Landesumweltamt Nordrhein-Westfalen

Forschungsvorhaben 35/00

Anwendung der Bussysteme in der Anlagensicherheit der Chemie-Industrie

„Kurzreferat“

von

Dipl.-Ing. Heinz Gall

Dipl.-Ing. Thomas Steffens

Dipl.-Ing. Klaus Kemp

TÜV Anlagentechnik GmbH
Automation, Software und Informationstechnologie (ASI)

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.

2 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.

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.

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 2-1 hervorgeht.

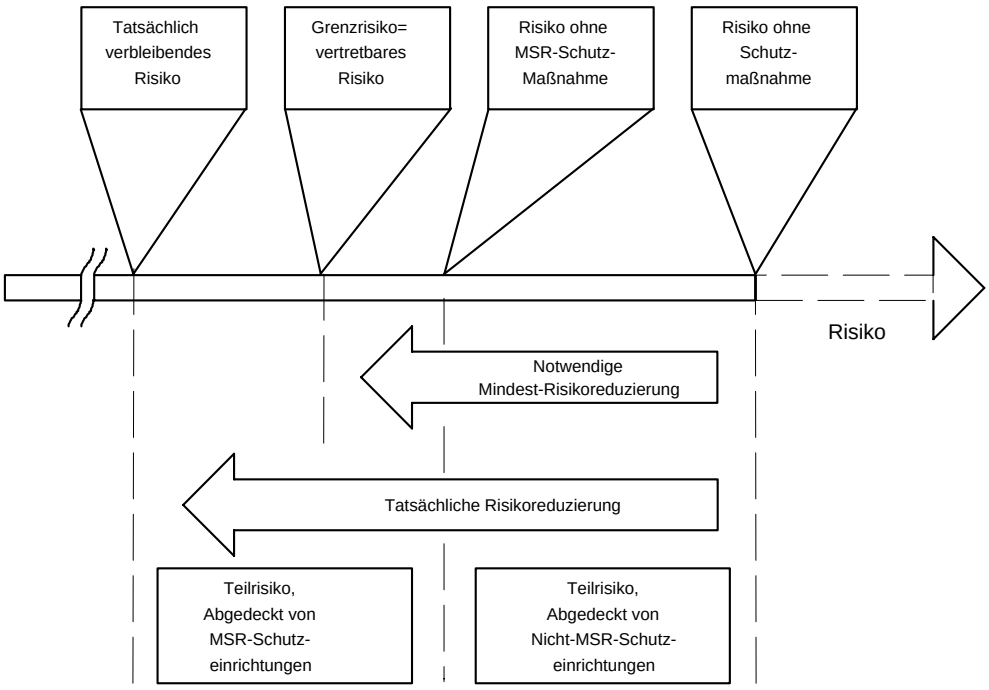

Abbildung 2-1 Risikoreduzierung nach DIN V 19250

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:

$$\mathbf{R = H \times S}$$

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

Um nun für eine Anwendung die sicherheitstechnischen Anforderungen zu erhalten, ist in der DIN V 19250 ein Risikograph zur Bestimmung der Anforderungsklassen vorgegeben. Die Abbildung 2-2 zeigt den Risikographen und den Bezug der einzelnen Risikoparameter zueinander.

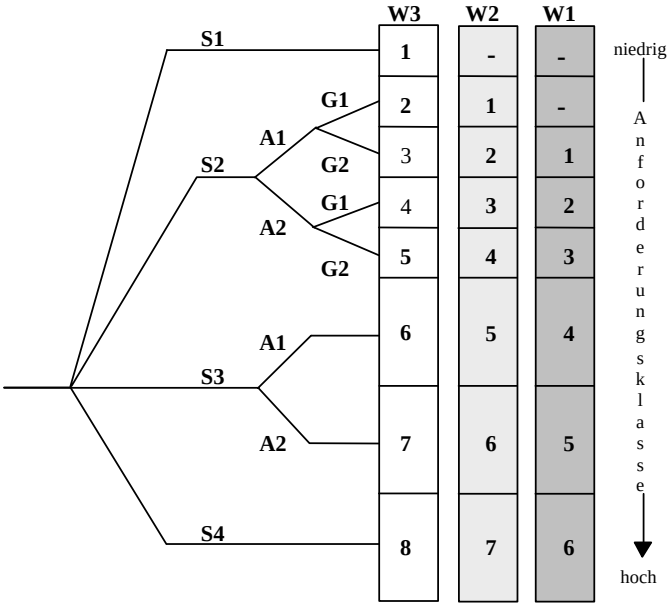

Abbildung 2-2 Risikograph und Anforderungsklassen nach DIN V 19250

Schadensausmaß S:

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

Eine so ermittelte Anforderungsklasse nach DIN V 19250 kann, wie in der nachfolgenden Tabelle gezeigt, in andere sicherheitstechnische Einstufungen der verschiedenen Normen und Richtlinien überführt werden.

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

Tabelle 2-1 Gegenüberstellung von Anforderungsklassen, Risikobereich und Safety Integrity Level

In der DIN V VDE 0801 wird ein Rechnersystem als Sicherheitssystem betrachtet, d. h. vom Eingang des Systems bis zu dessen Ausgang. Die weiteren Komponenten zur Anschaltung an die Anlage oder den Prozess (Feldinstrumentierung) werden in dieser Norm 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 2-3.

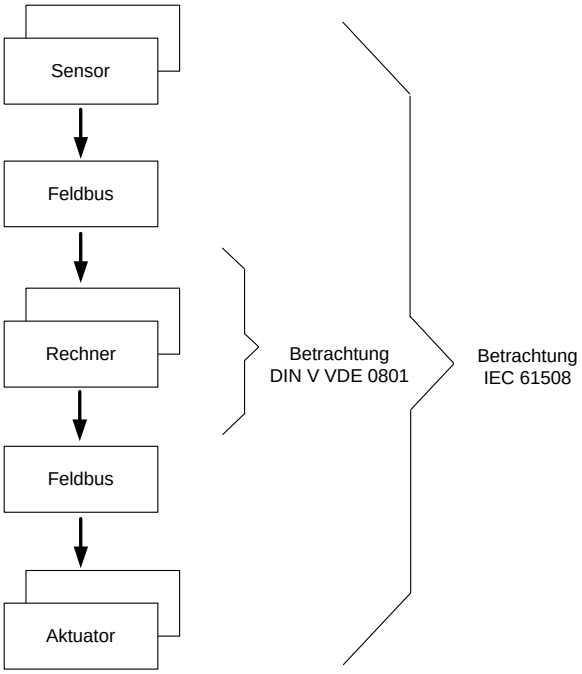

Abbildung 2-3 Vergleich der Sicherheitsbetrachtungen nach DIN V VDE 0801 und IEC 61508

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.

3 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 3-1 zeigt.

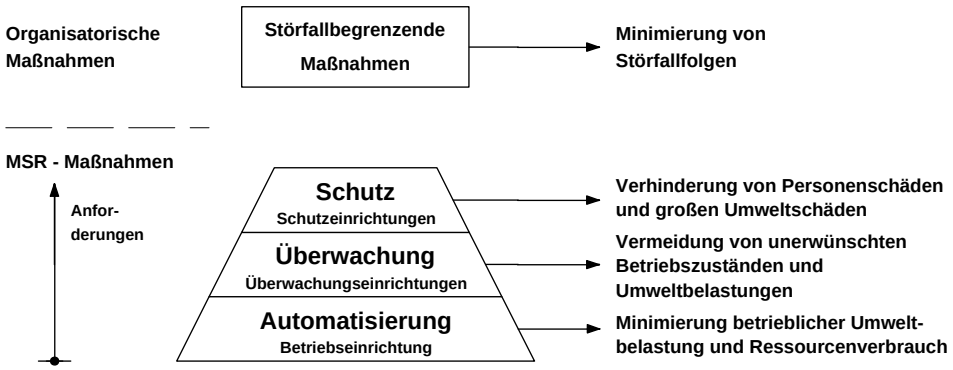

Abbildung 3-1 Hierarchisches Sicherheitskonzept

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 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.

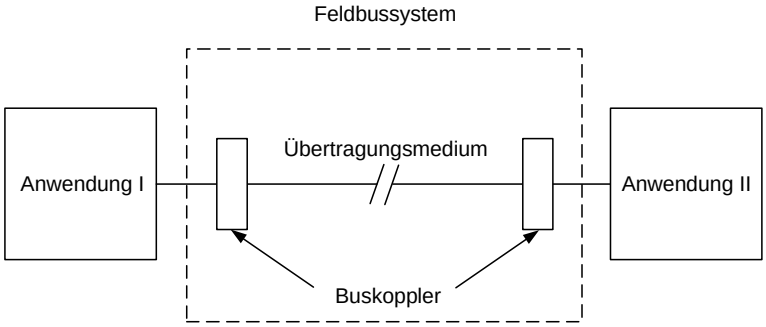

Abbildung 4-1 Vereinfachte Darstellung eines Feldbussystems

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.

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.
Auch die IEC 61511 „Functional Safety: Safety Instrumented Systems for the Process Industry“ Teil 1 lehnt sich an die IEC 61508 an.

Um eine Beurteilung gemäß IEC 61508 „Functional safety of electrical/electronic/programmable electronic safety- realted systems“ für ein Feldbussystem durchführen zu können, muss zuerst die Sicherheitsfunktion des Feldbusses im gesamten Sicherheitssystem eindeutig definiert werden.
Zur Aufrechterhaltung dieser Sicherheitsfunktion fordert die IEC 61508 abhängig vom geforderten SIL abgestufte **fehlerbeherrschende**, sowie **fehlervermeidende Maßnahmen.**

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 für das gesamte Schutzsystem nicht überschreiten.

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 $\leq 10^{-1}$

Tabelle 4-1 Versagenswahrscheinlichkeit, Systeme im Anforderungsmode

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 Forderungen gelten für das gesamte Sicherheitssystem und alle seine Komponenten und somit auch für ein in das Sicherheitssystem integriertes Feldbussystem.

4.1 Fehlerbeherrschende Maßnahmen

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.

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.

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.

4.2 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.
Der Anteil der PFD bei Feldbussystemen setzt sich zusammen aus der gefährlichen Versagenswahrscheinlichkeit aufgrund von Hardwareausfällen und gefährlichen Versagenswahrscheinlichkeit aufgrund von Übertragungsfehlern. Letzteres wird beschrieben durch die **Restfehlerwahrscheinlichkeit**.

4.3 Restfehlerwahrscheinlichkeit

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.

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

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

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

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].

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

mit

$$z = m_1 e^{-m_2}$$

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

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

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

Die folgende Abbildung 4-2 zeigt die Restfehlerwahrscheinlichkeit in Abhängigkeit von der Hamming-Distanz bei konstanter Telegrammlänge n = 80 Bits und einer angenommenen Bitfehlerrate von 10^{-3}.

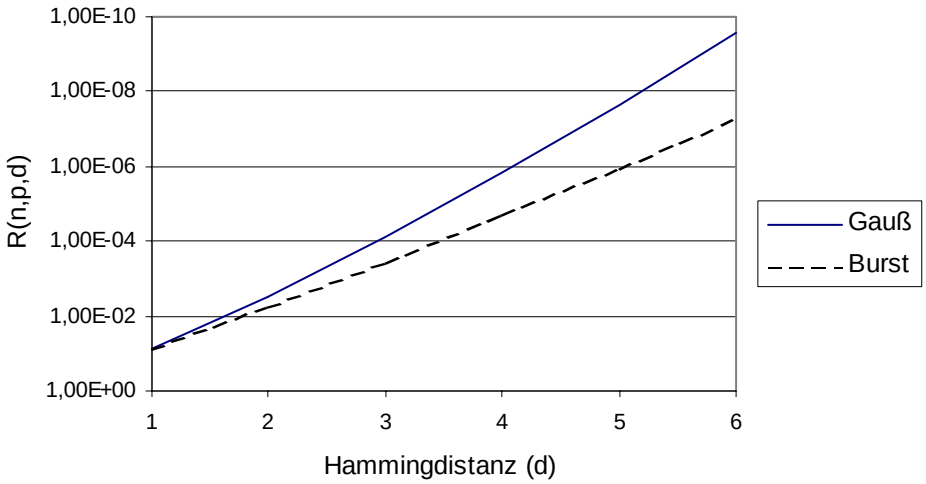

Abbildung 4-2 Restfehlerwahrscheinlichkeit in Abhängigkeit zur Hamming-Distanz

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

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.

4.4 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.

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.

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

und

$$\lambda = \lambda_D + \lambda_S$$

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

Gemäß der IEC 61508 wird der maximal erreichbare SIL eines Systems durch die Hardwarefehlertoleranz und die Safe Failure Fraction des Systems mitbestimmt.

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

Tabelle 4-2 Hardware safety integrity: architectural constraints on type B safety-related subsystems [IEC 61508]

4.5 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.

4.6 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.

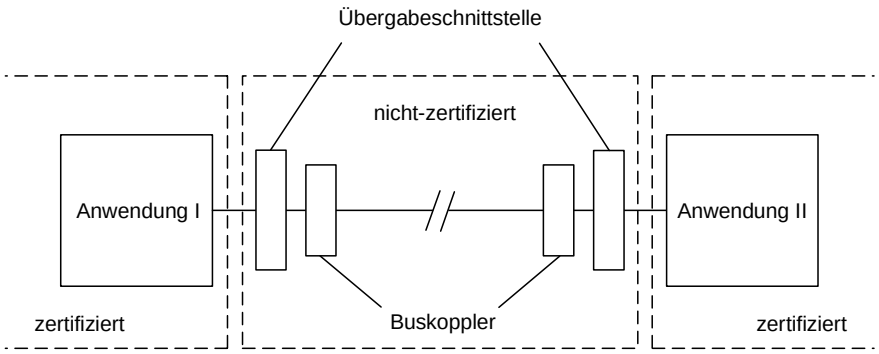

Abbildung 4-3 Nachrichtenfluss zwischen den Anwendungen

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.

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.

4.7 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.

Maßnahmen gegen Fehler bei der Datenübertragung können sein:

- Telegrammnummerierung
- Zeiterwartung
- Quittierung
- Datensicherung
- Eindeutige Adressierung
- Eindeutige Identifizierung von nicht-sicheren und sicheren Informationen
- Reduzierte Datengültigkeit
- Geeignete Busarchitektur (z. B. redundante Busstrukturen)

Nachfolgend soll beispielhaft die Maßnahme „Zeiterwartung“ etwas näher betrachtet werden.

Die Sicherheitsfunktion muss bei Anforderung innerhalb einer vordefinierten Reaktionszeit erfolgen und die Anlage in den sicheren Zustand überführen.

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 und somit die geforderte Reaktionszeit nicht garantiert werden kann.

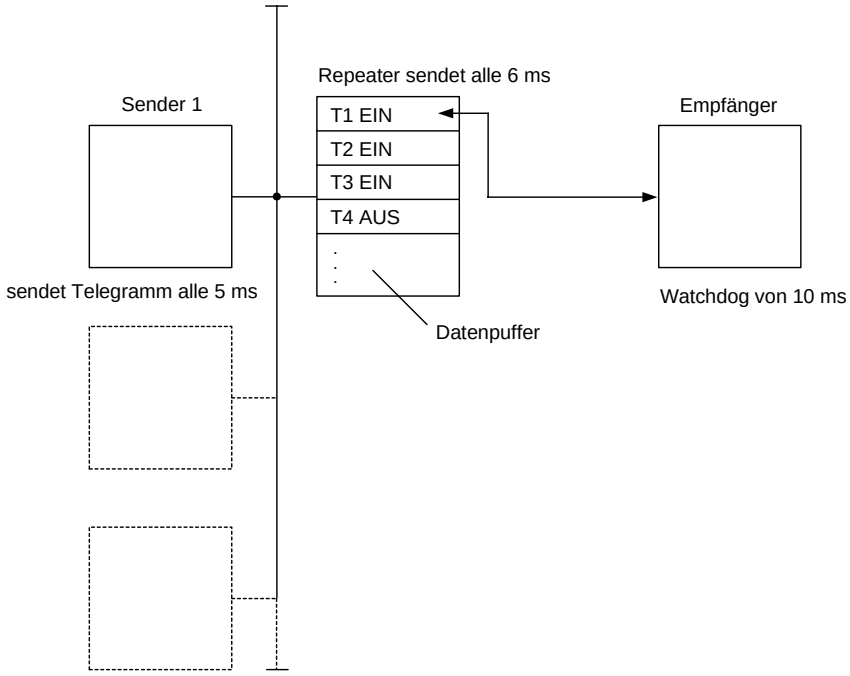

Abbildung 4-4 Problematik der Zeitverzögerungen durch Datenpuffer

Die Abbildung 4-4 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 in den meisten Fällen nicht aus.

5 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.

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 4-1) 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 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 in nicht allzu weiter Zukunft 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.

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