SCHLUSSENTWURF

Vorschlag eines Grundsatzes für die

Prüfung und Zertifizierung von

„Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten“

Auftrag durch:

Fachausschuss Elektrotechnik

Gustav-Heinemann-Ufer 130

50698 Köln

1 Allgemeines

1.1 Geltungsbereich

Dieser Grundsatz gilt für die Prüfung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten an Maschinen im Sinne der Maschinenrichtlinie. Die Kommunikation kann dabei zwischen verschiedenen verarbeitenden Einheiten einer Steuerung und/oder zwischen intelligenten Sensoren/Aktoren und verarbeitenden Einheiten einer Steuerung stattfinden.

Anmerkung: Derzeit werden nur gekapselte Bussysteme mit einer vom Hersteller definierten Anzahl und einem definierten Typ von Busteilnehmern betrachtet. Eine Öffnung des Systems für die Datenfernübertragung wird hier nicht betrachtet.

1.2 Funktionsbeschreibung

Ein Bussystem zur Übertragung sicherheitsrelevanter Nachrichten besteht neben den verarbeitenden Einheiten - als Quellen und Senken der Information - aus einer Übertragungsstrecke, die aus einem Übertragungsmedium (z. B. el. Leitungen, Lichtwellenleiter, Funkstrecke) und der Schnittstelle zwischen Nachrichtenquelle/-senke und Buselektronik (logische Protokollbausteine, Treiberstufen, etc.) besteht (siehe Abbildung 1).

1.3 Richtlinien, Vorschriften

Basis für diesen Grundsatz bilden:

Richtlinie des Rates vom 14. Juni 1989 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten für Maschinen (89/392/EWG).

EN 954-1	Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen
DIN V VDE 0801	Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben
DIN V VDE 0801/A1	Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben, Änderung A1
EN 60204-1	Elektrische Ausrüstung von Maschinen
DKE 226.0.3	Arbeitspapier Sicherheitsgerichtete Funktionen elektrischer Antriebssysteme in Maschinen
DIN IEC 61508	Funktionale Sicherheit. Sicherheitssysteme, Teile 1-7.

2 Begriffe

2.1 Bussystem:

Einrichtung zur Übertragung von Nachrichten zwischen verschiedenen Teilnehmern (Sendern und Empfängern).

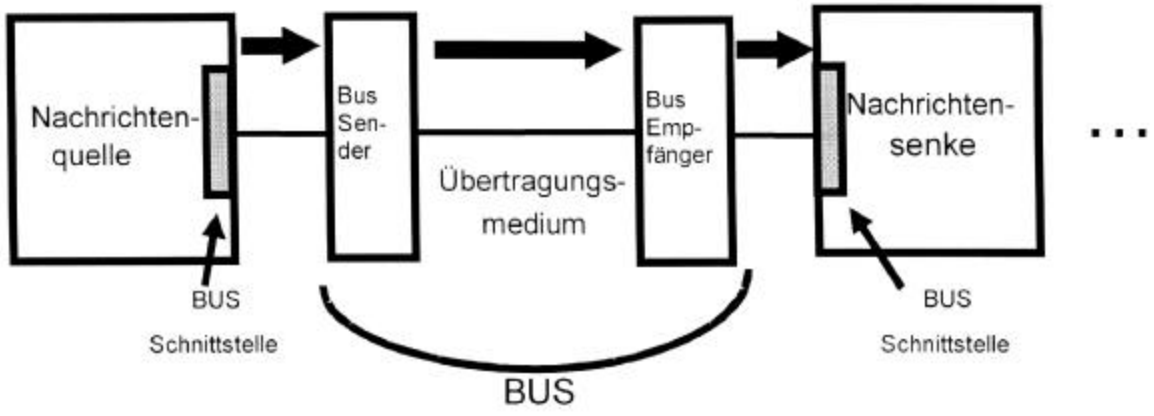


Abbildung 1: Einfaches Modell eines Bussystems

2.2 Gekapselte Bussysteme:

Eine feste Zahl oder eine festgelegte maximale Anzahl von Busteilnehmern, die durch ein Übertragungsmedium mit wohl definierten und festgelegten Eigenschaften verbunden sind, bilden ein gekapseltes Bussystem.

2.3 Modell für die Übertragung sicherheitsrelevanter Nachrichten (nach OSI)

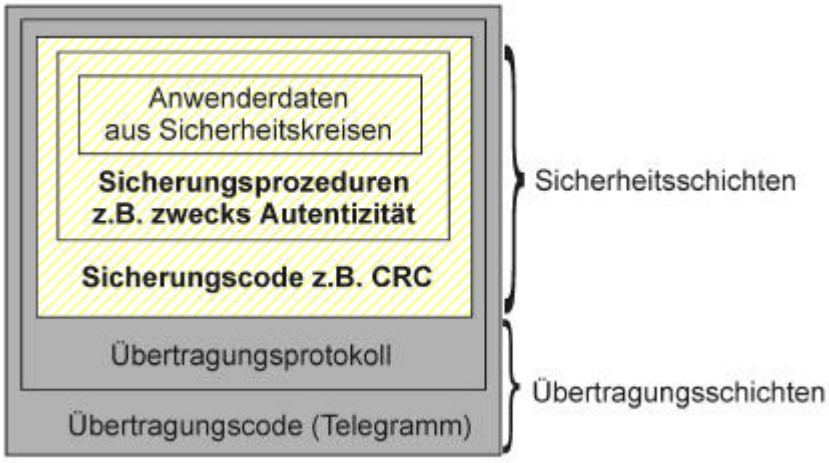


Abbildung 2: OSI-Modell für die Übertragung sicherheitsrelevanter Nachrichten.

Die Sicherheitsschichten beinhalten Sicherungsprozedur und Sicherungscode.

Die Übertragungsschichten beinhalten Übertragungsprotokoll und Übertragungscode.

2.4 Busarchitekturen

In diesem Grundsatz werden verschiedene Architekturen (Modell A bis Modell D) für Bussysteme betrachtet. Diese Modelle unterscheiden sich teilweise bezüglich ihrer Fehlertoleranz. Die wesentlichen Vor- und Nachteile werden diskutiert. Eine vollständige Betrachtung der sicherheitstechnischen Aspekte ist nicht Gegenstand dieses Papiers. Für die Ertüchtigung von Nachrichtenquellen und –senken sind die relevanten Normen aus Kap. 1.1 anzuwenden. In Kategorie 3 und 4 (gem. EN 954-1) sind die übergeordneten Busteilnehmer in der Regel zweikanalig aufgebaut, bei Abweichung sind die Anforderungen gemäß IEC 61508 vollständig zu erfüllen.

2.4.1 Modell A: Einkanaliges System:

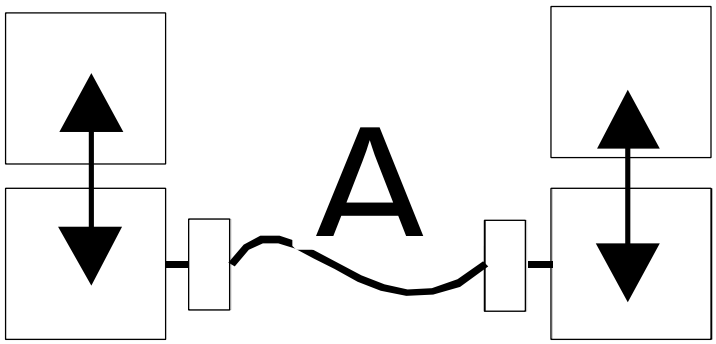


Abbildung 3: Architekturmodell A

Das in Abbildung 3 gezeigte System dient als Referenzmodell für die übrigen Modelle. Die Anbindung an das Bussystem ist einkanalig, die Nachrichten vom nicht am Bus angeschlossenen Kanal, werden abgesichert und an den angeschlossenen Kanal weitergeleitet.

2.4.2 Modell B:

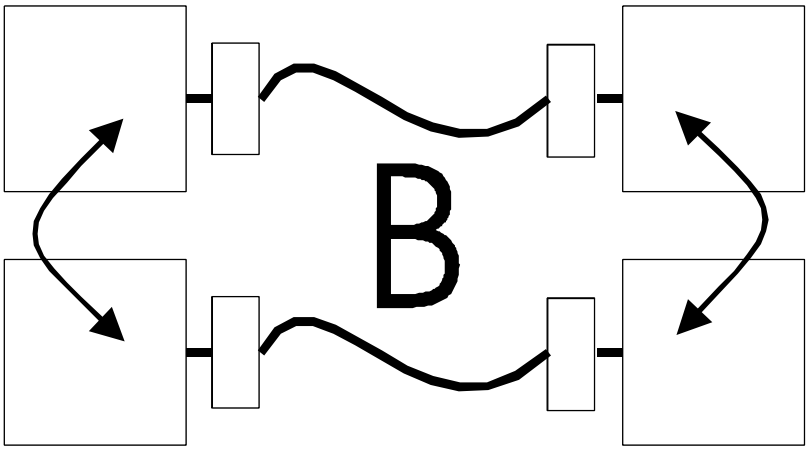


Abbildung 4: Architekturmodell B

Abbildung 4 beschreibt im Gegensatz zu Abbildung 3 ein redundantes System. Hierbei sind alle Sicherheitsschichten inkl. Übertragungsschichten zweifach ausgelegt.

2.4.3 Modell C

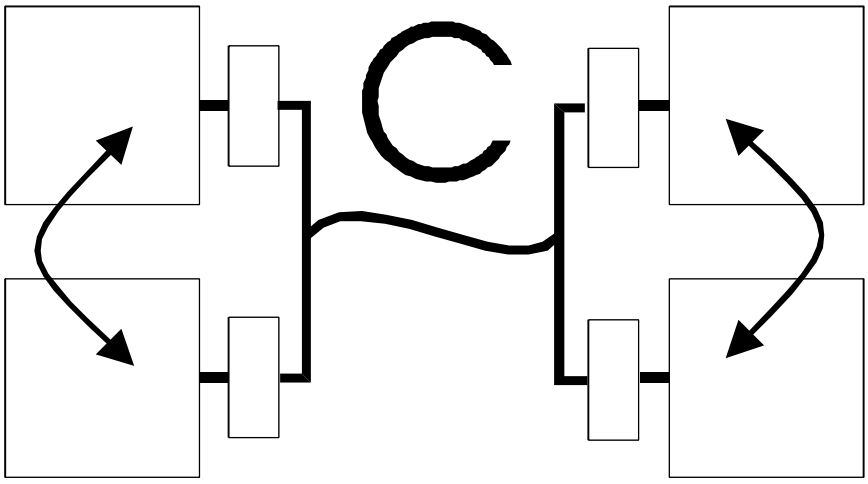


Abbildung 5: Architekturmodell C

Abbildung 5 beschreibt ein Modell, das dem Modell B entspricht, allerdings ist hier das Übertragungsmedium einkanalig.

2.4.4 Modell D:

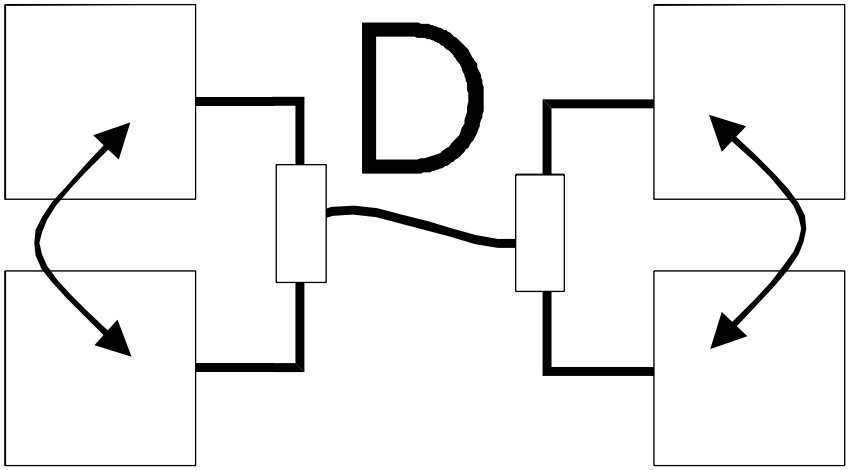


Abbildung 6: Architekturmodell D

Abbildung 6 zeigt ein System, bei dem Sicherheitsschichten zweikanalig existieren, während die Übertragungsschicht einkanalig vorhanden ist. Beide Sicherungsschichten haben unabhängig voneinander Zugriff auf die Übertragungsschicht. Dabei können die Daten entweder in einem Telegramm oder in zwei Telegrammen übermittelt werden.

2.5 Nachrichtenquelle (Nachrichtensender) und –senke (Nachrichtenempfänger):

Eine Nachrichtensenke ist der Empfänger einer sicherheitsrelevanten Nachricht.

Eine Nachrichtenquelle ist der Sender einer sicherheitsrelevanten Nachricht.

2.6 Nachricht:

Nachrichten bestehen aus Nutzdaten, Adressen, Daten zur Sicherung der Übertragung, etc.

2.7 Maximale Ausbaustufe:

Zahl der maximal am Nachrichtenaustausch beteiligten Sender und Empfänger.

2.8 Reaktionszeit:

Zeit vom „elektrischen“ Erkennen eines Gefahrenmoments bis zum „elektrischen“ Einleiten der Sicherheitsreaktion. Die Reaktionszeit setzt sich aus mehreren Einzelzeiten zusammen, u.a. den Busübertragungszeiten.

2.9 Übertragungsfehler:

2.9.1 Wiederholung:

Durch den Fehler eines Busteilnehmers werden alte, nicht aktuelle Nachrichten zur falschen Zeit wiederholt, so dass ein Empfänger gefährlich gestört wird.(z. B. Schutztür geschlossen obwohl bereits offen).

2.9.2 Verlust:

Durch den Fehler eines Busteilnehmers wird eine Nachricht gelöscht. (z. B. Anforderung „sicherer Betriebshalt“).

2.9.3 Einfügung:

Durch den Fehler eines Busteilnehmers werden Nachrichten eingefügt.

2.9.4 Falsche Abfolge

Durch den Fehler eines Busteilnehmers wird die Reihenfolge von Nachrichten verändert.

Beispiel: Vor Einleiten des sicheren Betriebshaltes soll die sicher reduzierte Geschwindigkeit angewählt werden. Bei Vertauschung dieser Nachrichten läuft die Maschine anstatt zu stehen.

Hinweis: Bussysteme können telegrammspeichernde Elemente enthalten (FIFO in Repeatern, Routern, etc.), welche die Abfolge verfälschen können.

2.9.5 Nachrichtenverfälschung:

Durch den Fehler eines Busteilnehmers oder durch Fehler auf dem Übertragungsmedium werden Nachrichten verfälscht.

2.9.6 Verzögerung:

1. Die Übertragungsstrecke ist durch den betriebsmäßigen Datenaustausch derart überlastet, dass die Sicherheitsfunktion verzögert oder verhindert wird.

2. Ein Busteilnehmer verursacht eine Überlastung der Übertragungsstrecke durch Vortäuschen falscher Nachrichten, so dass die Sicherheitsfunktion verzögert oder verhindert wird.

2.9.7 Kopplung sicherheitsrelevanter und nicht sicherheitsrelevanter Übertragungsfunktionen

Durch den Fehler eines Busteilnehmers werden sicherheitsrelevante und nicht sicherheitsrelevante Nachrichten vermischt.

3 Beschreibung von Maßnahmen zur Fehlerbeherrschung

Im folgenden Kapitel werden Maßnahmen aufgezählt die, der Fehlerbeherrschung von Übertragungsfehlern dienen.

3.1 Laufende Nummer

An jede Nachricht, die Sender und Empfänger austauschen, wird zusätzlich eine laufende Nummer angehängt. Diese laufende Nummer kann als ein zusätzliches Datenfeld definiert werden, das eine Zahl enthält, die sich in vordefinierter Art und Weise von Nachricht zu Nachricht ändert.

3.2 Zeitmarke

Der Inhalt einer Nachricht ist in der Regel nur zu einer bestimmten Zeit gültig. Die Zeitmarke ist z. B. ein Datum die einer Nachricht vom Sender angehängt wird. Man unterscheidet zwischen relativen Zeitmarken, absoluten Zeitmarken und „doppelten Zeitmarken“:

3.2.1 Relative Zeitmarke

Eine relative Zeitmarke ist eine Zeitmarke, die auf die lokale Uhr einer Komponente bezogen wird. In der Regel besteht keine Beziehung zwischen Zeitmarken verschiedener Komponenten.

3.2.2 Absolute Zeitmarke

Eine absolute Zeitmarke wird von einer globalen Zeit, auf die sich eine Gruppe von Komponenten bezieht, abgeleitet.

3.2.3 Doppelte Zeitmarke

Eine „doppelte Zeitmarke“ ist gegeben wenn zwei Teilnehmer ihre Zeitmarken austauschen und vergleichen. In diesem Fall sind die Zeitmarken der einzelnen Teilnehmer unabhängig voneinander.

3.3 Zeiterwartung (Time Out)

Bei einer Übertragung überprüft der Empfänger, ob die Verzögerung zwischen zwei Nachrichten einen vorgegebenen Wert überschreitet. Ist dies der Fall, muß ein Fehler angenommen werden.

Beispiel, zeitschlitzorientiertes Zugriffsverfahren:

Der Austausch von Nachrichten findet in festen Zyklen mit festgelegten Sendezeitschlitzen für jeden Teilnehmer statt.

Option: Jeder Teilnehmer muss in seinem Sendezeitschlitz seine Daten senden, auch wenn sie sich nicht geändert haben (dies ist ein Beispiel der zyklischen Kommunikation).

Zur Erkennung, ob ein Teilnehmer nicht im vereinbarten Zeitschlitz sendet wird zusätzlich eine Senderkennung eingeführt.

3.4 Empfangsbestätigung

Die Senke einer Nachricht sendet eine Nachricht über den **Inhalt** und den Erhalt der ursprünglichen Nachricht an die Quelle zurück. Die Empfangsbestätigung kann beispielsweise die Daten wiederholen, um dem Sender die Überprüfung des richtigen Empfangs zu ermöglichen.

Anmerkung: Bei verschiedenen Bussystemen werden die Begriffe Empfangsbestätigung, Echo und Quittung synonym verwendet.

3.5 Kennung für Sender und Empfänger

Nachrichten können eine einheitliche Senderkennung und/oder eine einheitliche Empfängerkennung beinhalten, die die logische Adresse der sicherheitsrelevanten Teilnehmer beschreibt (Authentizität).

3.6 Datensicherung

Die Datensicherung ist ein wesentlicher Bestandteil zum Erreichen eines gewünschten Sicherheitsniveaus. Aufgrund unterschiedlicher Strukturen und unterschiedlicher Ansätze werden in diesem Kapitel die wesentlichen Methoden für die jeweilige Kategorie (gem. EN 954-1) vorgestellt. Dabei kann der Hersteller zwischen verschiedenen Rechnungsmethoden wählen, die alle Abschätzungen für die Datenintegrität von Bussystemen angeben. Die aus den Methoden resultierenden Zahlen ergeben je nach Wahl entweder mehr Aufwand in der Gestaltung der Hard- und Software oder mehr Aufwand bei der Berechnung und des Nachweises der Zuverlässigkeit des gesamten Steuerungssystems. Abweichend von der EN 954-1 muß allerdings hier mit den Ausfallwahrscheinlichkeiten eines Steuerungssystems

gerechnet werden. Verschiedene pragmatische Ansätze werden diskutiert, die alle zur gewünschten Kategorie (gem. EN 954-1) bzw. zum gewünschten Sicherheits-Integritätslevel (gem. IEC 61508) führen können.

3.6.1 Datensicherung für Modell A und D, bei denen die Datensicherungsmechanismen der Übertragungsschicht nicht berücksichtigt werden

3.6.1.1 Allgemeines

In diesem Ansatz wird beschrieben, wie ohne hohen mathematischen Aufwand die Übertragung sicherheitsrelevanter Nachrichten bewerkstelligt werden kann.

3.6.1.2 Restfehlerwahrscheinlichkeit, Restfehlerrate

Alle Maßnahmen zur Datensicherung müssen in den übergeordneten Steuerungsteilen, die in der gewünschten Kategorie ausgeführt sind, erfolgen. Die Restfehlerrate berechnet sich aus der Restfehlerwahrscheinlichkeit des übergeordneten sicheren Datensicherungsmechanismus und der Übertragungsrate der sicherheitsrelevanten Nachrichten. Für die Restfehlerwahrscheinlichkeit gilt („worst case“):

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

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

n = Nachrichtenlänge, p = Bitfehlerwahrscheinlichkeit, d =Hammingdistanz des in der Steuerung realisierten Datensicherungsmechanismus.

Anmerkung: Wenn nicht anders nachgewiesen muss für die Bitfehlerwahrscheinlichkeit $p=10^{-2}$ angenommen werden. Bei manchen kommerziellen Bussystemen kann ein Fehlerzähler von der übergeordneten Steuerung sicher ausgewertet werden, der im Falle der Überschreitung eines Wertes, der einem zugrunde gelegten p entspricht, den sicheren Zustand einleitet. In diesem Falle kann auch ein geringeres p angenommen werden.

Um die aus R(p) resultierenden Fehler pro Zeit zu berechnen kann muss der folgenden Ansatz gewählt werden:

$\Lambda = 3600\ R(p)\nu(m-1)*100$ [Übertragungsfehler/Stunde]

mit

n = Anzahl der sicherheitsrelevanter Nachrichten/s,

R(p) siehe oben,

(m-1) ist die worst case Zahl der Übertragungen bei m Teilnehmern,

der Faktor **100** besagt, dass die Übertragung nur zu 1% zur Sicherheitsfunktion beiträgt.

Neben der Ertüchtigung der Hardware in der entsprechenden Kategorie geht hier nunmehr die **Zahl m der an einer Sicherheitsfunktion beteiligten Teilnehmer** in die Bewertung der Sicherheit (Kategorie bzw. SIL) ein. Da ein Bussystem frei projektierbar ist muss hier die maximale Ausbaustufe des Sicherheitsbussystems angenommen werden.

Für die Kategorie 4 (SIL 3) muss $\Lambda < 10^{-7}$ sein.

Für die Kategorie 3 (SIL 2) muss $\Lambda < 10^{-6}$ sein.

Für die Kategorie 2 (SIL 1) muss $\Lambda < 10^{-5}$ sein.

Beispiel für Kategorie 3 (SIL 2):

m=32, $R=10^{-16}$, ν=100/s => $\Lambda=1{,}1\ 10^{-7} < 10^{-6}$

In diesem Beispiel muss R durch die Sicherheitsschichten erreicht werden.

3.6.2 Datensicherung für Modell B und C, bei denen der einzelne Kanal der Übertragungsschichten als nicht sicher betrachtet wird.

In diesem Ansatz wird, vergleichbar zu Kap. 3.6.1 der einzelne Kanal des kommerziellen Bussystems als nicht sicher betrachtet. Die Zuverlässigkeit in der Datenübertragung wird durch hoch zuverlässige kommerzielle Bussysteme erreicht, die durch die Zweikanaligkeit auch fehlertolerant arbeiten. Hierbei wird die Datensicherung des kommerziellen Bussystems vollständig genutzt. Allerdings ist eine Fehlererkennung bei Ausfall des Datensicherungsmechanismus nur eines Kanals nicht notwendigerweise möglich. Dies ist zum Erreichen der Kategorie 4 gem. EN 954-1 nicht zulässig, gem. Kategorie 3 aber möglich. Deshalb sind solche Fehler durch entsprechende Maßnahmen bis zu einer Fehlertiefe von 3 in der Kategorie 4 notwendig. Einige Bussysteme garantieren allerdings aufgrund Ihrer Struktur (z.B. der CAN-Bus oder Interbus), dass andere Teilnehmer jede Nachricht mit überprüfen, so dass hier wiederum die Fehleranhäufung beherrscht werden kann.

Der hier vorgestellte Ansatz basiert auf der in Kap. 3.7 beschriebenen Redundanz mit Kreuzvergleich. Bei dieser Redundanz werden außerdem Nachrichten zweifach versendet und über einen Vergleicher auf Konsistenz geprüft. Dies bedeutet, dass ein Versgagen der Übertragung nur bei gleichartigem Übertragungsfehlern in der jeweiligen Partnernachricht möglich ist. Die Wahrscheinlichkeit, dass eine Nachricht gefälscht wird ist durch die maximale Restfehlerwahrscheinlichkeit R(p) des kommerziellen Bussystems bestimmt. Bei zwei Nachrichten ist somit das zusammengesetzte $R(p)_{BC}$ gleich dem Quadrat der einzelnen Restfehlerwahrscheinlichkeiten:

$$\mathbf{R(p)_{BC} = R(p)^2.}$$

Die Berechnung von L erfolgt analog zu Kap. 3.6.1.2 allerdings muss hier statt R(p) der Wert $\mathbf{R(p)_{BC} = R(p)^2}$ eingesetzt werden.

Für die Kategorie 4 (SIL 3) muss $\Lambda < 10^{-7}$ sein.

Für die Kategorie 3 (SIL 2) muss $\Lambda < 10^{-6}$ sein.

Für die Kategorie 2 (SIL 1) muss $\Lambda < 10^{-5}$ sein.

3.6.3 Datensicherung für Modell A und D, bei die Übertragungsschichten einen Anteil zur Sicherheit haben

Hier wird auf die Datenübertragungsqualität des kommerziellen Bussystems aufgebaut und der Rest, der evtl. zum Erreichen der gewünschten Kategorie bzw. SIL noch fehlt, in der übergeordneten Steuerung realisiert.

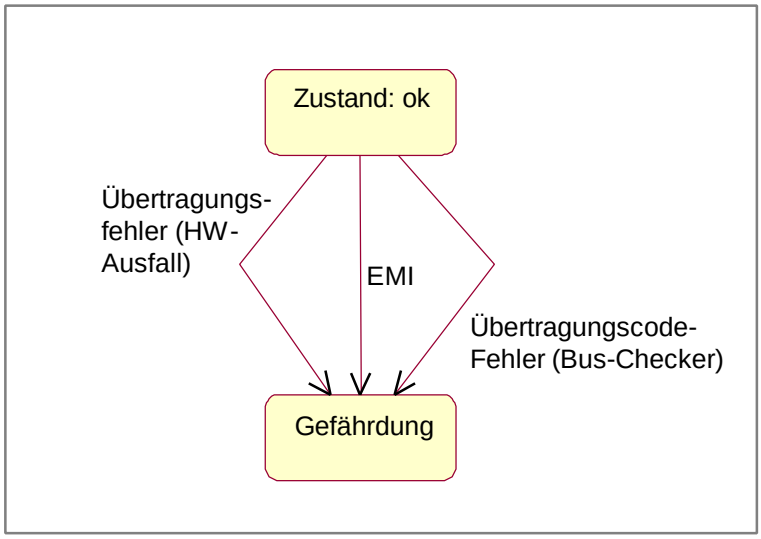


Abbildung 7: Vereinfachtes Markov-Modell

Da in diesem Ansatz die Hardwarefehlertoleranz der Busprotokollbausteine mitberücksichtigt werden muss, da bei Ausfall eines Busprotokollbausteins die Sicherheit gefährdet wird, muss die Lebensdauer der Busprotokollbausteine mit berücksichtigt werden.

Eine ausführliche Markov-Analyse dieses Modells kann gemäß EN50159-1 auf drei wesentliche Übergangswahrscheinlichkeiten (siehe Abbildung 7) zurückgeführt werden:

1. Die Hardware der Übertragungsschichten versagt, so dass die Telegramme verfälscht werden.

2. Bitverfälschungen aufgrund von elektromagnetischen Einflüssen (EMI) treten auf, die von der Übertragungseinrichtung nicht erkannt werden.

3. Jegliche verfälschte Nachricht wird von der Übertragungseinrichtung an die Sicherungseinrichtung weitergereicht, weil ausschließlich der entsprechende Teil (Bus-Checker) ausgefallen ist.

Die Restfehlerrate des Systems ist somit die Summe aller Einzelraten multipliziert mit dem Faktor 100 (1%-Regel):

$$\Lambda = 100 \cdot (R_{HW} + R_{EMI} + R_{TC})$$

Die einzelnen Terme werden wie folgt berechnet:

$$R_{HW}(Hardwarefehler) = (x1 \cdot \ l_{HWF} + x2 \cdot \ l_{HWS}) \cdot P_{US}$$

wobei

λ_{HWF} die Summe der Hardwareausfallwahrscheinlichkeiten der beiden gerade kommunizierenden sicherheitsrelevanten Teilnehmer,

λ_{HWS} die Summe der aller restlichen gerade nicht kommunizierenden sicherheitsrelevanten Teilnehmer,

x1 der Anteil der gefährlichen Fehler in den beteiligten Komponenten mit $0 < x1 \leq 1$,

x2 der Anteil der gefährlichen Fehler in den nicht beteiligten Komponenten
mit $0 < x2 \leq 1$

P_{US} die maximale Restfehlerwahrscheinlichkeit des übergeordneten (zusätzlich erforderlichen) Datensicherungsmechanismus

ist.

$$R_{EMI}(EMI - Einwirkung) = f_W \cdot P_{UB} \cdot P_{US}$$

wobei

f_W die Häufigkeit von verfälschten Nachrichten auf dem Übertragungssystem,

P_{UB} die Restfehlerwahrscheinlichkeit des kommerziellen Bussystems,

P_{US} die maximale Restfehlerwahrscheinlichkeit des übergeordneten (zusätzlich erforderlichen) Datensicherungsmechanismus

ist.

Dieser Term gilt laut EN50159-1 dann, wenn Sicherheitscode und der Übertragungscode unabhängig sind. Dies kann z.B. durch Simulation nachgewiesen oder durch Grenzwertabschätzungen mathematisch gefasst werden.

Weiterhin ist laut EN50159-1 die „Properness“ des CRC-Polynoms nachzuweisen. Hierzu müssen Berechnungen von Restfehlerraten als Funktion von Bitfehlerraten für ein gegebenes Polynom durchgeführt werden. Als „proper“ wird ein Polynom eingeschätzt, wenn sich bei steigender Bitfehlerrate keine ausgeprägte Höckerkurve ergibt, d.h. wenn sie monoton ansteigt.

Der dritte Term bezieht sich auf mögliche Ausfälle der Sicherungseinrichtungen in der Übertragungsschicht.

$$R_{TC}(Übertragungscodefehler) = P_{US} \cdot k \cdot 1/T$$

wobei

k der Bruchteil der Hardwareausfälle des Busprotokollbausteins, bei denen der Datensicherungsmechanismus versagt,

T die Zeitspanne, in der eine wohldefinierte maximale Zahl von verfälschten Nachrichten auf dem Übertragungssystem nicht überschritten werden darf, ohne dass das System in den sicheren Zustand übergeht,

ist.

Für die Kategorie 4 (SIL 3) muss $\Lambda < 10^{-7}$ sein.

Für die Kategorie 3 (SIL 2) muss $\Lambda < 10^{-6}$ sein.

Für die Kategorie 2 (SIL 1) muss $\Lambda < 10^{-5}$ sein.

3.7 Redundanz mit Kreuzvergleich

Hier werden Sender und Empfänger vollständig zweikanalig ausgelegt Modell B und Modell C. Die Nachrichten werden zweifach und unabhängig voneinander gesendet Zusätzlich werden über den Bus oder eine separate Verbindung innerhalb der zweikanaligen Sender/Empfängereinheit die gesendeten Nachrichten kreuzweise auf ihre Richtigkeit überprüft. Bei Abweichung muss ein Fehler in der Übertragung, der verarbeitenden Einheit des Senders, oder der verarbeitenden Einheit des Empfängers vorliegen. Bei zweikanaligen Medien muss ein Fehler gemeinsamer Ursache durch geeignete Maßnahmen (z.B. Diversität, zeitversetzte Nachrichten) beherrscht werden.

3.8 Unterschiedliche Datensicherung für sicherheitsrelevante (SI) - und nicht - sicherheitsrelevante Daten (NSI)

Werden über das Bussystem sicherheitsrelevante (SI) - und nicht - sicherheitsrelevante Daten (NSI) versendet, können unterschiedliche Datensicherungen oder Kodierungen eingesetzt werden (verschiedene CRC - Algorithmen, unterschiedliches Generatorpolynom), damit NSI - Nachrichten nicht Sicherheitsfunktionen auf SI - Empfängern auslösen können.

Anmerkung: Unterschiedliche Datensicherung kann auch bedeuten, dass NSI-Busteilnehmer keine zusätzliche Datensicherung besitzen.

4 Anforderungen

4.1 Maßnahmen zur Beherrschung von Übertragungsfehlern

4.1.1

Nachrichten, die sicher übertragen werden sollen müssen sicher (entsprechend der geforderten Steuerungskategorie gem. EN 954-1) erzeugt werden. Das Übertragungsmedium (z. B. Busleitung einschließlich Schnittstellen - ASICs) selbst wird dabei nicht als sicher angesehen. Die Sicherungsmechanismen obliegen alleinig den verarbeitenden Einheiten von Nachrichtenquelle und -senke.

4.1.2

Es muss grundsätzlich eine Zeiterwartung vorgesehen werden (Ruhestromprinzip).

4.1.3

Es muss ein Mechanismus zur Fehlererkennung und Fehlerreaktion am Empfänger vorgesehen werden, der die Aufgabe hat sicherheitsgerichtete Reaktionen innerhalb der Fehlertoleranzzeit einzuleiten.

4.1.4

Bei Übertragungsfehlern gem. Kap. 2.9 muss eine definierte Fehlerreaktion erfolgen (z. B. Stoppanforderung).

4.1.5

Die vom Hersteller spezifizierte maximale Reaktionszeit pro Sicherheitskreis und die Zeit bis zum Einleiten der sicherheitsgerichteten Reaktion dürfen auch im Fehlerfall nicht überschritten werden. muss auch im Fehlerfall eingehalten werden.

Anmerkung: Bei verschiedenen Bussystemen ist die Übertragungsrate und die Reaktionszeit von der Zahl der Teilnehmer abhängig. Insofern sei auf diese Abhängigkeit hingewiesen, bzw. ist bei Sicherheitsrelevanz von Übertragungsrate und Reaktionszeit die Zahl der Teilnehmer einzuschränken.

4.1.6

Für die Übertragung sicherheitsrelevanter Nachrichten über Bussysteme muss ein Maßnahmenpaket aus den in Kap. 3 genannten Maßnahmen zusammengestellt werden, so dass jeder in Kap. 2 beschriebene Fehler innerhalb der Fehlertoleranzzeit aufgedeckt wird. Tabelle 4 gibt eine Hilfe zur Auswahl der Einzelmaßnahmen.

4.1.7

Die Rückwirkungsfreiheit von nicht sicherheitsrelevanten Busteilnehmern auf sicherheitsrelevante muss nachgewiesen werden.

5 Umweltprüfungen und allgemeine Anforderungen

Die nachfolgend aufgeführten Bauartanforderungen und Prüfungen sind Mindestanforderungen an ein Sicherheitsbussystem einschließlich aller dazugehörigen Komponenten. Wenn ein Bussystem funktionaler Bestandteil eines sicherheitsrelevanten Produktes ist (z.B. BWS, Zweihandschaltung, Näherungsschalter) sind die Anforderungen der einschlägigen Produktnormen zu erfüllen.

5.1 Einsatzbereiche

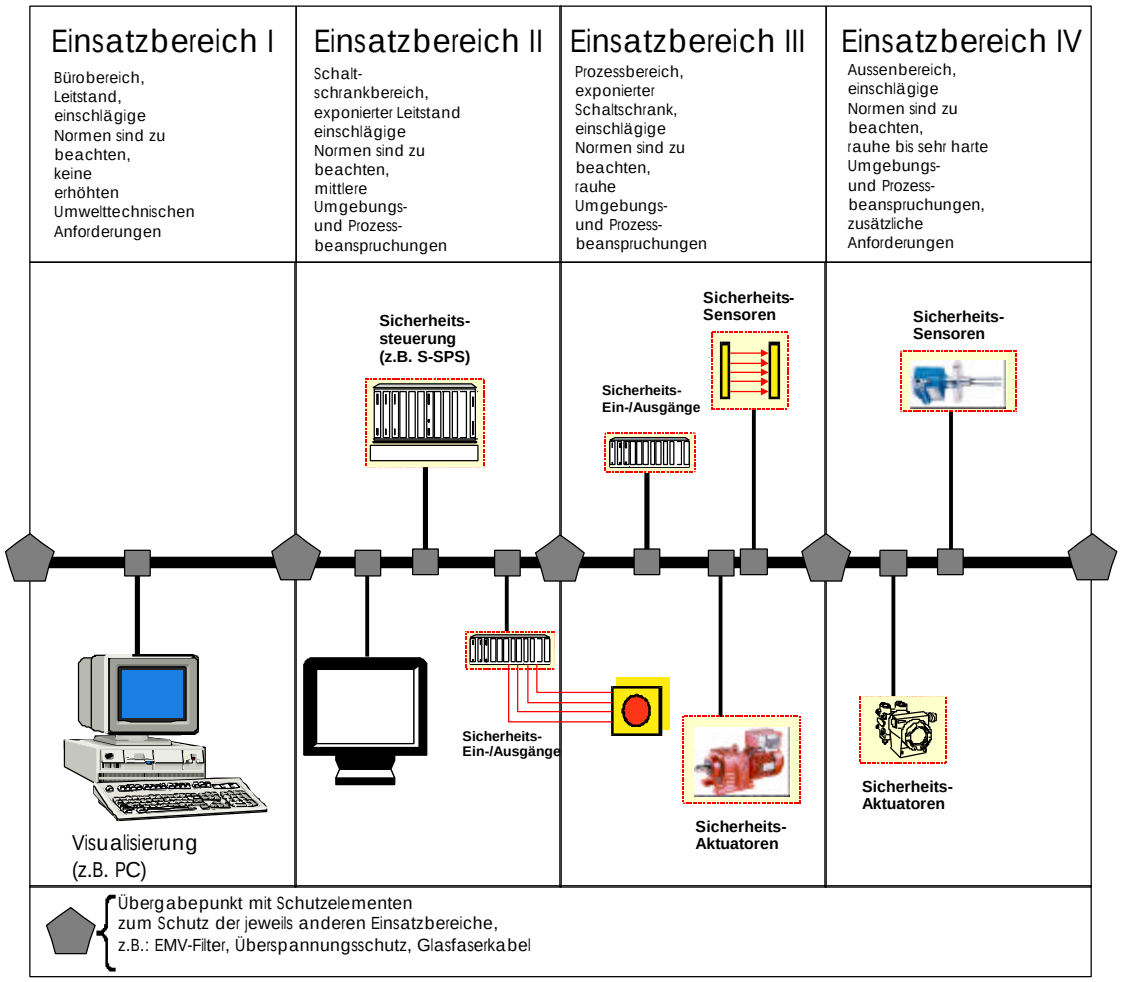


Abbildung 8: Beschreibung von Einsatzbereichen

In Abbildung 8 werden Einsatzbereiche dargestellt die als grobe Orientierungshilfe dienen sollen, um die erforderlichen umwelttechnischen Prüfungen durchzuführen. Hierbei ist zu beachten, dass es sich nur um Vereinfachungen handelt. Die korrekte Wahl umwelttechnischer Schärfegrade ist vom Verwendungszweck abhängig. Die für den jeweiligen Einsatzbereich notwendige korrekte Auswahl ist bei der Projektierung vorzunehmen. Dabei sind die tatsächlich zu erwartenden Umgebungs- und Prozessbeanspruchungen über eine Risikoanalyse zu ermitteln und zu beachten. Die Begleitdokumentation des Prüflings muss die genauen Einsatzbedingungen spezifizieren. Hiervon darf unter keinen Umständen abgewichen werden.

Es wird zwischen 4 Einsatzbereichen, die über die Anforderungen zur umwelttechnischen Ertüchtigung definiert sind, unterschieden:

1. Einsatzbereich I: Keine erhöhten Anforderungen.

2. Einsatzbereich II: Mittlere umwelttechnische oder betriebsbedingte Einflüsse sind zu erwarten, der Montageort (z. B. der elektrische Einbauraum) schütz die Installation vor starken Einflüssen (z.B. schwingungsgedämpfter Aufstellungsort des Schaltschrankes).
   Anmerkung: Es ist zu beachten, dass Schaltschränke auch an exponierten Orten aufgestellt sein können und damit in Einsatzbereichen III oder IV vorkommen können (z.B.: Schaltschränke an Pressen, die direkt mit dem Maschinenkörper verbunden werden).

3. Einsatzbereich III: Es wird von rauhen umwelttechnischen oder betriebsbedingten Einflüssen ausgegangen. Dies ist besonders für prozessnahe Installationen von Sensoren und Aktoren der Fall. Auch exponierte elektrische Einbauräume fallen unter diesen Einsatzbereich.

4. Einsatzbereich IV: Es handelt sich um den Außenbereich. Hier sind neben dem Einsatzbereich III zusätzliche oder härtere Anforderungen (z.B. Blitzschutz, Versprödung durch UV-Strahlen, Extremtemperaturen, schnelle Klimawechsel) zu beachten. Das vorliegende Papier befasst sich nicht mit Einsatzbereich IV. Einschlägige Bestimmungen und Normen sind unbedingt zu beachten.

Sofern in den hier geforderten Umweltprüfungen kein Einsatzbereich genannt ist, gilt die Prüfung sowohl für Einsatzbereich II, als auch für Einsatzbereich III.

5.2 Bewertungskriterien

Es sind die folgenden Bewertungskriterien festgelegt:

Bewertungskriterium	Beschreibung
A	Das Bussystem muss während und nach der Störbeinflussung weiterhin bestimmungsgemäß arbeiten.
B	Das Bussystem muss nach der Störbeinflussung bestimmungsgemäß arbeiten. Bei Überschreiten der Time-Out-Zeit aufgrund der Störbeeinflussung müssen die sicherheitsrelevanten Teilnehmer den sicheren Zustand einleiten. Das Wiederanlaufen ist anwendungsabhängig automatisch, oder durch explizite Freigabe zu realisieren. Die Buskommunikation wird nach Störbeeinflussung automatisch wieder aufgenommen. Anmerkung: Für Time-Out-Zeit vgl. Kap. 3.3
C	Die sicherheitsrelevanten Teilnehmer leiten den sicheren Zustand ein. Die Kommunikation ist ausgefallen. Alle sicherheitsrelevanten Teilnehmer verbleiben während und nach der Störbeeinflussung im sicheren Zustand. Die Wiederherstellung des bestimmungsgemäßen Betriebes erfolgt durch Einstell-/Bedienelemente (z.B. Netzaus/Netzein).

Tabelle 1: Bewertungskriterien für umwelttechnische Prüfungen

5.3 Prüfaufbau

Soweit durchführbar, müssen alle Teile eines Sicherheitsbussystems zusammen geprüft werden. Wo dies nicht durchführbar ist, dürfen Teile des Sicherheitsbussystem getrennt geprüft werden, insbesondere sind in diesem Falle Referenzsysteme bzw. Simulatoren festzulegen und bereitzustellen.

Es ist ein Prüfaufbau zu wählen, der die Worst-Case Bedingungen, z.B. aufgrund unterschiedlicher Bus-Topologien berücksichtigt. Die für die Sicherheitsfunktion notwendigen Signale sind in solchen Simulationen nachzubilden.

5.4 Allgemeine Prüfbedingungen

Während der Durchführung der Prüfungen muss das Prüfmuster unter den, in den Begleitunterlagen festgelegten Betriebsbedingungen betrieben werden.

Stromversorgungen und Umgebung	Prüfbedingungen
Netz	Bemessungsspannung und –frequenz
Temperatur	Raumtemperatur 20 ±5 °C
Relative Luftfeuchte	25 % bis 75 %
Luftdruck	86 kPa bis 106 kPa

Tabelle 2: Allgemeine Prüfbedingungen

Die Prüfungen sollen sicherstellen, dass das Sicherheitsbussystem den festgelegten technischen Daten entspricht. Zu Beginn jeder Prüffolge ist die einwandfreie Funktion des Prüflings festzustellen. Ziel der Prüfung ist es nachzuweisen, dass sich der Prüfling bei allen Messungen entsprechend seiner sicherheitsrelevanten Spezifikation verhält.

Die Prüfkriterien sind u.a.:

- Betrieb des Prüflings wie in den technischen Daten vorgesehen;
- keine Zerstörung eines Bauelementes des Prüflings;
- kein fehlerhaftes oder unbeabsichtigtes Verhalten des Prüflings;
- kein Anzeichen einer Überhitzung von Bauelementen;
- kein aktives Teil, welches bestimmungsgemäß berührungsgefährliche Spannung führt, darf berührbar werden;
- keine Gehäusebeschädigungen.
- Die Messabweichungen dürfen folgende Werte nicht überschreiten:
- für Messungen der Reaktionszeit: ±1 ms;
- für Temperaturmessungen: ±3° C;
- für elektrische Messungen: ±1 %, wo es technisch möglich und/oder sinnvoll ist;
- für Messungen der relativen Luftfeuchte (RH): ±3 % RH.

Alle Messungen müssen durchgeführt werden, nachdem konstante Temperaturbedingungen erreicht worden sind. Es ist davon auszugehen, dass dies erreicht ist, wenn der Anstieg oder Rückgang der Temperatur kleiner als 2 K/ h ist.

5.5 Benutzerinformation

Den Prüflingen ist eine Benutzerinformation beizulegen, die einen ordnungsgemäßen Anschluss und die Inbetriebnahme ermöglicht. Diese Betriebsanleitung muss, soweit zutreffend, mindestens enthalten:

a) Bestimmungsgemäße Verwendung

b) Name des Herstellers (Handelsname, Ursprungszeichen)

c) Typbezeichnung oder Seriennummer

d) Bemessungsbetriebsspannung(en) mit Angaben von Spannungsart und Frequenz (falls von 50 Hz abweichend)

e) Angaben zur Leistungs-/Stromaufnahme

f) Hinweise zur Steuerungskategorie gem. DIN EN 954-1

g) Angaben zur Parametrierung, Konfiguration bzw. Programmierung soweit erforderlich

h) Hinweise zur Ermittlung der maximalen Reaktionszeit(en)

i) vorzusehende Kurzschluss- oder Überstromschutzeinrichtungen, soweit zutreffend

j) Betriebstemperaturbereich

k) Angaben über die Schutzart; evtl. getrennt für verschiedene Einzelkomponenten

l) Angaben zur Bemessungsisolationsspannung und zum Verschmutzungsgrad

m) notwendige Belegung und Funktionsbeschreibung von Anschlussklemmen und Steckverbindern

n) notwendige Sicherheitshinweise

o) Verhalten bei Störungen

Prüfung: Durchsicht der eingereichten technischen Unterlagen; Prüfung auf Vollständigkeit, Korrektheit und Widerspruchsfreiheit

5.6 Aufschriften und Kennzeichnung

Die Hauptkomponenten des Bussystems sind mit folgenden Mindestaufschriften zu kennzeichnen:

a) Name oder Ursprungszeichen des Herstellers sowie Typbezeichnung oder Seriennummer

b) Bemessungsbetriebsspannung und Art sowie Bemessungsfrequenz, falls von 50 Hz abweichend

c) Anschlussleistung oder Bemessungsstrom

d) Absicherung der Betriebsspannung, falls notwendig

e) eindeutige Kennzeichnung von Anschlussklemmen und Steckverbindern

f) Angabe der IP-Schutzart.

Die Angaben zu b) bis f) können alternativ auch in der Benutzerinformation angeführt werden.

Die Größe von Bildzeichen, Buchstaben und Ziffern muss mindestens 2 mm betragen.

Die Aufschriften sind dauerhaft auszuführen.

Prüfung:

- Besichtigung/Messen der Aufschriften (Vollständigkeit, Korrektheit, Widerspruchsfreiheit)

- Reiben jeweils 15 s mit einem wasser- und einem benzingetränkten Tuch; Danach müssen die Aufschriften eindeutig lesbar sein, Aufkleber dürfen sich nicht gelöst haben.

5.7 . Versorgungsspannung

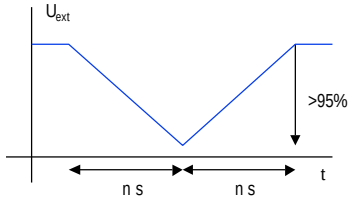
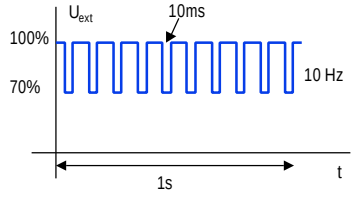
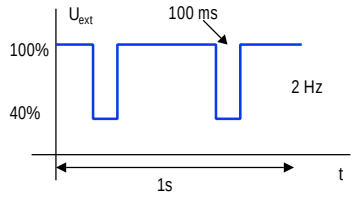
Anforderung (EN 61000-4-11)	***Einbrüche** von Versorgungsspannungen des Bussystems*
	Das Sicherheitsbussystem darf nicht gefahrbringend ausfallen, wenn die externe Versorgungsspannung gleichmäßig und kontinuierlich, in einer Zeit von n Sekunden, von der Nennspannung auf kleiner 5% reduziert wird und dann in gleicher Weise von kleiner 5% auf die Nennspannung erhöht wird (n = 5 und 60). Bewertungskriterium: C
Anforderung (EN 61000-4-11)	***Unterbrechungen** der externen Versorgungsspannungen des Bussystems*
	Das Sicherheitsbussystem darf den bestimmungsgemäßen Betrieb nicht verlassen, wenn die externe Versorgungsspannung Einbrüche um 30% für die Dauer von 10 ms mit einer Wiederholrate von 10 Hz aufweist. Bewertungskriterium: A
	Das Sicherheitsbussystem darf nicht gefahrbringend ausfallen, wenn die externe Versorgungsspannung Einbrüche um 60% für die Dauer von 100 ms mit einer Wiederholrate von 2 Hz aufweist. Bewertungskriterium: C

Tabelle 3: Veränderung von Versorgungsspannungen

Prüfung:

- Veränderung der Versorgungsspannung und Verhalten des Prüfling gemäß Tabelle 3.

5.8 Mechanische Prüfungen

Alle Komponenten von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten müssen eine ausreichende mechanische Festigkeit gegenüber den zu erwartenden Beanspruchungen, z. B. Erschütterungen, Schläge oder Stöße, haben (vgl. EN 954-1, Kat. B).

5.8.1 Schlagprüfung

Geschlossene Betriebsmittel mit einer Spannung, die nicht den Anforderungen von SELV oder PELV entspricht, müssen für die, beim Betrieb üblichen Schlagbeanspruchungen ausgelegt sein.

Prüfung:

- Das Gerät ist 2 h bei der minimal spezifizierten Umgebungstemperatur zu lagern mindestens jedoch bei –5° C , danach ist eine Schlagprüfung des Gerätes mit einem Prüfhammer gem. IEC 60069-2-75 folgendermaßen durchzuführen:

    - Drei Schläge werden mit 0,7 Nm auf die Stelle ausgeführt, die als die schwächste Stelle anzusehen ist, wobei besondere Aufmerksamkeit den Isolierstoffteilen, die aktive Teile abdecken, zu widmen ist.

    - Nach der Prüfung darf der Prüfling nicht beschädigt sein, im besonderen:

        1. dürfen aktive Teile nicht berührbar geworden sein,

        2. darf die Wirksamkeit von Isolierstoffauskleidungen und Trennwänden nicht beeinträchtigt worden sein,

        3. muss der Prüfling noch die spezifizierte IP-Schutzart aufweisen.

5.9 Schwingen

Das Prüfverfahren erfolgt gemäß DIN EN 60068-2-6, Prüfung Fc.

Auslenkung:	sinusförmig
Schwingungsart:	Frequenzdurchläufe mit einer Änderungsgeschwindigkeit von 1 Oktave/min (± 10 %)
Beanspruchungsdauer:	20 Frequenzdurchläufe pro Achse in jeder der zueinander senkrechten Achsen

Bewertungskriterium A gem. Tabelle 1.

Amplitude/Beschleunigung:

Einsatzbereich II:

10 = f = 57 Hz:	0,075 mm Amplitude
57 = f = 150 Hz:	1,0 g konstante Beschleunigung

Einsatzbereich III:

10 = f = 57 Hz:	0,35 mm Amplitude
57 = f = 150 Hz:	5,0 g konstante Beschleunigung

5.10 Schockprüfung

Einsatzbereich II:

Die Schockbelastung erfolgt gemäß IEC 61131-2, Prüfung Ea.

Beschleunigung: 15 g

Impulsdauer: 11 ms

Anzahl der Schocks: 2 je Achse, auf drei Achsen.

Bewertungskriterium: A gem. Tabelle 1 (abweichend von IEC 61131-2).

Während und nach der Prüfung darf keine Zerstörung an der Hardware, keine unbeabsichtigte Änderung des Systems und der gespeicherten oder ausgetauschten Daten erfolgen.

Einsatzbereich III:

Das Prüfverfahren erfolgt gemäß DIN EN 60068-2-29:

Beschleunigung: 10 g

Impulsdauer: 16 ms

Anzahl der Schocks: 1000 ±10 je Achse, auf drei Achsen.

Bewertungskriterium: A gem. Tabelle 1.

5.11 Thermische Belastbarkeit der Isolierstoffteile

5.11.1 (Gehäuse, Träger spannungsführender Teile)

Isolierstoffteile müssen ausreichend wärme- und feuerbeständig sein.

Prüfung:

- Es ist ein Glühdrahtprüfung nach DIN IEC 695-2-1 mit einer Temperatur von
    - 650° C ± 15 K an Gehäuseteilen,
    - 850° C ±15 K an Trägern spannungsführender Teile durchzuführen.
- Der Prüfling wird von dem Glühdraht (30 ± 1) s berührt. Jede Flamme oder jedes Glühen des Prüflings muss innerhalb 30 s nach Entfernen des Glühdrahtes erloschen sein. Jeder brennende oder geschmolzene Tropfen darf eine einfache

Lage Fließpapier, das horizontal in (200 ± 5) mm Entfernung unterhalb des Prüflings ausgebreitet ist, nicht entzünden.

5.12 Luft- und Kriechstrecken

Die Luft und Kriechstrecken sind gemäß DIN EN 50178 zu bemessen.

5.13 Klimaprüfung gem. IEC 68-2-1, IEC 68-2-2 und IEC 68-2-3

5.13.1 Trockene Wärme

Prüfbedingungen:

Prüfung bei maximal spezifizierter Temperatur bei Volllast auf der Busversorgung und auf den Ausgängen jedes zu prüfenden Busteilnehmers und bei maximal spezifizierter Betriebsspannung.

Dauer: Gem. IEC 68-2-2 nach Temperaturangleich 2h

Bewertungskriterium: A

Die Bauteilspezifikationen aller verwendeten Bauteile müssen bzgl. der Temperatur eingehalten werden.

Prüfung: Verfahren „Bd“ gemäss IEC 68-2-2

5.13.2 Trockene Kälte

Prüfbedingungen:

Prüfung bei minimal spezifizierter Temperatur bei minimaler Last auf der Busversorgung und auf den Ausgängen jedes zu prüfenden Busteilnehmers und bei minimal spezifizierter Betriebsspannung.

Dauer: Gem. IEC 68-2-1 nach Temperaturangleich 2h

Bewertungskriterium: A

Die Bauteilspezifikationen aller verwendeten Bauteile müssen bzgl. der Temperatur eingehalten werden.

Prüfung: Verfahren „Ad“ gemäss IEC 68-2-1

5.13.3 Feuchtelagerung

Gemäß IEC 68-2-3 wird der Prüfling 4 Tage feucht gelagert.

Prüfung: Isolationsfestigkeit gem. EN 50178 (vgl. Kap. 5.15).

5.14 Schutz gegen elektrischen Schlag

Jedes nach Schutzklasse I oder Schutzklasse II geschlossene Betriebsmittel muss mindestens der Schutzart IP 2X nach EN 60529-1 entsprechen.

Für offene Betriebsmittel wird die Einhaltung der IP 2X-Anforderungen nicht gefordert. Jedoch müssen Warnschilder, Gefahrensymbole 417-IEC-5036 und/oder mechanische Vorkehrungen zur Abschottung am vom Anwender beigestellten Gehäuse gefordert werden, um das Risiko eines Unfalles durch elektrischen Schlag bei Instandhaltungsarbeiten zu verringern. Das Öffnen des Gehäuses darf nur durch Benutzung eines Schlüssels oder eines Werkzeugs möglich sein.

Bei Sicherheitsbussystemen, die nach Schutzklasse I aufgebaut sind, sind Maßnahmen zum Schutz bei indirektem Berühren zu treffen. Metallische Gehäuseteile sind zuverlässig in das Schutzleitersystem einzubeziehen.

Austrittsöffnungen müssen bei Betriebsmitteln der Schutzklasse II mit dem Prüfstift, wie in Bild 20 der EN 60950 festgelegt, geprüft werden.

Bei Geräten, die über flexible Leitungen angeschlossen werden und deren Versorgungsspannung nicht den Anforderungen von SELV entspricht, muss der Ableitstrom mit den Grenzwerten, die in EN 60950 festgelegt sind, übereinstimmen.

Anmerkung: Die Isolationseigenschaften von Lack, Emaille, normalem Papier, Baumwolle, Oxidschicht auf Metallteilen und Isolierperlen sind nicht ausreichend, um den geforderten Schutz gegen zufälliges Berühren mit gefährlichen aktiven Teilen zu gewährleisten.

Prüfung:

- Einsichtnahme der technischen Unterlagen und Vergleich mit dem Baumuster,
- Prüfung mit den Prüfsonden nach EN 60529; Messung von Eintrittsöffnungen und Abständen,
- Messung von Ableitströmen.

5.15 Isolationsfestigkeit

Komponenten von Sicherheitsbussystemen müssen gem. DIN EN 50178 ausreichend spannungsfest sein.

Prüfung: gem. DIN EN 50178.

5.16 IP-Schutzart

Die Betriebsmittel müssen so konstruiert sein, dass sie den am vorgesehenen Verwendungszweck üblicherweise auftretenden Umgebungsbedingungen standhalten können (siehe auch Kap. 5.14).

Prüfung: Besichtigung und Schutzartprüfung gemäß EN 60529-1.

5.17 Eignung der verwendeten Bauteile

Die Bauteile des Sicherheitsbussystems müssen:

- mit bestehenden Normen übereinstimmen,
- für den vorgesehenen Einsatz geeignet sein,
- innerhalb ihrer festgelegten Bemessungswerte betrieben werden.

Prüfung: Besichtigung, evtl. Berechnung und Vergleich mit den technischen Unterlagen

5.18 Schutz gegen Umgehen auf einfache Weise

Es sind Maßnahmen gegen das einfache Umgehen von Sicherheitsfunktionen vorzusehen (z.B. Passwortschutz mit separater Inbetriebnahmesoftware).

Prüfung: Besichtigung, Überprüfung der Plausibilität

5.19 EMV-Mindestanforderungen

Einsatzbereich I, II und III:

Grundlage für die Prüfung sind die Anforderungen von EN 50082-2.

Die Bewertungskriterien aus EN 50082-2 sind durch Tabelle 1 zu ersetzen.

Zusätzlich ist die Primärseite der Spannungsversorgung mit schnellen Transienten (Surge) zu beaufschlagen, Bewertungskriterium C.

	Maßnahmen pro Nachricht					
Fehler	laufende Nummer Kap. 3.1	Zeitmarke Kap. 3.2	Zeiterwartung Kap. 3.3	Empfangsbestä-tigung Kap. 3.4	Kennung für Sender und Empfänger Kap. 3.5	Datensi Kap.
Wiederholung Kap. 2.9.1	X	X				
Verlust Kap. 2.9.2	X			X		
Einfügung Kap. 2.9.3	X			X 1)	X 2)	
falsche Abfolge Kap. 2.9.4	X	X				
Nachrichtenver-fälschung Kap. 2.9.5				X		X
Verzögerung Kap. 2.9.6		X	XX 3)			
Kopplung von SI - und Nicht-SI – Nachrichten Kap. 2.9.7				X 1)	X	

1) anwendungsabhängig
2) nur für Sender Kennung. Erkennt nur eine Einfügung von einer ungültigen Quelle!
3) Diese Maßnahme ist grundsätzlich erforderlich (Ruhestromprinzip)
4) Diese Maßnahme ist nur dann mit einer hochwertigen Datensicherung vergleichbar, wenn rechnerisch nach
Restfehlerrate L, bei versenden zweier Nachrichten in unabhängigen Busprotokollbausteinen die in Kap

Tabelle 4: Übersicht über die Wirkung der einzelnen Maßnahmen auf die möglich