DGUV Test
Prüf- und Zertifizierungsstelle
Elektrotechnik
Fachbereich Energie Textil
Elektro Medienerzeugnisse

Grundsätze für die Prüfung und Zertifizierung von „Bussystemen für die Übertragung sicherheitsbezogener Nachrichten“

Stand: 2014-03

Prüfgrundsatz
Bussysteme für die Übertragung
sicherheitsbezogener Nachrichten
GS-ET-26

GS-ET-26

Fachbereich Energie Textil Elektro Medienerzeugnisse
Prüf- und Zertifizierungsstelle im DGUV Test
Gustav-Heinemann-Ufer 130
50968 Köln

Der Prüfgrundsatz dient als Nachweis, dass die Anforderungen des Produktsicherheitsgesetzes (ProdSG), und so die 9. Verordnung zum ProdSG, eingehalten sind.

Diese Grundsätze werden, den neuesten Erkenntnissen auf dem Gebiet der Arbeitssicherheit und dem technischen Fortschritt folgend, von Zeit zu Zeit überarbeitet und ergänzt. Für die Prüfung durch die Prüf- und Zertifizierungsstelle Elektrotechnik des Fachbereichs ETEM ist stets die neueste Ausgabe verbindlich.

Änderungen gegenüber der Ausgabe 05-2002:

- Grundlegende Überarbeitung
- Anpassung an aktuelle Maschinenrichtlinie
- Anpassung an aktuelle Normen

Inhaltsverzeichnis ..... Seite

1 Allgemeines

1.1 Geltungsbereich

Dieser Grundsatz gilt für die Prüfung von Bussystemen für die Übertragung sicherheitsbezogener Nachrichten an Maschinen im Sinne der Maschinenrichtlinie. Die Kommunikation kann dabei zwischen verschiedenen Logikeinheiten für Sicherheitsfunktionen und/oder zwischen intelligenten Sensoren/Aktoren und Logikeinheiten für Sicherheitsfunktionen stattfinden.

ANMERKUNG: Derzeit werden nur gekapselte Bussysteme mit einem Performance Level c bis e (nach DIN EN ISO 13849-1) bzw. SIL 1 bis SIL 3 (nach DIN EN 61508) mit einer vom Hersteller definierten Anzahl und einem definierten Typ von Busteilnehmern betrachtet. Eine Schnittstelle für den Fernzugriff auf das sicherheitsbezogene System oder die Sicherheitsdaten (z.B. Internet, WLAN oder Bluetooth) wird hier nicht betrachtet. Dieser Prüfgrundsatz behandelt ausschließlich Safety-Aspekte und keine Security-Aspekte.

ANMERKUNG 2: Im Folgenden wird im Prüfgrundsatz die Abschätzung des Performance Levels herangezogen. Für eine Zuordnung der äquivalenten Parameter gemäß DIN EN 62061 kann das im Anhang A.1 dieses Prüfgrundsatzes beschriebene Verfahren verwendet werden.

1.2 Technische Regelwerke, Vorschriften

RICHTLINIE 2006/42/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung).

DIN EN ISO 13849-1	Sicherheit von Maschinen; Sicherheitsbezogene Teile von Steuerungen Teil 1: Allgemeine Gestaltungsleitsätze
DIN EN ISO 13849-2	Sicherheit von Maschinen; Sicherheitsbezogene Teile von Steuerungen Teil 2: Validierung
DIN EN 60204-1	Elektrische Ausrüstung von Maschinen
DIN EN 61800-5-2	Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit
DIN EN 61508	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teile 1 – 7

DIN EN 61784-3	Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilfestlegungen
DIN EN 61784-3 Bb. 1	Industrielle Kommunikationsnetze – Profile – Beurteilungsleitfaden für Sicherheitsgeräte, die funktional sichere Übertragung nach den Profilen der IEC 61784-3 verwenden
DIN EN 61131-2:2008-04	Speicherprogrammierbare Steuerungen – Teil 2: Betriebsmittelanforderungen und Prüfungen
DIN EN 61326-3-1 :2008-11	Elektrische Mess-, Steuer-, Regel-, und Laborgeräte –EMV Anforderungen – Teil 3-1: Störfestigkeitsanforderungen für sicherheitsbezogene Systeme und für Geräte, die für sicherheitsbezogene Funktionen vorgesehen sind (Funktionale Sicherheit) – Allgemeine industrielle Anwendungen

ANMERKUNG: Wird auf normative Dokumente datiert verwiesen, so werden in diesem Prüfgrundsatz Prüfverfahren referenziert welche in Abschnitten genau dieser Normen festgelegt sind.

1.3 Funktionsbeschreibung

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

2 Begriffe

2.1 Allgemeines

2.1.1 Bussystem

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

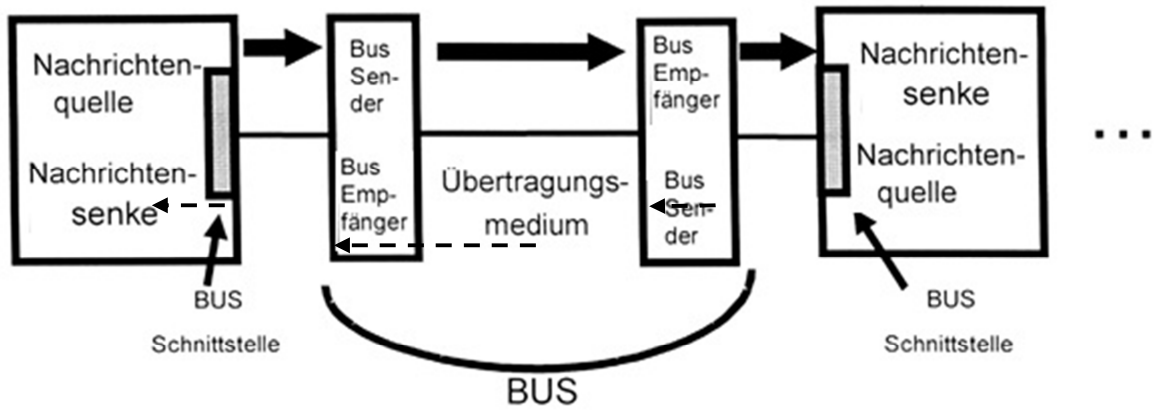

Abbildung 1: Einfaches Modell eines Bussystems

2.1.2 Gekapselte Bussysteme

Eine feste Zahl oder eine festgelegte maximale Anzahl von Busteilnehmern, die durch ein Übertragungsmedium mit definierten Eigenschaften verbunden sind, bilden ein gekapseltes Bussystem. Das gekapselte Bussystem verfügt über keine Möglichkeit des Fernzugriffs auf Sicherheitsdaten außer zum Auslesen von Sicherheitsdaten.

ANMERKUNG: Das Lesen von Statusinformation von Busteilnehmern durch Fernzugriff ist möglich. Eine Übertragung von Nachrichten in das gekapselte Bussystem ist nicht vorgesehen.

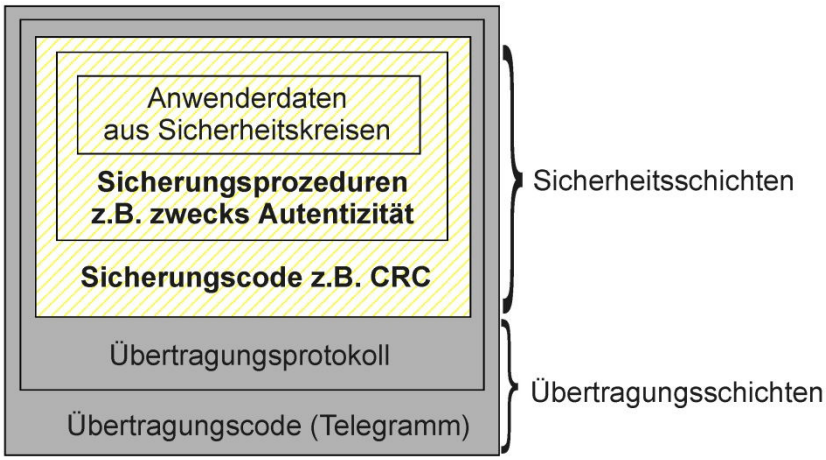

Abbildung 2: OSI-Modell für die Übertragung sicherheitsbezogener Nachrichten

Abbildung 2 besagt, dass das Sicherheits-Bussystem auf Standardübertragungsprozeduren (Übertragungsprotokolle und Übertragungscode) beruht, welche um zusätzliche sicherheitsbezogene Mechanismen (Sicherheitsprozedur und Sicherheitscode) erweitert werden.

2.1.3 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 erläutert. Eine vollständige Betrachtung der sicherheitstechnischen Aspekte ist nicht Gegenstand dieses Papiers. Für die Ertüchtigung von Nachrichtenquellen und –senken sind die relevanten Normen aus Kapitel 1.2 anzuwenden. In Performance Level d und e (DIN EN ISO 13849-1) sind die übergeordneten Busteilnehmer in der Regel zweikanalig aufgebaut.

2.1.3.1 Architekturmodell A

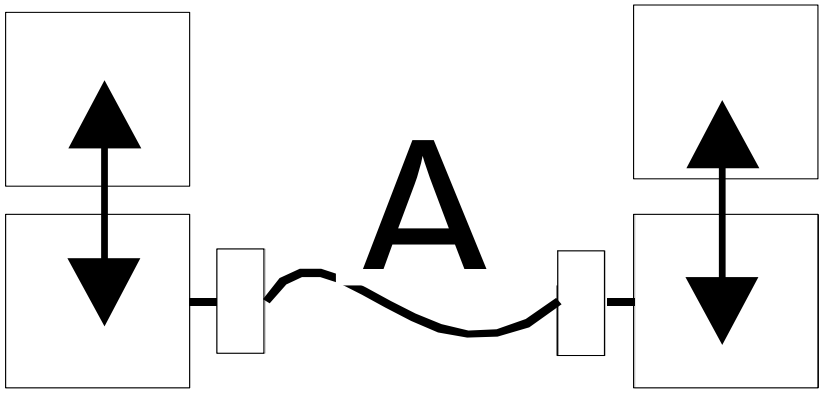

Abbildung 3: Architekturmodell A; Übertragungsschichten u. Sicherheitsschichten einkanalig

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.

2.1.3.2 Architekturmodell B

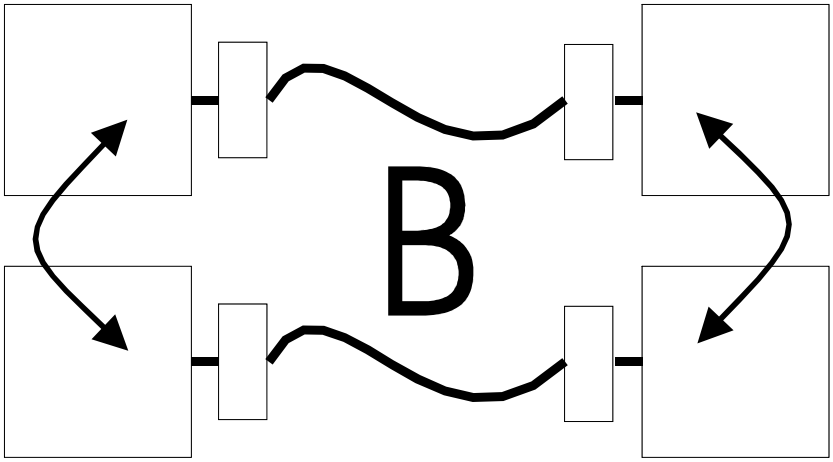

Abbildung 4: Architekturmodell B; Übertragungsschichten u. Sicherheitsschichten zweikanalig

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

2.1.3.3 Architekturmodell C

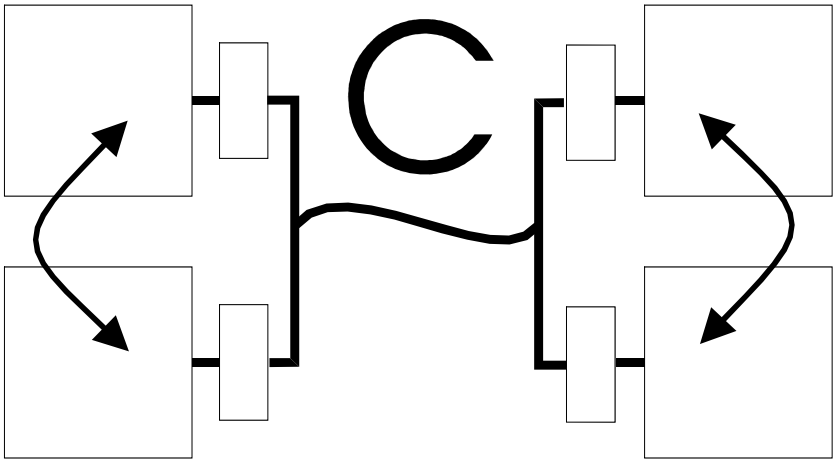

Abbildung 5: Architekturmodell C; Übertragungsschichten einkanalig u. Sicherheitsschichten zweikanalig

Abbildung 5 beschreibt ein Modell, dass dem Modell aus Abbildung 4 entspricht, allerdings ist hier das Übertragungsschicht einkanalig.

2.1.3.4 Architekturmodell D

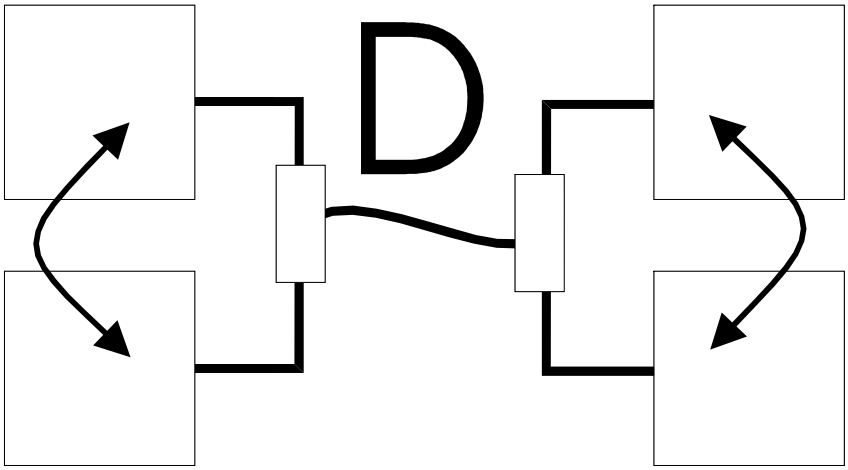

Abbildung 6: Architekturmodell D; Übertragungsschichten einkanalig u. Sicherheitsschichten zweikanalig

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.

2.1.4 Nachrichtenquelle (Nachrichtensender) und –senke (Nachrichtenempfänger)

Eine Nachrichtensenke ist der Empfänger einer sicherheitsbezogenen Nachricht.
Eine Nachrichtenquelle ist der Sender einer sicherheitsbezogenen Nachricht.

2.1.5 Nachricht

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

2.1.6 Maximale Ausbaustufe

Zahl der maximal am Nachrichtenaustausch beteiligten Sender und Empfänger.

2.1.7 Ansprechzeit

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

2.1.8 Fehlertoleranzzeit

Die Fehlertoleranzzeit ist die Zeit, in der eine Funktionseinheit eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen ausführen kann.

ANMERKUNG: Die Größe der Fehlertoleranzzeit ist abhängig von der Risikoanalyse. Speziell für kabellose Fernsteuerungen existieren normative Vorgaben (IEC 62745)

2.1.9 Busübertragungszeit

Die Busübertragungszeit setzt sich wie folgt zusammen:
Zeit zur Codierung des sicherheitsbezogenen Telegramms, die Signallaufzeit, Zeit zur Decodierung des sicherheitsbezogenen Telegramms.

2.2 Übertragungsfehler

2.2.1 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 geöffnet).

2.2.2 Verlust

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

2.2.3 Einfügung

Durch den Fehler eines Busteilnehmers werden Nachrichten eingefügt.

2.2.4 Falsche Abfolge

Durch den Fehler eines Busteilnehmers wird die Reihenfolge von Nachrichten verändert.
Beispiel: Vor Einleiten des sicheren Betriebshalts 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.

2.2.5 Nachrichtenverfälschung, fehlerhafte Adressierung

Durch den Fehler eines Busteilnehmers oder durch Fehler auf dem Übertragungsmedium werden Nachrichten verfälscht oder an den falschen sicherheitsbezogenen Teilnehmer gesandt.

2.2.6 Verzögerung

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

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

2.2.7 Maskerade

Durch den Fehler eines Busteilnehmers werden sicherheitsbezogene und nicht sicherheitsbezogene Nachrichten vermischt. Die nicht sicherheitsbezogenen Nachrichten werden als sicherheitsbezogene Nachrichten behandelt oder umgekehrt.

3 Qualitative und quantitative Maßnahmen zur Fehlerbehandlung und Fehlerbewertung

3.1 Beschreibung von Maßnahmen zur Fehlererkennung/Fehlerbeherrschung

Im folgenden Kapitel werden qualitative Maßnahmen aufgezählt, die der Erkennung und Beherrschung von Übertragungsfehlern dienen.

3.1.1 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. Die laufende Nummer muss in der betrachteten Zeiteinheit eineindeutig sein.

ANMERKUNG: Ein Toggle-Bit wird nicht als laufende Nummer im Sinne der o.g. Anforderung gewertet.

Prüfung: Soweit spezifiziert, Prüfung der Dokumentation und Softwarerealisation im System. Verifikation der Maßnahme durch Verfälschung der laufenden Nummer.

3.1.2 Zeitstempel

Der Inhalt einer Nachricht ist in der Regel nur in einem bestimmten Zeitraum gültig. Der Zeitstempel ist z.B. ein Datum das einer Nachricht vom Sender angehängt wird. Man unterscheidet zwischen relativen Zeitstempeln und absoluten Zeitstempeln. Nicht synchrone Zeitbasen müssen zum sicheren Zustand führen.

3.1.2.1 Relative Zeitstempel

Ein relativer Zeitstempel ist ein Zeitraum, in welchem die sicherheitsbezogenen Nachrichten gültig sind.

Prüfung: Soweit spezifiziert, Prüfung der Dokumentation und Softwarerealisation im System. Verifikation der Maßnahme durch Verfälschung des relativen Zeitstempels.

3.1.2.2 Absolute Zeitstempel

Ein absoluter Zeitstempel gibt Beginn und Ende des Zeitraumes an, in welchem die sicherheitsbezogenen Nachrichten gültig sind.

Prüfung: Soweit spezifiziert, Prüfung der Dokumentation und Softwarerealisation im System. Verifikation der Maßnahme durch Verfälschung des absoluten Zeitstempels.

3.1.3 Zeiterwartung (Timeout)

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.

Prüfung: Maßnahme immer notwendig, Prüfung der Dokumentation und Softwarerealisation im System. Verifikation der Maßnahme durch Verzögerung der Nachrichtenübertragung.

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.

3.1.4 Rückmeldung

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

ANMERKUNG: Bei verschiedenen Bussystemen werden die Begriffe Rückmeldung, Echo und Quittung synonym verwendet.

Prüfung: Soweit spezifiziert, Prüfung der Dokumentation und Softwarerealisation im System. Verifikation der Maßnahme durch Verfälschung der Rückmeldung.

3.1.5 Verbindungsauthentizität

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

Prüfung: Soweit spezifiziert, Prüfung der Dokumentation und Softwarerealisation im System. Verifikation der Maßnahme durch Verfälschung der Senderkennung.

3.2 Datensicherung

Die Datensicherung ist ein wesentlicher Bestandteil zum Erreichen eines gewünschten Sicherheitsniveaus. Aufgrund unterschiedlicher Strukturen und unterschiedlicher Ansätze werden in diesem Kapitel die wesentlichen quantitativen Methoden für den jeweiligen Performance Level (gemäß DIN EN ISO 13849-1) 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.

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

3.2.1.1 Allgemeines

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

Restfehlerwahrscheinlichkeit, Restfehlerrate

Alle Maßnahmen zur Datensicherung müssen in den übergeordneten Steuerungsteilen, welche die Anforderungen für den erforderlichen Performance Level erfüllen, ausgeführt werden. Die Restfehlerrate berechnet sich aus der Restfehlerwahrscheinlichkeit des übergeordneten sicheren Datensicherungsmechanismus und der Übertragungsrate der sicherheitsbezogenen Nachrichten.

Für die Restfehlerwahrscheinlichkeit gilt („worst case“):

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

mit

$$A_{n,i} = \binom{n}{i} = \frac{n!}{i! * (n-i)!} \qquad (2)$$

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 der folgende Ansatz für die maximal zulässige Restfehlerrate für das funktional sichere Bussystem gewählt werden:

$$\Lambda = R(p) * \nu * m \qquad (3)$$

v = Anzahl der sicherheitsbezogenen Nachrichten pro Stunde,
R(p) = Restfehlerwahrscheinlichkeit,
m = maximale Anzahl an Informationssenken die in einer einzelnen Sicherheitsfunktion zugelassen sind

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 (Performance Level) ein. Da ein Bussystem frei projektierbar ist muss hier die maximale Ausbaustufe des Sicherheitsbussystems angenommen werden.

Für den Performance Level e muss $\Lambda < 10^{-9}$ /h sein.
Für den Performance Level d muss $\Lambda < 10^{-8}$ /h sein.
Für den Performance Level c muss $\Lambda < 3*10^{-8}$ /h sein.

Beispiel für Performance Level d

m = 32, R(p) = 10^{-16}, ν = 360000/h => Λ = 1,15 * 10^{-9}/h

Dies ist weniger als 1% der gesamten Versagenswahrscheinlichkeit eines Performance Level d-Systems

Prüfung: Soweit spezifiziert, Prüfung der Dokumentation und Softwarerealisation im System, Überprüfung der vom Hersteller vorgelegten Berechnungen. Überprüfung der für die Berechnung notwendigen Werte.

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

In diesem Ansatz wird 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 für eine Kategorie 4 Struktur nach DIN EN ISO 13849-1 nicht zulässig, für 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), dass andere Teilnehmer jede Nachricht mit überprüfen, so dass hier wiederum die Fehleranhäufung beherrscht werden kann.
Der hier vorgestellte Ansatz basiert auf Redundanz mit Kreuzvergleich. Bei dieser Redundanz werden außerdem Nachrichten zweifach versendet und über einen Vergleicher auf Konsistenz geprüft. Dies bedeutet, dass ein Versagen der Übertragung nur bei gleichartigen 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:

$$R(p)_{BC} = R(p)^2 \qquad (4)$$

Die Berechnung von Λ erfolgt analog zu Formel (1) allerdings muss hier statt R(p) der Wert nach Formel (4) eingesetzt werden.

Für den Performance Level e muss $\Lambda < 10^{-9}$ /h sein.
Für den Performance Level d muss $\Lambda < 10^{-8}$ /h sein.
Für den Performance Level c muss $\Lambda < 3*10^{-8}$ /h sein.

Prüfung: Soweit spezifiziert, Prüfung der Dokumentation und Softwarerealisation im System, Überprüfung der vom Hersteller vorgelegten Berechnungen. Überprüfung der für die Berechnung notwendigen Werte.

3.2.3 Datensicherung für Modell A und D, bei dem 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. Performance Level noch fehlt, in der übergeordneten Steuerung realisiert.

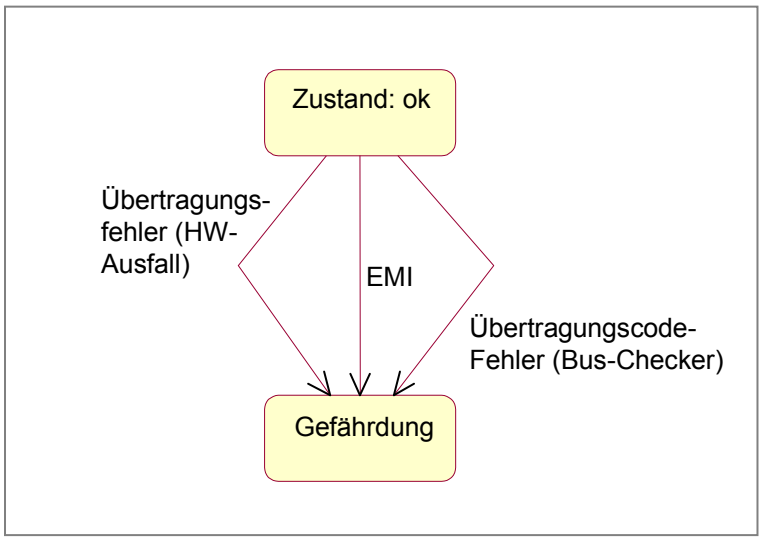

Abbildung 7: Vereinfachtes Markov-Modell

Da in diesem Ansatz die Hardwarefehlertoleranz der Busprotokollbausteine mit berücksichtigt 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 auf drei wesentliche Übergangswahrscheinlichkeiten (siehe Abbildung 7) zurückgeführt werden:

1. Die Hardware der Übertragungsschichten versagt, so dass die Telegramme verfälscht werden (R_{HW}).
2. Bitverfälschungen aufgrund von elektromagnetischen Einflüssen (EMI) treten auf, die von der Übertragungseinrichtung nicht erkannt werden (R_{EMi}).
3. Jegliche verfälschte Nachricht wird von der Übertragungseinrichtung an die Sicherungseinrichtung weitergereicht, weil ausschließlich der entsprechende Teil (Bus-Checker) ausgefallen ist (R_{TC}).

Die Restfehlerrate des Systems ist somit die Summe aller Einzelraten:

$$R_{AD} = R_{HW} + R_{EMI} + R_{TC} \qquad (5)$$

R_{AD} = Restfehlerwahrscheinlichkeit des Systems

Die einzelnen Terme werden wie folgt berechnet:

$$R_{HW} = (x_1 * \lambda_{HWF} + x_2 * \lambda_{HWS}) * P_{US} \qquad (6)$$

wobei

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

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

x_1 = der Anteil der gefährlichen Fehler in den beteiligten Komponenten mit $0 < x_1 \leq 1$,

x_2 = der Anteil der gefährlichen Fehler in den nicht beteiligten Komponenten mit $0 < x_2 \leq 1$,

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

$$R_{EMI} = f_W * P_{UB} * P_{US} \qquad (7)$$

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 dann, wenn der Sicherheitscode und der Übertragungscode unabhängig sind. Dies kann z.B. durch Simulation nachgewiesen oder durch Grenzwertabschätzungen mathematisch gefasst werden.

Weiterhin ist 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.

$$R_{TC} = P_{US} * k * \frac{1}{T} \qquad (8)$$

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.

Für den Performance Level e muss $\Lambda < 10^{-9}$ /h sein.
Für den Performance Level d muss $\Lambda < 10^{-8}$ /h sein.
Für den Performance Level c muss $\Lambda < 3*10^{-8}$ /h sein.

Prüfung: Soweit spezifiziert, Prüfung der Dokumentation und Softwarerealisation im System. Überprüfung der vom Hersteller vorgelegten Berechnungen. Überprüfung der für die Berechnung notwendigen Werte.

3.3 Redundanz mit Kreuzvergleich

In sicherheitsbezogenen Busanwendungen können Sicherheitsdaten zweifach, innerhalb einer oder in zwei getrennten Nachrichten gesendet werden, wobei identische oder unterschiedliche Integritätsmaßnahmen unabhängig vom unterlagerten Bus zum Einsatz kommen. Zusätzlich werden über den Bus oder einer separate Verbindung innerhalb der zweikanaligen Sender/Empfängereinheit (Modell B und Modell C) in 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 sollten Fehler gemeinsamer Ursache durch geeignete qualitative Maßnahmen (z.B. Diversität, zeitversetzte Nachrichten) aufgedeckt werden.

Prüfung: Soweit spezifiziert, Prüfung der Dokumentation und Softwarerealisation im System. Verifikation der Maßnahme z.B. durch Signalverfälschung in einem Kanal.

3.4 Unterschiedliche Datensicherung für sicherheitsbezogene (SI) - und nicht sicherheitsbezogene Daten (NSI)

Werden über das Bussystem sicherheitsbezogene (SI) - und nicht - sicherheitsbezogene Daten (NSI) versendet, sind unterschiedliche Datensicherungen oder Codierungen (verschiedene CRC - Algorithmen, unterschiedliches Generatorpolynom) so einzusetzen, damit eine Rückwirkungsfreiheit gegeben ist.

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

Prüfung: Soweit spezifiziert, Prüfung der Dokumentation und Softwarerealisation im System.

4 Anforderungen

Es sind Vorkehrungen zur Fehlererkennung und Fehlerreaktion am Empfänger vorzusehen, die die Aufgabe haben sicherheitsbezogene Reaktionen in einer Zeit einzuleiten, ohne dass ein gefährlicher Zustand eintritt.

4.1 Verifikation der Sicherheitsmaßnahmen

Sicherheitsbezogene Nachrichten müssen entsprechend dem geforderten Performance Level 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.

Prüfung: Es sind die Anforderungen der DIN EN ISO 13849-1/2 zu überprüfen. Dies liegt außerhalb des Geltungsbereiches des Prüfgrundsatzes und ist normativ geregelt.

4.2 Ruhestromprinzip

Es muss grundsätzlich eine Zeiterwartung vorgesehen werden.

Prüfung: Prüfung der Dokumentation und Softwarerealisation im System, Funktionsprüfung. Verifikation der Maßnahme durch Verzögerung der Nachrichtenübertragung.

4.3 Übertragungsfehler

Bei Übertragungsfehlern ist es zulässig, dass innerhalb der Fehlertoleranzzeit z.B. Telegrammwiederholungen erfolgen bevor eine definierte Fehlerreaktion ausgelöst wird. Der maximale Wert der Fehlertoleranzzeit darf 500 ms nicht überschreiten.

Prüfung: Prüfung der Dokumentation und Softwarerealisation im System, Funktionsprüfung. Verifikation der Maßnahme durch Störung der Übertragung.

4.4 Sicherheitsreaktions- und Antwortzeiten

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

Prüfung: Sichtung der Dokumentation, Überprüfung der Softwarerealisation, Messung der Reaktionszeiten unter den für das jeweilige System ungünstigsten Bedingungen. Überprüfung ob der Hersteller die maximal mögliche Anzahl an Teilnehmern und die Zeitbedingungen angegeben hat.

4.5 Kombinierte Maßnahmen

Für die Übertragung sicherheitsbezogener Nachrichten über Bussysteme muss ein Maßnahmenpaket aus dem in Kapitel 3.1 genannten Maßnahmen zusammengestellt werden, so dass jeder im Kapitel 2.2 beschriebene Fehler innerhalb der Fehlertoleranzzeit aufgedeckt wird. Tabelle 3 gibt eine Hilfe zur Auswahl der Einzelmaßnahmen.

Prüfung: Alle Maßnahmen müssen auf Vollständigkeit und Wirksamkeit gemäß Tabelle 3 überprüft werden.

4.6 Rückwirkungsfreiheit

Die Rückwirkungsfreiheit bezüglich des gefährlichen Ausfalls von nicht sicherheitsbezogenen Busteilnehmern auf sicherheitsbezogene Busteilnehmer muss nachgewiesen werden.

Prüfung: Sichtung der Dokumentation, Überprüfung der Softwarerealisation, Funktionstests und Funktionstests unter Einfluss von simulierten Rückwirkungen z.B. durch PC-Simulation. Hierbei sind die Fehler gemäß Kapitel 2.2 für den nicht sicherheitsbezogenen Busteilnehmer anzunehmen, wobei die Reaktion zum sicheren Zustand führen muss.

5 Prüfungen gegenüber Umgebungsbedingungen, allgemeine Anforderungen

Die nachfolgend aufgeführten Bauartanforderungen und Prüfungen sind Mindestanforderungen an ein Sicherheitsbussystem einschließlich aller dazugehörigen Komponenten. Wenn ein Bussystem funktionaler Bestandteil eines sicherheitsbezogenen Produktes ist (z.B. SPS, Frequenzumrichter) sind zusätzlich die Anforderungen der einschlägigen Produktnormen zu erfüllen. Die Komponenten des Sicherheitsbussystems müssen für den vorgesehenen Einsatz geeignet sein, und innerhalb ihrer festgelegten Bemessungswerte betrieben werden.

5.1 Bewertungskriterien

Es sind die folgenden Bewertungskriterien festgelegt:

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

Tabelle 1: Bewertungskriterien für Prüfungen gegenüber Umgebungsbedingungen

5.2 Prüfaufbau

Soweit durchführbar, müssen alle Teile eines Sicherheitsbussystems zusammen geprüft werden. Wo dies nicht durchführbar ist, dürfen Teile des Sicherheitsbussystems 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, das heißt, dass nicht in jedem Fall ein Ausbau auf die maximale Anzahl an Busteilnehmern erforderlich ist. Die für die Sicherheitsfunktion notwendigen Signale sind in solchen Simulationen nachzubilden.

5.3 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 Prüfaufbaus festzustellen. Ziel der Prüfung ist es nachzuweisen, dass sich das Sicherheitsbussystem (Prüfling) bei allen Prüfungen entsprechend seiner sicherheitsbezogenen Spezifikation verhält.

Die Prüfkriterien sind u. a.

- Betrieb des Prüflings wie in den technischen Daten vorgesehen
- keine Zerstörung eines Bauelementes des Prüflings (außer EMV)
- kein fehlerhaftes oder unbeabsichtigtes Verhalten des Prüflings (außer EMV)
- kein Anzeichen einer Überhitzung von Bauelementen
- kein aktives Teil, welches bestimmungsgemäß berührungsgefährliche Spannung führt, darf berührbar werden
- keine Gehäusebeschädigungen.

Für alle Messungen sind die Messunsicherheiten zu bestimmen und bei der Bewertung der Prüfergebnisse zu berücksichtigen (siehe Anhang B).

5.4 Betriebsanleitung

Jedem Sicherheitsbussystem muss eine Betriebsanleitung in der oder den Amtssprachen der Gemeinschaft des Mitgliedstaats beiliegen, in dem das Sicherheitsbussystem in Verkehr gebracht und/oder in Betrieb genommen wird. Ist diese Produktinformation nicht in deutscher Sprache abgefasst, ist eine deutsche Übersetzung vorzulegen. Die Prüfung erfolgt anhand der deutschen Übersetzung.

Den Geräten ist eine Betriebsanleitung beizulegen, die einen ordnungsgemäßen Anschluss und die Inbetriebnahme ermöglicht. Es ist möglich eine Betriebsanweisung in digitaler Form beizulegen, wenn zur Integration der Sicherheitskomponente Werkzeuge (PC, Tablet usw.) notwendig sind. Werden solche Werkzeuge nicht benötigt, muss die

Betriebsanleitung in Papierform beigelegt werden (vgl. VG 11 Beschluss CNB/M/11.054 Revision 01). Zusätzlich zu den Anforderungen der Normen muss diese Betriebsanleitung mindestens enthalten:

a) Firmenname und vollständige Anschrift des Herstellers und seines Bevollmächtigten
b) Typbezeichnung oder Seriennummer
c) EG-Konformitätserklärung
d) Allgemeine Beschreibung des Sicherheitsbussystems
e) Die für Verwendung, Wartung und Instandsetzung des Sicherheitsbussystems und zur Überprüfung ihres Ordnungsgemäßen Funktionierens erforderlichen Zeichnungen, Schaltpläne, Beschreibungen und Erläuterungen
f) Bestimmungsgemäße Verwendung
g) Warnhinweise in Bezug auf Fehlanwendung des Sicherheitsbussystems, zu denen es erfahrungsgemäß kommen kann
h) Anleitung zur Montage, zum Aufbau und zum Anschluss des Sicherheitsbussystems einschließlich Zeichnungen Schaltpläne und der Befestigungsmöglichkeit
i) Hinweise zur Inbetriebnahme und zum Betrieb des Sicherheitsbussystems
j) Angaben zu Restrisiken
k) Vorgehen bei Störungen
l) Beschreibung der vom Benutzer durchzuführenden Einrichtungs- und Wartungsarbeiten, sowie der zu treffenden vorbeugenden Wartungsmaßnahmen
m) Spezifikation der zu verwendenden Ersatzteile
n) Angabe bei Verwendung von nichtionisierender Strahlung (z.B. Laser)
o) Bemessungsbetriebsspannung(en) mit Angaben von Spannungsart und Frequenz
p) Angaben zur Leistungs-/Stromaufnahme
q) Angaben gemäß DIN EN ISO 13849-1
   - Kategorie
   - PL
   - z.B. Kat. 3, PL e; DIN EN ISO 13849-1:2008-12
r) Angaben zur Parametrierung, Konfiguration bzw. Programmierung soweit erforderlich
s) Hinweise zur Ermittlung der maximalen Reaktionszeit(en)
t) vorzusehende Kurzschluss- oder Überstromschutzeinrichtungen, soweit zutreffend
u) Betriebstemperaturbereich
v) Angaben über die Schutzart; evtl. getrennt für verschiedene Einzelkomponenten
w) Angaben zur Bemessungsisolationsspannung und zum Verschmutzungsgrad
x) notwendige Belegung und Funktionsbeschreibung von Anschlussklemmen und Steckverbindern

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

5.5 Aufschriften und Kennzeichnung

Die Hauptkomponenten des Bussystems sind mit folgenden Mindestaufschriften zu kennzeichnen:

a) Firmenname und vollständige Anschrift des Herstellers

b) Bezeichnung des Geräts
c) CE-Kennzeichnung
d) Baureihen oder Typbezeichnung
e) Baujahr
f) Entsprechender Hinweis, wenn Einsatz in explosionsgefährdeter Umgebung vorgesehen.
g) Bemessungsbetriebsspannung und Art sowie Bemessungsfrequenz
h) Anschlussleistung oder Bemessungsstrom
i) Hardwareserien oder -revisionsnummer
j) Absicherung der Betriebsspannung, falls notwendig
k) eindeutige Kennzeichnung von Anschlussklemmen und Steckverbindern
l) Angabe der IP-Schutzart.

Die Angaben zu g) bis l) können alternativ auch in der Betriebsanleitung 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, Widerspruchs Freiheit)

Um die Dauerhaftigkeit der Aufschriften zu Prüfen jeweils 15 s mit einem wasser- und einem benzingetränkten Tuch reiben; Danach müssen die Aufschriften eindeutig lesbar sein, Aufkleber dürfen sich nicht gelöst haben. Das für die Prüfung zu verwendende Benzin (en: petroleum spirit) ist ein aliphatisch lösliches Hexan mit einem Höchstgehalt an aromatischen Volumenanteilen von 0,1%, einem Kauri-Butanol-Wert 29, einer Siede-Einsatztemperatur (andere Bezeichnung: unterer Siedepunkt) von etwa 65 °C, einer Verdampfungstemperatur (andere Bezeichnung: Trockenpunkt) von etwa 69 °C und einer spezifischen Masse von etwa 0,7 kg/l. Alternativ darf ein Reagens der Hexan-Klasse (en: reagent grade hexane) mit mindestens 85% n-Hexan benutzt werden.

Als Testflüssigkeit ist z.B. das chemische Produkt mit der Handelsbezeichnung „n-Hexan zur Analyse“, welches die Anforderungen der in DIN EN 60335-1 und DIN EN 60950-1 definierten Testflüssigkeit erfüllt, zu verwenden.

5.6 Mechanische Prüfungen

Alle Komponenten von Bussystemen für die Übertragung sicherheitsbezogener Nachrichten müssen eine ausreichende mechanische Festigkeit gegenüber den zu erwartenden Beanspruchungen, z. B. Erschütterungen, Schläge oder Stöße haben.

5.6.1 Schlagprüfung

Geschlossene Betriebsmittel mit einer Spannung, die nicht den Anforderungen von SELV oder PELV entspricht, müssen für die, beim Betrieb üblichen Schlagbeanspruchungen ausgelegt sein, sodass der Schutz gegen direktes Berühren gewährleistet bleibt.

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. DIN EN 60068-2-75 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.

5.6.2 Schwingen

Das Prüfverfahren erfolgt gemäß DIN EN 60068-2-6 Tabelle C.2

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

10 ≤ f ≤ 55 Hz: 0,35 mm Amplitude

Bewertungskriterium A gemäß Tabelle 1.

5.6.3 Schockprüfung

Das Prüfverfahren erfolgt gemäß DIN EN 60068-2-27 Prüfung Ea:
Schockform Halbsinus
Beschleunigung: 10 g
Impulsdauer: 16 ms
Anzahl Schocks: 1000 ± 10 je Achse, auf drei senkrecht aufeinander stehenden Achsen in je zwei Richtungen.

Befestigungsart: nach Herstellerspezifikation

Bewertungskriterium A gemäß Tabelle 1.

5.7 Thermische Belastbarkeit der Isolierstoffteile

5.7.1 Träger aktiver Teile

Isolierstoffteile müssen ausreichend wärme- und feuerbeständig sein.
Prüfung: Es ist ein Glühdrahtprüfung nach DIN EN 60695-2-11 mit einer Temperatur von 750° C ±15 K an Trägern aktiver 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.

5.7.2 Gehäusewerkstoffe (Prüfung der Flammausbreitungsgeschwindigkeit gemäß DIN EN 61131-2 Kapitel 11.5)

Gehäuseteile, die die äußere Umhüllung bilden, müssen mit der Flammausbreitungsgeschwindigkeit nach V-0, V-1, V-2 übereinstimmen. Nachweis durch z.B. Produktdatenblatt.

5.8 Luft- und Kriechstrecken

Die Luft und Kriechstrecken sind gemäß DIN EN 61131-2 Abschnitt 11.4 zu bemessen.

5.9 Klimaprüfung

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

5.9.1 Temperaturwechsel

Prüfbedingungen:

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

Die Prüfung wird in 2 Zyklen durchgeführt. In Abbildung 8 ist der Temperaturverlauf für die Mindestanforderung von einer niedrigen Temperatur von 5 °C und einer hohen Temperatur von 40 °C dargestellt.

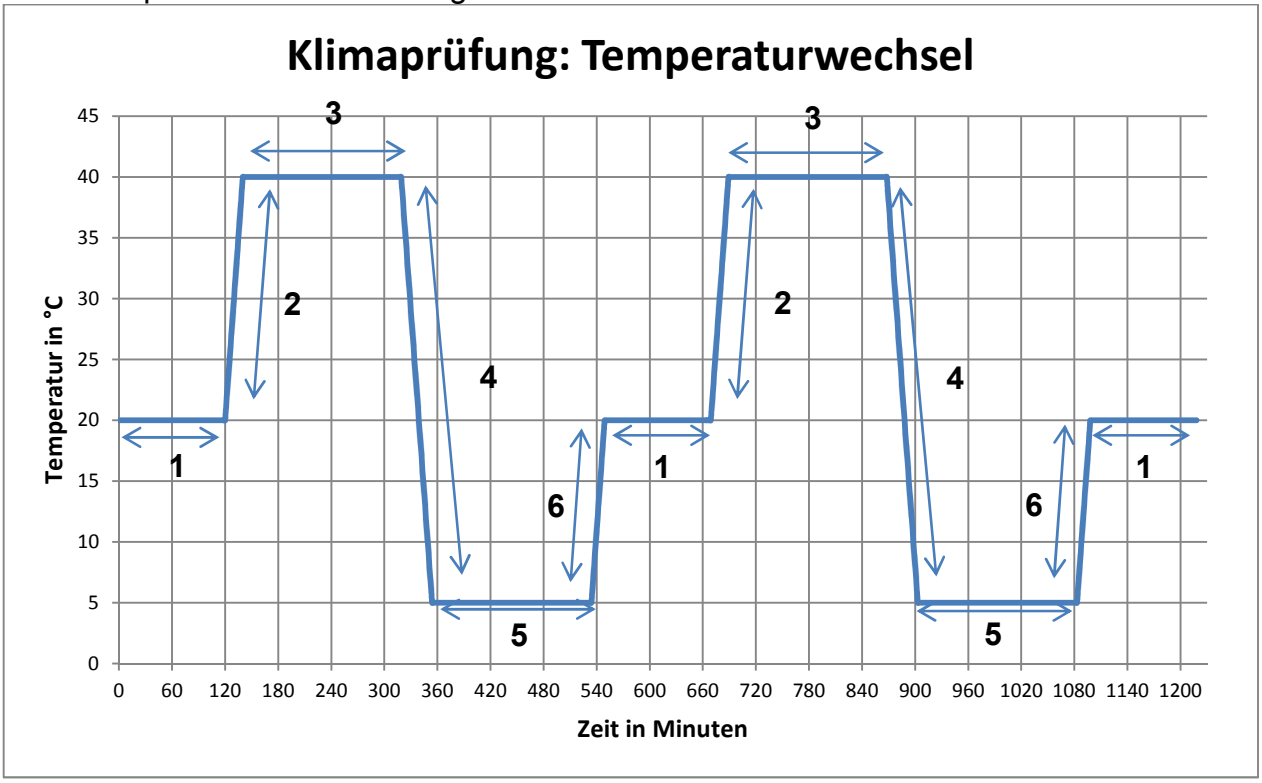

Abbildung 8: Temperaturverlauf der Prüfung Temperaturwechsel

1. 120 min bei 20 ± 5 °C verharren
2. Steigerung der Temperatur mit 1 °C/Minute bis zur höchsten vom Hersteller spezifizierten Temperatur, jedoch auf min. 40 ± 5 °C
3. 180 min bei höchster Temperatur verharren
4. Senkung der Temperatur mit 1 °C/Minute bis zur niedrigsten vom Hersteller spezifizierten Temperatur, jedoch auf min. 5 ± 5 °C
5. 180 min bei niedrigster Temperatur verharren
6. Steigerung der Temperatur mit 1 °C/Minute bis 20 ± 5 °C

Die Punkte 1-6 werden 2 Mal durchlaufen, abschließend wird Punkt 1 erneut durchlaufen (siehe Abbildung 8).

5.10 Schutz gegen elektrischen Schlag

Jedes geschlossene Betriebsmittel muss mindestens der Schutzart IP 2X nach DIN EN 60529-1 entsprechen.

Für offene Betriebsmittel wird die Einhaltung der IP 2X-Anforderungen nicht gefordert. Jedoch müssen Warnschilder, Gefahrensymbole nach IEC 60417 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.

5.11 Berührbarkeitsprüfungen

Berührbarkeitsprüfungen und Untersuchungen von Öffnungen sind nach DIN EN 61131-2 Abschnitten 12.1.2 und 12.1.3 durchzuführen.

Bei Geräten, die über flexible Leitungen angeschlossen werden und deren Versorgungsspannung nicht den Anforderungen von SELV oder PELV entspricht, muss der Ableitstrom mit den Grenzwerten, die in DIN EN 60950-1:2011-01 Abschnitt 5.1 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 DIN EN 61131-2 Anhang C
Messung von Ableitströmen DIN EN 60950-1:2011-01 Abschnitt 5.1

5.12 Isolationsfestigkeit

Komponenten von Sicherheitsbussystemen müssen gemäß DIN EN 61131-2 Abschnitt 11.2.2 ausreichend spannungsfest sein.

Prüfung: gemäß DIN EN 61131-2 Abschnitt 12.2.1.

5.13 IP-Schutzart

Die Betriebsmittel müssen so konstruiert sein, dass sie den am vorgesehenen Verwendungszweck üblicherweise auftretenden Umgebungsbedingungen standhalten können. Die Mindestschutzart ist grundsätzlich IP20.

Prüfung: Besichtigung und Schutzartprüfung gemäß DIN EN 60529.

5.14 Schutz gegen Umgehen auf einfache Weise

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

Prüfung: Besichtigung, Überprüfung auf Plausibilität

5.15 EMV-Anforderungen

Anforderungen zur Störaussendung werden in diesem Prüfgrundsatz nicht betrachtet.

Anforderungen zur Störfestigkeit:

Die Erfüllung der grundlegenden Störfestigkeitsanforderungen hat durch Nachweis der Störfestigkeit für Zone B nach DIN EN 61131-2 Abschnitt 8.3 zu erfolgen.

Die Erfüllung der erhöhten Störfestigkeitsanforderungen für sicherheitsbezogene Systeme hat durch Nachweis der Störfestigkeit nach DIN EN 61326-3-1 zu erfolgen.

Prüfung: Störfestigkeit nach DIN EN 61131-2 Abschnitt 8.3 und DIN EN 61326-3-1 prüfen.

	Maßnahmen pro Nachricht							
Fehler	Laufende Nummer	Zeitstempel	Zeiterwartung (Time Out)	Verbindungsauthentizität	Rückmeldung	Datensicherung	Redundanz mit Kreuzvergleich	
Nachrichten-verfälschung, Adressierung					X [d)]	X	X (nur bei seriellem Bus [c)])	
Wiederholung	X	X					X	
Falsche Abfolge	X	X					X	
Verlust	X						X	
Verzögerung		X	X [b)]					
Einfügung	X			X [a)]	X		X	
Maskerade				X	X			

a) Nur für die Senderidentifikation. Deckt nur die Einfügung einer ungültigen Quelle auf.
b) In allen Fällen erforderlich.
c) Diese Maßnahme ist nur dann mit einem qualitativ hochwertigen Datensicherungsmechanismus vergleichbar, wenn mit einer Rechnung nachgewiesen werden kann, dass im Falle des Versands von zwei Nachrichten über unabhängige Sende-/Empfangseinrichtungen die Restfehlerrate die geforderten Werte für den angestrebten Performance Level erreicht.
d) Nur dann wirksam, wenn die Rückmeldung Originaldaten oder Informationen über die Originaldaten enthält.

Tabelle 3: Übersicht über die Wirkung der einzelnen Maßnahmen auf die möglichen Fehler.

Anhang A

A.1 Beziehung zwischen PL und SIL

Tabelle A.1 gibt die Beziehung zwischen PL und SIL basierend auf der mittleren Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde an. Beide Normen (DIN EN ISO 13849 und DIN EN 61508) haben zusätzliche Anforderungen zu den Wahrscheinlichkeitsabschätzungen, die auch zur Abschätzung der sicherheitsbezogenen Steuerung angewendet werden. Die Schärfe der Anforderungen ist ähnlich (siehe Tabelle A.1).

Performance Level (PL)	Mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde (PFH_D)	Sicherheits-Integritätslevel (SIL)
a	$\geq 10^{-5}$ bis $< 10^{-4}$	keine Entsprechung
b	$\geq 3 \times 10^{-6}$ bis $< 10^{-5}$	1
c	$\geq 10^{-6}$ bis $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ bis $< 10^{-6}$	2
e	$\geq 10^{-8}$ bis $< 10^{-7}$	3

Tabelle A.1 Beziehung zwischen PL und SIL basierend auf der mittleren Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde

Anhang B

B.1 Messunsicherheiten

Nachfolgend die Tabelle aus der sektoralen Regel zur Messunsicherheit für das Sachgebiet Industrielle Niederspannung (DAkkS 71 SD 2 008).

Messgröße	Messunsicherheit (k=2)	Anmerkung
Spannung	± 2 mV für U ≤ 150 mV ± 1,5 % für 150 mV < U ≤ 100 V ± 3 % für 100 V < U ≤ 10 kV	5, 6
Strom	± 1,5 % für I ≤ 5 A ± 2,5 % für 5 A < I < 100 A ± 3 % für I ≥ 100 A ± 5 % für I ≥ 100 A (Kurzzeitströme bis 3 s) ± 3 % für I ≥ 100 A (Impulsströme z.B. 8/20 µs)	1, 6
Leistung	± 20 mW für S, P, Q ≤ 1 W ± 3 % für 1 W < S, P, Q ≤ 3 kW ± 5 % für S, P, Q > 3 kW	2, 6
Joule Integral	± 15 %	6
Leistungsfaktor	± 0,05 %	
Frequenz	± 0,2 % für f < 10 kHz	
Widerstand	± 5 % für R < 100 mΩ oder R > 1 MΩ ± 10 % bei Messungen des Isolationswiderstandes ± 1 % in allen anderen Fällen	
Temperatur	± 2° C für T ≤ 100° C ± 2 % 100° C < T ≤ 500° C ± 3 % für T > 500° C	3 Nicht im Zusammenhang bei der Messung von Feuchte
Relative Feuchtigkeit	± 5 % für 30 % < RH < 95 %	Dies bedingt eine Unsicherheit bei der Temperatur von ± 0,1° C
Zeit	± 5 % für 1 ms < t ≤ 200 ms ± 10 ms für 200 ms < t ≤ 1 s ± 1 % für t > 1 s	
Strecken, lineare Abmessungen	± 0,05 mm für 1 mm ≤ l ≤25 mm ± 0,25 % für l > 25 mm	
Masse	± 1 % für 10 g < M ≤ 100 g ± 2 % für M> 100 g	
Kraft	± 2 %	
Mechanische Energie	± 10 %	
Drehmoment	± 10 %	
Winkel	± 1 Grad	
Luftdruck	± 0,01 MPa	
Drucke von Gasen und Flüssigkeiten	± 5 %	4, bei statischen Messungen

Anmerkungen

1) Bei Erwärmungsprüfungen mit Wechselstrom müssen Echt-Effektivwert Messgeräte verwendet werden, es sei denn, der Strom ist frei von signifikanten Oberwellen.
2) Für Messungen der Leistung/Verlustleistung bei AC müssen Echteffektivwert anzeigende Messgeräte verwendet werden.
3) Wenn die Unsicherheit auf die von einem Thermoelement und damit verbundenem Anzeigeinstrument gemessene Temperatur angewendet wird, sollte beachtet werden, dass die größten Ungenauigkeiten durch die Leitungen des Thermoelementes auftreten (beachte IEC 584-1: 1989, IEC 584-2: 1989 und IEC 584-3: 1989). Für bestimmte Temperaturmessungen sollte von Laboratorien bevorzugt Material verwendet werden, das mit der Klasse 1 der IEC 584-2:1989 übereinstimmt.
4) Die erweiterte Messunsicherheit der Druckmessung durch Messinstrumente darf ± 5 % des Vollausschlages des Instrumentes nicht überschreiten. Die eigentliche Messung soll zwischen 10 % und 90 % des Vollausschlags vorgenommen werden.
5) Für Impulsspannungen siehe IEC 61180-1 und IEC 61180-2
6) Die geforderte Messunsicherheit ist für einen Frequenzbereich 0,1 x fn < f < 7 x fn, wobei fn die Bemessungsfrequenz der jeweiligen Prüfung ist.

Tabelle B.1: Sektorale Regel zur Messunsicherheit für das Sachgebiet Industrielle Niederspannung (DAkkS 71 SD 2 008)

Können die oben genannten Vorzugswerte nicht eingehalten werden, muss die Auswirkung der Messunsicherheit auf die Gültigkeit des Prüfergebnisses untersucht werden.

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.