedoch nur auf die Anwendungsseite der Komponenten.

Sollen diese Anwendungen um ein Feldbussystem erweitert werden, so muss ab der Datenschnittstelle (Übergabeschnittstelle) zum Buskoppler eine zusätzliche Zertifizierung durchgeführt werden. Für den Nachweis der Eignung der einzelnen Komponenten einschließlich des Feldbussystems wird vorgeschlagen den internationalen Standard IEC 61508 zugrunde zu legen.

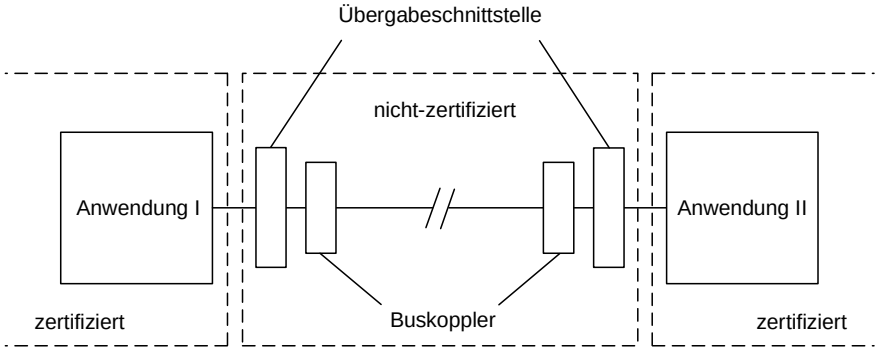


Abbildung 6-6 Nachrichtenfluss zwischen den Anwendungen

Die Standardfeldbussysteme wurden bisher noch nicht als Bestanteil einer Sicherheitskette nach der IEC 61508 zertifiziert und sind aus diesem Grund nicht ohne weiteres in einem Sicherheitssystem einsetzbar. Allerdings können generelle Aussagen über die mögliche Eignung der Standardfeldbussysteme gemacht werden. Insbesondere ob die fehlerbeherrschenden und fehlervermeidenden Maßnahmen, wie sie teilweise in den Standardfeldbussystemen bereits implementiert sind, ausreichen.

Wird ein Sicherheitssystem mit einem integrierten Standardfeldbus betrachtet, so müssen Maßnahmen zur Fehlererkennung gegen die in der IEC 61508 unterstellten Fehler bei der Datenkommunikation getroffen werden. Bei diesen angenommenen Fehlern handelt es sich um Fehler, wie Wiederholung, Verlust, Einfügung, falsche Abfolge, Verzögerung, Verfälschung und Maskierung von Daten. Wobei der Fehler „Maskierung“ nur für Feldbussysteme mit sicherheits- und nicht sicherheitsrelevanten Feldbusteilnehmer zu betrachten ist.

Die zur Zeit auf dem Markt erhältlichen Feldbusse besitzen nur einige der notwendigen Fehlererkennungsmaßnahmen. Für den Einsatz in einem Sicherheitssystem ist es allerdings notwendig, dass alle geforderten Fehlererkennungsmaßnahmen implementiert sind und die geforderte Wirksamkeit haben. Dabei ist zu beachten, dass diese Fehlererkennungsmaßnahmen über den gesamten Übertragungsweg, von der Datenschnittstelle der sendenden Anwendung, dem eigentlichen Feldbus und der Datenschnittstelle der empfangenden Anwendung, wirken.

Bei den üblichen Feldbussystemen ist nur die eigentliche Übertragungsstrecke durch einen CRC-Mechanismus abgesichert und nicht der Weg von der Datenschnittstelle der eigentlichen Anwendung bis zur Datenschnittstelle der empfangenden Anwendung, so dass beispielsweise ein Fehler im Buskoppler nicht aufgedeckt werden kann. Ähnlich verhält es sich bei der gemeinsamen Übertragung von sicherheitsrelevanten und nicht sicherheitsrelevanten Daten über ein Standardfeldbussystem. Auch hier fehlen geeignete Fehlererkennungsmaßnahmen wie sie in dem Standard gefordert werden, z. B. muss eine Verfälschung der sicherheitsrelevanten Daten (Maskierung) durch einen nicht sicheren Busteilnehmer ausgeschlossen oder aufgedeckt werden.

Darüber hinaus muss zusätzlich zu dem Nachweis über die Wirksamkeit der fehlerbeherrschenden Maßnahmen ein Nachweis über die Wirksamkeit der angewendeten fehlervermeidenden Maßnahmen erbracht werden. Im Rahmen dieser Arbeit kann allerdings keine Aussage über die Vollständigkeit der angewendeten fehlervermeidenden Maßnahmen während der Entwicklung der Standardfeldbussystemen gemacht werden, da dies nur im Rahmen einer Einzelprüfung anhand der Entwicklungsunterlagen des Hersteller möglich ist.

Generell sind die Standardfeldbussystemen ohne zusätzliche Maßnahmen zur Fehlerbeherrschung als Teilkomponente innerhalb einer Sicherheitskette nicht einsetzbar. Des weiteren fehlen auch die notwendige Angaben über die gefährliche Versagenswahrscheinlichkeit, der Hardwarefehlertoleranz und der Safe Failure Fraction um eine Qualifizierung gemäß IEC 61508 durchführen zu können.

An dieser Stelle sei nochmals darauf hingewiesen, dass für eine Beurteilung der Eignung eines Feldbussystems zur Übertragung sicherheitsgerichteter Daten in der chemischen Industrie zusätzlich die Anforderungen aus den entsprechenden Anwendungsnormen und die Vorschriften, wie z. B. die IEC 61511, die VDI/VDE 2180 und die NAMUR Empfehlungen zu beachten sind.

Die prinzipiellen Möglichkeiten, Standard-Feldbussysteme dennoch in einer Sicherheitskette einzusetzen, ohne dass das einmal festgelegte und teilweise genormte Übertragungsprotokoll geändert wird, ist in dem folgenden Kapitel behandelt.

6.3 Ertüchtigung zur funktionalen Sicherheit

Soll ein Standardfeldbussystem für den sicherheitsrelevanten Einsatz ertüchtigt werden, so ist es nur sinnvoll, die zusätzlich notwendigen fehlerbeherrschende Maßnahmen so in das Feldbussystem zu integrieren, dass die unteren Layer von diesen Änderungen nicht tangiert werden und eine Änderung der Buskoppler-Hardware nicht nötig wird. Weiterhin sollten auch die teilweise genormten Übertragungsprotokolle unverändert bestehen bleiben, um kompatibel zur bestehenden Installation zu bleiben.

Unter diesen Randbedingungen erscheint es sinnvoll, dass die fehlenden fehlerbeherrschende Maßnahmen in dem eigentlichen Nutzdatenbereich der Telegramme implementiert werden oder z. B. durch eine Mehrfachübertragung realisiert werden.

Nachfolgend sind einige Beispiele für fehlerbeherrschende Maßnahmen angegeben, die im Allgemeinen gegen mehrere Fehlerarten wirken.

Telegrammnummerierung

Durch das Nummerieren der Telegramme ist es möglich die Fehlerarten der unzulässigen „*Wiederholung*“ eines Telegramms, sowie der „*falschen Abfolge*“ aufzudecken und bei Einleiten geeigneter Maßnahmen somit zu beherrschen. Diese Maßnahme könnte derartig erfolgen, dass ein neues Datenfeld für diese Nummerierung im Telegramm definiert wird, welches sich dann von Telegramm zu Telegramm zyklisch in einer vordefinierten Art ändert. Diese Maßnahme kann auch realisiert werden in dem anstelle einer Nummerierung dem Telegramm ein Zeitstempel hinzugefügt wird.

Zeiterwartung

Die Sicherheitsfunktion muss bei Anforderung innerhalb einer vordefinierten Reaktionszeit erfolgen und die Anlage in den sicheren Zustand überführen. Der erforderliche Zyklus ergibt sich aus der geforderten Reaktionszeit des Sicherheitssystem.

Erfolgt im einfachsten Fall die Realisierung durch eine zyklische Telegrammübertragung von einem sicherheitsgerichteten Sensor zur verarbeitenden Einheit mit sicherheitsgerichteter Abschaltfunktion und Zeitüberwachung wird bei Überschreitung der Zeitbedingung die Abschaltung eingeleitet.

Hierbei kann es aber vorkommen, dass durch das permanente zyklische Senden des sicherheitsgerichteten Sensors sich mehrere ältere Telegramme irgendwo in einem Datenpuffer (z. B. Stack) auf der Übertragungsstrecke oder in einem der Buscontroller befinden, so dass eine gesendete Abschaltinformation die zu verarbeitende Einheit zu spät erreicht, da erst die älteren Telegramme in ihrer Reihenfolge abgearbeitet werden wie sie versendet worden sind.

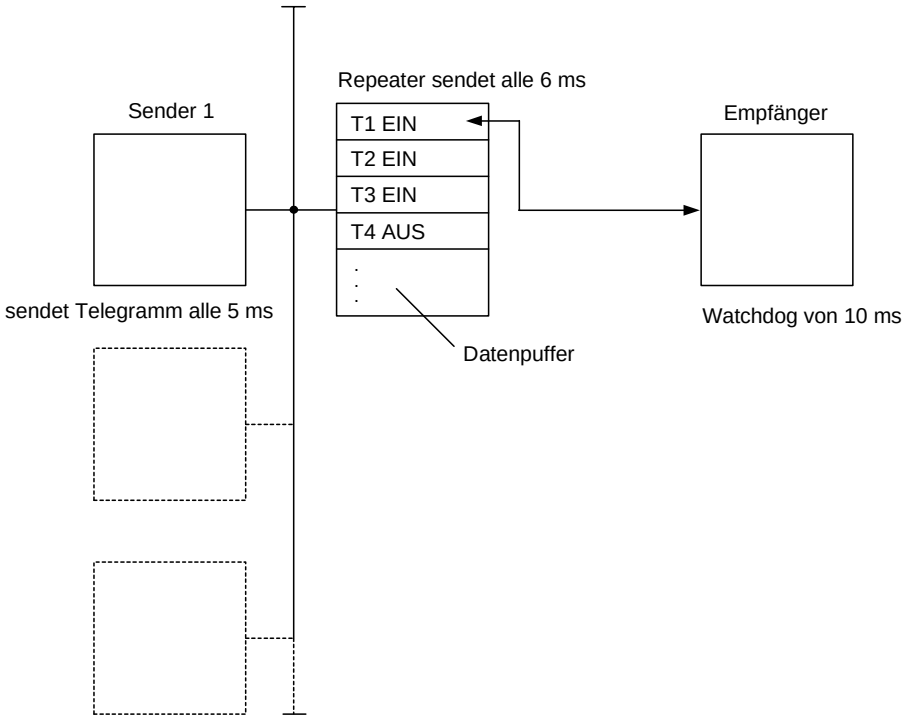


Abbildung 6-7 Problematik der Zeitverzögerungen durch Datenpuffer

Die Abbildung 6-7 zeigt zum Beispiel eine mögliche Busarchitektur bestehend aus mehreren Sendern, einem Repeater für die Verstärkung des Signals und einem Empfänger. Der Empfänger erwartet entsprechend seiner vorgegebenen Watchdog Zeit alle 10 ms ein Telegramm vom Sender 1. Der Sender 1 verschickt alle 5 ms ein Telegramm über den Repeater an den Empfänger.

Der Repeater leitet aber aufgrund einer hohen Busauslastung, verursacht durch die anderen Teilnehmer, die Telegramme nur alle 6 ms an den Empfänger weiter. Dadurch kann es über einen längeren Zeitraum zu einer Aufstauung von älteren Telegrammen im Datenpuffer des Repeater kommen. Dies hat zur Folge, dass eine Abschaltinformation vom Sender 1 verspätet beim Empfänger eintrifft und er nicht entsprechend innerhalb der erforderlichen Reaktionszeit reagieren kann.

Die an diesem Beispiel erläuterte Problematik besteht prinzipiell bei allen Datenpuffern innerhalb eines Feldbussystems, z. B. auch im Bus-Controller selber.

Aus diesem Grund reicht einen einfache zyklische Telegrammwiederholung als Zeitüberwachung nicht aus. Es müssen Maßnahmen getroffen werden, die sicherstellen, dass das Telegramm mit der sicherheitsgerichteten Information unabhängig von irgendwelchen Datenstaus auf der Übertragungsstrecke bei der verarbeitenden Einheit innerhalb der Reaktionszeit ankommt oder das Ausbleiben dieser sicherheitsgerichteten Information festgestellt wird.

Mit diesen zusätzlichen Maßnahme werden die möglichen Fehlerarten des „*Verlustes*“ und der „*Verzögerung*“ eines Telegramms aufgedeckt und können durch geeignete Maßnahmen beherrscht werden. Zusätzlich erfüllt man auch die Forderung nach der Dynamisierung des Feldbusses.

Quittierung

Durch ein Quittieren der empfangenen Telegramme von sicherheitsgerichteten Busteilnehmern kann sicher gestellt werden, dass der Adressat die notwendige Information auch erhalten hat.

Besteht die Quittierung darin, die gleichen Informationen an den Sender zurückzugeben, so besteht die Möglichkeit, diese auf Richtigkeit zu überprüfen und gegebenenfalls, wenn es in der verfügbaren Zeit möglich ist, bei einer Verfälschung die Information ein weiteres mal zu senden.

Eine Quittierung ist auch eine Maßnahme gegen eine falsche Adressierung und Datenverlust. Ist die Nachricht falsch zugestellt worden, so wird der Sender die Quittung von einem falschen Empfänger erhalten und kann somit wiederum Maßnahmen einleiten. Erhält der Sender in einer vordefinierten Zeit keine Quittung, so muss er davon ausgehen, dass die Nachricht verloren gegangen ist. Die meisten gängigen Feldbussysteme verfügen bereits über die Maßnahme der Quittierung, ob diese implementierte Maßnahme ausreichend ist, muss gemäß den Anforderungen beurteilt werden.

Datensicherung

Durch die bereits implementierten Datensicherungsmethoden, wie sie im Kapitel 5.6 beschrieben sind, können Verfälschungen, welche auf der Übertragungsstrecke stattfinden aufgedeckt werden.

Inwieweit diese vorhandene Maßnahme schon ausreicht, um die Anforderungen die an das Sicherheitssystem gestellt werden zu erfüllen, muss rechnerisch nachgewiesen werden.

Der Bereich zwischen der Datenschnittstelle und dem CRC-Mechanismus im Buscontrollerchip ist zunächst einmal als unsicher anzusehen und ist bei der Bewertung entsprechend zu berücksichtigen. Die Vorgehensweise des rechnerischen Nachweises ist im Kapitel 6.1.2 beschrieben.

Eindeutige Adressierung

Eine weitere Maßnahme ist die eindeutige Zuordnung der sicherheitsgerichteten Busteilnehmer zueinander, z. B. jeder sicherheitsgerichtete Teilnehmer verfügt über eine Liste mit den Adressen der Busteilnehmer, von denen er Telegramme empfangen darf. Mittels einer Plausibilitätsbewertung kann der Busteilnehmer nun entscheiden, ob dieses Telegramm fälschlich an ihn gesendet worden ist oder nicht. Weiterhin kann diese Liste dafür benutzt werden, festzustellen, ob alle gelisteten Teilnehmer ihr Senderecht wahrgenommen haben. Diese Maßnahme stellt hohe Anforderungen an die Netzorganisation.

In einem Feldbussystem mit sicherheitsgerichteten Busteilnehmer und nicht sicheren Busteilnehmern muss sichergestellt werden, dass die nicht sicheren Busteilnehmer sich nicht als sichere Busteilnehmer ausgeben können.

Um diese Rückwirkungsfreiheit zwischen diesen Busteilnehmergruppen zu erreichen sollte ein Adressbereich definiert werden, der von den nicht sicheren Busteilnehmern nicht verwendet werden darf und auch nicht generiert werden kann.

Eindeutige Identifizierung von nicht-sicheren und sicheren Informationen

Bei einem Mischbetrieb von sicheren und nicht sicheren Busteilnehmern müssen Maßnahmen getroffen werden, die es in der Applikation ermöglichen eindeutig zwischen sicherheitsrelevanten und nicht sicherheitsrelevanten Informationen zu unterscheiden. Eine Möglichkeit wäre es die Daten der sicherheitsrelevanten und nicht sicherheitsrelevanten Busteilnehmer durch unterschiedliche CRC zu sichern.

Reduzierung der Datengültigkeit

Diese Reduzierung könnte derart erfolgen, dass für einen sicherheitsgerichteten Busteilnehmer nur zwei gültige Bitkombinationen definiert werden z. B. „Abschalten“ oder „Nicht Abschalten“ und alle anderen Kombination per Definition nicht zulässig sind.

Busarchitektur

Eine weitere Möglichkeit, einen Teil der zuvor genannten Fehler zu erkennen, besteht darin, den Feldbus redundant auszulegen. Hierbei ist zu unterscheiden, ob nur ein Teil oder das komplette Feldbussystem redundant ausgelegt wird. Im folgenden sollen einige mögliche Feldbusarchitekturen genannt und erläutert werden.

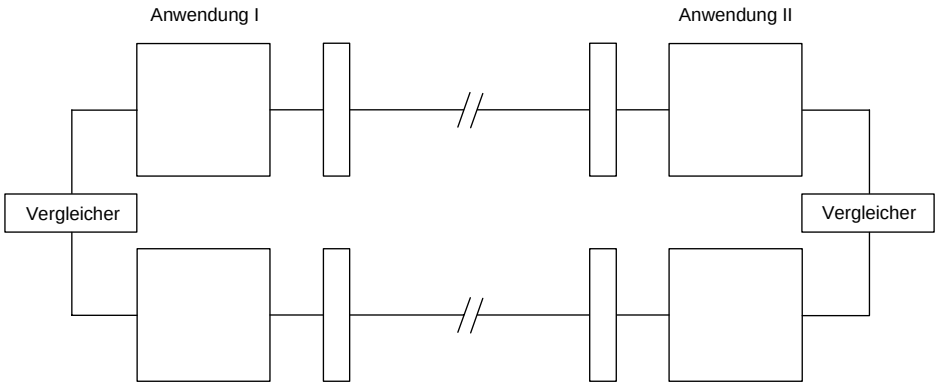


Abbildung 6-8 Vollständig redundantes Feldbusarchitektur

Bei einer komplett redundanten Lösung, wie sie in der Abbildung 6-8 prinzipiell dargestellt ist, werden jeweils die Telegramme beider Kanäle unabhängig übertragen und anschließend auf Gleichheit überprüft.

Durch diese Architektur werden prinzipiell alle Einfachfehler durch Hardwareausfälle innerhalb des redundanten Feldbussystems, bis auf mögliche Common Cause Anteile, aufgedeckt. Jedoch ist eine Erkennung von Telegrammwiederholungen nicht möglich, wenn z. B. permanent ein identisches Telegramm mit dem gleichen Informationsgehalt „Nicht Abschalten“ versendet wird.

Die Aufdeckung dieser Fehlerart würde erst erfolgen, wenn es zu einer Anforderung kommt und dadurch eine Ungleichheit zwischen den beiden Kanälen entsteht. Erfolgt eine Anforderung nur sehr selten, so könnte es durch eine Fehlerhäufung zum gleichartigen Versagen des zweiten Kanals kommen und das Sicherheitssystem wäre gefährlich ausgefallen.

Eine weitere Stärke dieser Architektur ist die Erkennung von Datenverfälschungen die zwischen der Anwendung und dem Datensicherungsmechanismus im Buskoppler entstehen.

Durch die redundante Auslegung ist die Wahrscheinlichkeit, dass ein Übertragungsfehler nicht erkannt wird gleich dem Quadrat der Restfehlerwahrscheinlichkeit plus einem Common Cause Anteil.

In der folgender Busarchitektur ist die reine Übertragungsstrecke einkanalig aufgebaut, aber die Buskontroller des Senders und des Empfängers jeweils zweikanalig.

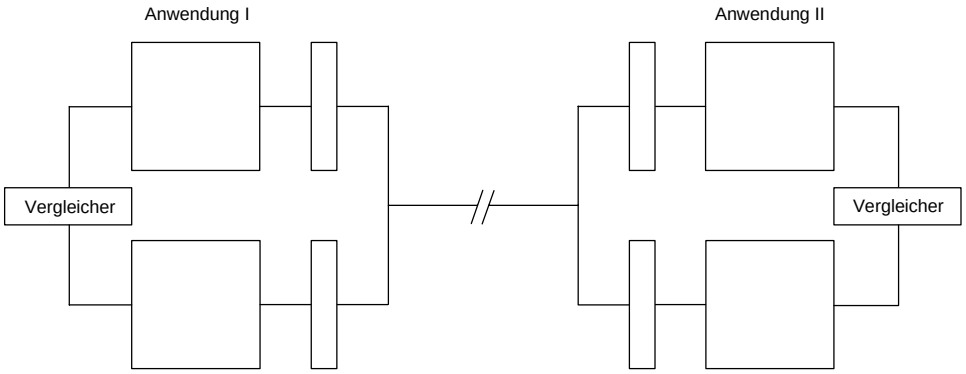


Abbildung 6-9 Teilredundante Feldbusarchitektur

In dieser Feldbusarchitektur werden Übertragungsfehler, die durch Störungen auf der einkanaligen Übertragungsstrecke entstehen, mit der gleichen Fehleraufdeckung wie im vorherigen Beispiel aufgedeckt. Hier hat die einkanalige Übertragungsstrecke den zusätzlichen Vorteil, dass die beiden Telegramme nacheinander übertragen werden und das dadurch kurzzeitige Störungen sich sehr selten auf beide Telegramme auswirken, wie es bei der vorherigen Struktur theoretisch möglich wäre.

Durch das Vorhandensein von redundanten Teilen in dieser Architektur sind auch hier mögliche Common Cause Anteile zu berücksichtigen. Da auch hier durch die redundante Struktur der Buskoppler immer zwei identische Telegramme versendet werden ist auch hier die Wahrscheinlichkeit, dass ein Übertragungsfehler nicht erkannt wird gleich dem Quadrat der Restfehlerwahrscheinlichkeit plus einen Common Cause Anteil, welcher sich nur auf die redundanten Teile bezieht.

Eventuell ist es zusätzlich notwendig, dass die Fehlererkennungsmaßnahmen regelmäßig getestet werden müssen.

In den zuvor betrachteten Busarchitekturen zeigt sich, dass dort die Wahrscheinlichkeit, dass ein Übertragungsfehler nicht erkannt wird gleich dem Quadrat der Restfehlerwahrscheinlichkeit ist, unabhängig ob der Übertragungskanal vollständig redundant oder nur teilredundant aufgebaut ist. Wichtig ist hierbei der Punkt, dass ein identisches Telegramm mehrfach übertragen wird.

Werden identische Daten mehrfach versendet, so wird sich die Wirksamkeit der Fehlererkennung bei Datenverfälschungen erhöhen. Des weiteren kann die Verfügbarkeit eines Systems erhöht werden, indem die Richtigkeit einer Information aus einer Vielzahl von empfangenen Telegrammen durch das Mehrheitsprinzip entschieden wird.

Ob diese Möglichkeit realisiert werden kann, ist im starken Maße von der zur Verfügung stehenden Reaktionszeit abhängig. Hier könnte sich ein Vorteil für die Anwendung in der chemischen Industrie zeigen, da die Reaktionszeiten zum Teil sehr viel größer sind als in der Maschinenbau- oder in der Automobilindustrie. In den folgenden Kapiteln soll der Einfluss der Reaktionszeit, sowie die Relevanz der Verfügbarkeit näher erläutert werden.

6.4 Reaktionszeit

Die Reaktionszeit ist die maximale Zeit zwischen den Anforderungen an das Sicherheitssystem und dem Erreichen des sicherheitsgerichteten Signals am Aktor, der für die Ausführung der Sicherheitsfunktion verantwortlich ist.

Dabei ergibt sich die gesamte Reaktionszeit aus der Summe der einzelnen Reaktionszeiten aller in einer Sicherheitskette befindlichen Komponenten einschließlich der maximal auftretenden Telegrammlaufzeiten.

Während die Maschinenbau- und die Automobilindustrie schnelle Feldbusse mit Reaktionszeiten von einigen ms fordern, sind in der Verfahrenstechnik, Petrochemie, Pharma- oder Chemie-Industrie teilweise Reaktionszeiten von einigen 100 ms ausreichend. Maßgebliche Einflussfaktoren auf die Reaktionszeit eines Feldbussystems sind, neben den in gewissen Grenzen festen Auswerte- und Berechnungszeiten, die, die Feldbusteilnehmer für Modulation und Demodulation des Signals etc. benötigen, die verwendete Datenübertragungsrate und die momentane Busbelastung.

Je nach dem verwendeten Buszugriffverfahren unterliegt die Busbelastung sehr starken Schwankungen. Um diese schwankende Busbelastung zu reduzieren und somit die Reaktionszeit möglichst konstant zu halten, könnten beispielsweise alle sicherheitsgerichteten Teilnehmer immer ein Senderecht zu definierten Zeiten bekommen.

Eine weitere Maßnahme könnte darin bestehen, dass die sicherheitsgerichteten Teilnehmer immer ein bevorzugtes Senderecht erhalten. Somit wäre es den nicht-sicheren Teilnehmern nur möglich den Bus zu nutzen, wenn er von keinem sicherheitsgerichteten Teilnehmer angefordert wird.

Busteilnehmer die eine sichere Funktion ausführen sollen und aufgrund der Forderung nach dem dynamischen Prinzip permanent ihre Telegramme senden bedeuten für den Feldbus eine zusätzliche Belastung.

Besitzt der empfangende Busteilnehmer eine Zeiterwartung und wird sie aufgrund einer unzulässigen Busbelastung überschritten kann dieser Teilnehmer selbstständig in den Failsafe-Zustand übergehen.

Für die Bestimmung der maximal garantierten Reaktionszeit eines Feldbussystems ist es erforderlich, dass alle Parameter, wie beispielsweise die Anzahl der Busteilnehmer, die Übertragungsrate und das verwendete Buszugriffverfahren berücksichtigt werden.

Bei nicht echtzeitfähigen Feldbussystemen, die beispielsweise mit einem Buszugriffsverfahren "Buszugriff nach Bedarf" (siehe Kapitel 5.4.2) arbeiten, kann sich die genaue Bestimmung der Reaktionszeit als schwierig gestalten.
Zur Überwachung der Reaktionszeit müssen alle sicherheitsrelevanten Busteilnehmer mit einer Zeiterwartung versehen werden.

6.5 Verfügbarkeit

Ebenso wichtig, wie die Fehlererkennung bezüglich der Sicherheit, ist die Betrachtung bezüglich der Verfügbarkeit in einem Feldbussystem.
Wenn durch die implementierten fehlererkennenden Maßnahmen das Feldbussystem zu häufig in den sicheren Zustand geht, ist dieses System zwar sehr sicher, aber letztendlich für die Praxis nicht zu gebrauchen, da die Verfügbarkeit gegen Null geht.

Bisher wurden herkömmliche Feldbussysteme nur zur Übertragung von Nutzdaten (Prozessdaten) verwendet, welche in direkter Hinsicht keine sicherheitstechnische Relevanz darstellten. Fehlerhafte Telegramme werden hier in einem gewissen Umfang akzeptiert und führen nicht zur Abschaltung der Anlage. Kommt es zu fehlerhaften Telegrammen, so wird dies zum Teil erkannt und das Telegramm wird verworfen und es erfolgt ein erneutes Senden dieser Daten.

Dieses erneute Senden der Daten erfolgt so oft, bis entweder ein korrektes Telegramm empfangen wird oder durch ein entsprechendes aktuelleres Telegramm überschrieben wird. Die Daten von denen hier gesprochen wird, sind Daten mit reinem informativen Charakter und dienen lediglich der Prozessverfolgung oder der Prozesssteuerung.

Bei Daten zur Prozesssteuerung kann z. B. durch Plausibilitätsprüfungen oder durch Trendanalysen festgestellt werden, ob diese Daten zur Weiterführung des Prozesses verwendet werden können oder ob neue Daten angefordert werden müssen.

Die sicherheitsrelevanten Daten eines Schutzsystems wurden nicht über den Bus übertragen, sondern durch Punkt-zu-Punkt-Verdrahtungen realisiert und wurden den Nutzdaten hierarchisch übergeordnet.

Diese Punkt-zu-Punkt-Verdrahtungen verursachten zwar einen erheblicheren Verdrahtungsaufwand, waren aber in der Übertragung der Daten sehr zuverlässig und garantierten der Anlage somit eine hohe Verfügbarkeit.

Diese Art der Realisierung der Sicherheitstechnik hatte nicht nur einen hohen Verdrahtungsaufwand zur Folge, sondern verursachte auch hohe Kosten bezüglich Installation und Wartung, insbesondere in Anlagen mit großer räumlichen Ausdehnung, sowie bei Erweiterungen und Änderungen.

Sollen nun die sicherheitsgerichteten Daten auch über Feldbussysteme übertragen werden, so muss im höchsten Maße sichergestellt werden, dass diese Daten am Empfänger so empfangen werden wie sie vom Sender gesendet worden sind.

Ein Maß dafür, wie groß die Wahrscheinlichkeit einer Datenverfälschung ist, stellt die Restfehlerwahrscheinlichkeit dar. Sie ist ausführlich in Kapitel 6.1.2.2 erläutert.

Im Gegensatz zu den herkömmlichen Feldbussystemen zur reinen Nutzdatenübertragung dürfen bei der Übertragung von sicherheitsrelevanten Daten fehlerhafte Telegramme nicht oder kaum akzeptiert werden.

Feldbusse für Schutzsysteme müssen hohen Anforderungen bezüglich der Fehlererkennung genügen und haben dadurch einen sehr viel größeren Aufdeckungsgrad von fehlerhaften Telegrammen als herkömmliche Systeme. Diese Tatsache kann jedoch zur Reduzierung der Verfügbarkeit führen.

Handelt es sich um einen proprietären Feldbus für eine sichere Datenübertragung, so kann ohne weiteres davon ausgegangen werden, das jedes Telegramm einen sicherheitsrelevanten Stellenwert besitzt und es im Falle einer Datenkorrumpierung zur kontrollierten Abschaltung kommen muss. Die Abschaltung muss auf jeden Fall sofort initiiert werden, wenn eine Korrektur des Telegramms nicht möglich ist und die geforderte Reaktionszeit ein erneutes Senden des Telegramms nicht zulässt.

Bei der Datenübertragung wird häufig die Verfügbarkeit durch Übertragungsfehler, bedingt durch EMV Störungen, herabgesetzt.

Eine denkbare Strategie ist es, Telegramme, welche keinerlei sinnvolle Informationen enthalten, zu verwerfen und erneut anzufordern und dadurch die Verfügbarkeit zu erhöhen, sofern es die geforderte Reaktionszeit zulässt.

Werden hingegen immer zwei Telegramme mit gleicher Information gesendet und diese beiden Telegramme durch Vergleich zur Fehlererkennung verwendet, so wird die Sicherheit des Systems zwar erhöht, aber auch zugleich die Wahrscheinlichkeit der Abschaltung und somit die Verfügbarkeit des Systems wiederum verringert. Hierbei muss die Regel gelten, dass das Sicherheitssystem nicht anspricht, wenn beide Telegramme fehlerfrei empfangen wurden und die Information “nicht abschalten” beinhalten. In allen anderen Fällen muss das Sicherheitssystem ansprechen.

Um die Sicherheit und gleichermaßen die Verfügbarkeit des Feldbussystems zu erhöhen ist eine mehrfach Übertragung gleicher Informationen denkbar. Dieses Vorgehen ist allerdings nur möglich, wenn es die Reaktionszeit zulässt. Bei diesem Verfahren wird die Entscheidung über die Korrektheit der Information nach dem Mehrheitsprinzip gefällt.

Eine weitere Maßnahme zur Erhöhung der Verfügbarkeit ist es das Telegramm mit redundanten Bits zur Fehlerkorrektur zu ergänzen.

Diese Maßnahme wurde bei der Übertragung von einfachen Nutzdaten nicht für Notwendig erachtet, da sie unter Umständen die Effizienz der Datenübertragung einschränkt. Sie bekommt aber bei der Übertragung von sicherheitsrelevanten Daten einen ganz anderen Stellenwert, da die Akzeptanz durch den Nutzer maßgeblich auch von der Verfügbarkeit des Systems abhängig ist.

Um Verfügbarkeitsprobleme durch umgebungsbedingte Interferenzen zu vermeiden, muss bei der Neukonzipierung sicherheitsgerichteter Feldbussysteme besonders Wert auf die Widerstandsfähigkeit gegenüber Störeinflüssen gelegt werden.

Maßnahmen zur Erhöhung der Störsicherheit sind die Verwendung von Übertragungsmedien mit möglichst geringer Bitfehlerrate und geringer Empfindlichkeit gegenüber EMV-Einflüssen, sowie die Verwendung von Komponenten mit ausreichenden Schutz gegenüber Einflüssen aus der Umgebung.

Soll ein bereits in Betrieb befindliches Feldbussystem nachträglich für sicherheitsrelevante Kommunikation verwendet werden und waren entsprechende EMV-Überlegungen nicht schon ein wesentlicher Bestandteil des bereits installierten Feldbussystems, so kann es hier zu erheblichen Verfügbarkeitsproblemen kommen.

7 Zusammenfassung und Bewertung

Das Bundes-Immissionsschutzgesetz (BImSchG) gemäß §5 Satz 1 Pkt3 und die Störfall-Verordnung gemäß §3 Abs. 4 fordern, dass die Beschaffenheit und der Betrieb einer Anlage dem Stand der Sicherheitstechnik entsprechen muss. Ausgehend von dieser allgemeinen rechtlichen Grundlage wurde untersucht, welche technischen Standards für die Bewertung von Feldbussystemen geeignet sind und welche Anforderungen sich aus diesen Standards für die Feldbussysteme ableiten lassen.

Neben einer grundlegenden Sicherheitsbetrachtung wurde das ISO-OSI-Schichtenmodell erläutert und die prinzipielle Funktionsweise heutiger Feldbussysteme, wie beispielsweise die unterschiedlichen Buszugriffsverfahren und die verschiedenen Übertragungsverfahren, beschrieben. Ebenso wurden die verschiedenen Datensicherungsmechanismen der herkömmlichen Feldbussysteme vorgestellt und ihre Vor- und Nachteilen beschrieben.

Anhand der Anforderungen, die sich aus den internationalen Standards ergeben, wurden die unterschiedlichen Möglichkeiten diskutiert, ob oder unter welchen Randbedingungen und für welche Zwecke heutige Feldbussysteme in MSR-Schutzeinrichtungen in der chemischen Industrie eingesetzt werden können. Darüber hinaus wurden Berechnungsmethoden für die Bestimmung der Restfehlerwahrscheinlichkeit vorgestellt, die eine Bewertung der Datensicherungsmaßnahmen für die Übertragungsstrecke ermöglichen.

Bevor ein Feldbussystem in einer MSR-Schutzeinrichtung eingesetzt werden kann, ist in jedem Fall ein Nachweis zu erbringen, dass das Feldbussystem die Anforderungen, die an diese MSR-Schutzeinrichtung durch die Normung vorgegeben werden, erfüllt.
Prinzipiell müssen in einem Feldbussystem, wenn es in einer MSR-Schutzeinrichtung eingesetzt werden soll, fehlerbeherrschende Maßnahmen gegen folgende Fehler implementiert sein:

- Übertragungsfehler
- Wiederholung
- Verlust
- Einfügung
- falsche Abfolge
- Nachrichtenverfälschung
- zeitliche Verzögerung
- Maskierung/fehlerhafte Adressierung

Zur Aufdeckung passiver Fehler innerhalb eines Feldbussystems sind regelmäßige Funktionsprüfungen erforderlich, wenn nicht nachgewiesen werden kann, dass die implementierten fehlerbeherrschenden Maßnahmen alle passiven Fehler aufdecken.

Sollen in einem Feldbussystem sicherheitsrelevante Nutzdaten und nicht sicherheitsrelevante Nutzdaten gemischt übertragen werden, muss sichergestellt werden, dass nicht sicherheitsrelevante Nutzdaten keine Sicherheitsfunktionen beim Empfänger verhindern oder auslösen können. Durch unterschiedliche Algorithmen und Generatorpolynome für die Datensicherung der sicherheitsrelevanten Nutzdaten und der nicht sicherheitsrelevanten Nutzdaten wäre ein Mischbetrieb möglich.

Die Forderungen der Chemie-Industrie nach einer hohen Verfügbarkeit einer MSR-Schutzeinrichtung und somit auch an ein Feldbussystem kann durch folgende Maßnahmen erreicht werden:

- verkleinern der Ausfallrate
- Erhöhung der Übertragungssicherheit
- redundante Auslegung

Durch die vereinfachte und übersichtliche Installation von Feldbussystemen und dem Einsatz von geeigneten Tools zur Parametrierung, Diagnose und Wartung gegenüber der herkömmlichen Verdrahtung der Schutzsysteme, mit den daraus resultierenden Fehlerquellen, ist eine Erhöhung der Sicherheit zu erwarten.

Ein Nachweis über die Wirksamkeit dieser fehlervermeidenden und fehlerbeherrschenden Maßnahmen ist durch eine Zertifizierung möglich.

Wird hierfür der internationale Standard IEC 61508 verwendet, ist neben dem Nachweis über die Wirksamkeit der fehlerbeherrschenden Maßnahmen auch eine Bewertung der fehlervermeidenden Maßnahmen sowie die Berechnung der gefährlichen Versagenswahrscheinlichkeit (PFD) vorzunehmen. Des weiteren ist die Hardwarefehlertoleranz (HFT) und die Safe Failure Fraction (SFF) für das Feldbussystem zu bestimmen. An dieser Stelle soll nochmals darauf hingewiesen werden, dass die Angabe in der IEC 61508 bezüglich der gefährlichen Versagenswahrscheinlichkeit immer für die gesamte Sicherheitskette einer Schutzeinrichtung gilt, d. h. dass die gefährliche Versagenswahrscheinlichkeit eines Feldbussystems nur einen Teil der gesamten gefährlichen Versagenswahrscheinlichkeit (siehe Tabelle 3-2) ausmachen darf.

Da immer mehr MSR-Schutzeinrichtungen, welche dem Standard IEC 61508 entsprechen, mit einem Feldbussystem kombiniert werden sollen, ist eine Zertifizierung nach dem Standard IEC 61508 auch für die Feldbussysteme zu empfehlen.

Zusätzlich zu dem anwendungsunabhängigen Standard IEC 61508 sind darüber hinaus selbstverständlich auch immer die anwendungsbezogenen Standards zu berücksichtigen.

Die in diesem Forschungsbericht betrachteten Standardfeldbussysteme erfüllen die Anforderungen der IEC 61508 bezüglich der fehlerbeherrschenden Maßnahmen nur teilweise. Aus diesem Grund sind diese Standardfeldbussysteme ohne zusätzliche Maßnahmen zur Fehlerbeherrschung nicht in MSR-Schutzeinrichtungen einsetzbar. Hinzu kommt, dass keine Aussage über die Wirksamkeit der fehlervermeidenden Maßnahmen sowie über die gefährliche Versagenswahrscheinlichkeit, die Hardwarefehlertoleranz und die Safe Failure Fraction dieser Standardfeldbussysteme gemacht werden kann, da zum Teil die notwendigen Informationen und Entwicklungsunterlagen erst im Rahmen einer angestrebten Zertifizierung durch den jeweiligen Feldbushersteller zur Verfügung gestellt werden.

Dennoch bleibt festzustellen, dass die heutigen Feldbussysteme durch zusätzliche fehlerbeherrschende Maßnahmen, wie sie im Kapitel 6.3 aufgezeigt wurden, prinzipiell für den Einsatz in MSR-Schutzeinrichtungen ertüchtigt werden können.

Zur Zeit gibt es in der Industrie vielversprechende Ansätze und teilweise erste Prototypen von Feldbussystemen, die eine Zertifizierung nach der IEC 61508 und entsprechenden Anwendungsstandards erwarten lassen, so dass zukünftig sowohl sicherheitsgerichtete Signale als auch Nutzsignale, d. h. Signale der Schutzeinrichtungen als auch Signale der Betriebs- und Überwachungseinrichtungen, auf **einem** Feldbussystem **gemeinsam** übertragen werden können.

Indexverzeichnis

M

N

P

Q

R

S

T

Ü

V

W

Z

Abkürzungsverzeichnis

Abkürzung	
AK	**A**nforderungs**k**lasse
ASI	**A**ktor-**S**ensor-**I**nterface
BER	**B**it **e**rror **r**ate (Bitfehlerrate)
CAN	**C**ontroller **A**rea **N**etwork
CRC	**C**yclic **R**edundancy **C**heck (Datensicherungsmethode)
CSMA	**C**arrier **S**ense **M**ultiple **A**ccess (Alle Busteilnehmer können die Masterfunktion übernehmen)
CSMA/**CA**	**C**ollision **A**voidance (Kollision vermeiden)
CSMA/**CD**	**C**ollision **D**etection (Kollision detektieren)
DFÜ	**D**aten**f**ern**ü**bertragung
EMV / EMI	**E**lektro**m**agnetische **V**erträglichkeit **E**lectro**m**agnetic **I**nterference
FISCO	**F**ieldbus **I**ntrinsically **S**afe **Co**ncept (Eigensicherheitsanforderungen)
FM	**F**requenz**m**odulation
FMEA	**F**ailure **m**ode and **e**ffect **a**nalysis **F**ehler-**M**öglichkeits- und **E**influss-**A**nalyse
HART	**H**ighway **A**ddressable **R**emote **T**ransducer (Protokoll für busadressierte Feldgeräte)
HFT	**H**ardware **f**ailure **t**olerance **H**ardware**f**ehler**t**oleranz
IEC	**I**nternational **E**lectrotechnical **C**ommission
ISO	**I**nternational **S**tandard **O**rganisation
OSI	**O**pen **S**ystem **I**nterconnection
LAN	**L**ocal **A**rea **N**etwork

Abkürzungsverzeichnis

Abkürzung	Deutsch
LON	**L**ocal **O**perating **N**etwork
LWL	**L**icht**w**ellen**l**eiter
MSR	**M**ess-, **S**teuer- und **R**egeleinrichtungen
NAMUR	**N**ormen**a**rbeitsgemeinschaft für **M**ess- **u**nd **R**egeltechnik in der chemischen Industrie
NRZ	**N**on **R**eturn to **Z**ero (Kodierungseigenschaft)
PB	Bitfehlerwahrscheinlichkeit
PFD	**P**robability of **f**ailure of **d**emand
PLT	**P**rozess**l**eit**t**echnik
PNK	**P**rozess**n**ahe **K**omponente
Profibus **PA**	**P**rozess **A**utomation
Profibus **DP**	**D**ezentrale **P**eripherie
PT	Telegrammfehlerwahrscheinlichkeit
PTB	**P**hysikalisch **T**echnische **B**undesanstalt
SFF	**S**afe **F**ailure **F**raction
SIL	**S**afety **I**ntegrity **L**evel
SPS	**S**peicher**p**rogrammierbare **S**teuerung
TTL	**T**ransistor **T**ransistor **L**ogik
World**FIP**	**F**actory **I**nstrumentation **P**rotocol Standardfeldbusprotokoll

Normen und Literaturverzeichnis

[DIN V 19250] Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen, 1994

[DIN 19251] MSR-Schutzeinrichtungen Anforderungen und Maßnahmen zur gesicherten Funktion, 1993

[DIN V VDE 0801] Grundsätze für Rechner in Systemen mit Anhang A1 Sicherheitsaufgaben, 1990

[IEC 61508] Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 1 - 7, 2000

[DIN 19245] PROFIBUS
Teil 1: Übertragungstechnik, 1993
Teil 2: Kommunikations-Modell, 1991
Teil 3: Dezentrale Peripherie (DP), 1994

[DIN EN 50170] Universelles Feldkommunikationssystem; Änderung A2, 2000

[prEN 50159] Bahnanwendungen- Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme, 1996
Teil 1: Sicherheitsrelevante Kommunikation in geschlossenen Übertragungssystemen
Teil 2: Sicherheitsrelevante Kommunikation in offenen Übertragungssystemen

[VDI VDE 2180] Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozeßleittechnik (PLT) Blatt 1 - 5, 1998

[NAMUR NE 31] Anlagensicherung mit Mitteln der Prozeßleittechnik, 1993

[NAMUR NE 53] Software von Feldgeräten und signalverarbeitenden Geräten mit Digitalelektronik, 1995

[NAMUR NA 74] NAMUR-Anforderungen an den Feldbus, 1997

[NAMUR NE 79] Mikroprozessorbestückte Geräte in der Anlagensicherung, 1999

[REI98] Feldbussysteme; B. Reißenweber,
Verlag R. Oldenbourg, München, 1998

[BIA00] Bussysteme für die Übertragung sicherheitsrelevanter Nachrichten, Berufsgenossenschaftliches Institut für Arbeitssicherheit, Sankt Augustin, 2000

[WEST96] Elektrotechnik Tabellen Kommunikationselektronik
Verlag Westermann Schulbuchverlag, Braunschweig, 1996

[BRON91] Taschenbuch der Mathematik, Bronstein, Semendjajew,
Verlag Nauka Moskau, 1991

[LOC97] Digitale Nachrichtentechnik, Prof. Dr.-Ing. D. Lochmann,
Verlag Technik GmbH, 1997

[StörfallV00] Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfall-Verordnung)
- 12. BImSchV, 2000

[StörfallVwV93] Erste Allgemeine Verwaltungsvorschrift zur Störfall-Verordnung - 1. Störfall VwV, 1993

[SWO73] Codierung zur Fehlerkorrektur und Fehlererkennung, Dr.-tech. Joachim Swoboda, Oldenbourg Verlag München, 1973

[Fb888] Betriebsbewährung von Hard- und Software von Rechnern für Sicherungsaufgaben,
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin Dortmund, Fb888