GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

INDUSTRIAL RADIO.DE®

Aspekte der Zuverlässigkeits-bewertung in ZDKI

Fachgruppe 1

Anwendungen, Anforderungen und Validierung im BMBF-Förderprogramm „IKT 2020 – Zuverlässige drahtlose Kommunikation in der Industrie“ (BZKI)

Editor: Sarah Willmann
ifak e.V. Magdeburg
Version: 1.0 (02.06.2017)

Autoren
André Gnad, ifak e.V. Magdeburg
Elke Hintze, ifak e.V. Magdeburg
Marko Krätzig, ifak e.V. Magdeburg
Lutz Rauchhaupt, ifak e.V. Magdeburg

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter den Förderkennzeichen 16KIS0303 gefördert. Die Inhalte wurden im Rahmen der Arbeit der Fachgruppe 1 „Anwendungen, Anforderungen und Validierung“ im BMBF-Förderprogramm „IKT 2020 – Zuverlässige drahtlose Kommunikation in der Industrie“ (BZKI) mit Forschungspartnern erörtert.

Die Autoren bedanken sich bei allen Forschungspartnern, die mit ihren Kommentaren beigetragen haben diese Ausarbeitung zu vervollständigen und verständlich zu gestalten. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Inhaltsverzeichnis

		Seite
Autoren		2
Inhaltsverzeichnis		3
Abbildungsverzeichnis		5
Tabellenverzeichnis		5
1	**Zweck des Dokuments**	**6**
2	**Definitionen, Abkürzungen und Formelzeichen**	**6**
2.1	Definitionen	6
2.2	Abkürzungen und Formelzeichen	7
3	**Begriff Zuverlässigkeit**	**8**
3.1	Vorgehensweise	8
3.2	Allgemeine Definitionen	8
3.3	Technische Definitionen	8
3.4	Definition in der Telekommunikation	9
3.5	Fazit	10
4	**Leistungsmerkmale, Kenngrößen und Maßgrößen zur Bewertung der Zuverlässigkeit**	**10**
4.1	Allgemeines	10
4.2	Leistungsmerkmale	11
4.2.1	Verfügbarkeit	11
4.2.2	Funktionsfähigkeit	11
4.2.3	Wiederherstellbarkeit	11
4.2.4	Selbst-Wiederherstellbarkeit	12
4.2.5	Instandhaltbarkeit	12
4.2.6	Instandhaltungsbereitschaft	12
4.2.7	Haltbarkeit	12
4.2.8	Sicherheit	12
4.2.9	Dienstgüte	13
4.3	Allgemeine Zuverlässigkeitskenngrößen	13
4.3.1	Übersicht	13
4.3.2	Klarzeitintervall	14
4.3.3	Betriebszeitintervall	14
4.3.4	Unklarzeitintervall	14
4.3.5	Betriebszeit bis zum Ausfall	14
4.3.6	Ausfallabstand	14
4.3.7	Betriebszeit zwischen Ausfällen	15
4.3.8	Betriebszeit bis zum ersten Ausfall	15
4.3.9	Wiederanlaufzeit	15
4.4	Unterschiede und Beziehungen zwischen den Zuverlässigkeitskenngrößen	15
4.5	Allgemeine wahrscheinlichkeitstheoretische Maßgrößen	17
4.5.1	Verfügbarkeit	17
4.5.2	Überlebenswahrscheinlichkeit	18
4.5.3	Verteilungsfunktion der Klarzeit FU(t)	18
4.5.4	Komplement der Verteilungsfunktion der Klarzeit RU(t)/ Klarzeitüberlebens-funktion	18
4.5.5	Ausfallrate	18
4.5.6	Mittlere Betriebszeit bis zum Ausfall	19
4.5.7	Mittlere Betriebszeit zwischen Ausfällen	19
4.5.8	Mittlere Klardauer	19
4.5.9	Mittlere Unklardauer	19
4.6	Fazit	20
5	**Betrachtungsraum industrielle Funkkommunikation**	**20**
5.1	Betrachtungsraum	20
5.2	Logische Verbindung	22
5.2.1	Wesen und Funktion	22
5.2.2	Nachrichtentransformation	23
5.2.3	Kommunikationsfehler	25
5.3	Kommunikationsgerät	26
5.4	Physikalische Verbindung	28
5.5	Kommunikationssystem	28
5.6	Funktionsbeeinflussende Bedingungen	29
5.7	Fazit	30
6	**Leistungsmerkmale, Kenn- und Maßgrößen zur Bewertung der Zuverlässigkeit einer logischen Verbindung**	**30**

Seite

6.1 Relevante Leistungsmerkmale 30
6.2 Kenngrößen und deren wahrscheinlichkeitstheoretischen Maßgrößen 31
6.2.1 Klarzeitintervall 31
6.2.2 Betriebszeitintervall 32
6.2.3 Unklarzeitintervall 33
6.2.4 Betriebszeit bis zum Ausfall 33
6.2.5 Ausfallabstand 34
6.2.6 Betriebszeit zwischen Ausfällen 35
6.2.7 Wiederanlaufzeit 35
6.2.8 Übertragungszeit 36
6.2.9 Aktualisierungszeit 37
6.2.10 Antwortzeit 38
6.2.11 Anzahl korrekt empfangener Nachrichten 38
6.2.12 Anzahl inkorrekt empfangener Nachrichten 39
6.2.13 Anzahl empfangener Nachrichten unrechtmäßiger Herkunft 39
6.2.14 Anzahl verlorener Nachrichten 40
6.2.15 Ausfallrate 42
6.2.16 Nachrichtenfehlerquote 42
6.2.17 Nachrichtenverlustquote 42
6.2.18 Restfehlerquote 43
6.3 Leistungsmerkmale 44
6.3.1 Verfügbarkeit 44
6.3.2 Funktionsfähigkeit 44
6.4 Fazit 45

Seite

7 Leistungsmerkmale, Kenn- und Maßgrößen zur Bewertung der Zuverlässigkeit der anderen Betrachtungseinheiten 46
7.1 Allgemeines 46
7.2 Kommunikationsgerät 46
7.2.1 Allgemeines 46
7.2.2 Anzahl korrekt empfangener Pakete 48
7.2.3 Anzahl inkorrekt empfangener Pakete 49
7.2.4 Anzahl empfangener Pakete unrechtmäßiger Herkunft 50
7.2.5 Anzahl verlorener Pakete 50
7.2.6 Paketfehlerquote und Paketfehlerwahrscheinlichkeit 51
7.2.7 Paketverlustquote 51
7.2.8 Paketstörquote 51
7.3 Physikalische Verbindung 52
7.4 Kommunikationssystem 52
8 Zuverlässigkeitsbetrachtungen am Beispiel funktionaler Sicherheit 53
8.1 Motivation 53
8.2 Prinzipien für Sicherheitskommunikationssysteme 53
8.3 Sicherheits-Integritätslevel 54
8.4 Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde 55
9 Zusammenfassung 55
10 Quellen 57

Abbildungsverzeichnis

Seite

Abbildung 1: Zuverlässigkeit, Leistungsmerkmale und Maßgrößen 10
Abbildung 2: Zeitbegriffe zur Charakterisierung von Betrieb und Instandhaltung [2] 13
Abbildung 3: Zusammenhang zwischen Klarzeit, Betriebszeit, Wartezeit und Unklarzeit in Anlehnung an [18] 15
Abbildung 4: Zusammenhang zwischen Ausfallabstand, Betriebszeit, Betriebszeit bis zum ersten Ausfall und Betriebszeit zwischen Ausfällen 16
Abbildung 5: Systemzustände und deren Abbildung durch gemessene Kenngrößenwerte 16
Abbildung 6: Zusammenhang zwischen Störung, Unklarzeit und Wiederanlaufzeit 17
Abbildung 7: Leistungsmerkmale, Zuverlässigkeitskenngrößen und Maßgrößen der Zuverlässigkeit 20
Abbildung 8: Abstraktion des Betrachtungsraums industrieller Funkkommunikation 21
Abbildung 9: Logische Verbindung im Betrachtungsraum 22
Abbildung 10: Betrachtungseinheit „Logischen Verbindung“ 23
Abbildung 11: Übertragung einer Nachricht als Pakete und Bitströme 24
Abbildung 12: Betrachtungseinheit „Kommunikationsgerät“ 26
Abbildung 13: Betrachtungseinheit „Physikalische Verbindung“ 28
Abbildung 14: Betrachtungseinheit „Kommunikationssystem“ 29
Abbildung 15: Klarzeitintervall einer logischen Verbindung 31
Abbildung 16: Betriebszeitintervall einer logischen Verbindung 32
Abbildung 17: Unklarzeitintervall einer logischen Verbindung 33
Abbildung 18: Betriebszeit bis zum Ausfall einer logischen Verbindung 34
Abbildung 19: Ausfallabstand einer logischen Verbindung 35
Abbildung 20: Definition der Übertragungszeit 36
Abbildung 21: Definition der Aktualisierungszeit 37
Abbildung 22: Empfangen einer Nachricht unrechtmäßiger Herkunft 40
Abbildung 23: Beispiel: Nachrichten vor der Auswertung 41
Abbildung 24: Beispiel: Nachrichten nach der Auswertung 41
Abbildung 25: Mengen gesendeter, empfangener und verlorener Nachrichten 42
Abbildung 26: Auswirkungen von Paketfehler und Paketverlust 43
Abbildung 27: Unterschied zwischen hoher Funktionsfähigkeit (a) und hoher Verfügbarkeit (b) 45
Abbildung 28: Zuverlässigkeit, Leistungsmerkmale, Zuverlässigkeitskenngrößen und Maßgrößen 45
Abbildung 29: Zuverlässigkeit, Leistungsmerkmale, Zuverlässigkeitskenngrößen und Maßgrößen 47
Abbildung 30: Funktional sichere Kommunikation als Teil einer Safety-Funktion 55

Tabellenverzeichnis

Seite

Tabelle 1: Betrachtungseinheiten der Zuverlässigkeitsbewertung im ZDKI 30
Tabelle 2: Übersicht über Leistungsmerkmale der Zuverlässigkeit für eine logische Verbindung 31
Tabelle 3: Übersicht über Leistungsmerkmale der Zuverlässigkeit für ein Kommunikationsgerät 47
Tabelle 4: Übersicht über Leistungsmerkmale der Zuverlässigkeit für eine physikalische Verbindung 52
Tabelle 5: Übersicht über Leistungsmerkmale der Zuverlässigkeit für ein Kommunikationssystem 53
Tabelle 6: Überblick von Maßnahmen zur Erkennung von Kommunikationsfehlern [26] 54
Tabelle 7: Sicherheits-Integritätslevel: Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben wird [28] 54

1 Zweck des Dokuments

Im Verlauf der Arbeiten der Verbundvorhaben im BMBF-Förderprogramm „IKT 2020 – Zuverlässige drahtlose Kommunikation in der Industrie“ sowie bei Diskussionen in den Fachgruppen der Begleitforschung BZKI hat sich gezeigt, dass der Begriff Zuverlässigkeit nicht einheitlich interpretiert und angewendet wird. Da die Bewertung der Zuverlässigkeit der in diesem Förderprogramm zu erforschenden Funkkommunikationslösungen aber eine zentrale Rolle spielt, werden in diesem Dokument die Aspekte zuverlässiger drahtloser Kommunikation aufbereitet und damit den Verbundvorhaben zur einheitlichen Verwendung bereitgestellt.

Das vorliegende Dokument zeigt die Vielfalt an existierenden Normen, Richtlinien, Begriffsdefinitionen und Größen zur Bewertung der Zuverlässigkeit. Diese Vielfalt wird strukturiert und mit Blick auf die Kommunikation aus Sicht der Anwendung bewertet. Letztendlich wird das Ziel verfolgt, messbare Größen zu finden, mit denen die Zuverlässigkeit der Funkkommunikation quantitativ bewertet werden kann.

2 Definitionen, Abkürzungen und Formelzeichen

2.1 Definitionen

Datendurchsatz – data throughput
ist die Anzahl von Nutzdatenbytes oder Nutzdatenbits, die pro Zeiteinheit in einer Quelle von der Kommunikationsschnittstelle an die Anwendung übergeben werden.
[Quelle: [1], modfiziert]

…gehalt/…quote (in Zusammensetzungen) - …rate
Faktor, der gewöhnlich als Prozentsatz oder als Dezimalbruch wie ein Tausendstel oder ein Millionstel ausgedrückt wird.
[Quelle: IEV 112-03-19 [2]]

Kenngröße – Characteristic parameter
mathematischer Größe zur quantitativen Beschreibung von Eigenschaften und Zuständen

Nutzdatenlänge – User data length
Anzahl der atomaren Informationseinheit, die an der Bezugsschnittstelle ausgetauscht wird
[Quelle: [3], modifiziert]

Quote – Rate/Ratio
Anteil bzw. Verhältnisteil, der jeweils festgesetzt wird oder sich nach einer Verhältnisrechnung ergibt.
[Quelle: [4], modifiziert]

…rate (in Zusammensetzungen) - …rate
Quotient einer Größe bezogen auf einen Zeitraum
[Quelle: IEV 112-03-18 [2], modifiziert]

Resilienz – Resilience
Fähigkeit einer Betrachtungseinheit, auf selbstständig auf Störungen zu reagieren, das heißt nach einer Störung automatisch die geforderte Funktion wieder auszuführen und die Robustheit gegen die Störung zu verbessern

Sendezeitabstand – Transfer interval
Zeitdifferenz zwischen zwei aufeinanderfolgenden Übertragungen von Nutzdaten von der Automatisierungsfunktion über die Bezugsschnittstelle an die Funkübertragungsfunktion
[Quelle: [3]]

Statistische Maßgröße
statistischer Parameter einer Kenngröße, z. B. Mittelwert

Wahrscheinlichkeitstheoretische Maßgröße – Probabilistic measure
statistischer Parameter einer Zuverlässigkeitskenngröße, z. B. Erwartungswert

Zuverlässigkeitskenngröße – Dependability parameter
Kenngröße zur Quantifizierung der Zuverlässigkeit

2.2 Abkürzungen und Formelzeichen

A	Verfügbarkeit
$a_i(to)$	Verfügbarkeit im Betrachtungszeitraum
BER	Bitfehlerquote, Bitfehlerrate(veraltet)
BZ	Betriebszeit
c	Korrektheit
Co	Dateninhalt
CRC	Zyklische Redundanzprüfung (Cyclic Redundancy Code)
$E/E/PE$	elektrischen, elektronischen und programmierbaren elektronischen
IEV	Internationales Elektrotechnisches Vokabular
$M(O)TBF$	Betriebszeit zwischen Ausfällen
MDT	Mittlere Unklarzeit
MER	Nachrichtenfehlerquote
Me_{Rxi}	Empfangene Nachricht
$MTTF$	Mittlere Betriebszeit bis zum Ausfall
MUT	Mittlere Klarzeit
N_{AFP}	Anzahl empfangener Pakete unrechtmäßiger Herkunft
N_{AN}	Anzahl empfangener Nachrichten unrechtmäßiger Herkunft
N_D	Anzahl der Kommunikationsfehler im Betrachtungszeitraum
N_{Fx}	Anzahl inkorrekt empfangener Nachrichten
N_{LM}	Anzahl verlorener Nachrichten
N_{LP}	Anzahl verlorener Pakete
N_{RCP}	Anzahl korrekt empfangener Pakete
N_{RFP}	Anzahl inkorrekt empfangene Pakete
N_{RM}	Anzahl empfangener Nachrichten
N_{Rx}	Anzahl korrekt empfangener Nachrichten
N_{TP}	Anzahl gesendeter Pakete
N_{Tx}	Anzahl gesendeter Nachrichten
p	Bitfehlerwahrscheinlichkeit
p_E	Paketfehlerwahrscheinlichkeit
PER	Paketfehlerquote
PES	Programmierbares Elektronisches System
PFH	Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde Average (frequency of dangerous failure [h-1] per hour)
$plr_i(to)$	Paketverlustquote im Betrachtungszeitraum
P_{Ri}	Empfangene Pakete
R	Restfehlerwahrscheinlichkeit
$R(t)$	Überlebenswahrscheinlichkeitsfunktion
RII	Nachrichtenstörquote

RIL	Nachrichtenverlustquote
RPI	Paketstörquote
RPL	Paketverlustquote
SIL	Sicherheits-Integritätslevel (Safety Integrity Level)
SN	Sequenznummer
TBF	Betriebszeit zwischen Ausfällen
to	Betrachtungszeitraum
t_R	Antwortzeit
t_T	Übertragungszeit
$TTFF$	Betriebszeit bis zum ersten Ausfall
t_{TI}	Sendezeitabstand
T_{Tmax}	Grenzwert der Übertragungszeit
t_U	Zeit der fehlerfreien Datenübertragung
λ	Ausfallrate
Λ	Restfehlerquote
$\overline{\lambda}$	Mittlere Ausfallrate

3 Begriff Zuverlässigkeit

3.1 Vorgehensweise

Um das Wesen des Begriffes Zuverlässigkeit zu erfassen, wurde in unterschiedlichen nationalen und internationalen Quellen recherchiert. Nachfolgend werden allgemeine Definitionen, technische Definitionen und Definitionen bezogen auf die Kommunikation zitiert. Es zeigt sich, dass für unterschiedliche Fachdisziplinen eigene Definitionen entwickelt wurden. Übersetzungen von Definitionen können inhaltlich abweichen. Es folgt eine Auswahl relevanter Definitionen.

3.2 Allgemeine Definitionen

„Die Zuverlässigkeit ist eine Eigenschaft von Wesen, Objekten und Vorgängen, welche angibt, in welchem Maß die erwartete Qualität oder Handlungsweise erfüllt wird. Die Zuverlässigkeit muss ständig neu überprüft werden, da sich diese im Verlauf der Zeit ändern kann.“ [4]

„Die eigene Zuverlässigkeit lernt man erst schätzen, wenn man sich auf andere verlassen muss.“ [Italienisches Sprichwort]

„Wer in kleinsten Dingen zuverlässig ist, der ist es auch in den großen.“ [Lukas 16.10]

„Zuverlässigkeit kann auch darin bestehen, dass jemand regelmäßig versagt.“ [Amintore Fanfani]

3.3 Technische Definitionen

Zuverlässigkeit
„Fähigkeit zu funktionieren, wie und wann gefordert

Anmerkung 1: Zur Zuverlässigkeit gehören Verfügbarkeit, Funktionsfähigkeit, Wiederherstellbarkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft und in manchen Fällen weitere Merkmale wie Haltbarkeit und Sicherheit.

Anmerkung 2: Zuverlässigkeit ist ein Gattungsbegriff für zeitbezogene Qualitätsmerkmale einer Einheit.“
[Quelle: IEV 192-01-22 [2]]

Zuverlässigkeit
„ist ein zusammenfassender Ausdruck für Funktionszuverlässigkeit, Verfügbarkeit, Sicherheit, Instandhaltbarkeit.“
[Quelle: [6]]

Zuverlässigkeit
„ist die Beschaffenheit einer Einheit bezüglich ihrer Eignung, während oder nach vorgegebenen Zeitspannen bei vorgegebenen Anwendungsbedingungen die Zuverlässigkeitsforderung zu erfüllen."
[Quelle: [7]]

Zuverlässigkeit
„ist die Fähigkeit eines technischen Systems, innerhalb vorgegebener Grenzen und während einer bestimmten Zeitdauer den durch den Verwendungszweck bedingten Anforderungen zu genügen."
[Quelle: [8]]

Zuverlässigkeit
„Die Zuverlässigkeit eines technischen Produkts ist eine Eigenschaft – Verhaltensmerkmal –, die angibt, wie verlässlich eine dem Produkt zugewiesene Funktion in einem Zeitintervall erfüllt wird. Sie unterliegt einem stochastischen Prozess und kann qualitativ oder auch quantitativ (durch die Überlebenswahrscheinlichkeit) beschrieben werden – sie ist nicht unmittelbar messbar. Hiervon sind die so genannten deterministischen Eigenschaften (Merkmale) eines Produktes zu unterscheiden, welche direkt messbar sind (wie Gewicht, Abmessungen, Festigkeit, Farbe, elektrische und Wärmeleitfähigkeit)."
[Quelle: [9]]

Reliability
„The ability of an item to perform a required function under given conditions for a given time interval."
[Quelle: [10]]

Reliability
„The probability that an automated system can perform a required function under given conditions for a given time interval (t_1, t_2)"
[Quelle: [11]]

Zuverlässigkeit einer Betrachtungseinheit
„Fähigkeit einer Betrachtungseinheit, eine geforderte Funktion unter vorgegebenen Bedingungen während eines festgelegten Zeitintervalls zu erfüllen."
[Quelle: IEV 603-05-01 [2]]

Funktionszuverlässigkeit
„ist die Fähigkeit einer Betrachtungseinheit, eine geforderte Funktion unter gegebenen Bedingungen für ein gegebenes Zeitintervall zu erfüllen. Die Funktionszuverlässigkeit kann einerseits qualitativ beschrieben oder andererseits quantitativ als Überlebenswahrscheinlichkeit ermittelt werden."
[Quelle: [6]]

3.4 Definition in der Telekommunikation

In Bezug auf Telekommunikation bedeutet Zuverlässigkeit, dass Nachrichten mit einer angestrebten Quality of Service (QoS) übermittelt werden [12].

Folgend ein Auszug aus ITU-R, ITU-T und ETSI Empfehlungen.

Reliability
- „probability that a required performance is achieved"
- „is a figure of merit of performance"

[Quelle: [13]]

Reliability
„The probability that a product or system will perform as required for a specified period of time."
[Quelle: [14]]

Reliability
„ability of an item to perform a required function under stated conditions for a given time period

NOTE 1: It is generally assumed that the item is in a state to perform this required function at the beginning of the time interval."
[Quelle: [15]]

Reliability (%)
„The amount of sent network layer packets successfully delivered to a given node within the time constraint required by the targeted service, divided by the total number of sent network layer packets."
[Quelle: [16]]

3.5 Fazit

Die hier zusammengetragenen Begriffsdefinitionen stellen eine Auswahl dar, die aber bereits folgende Schlussfolgerungen zulässt:

1. Der Begriff Zuverlässigkeit bezeichnet keine Kenngröße, die gemessen oder berechnet werden kann. Es handelt sich vielmehr um einen Gattungsbegriff. Er fasst verschiedene Leistungsmerkmale zusammen, die je nach Kontext mithilfe verschiedener Kenngrößen quantifiziert werden können.

2. Zuverlässigkeitskenngrößen beschreiben nicht nur den Anteil fehlerfreier Funktion, sondern auch die Bereitschaft zur Funktion sowie die Fähigkeit zur Erhaltung bzw. zur Wiederherstellung der Funktion.

3. Zuverlässigkeitskenngrößen sind Zufallsgrößen, die stochastische Prozesse beschreiben. Demzufolge sind zu deren Charakterisierung die Mittel der Stochastik bzw. der mathematischen Statistik anzuwenden.

Die zweite Schlussfolgerung macht deutlich, dass Zuverlässigkeitskenngrößen nicht nur für die statische Bewertung eines Systems geeignet sind, sondern auch zur Bewertung von Betriebszuständen und den Möglichkeiten zur Erhaltung oder Wiederherstellung der fehlerfreien Funktion. Das macht die Zuverlässigkeitskenngrößen zu einem entscheidenden Bestandteil beim Entwurf resilienter Systeme.

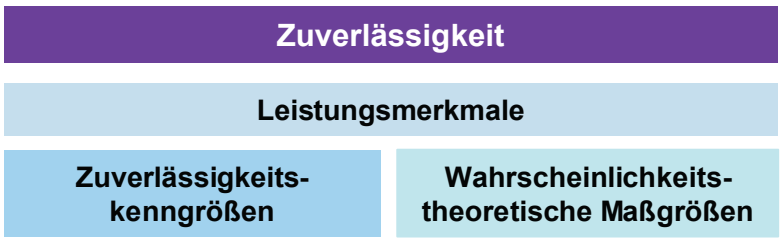


Abbildung 1: Zuverlässigkeit, Leistungsmerkmale und Maßgrößen

In Abbildung 1 ist die Klassifizierung nach Leistungsmerkmalen, Kenngrößen und Maßgrößen der Zuverlässigkeit in Anlehnung an [18] S. 91 erfolgt.

Im folgenden Kapitel werden als Grundlage zum einheitlichen Verständnis Leistungsmerkmale, Kenn- und Maßgrößen zur Bewertung der Zuverlässigkeit beschrieben.

4 Leistungsmerkmale, Kenngrößen und Maßgrößen zur Bewertung der Zuverlässigkeit

4.1 Allgemeines

In diesem Kapitel sind relevante Leistungsmerkmale, Kenn- und Maßgrößen zur Bewertung der Zuverlässigkeit aus der Literatur zusammengetragen. Die verwendeten Begriffe sind nicht durchgängig konsistent, da es sich um Zitate aus verschiedenen Quellen handelt. Die Zitate wurden in diesem Kapitel bewusst nicht angepasst. Erst bei der Anwendung der Begriffe auf die Betrachtungseinheiten der Kommunikation in den Kapiteln 6 und 7 wird auf eine Vereinheitlichung geachtet.

4.2 Leistungsmerkmale

4.2.1 Verfügbarkeit

Verfügbarkeit – Availiability
„Fähigkeit, in einem wie geforderten funktionsfähigen Zustand zu sein

Anmerkung 1: Verfügbarkeit hängt von den kombinierten Merkmalen der Funktionsfähigkeit, Wiederherstellbarkeit, und Instandhaltbarkeit der Einheit sowie der Instandsetzungsbereitschaft ab.

Anmerkung 2: Die Verfügbarkeit kann anhand geeigneter Messgrößen quantifiziert werden, siehe Abschnitt 192-08 aus [2]“
[Quelle: IEV 192-01-23 [2]]

Availiability
„Availability of an item to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval, assuming that the external resources, if required, are provided.“
[Quelle: Definition 3.1.1.5.4 [19]]

4.2.2 Funktionsfähigkeit

Funktionsfähigkeit – Reliability
„Fähigkeit, unter gegebenen Bedingungen und für ein gegebenes Zeitintervall wie gefordert ohne Ausfall zu funktionieren

Anmerkung 1: Die Dauer des Zeitintervalls kann in Maßeinheiten ausgedrückt werden, die für das betreffende Objekt angebracht sind, beispielsweise Kalenderzeit, Betriebszyklen, zurückgelegte Entfernungen usw. Die Einheiten sollten dabei immer eindeutig angegeben werden.

Anmerkung 2: Zu den gegebenen Bedingungen gehören auch Gesichtspunkte, die sich auf die Funktionsfähigkeit auswirken, wie etwa: Betriebsart, Beanspruchungsniveaus, Umweltbedingungen und Instandhaltung.

Anmerkung 3: Die Funktionsfähigkeit kann anhand von Messgrößen quantifiziert werden, siehe Abschnitt 192-05 aus [2]

Nationale Fußnote: Wenn eine Verwechselung mit den Komponenten der Zuverlässigkeit außer der Funktionsfähigkeit ausgeschlossen ist, kann „reliability“ auch mit „Zuverlässigkeit“ ins Deutsche übersetzt werden.“
[Quelle: IEV 192-01-24 [2]]
Ähnliche Beiträge: IEV 312-07-06, IEV 395-07-131

4.2.3 Wiederherstellbarkeit

Wiederherstellbarkeit – Recoverability
„Fähigkeit, nach einem Ausfall wieder ohne Instandsetzung funktionsfähig zu werden

Anmerkung 1: Die Fähigkeit der Wiederherstellbarkeit kann gegebenenfalls externer Maßnahmen bedürfen. Sofern keine externen Maßnahmen erforderlich sind, wird auf die Selbstwiederherstellbarkeit (192-01-26) verwiesen.

Anmerkung 2: Wiederherstellbarkeit kann anhand von Messgrößen quantifiziert werden, etwa durch die Wahrscheinlichkeit, sich innerhalb eines festgelegten Intervalls zu erholen.“
[Quelle: IEV 192-01-25 [2]]

4.2.4 Selbst-Wiederherstellbarkeit

Selbst-Wiederherstellbarkeit – Self-recoverability
„Fähigkeit, nach einem Ausfall ohne externe Maßnahmen wieder funktionsfähig zu werden

Anmerkung: Die Selbst-Wiederherstellbarkeit ist ein Sonderfall der Wiederherstellbarkeit (192-01-25)“
[Quelle: IEV 192-01-26 [2]]

4.2.5 Instandhaltbarkeit

Instandhaltbarkeit – Maintainability
„Fähigkeit, unter gegebenen Anwendungs- und Instandhaltungsbedingungen in einem wie geforderten funktionsfähigen Zustand erhalten bzw. in ihn zurückversetzt werden zu können

Anmerkung 1: Zu den gegebenen Bedingungen gehören Gesichtspunkte mit Auswirkungen auf die Instandhaltbarkeit, wie etwa: Ort der Instandhaltung, Zugänglichkeit, Instandhaltungsverfahren und Instandhaltungsmittel.

Anmerkung 2: Instandhaltbarkeit kann anhand von Messgrößen quantifiziert werden, siehe Abschnitt 192-07 aus [2]“
[Quelle: IEV 192-01-27 [2]]

4.2.6 Instandhaltungsbereitschaft

Instandhaltungsbereitschaft –
Maintenance support performance
„Fähigkeit einer Organisation, eine Instandhaltungsunterstützung bereitzuhalten

Anmerkung: Instandhaltungsbereitschaft kann anhand von Messgrößen quantifiziert werden, siehe Abschnitt 192-07 aus [2]“
[Quelle: IEV 192-01-29 [2]]

4.2.7 Haltbarkeit

Haltbarkeit – Durability
„Fähigkeit, unter gegebenen Anwendungs- und Instandhaltungsbedingungen bis zum Ende der Brauchbarkeitsdauer wie gefordert zu funktionieren“
[Quelle: IEV 192-01-21 [2]]

4.2.8 Sicherheit

Sicherheit – Security/Safety
„Freiheit von unvertretbarem Risiko eines von den betrachteten sicherheitsrelevanten Systemen ausgehenden außerhalb derselben auftretenden Schadens

Anmerkung 1: Die zur mit anderen Wörtern kombinierten Benennung „Sicherheit“ gehörenden Begriffsbestimmungen können teilweise […] oder vollständig (wie in „Arbeitssicherheit“, „Sicherheitsgurt“ oder „funktionale Sicherheit“) variieren.[…]

Anmerkung 2: In der Normung wird im Allgemeinen die Sicherheit von Produkten, Prozessen und Dienstleistungen im Hinblick auf die Erzielung eines optimalen Ausgleichs einer Anzahl von Faktoren betrachtet, wobei auch nichttechnische Faktoren wie menschliches Verhalten eingeschlossen sind und vermeidbare Schadensrisiken für Personen und Güter auf ein vertretbares Ausmaß vermindert werden.“
[Quelle: IEV 351-57-05 [2]]

Informationssicherheit – Information security

„The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."
[Quelle: [40]]

Funktionale Sicherheit – Functional safety

„Teil der Gesamtsicherheit, der davon abhängig ist, dass ein System oder ein Betriebsmittel korrekte Antworten auf ihre Eingangszustände liefert"
[Quelle: IEV 351-57-06 [2]]

4.2.9 Dienstgüte

Dienstgüte – Quality of service

„Gesamteindruck der Merkmale der Qualität eines Dienstes, der die Zufriedenheit eines Nutzers mit dem Dienst bestimmt

Anmerkung: Diese Merkmale können sich zum Beispiel auf Übertragungsgüte, Wähltonverzug, Ausfälle, Fehlerzustandshäufigkeit und -dauer beziehen."
[Quelle: IEV 715-07-14 [2]]

4.3 Allgemeine Zuverlässigkeitskenngrößen

4.3.1 Übersicht

In Abbildung 2 ist der Zusammenhang wesentlicher Zeitbegriffe für die Charakterisierung von Betrieb und Wartung von Betrachtungseinheiten dargestellt. Einige dieser Begriffe sind nachfolgend definiert, da sie als Zuverlässigkeitskenngrößen verwendet werden können.

<table>
<tr><td colspan="8">ZEITEN UND DAUERN</td></tr>
<tr><td colspan="4">Klarzeit(intervall) (192-02-02)</td><td colspan="4">Unklarzeit(intervall) (192-02-21)</td></tr>
<tr><td colspan="3">Betriebsbereites Zeitintervall (192-02-17)</td><td>Nichtverfügbarkeitszeit (intervall) (192-02-19)</td><td>Betriebsbereites Zeitintervall (192-02-17)</td><td colspan="3">Nichtverfügbarkeitszeit(intervall) (192-02-19)</td></tr>
<tr><td rowspan="3">Betriebszeitintervall (192-02-05)</td><td colspan="3">Nichtbetriebszeitintervall (192-02-07)</td><td>Betriebszeitintervall (192-02-05)</td><td colspan="3">Nichtbetriebszeitintervall (192-02-07)</td></tr>
<tr><td rowspan="2">Zeitintervall des betriebsfreien Zustands (192-02-15)</td><td rowspan="2">Zeitintervall des Stand-by-Zustands (192-02-13)</td><td rowspan="2">Extern bedingte(s) Nichtverfügbarkeitszeit (intervall) (192-02-24)</td><td rowspan="2">Wartungsdauer (192-07-05)</td><td colspan="3">Dauer der Wiederherstellung (192-07-06)</td></tr>
<tr><td>Instandsetzungsdauer (192-07-07)</td><td rowspan="2">Fehlerzustandserkennungs-dauer (192-07-11)</td><td rowspan="2">Administrative Verzugsdauer (192-07-12)</td></tr>
<tr><td colspan="4">Instandhaltungsdauer (192-07-02)</td></tr>
</table>

Anmerkung 1: Alle in diesem Bild genannten Zeiten sind Zeitintervalle oder aufeinanderfolgende Zeitintervalle.

Abbildung 2: Zeitbegriffe zur Charakterisierung von Betrieb und Instandhaltung [2]

4.3.2 Klarzeitintervall

Klarzeitintervall/Klarzeit – Up time
„Zeitintervall, während dessen eine Einheit im betriebsfähigen Zustand ist."
[Quelle: IEV 192-02-02 [2]]

4.3.3 Betriebszeitintervall

Betriebszeitintervall/Betriebszeit – Operating time
„Zeitintervall, während dessen eine Einheit in Betrieb ist.

Anmerkung: Die Dauer der Betriebszeit kann in verschiedenen, der Einheit gemäßen Maßeinheit ausgedrückt werden, beispielsweise Kalenderzeit, Betriebszyklen, zurückgelegte Entfernung usw. Die Maßeinheiten sollten eindeutig angegeben werden."
[Quelle: IEV 192-02-05 [2]]

4.3.4 Unklarzeitintervall

Unklarzeitintervall/Unklarzeit – Down time
„Zeitintervall, während dessen eine Einheit in einem Unklarzustand ist

Anmerkung: Unklarzeitintervall schließt das Zeitintervall der Nichtverfügbarkeit infolge Fehlens externer Ressourcen aus, allerdings schließt es die Instandhaltungsdauer ein."
[Quelle: IEV 192-02-21 [2]]

4.3.5 Betriebszeit bis zum Ausfall

Betriebszeit/Dauer bis zum Ausfall – Operating time to failure
„akkumulierte Betriebszeit ab Anwendungsbeginn oder ab Wiederherstellung bis zum Ausfall

Anmerkung: siehe auch Betriebszeit(intervall) (192-02-05)"
[Quelle: IEV 192-05-01 [2]]

4.3.6 Ausfallabstand

Ausfallabstand – Time between failures
„Dauer zwischen aufeinanderfolgenden Ausfällen

Anmerkung: Zum Ausfallabstand gehören die Klar- und Unklarzeitintervalle"
[Quelle: IEV 192-05-03 [2]]

4.3.7 Betriebszeit zwischen Ausfällen

Betriebszeit zwischen Ausfällen – Operating time between failures
„Akkumulierte Betriebszeit zwischen aufeinanderfolgenden Ausfällen

Anmerkung: Die Betriebszeit zwischen Ausfällen ist ein Sonderfall der Dauer bis zum Ausfall (192 05 01), nur anwendbar auf instandsetzbare Einheiten“
[Quelle: IEV 192-05-04 [2]]

4.3.8 Betriebszeit bis zum ersten Ausfall

Betriebszeit/Dauer bis zum ersten Ausfall – Operating time to first failure
„akkumulierte Betriebszeit ab Anwendungsbeginn bis zum Ausfall

Anmerkung 1: Die Dauer bis zum ersten Ausfall ist ein Sonderfall der Betriebszeit bis zum Ausfall

Anmerkung 2: Bei nicht instandsetzbaren Einheiten ist die Dauer bis zum ersten Ausfall gleich der Dauer bis zum Ausfall“
[Quelle: IEV 192-05-02 [2]]

4.3.9 Wiederanlaufzeit

Wiederanlaufzeit (in der Fernwirktechnik) – Restart time
„Dauer, die ein Fernwirksystem benötigt, um nach einem Netzausfall wieder voll betriebsfähig zu werden“
[Quelle: IEV 371-08-22 [2]]

4.4 Unterschiede und Beziehungen zwischen den Zuverlässigkeitskenngrößen

Folgende Abbildungen sollen der besseren Unterscheidung der Kenngrößen und deren Beziehungen dienen. In Abbildung 3 sind Klarzeit, Betriebszeit und Unklarzeit dargestellt. Der Klarzustand umfasst einen aktiven Zustand, den Betriebszustand, und einen inaktiven Zustand, den Wartezustand. Demzufolge können innerhalb der Klarzeit Betriebszeiten einer Betrachtungseinheit durch eine Wartezeit getrennt sein. Tritt eine Fehlfunktion auf, wechselt die Betrachtungseinheit vom Klarzustand in den Unklarzustand bis der Klarzustand durch Instandsetzung oder Wiederanlauf wiederhergestellt ist.

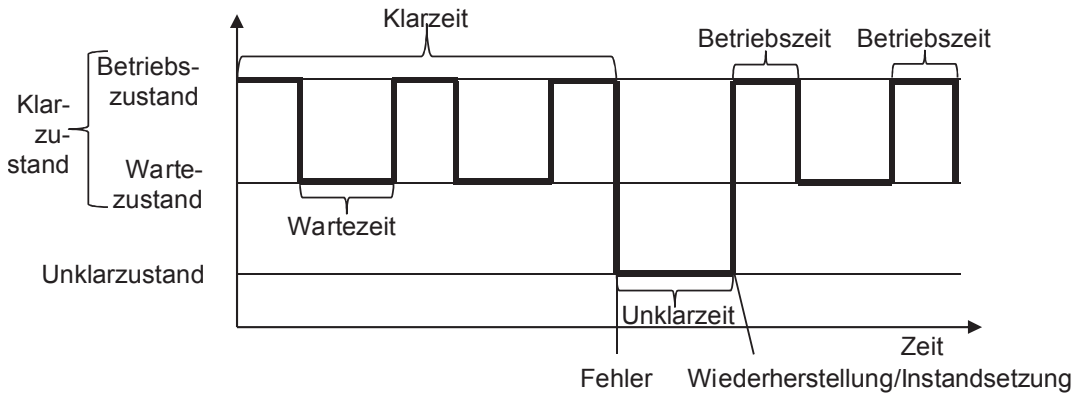


Abbildung 3: Zusammenhang zwischen Klarzeit, Betriebszeit, Wartezeit und Unklarzeit in Anlehnung an [18]

In Abbildung 4 ist der Ausfallabstand dargestellt. Die Betriebszeit (*BZ*) bis zum ersten Ausfall (*TTFF*) ergibt sich aus der Summe aller Betriebszeiten bis zum ersten Ausfall, das heißt die Betriebszeiten der ersten Klarzeit. Die Betriebszeit zwischen Ausfällen (*TBF*) ergibt sich aus der Summe der einzelnen Betriebszeiten zwischen zwei Ausfällen, das heißt die Betriebszeiten innerhalb eines Ausfallabstandes.

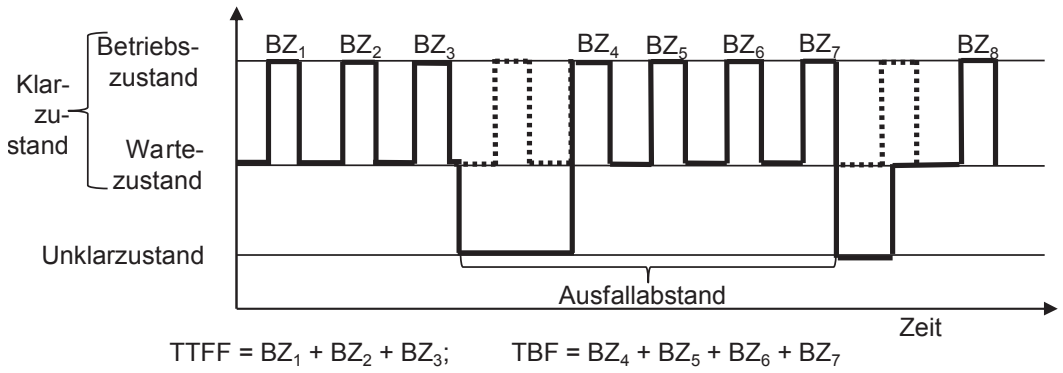


Abbildung 4: Zusammenhang zwischen Ausfallabstand, Betriebszeit, Betriebszeit bis zum ersten Ausfall und Betriebszeit zwischen Ausfällen

Es ist möglich, dass ein Ausfall im Wartezustand messtechnisch nicht sofort erfasst werden kann. Der Unklarzustand wird dann erst wahrgenommen, wenn ein erwarteter Betrieb nicht eintritt. Dieser Fall ist in Abbildung 5 dargestellt.

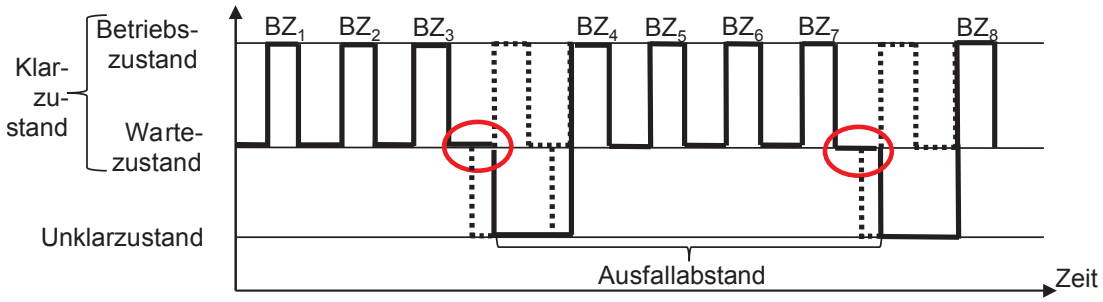


Abbildung 5: Systemzustände und deren Abbildung durch gemessene Kenngrößenwerte

Die Wiederanlaufzeit (*WZ*) ist Teil der Unklarzeit. Es ist die Zeitspanne die benötigt wird, um nach einer Störung den Klarzustand wiederherzustellen (siehe Abbildung 6).

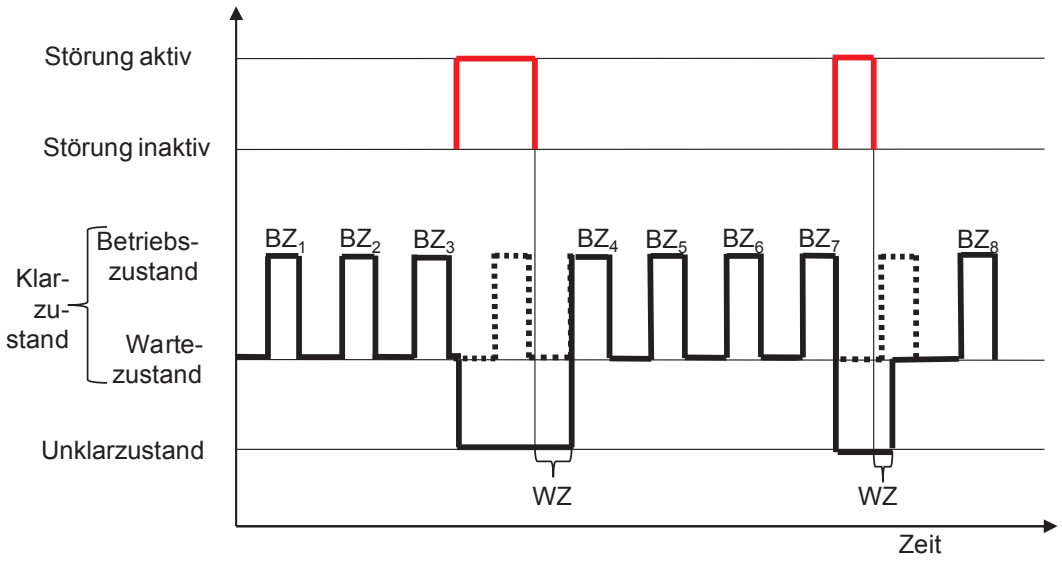


Abbildung 6: Zusammenhang zwischen Störung, Unklarzeit und Wiederanlaufzeit

4.5 Allgemeine wahrscheinlichkeitstheoretische Maßgrößen

4.5.1 Verfügbarkeit

Momentane Verfügbarkeit – Instantaneous availability

„Wahrscheinlichkeit, eine Einheit zu einem gegebenen Zeitpunkt in einem wie geforderten funktionsfähigen Zustand anzutreffen“

[Quelle: IEV 192-08-01 [2]]

Inhärente Verfügbarkeit – Inherent availability

„Verfügbarkeit aufgrund des Entwurfs unter idealen Betriebs- und Instandhaltungsbedingungen“

[Quelle: IEV 192-08-02 [2]]

Betriebliche Verfügbarkeit – Operational availability

„unter reellen Betriebs- und Instandhaltungsbedingungen erhaltene Verfügbarkeit“

[Quelle: IEV 192-08-03 [2]]

Mittlere Verfügbarkeit – Mean/Average availability

„Mittelwert der momentanen Verfügbarkeit während eines gegebenen Zeitintervalls (t_1, t_2)

Anmerkung: Die mittlere Verfügbarkeit steht mit der momentanen Verfügbarkeit $A(t)$ in folgender Beziehung:

$$\overline{A}(t_1, t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(t)dt \qquad (1)$$

[Quelle: IEV 192-08-05 [2]]

4.5.2 Überlebenswahrscheinlichkeit

Überlebenswahrscheinlichkeit – Reliability
„Wahrscheinlichkeit, eine geforderte Funktion unter gegebenen Bedingungen für das Zeitintervall (t_1, t_2) zu erfüllen

Anmerkung 1: Zu den gegebenen Bedingungen gehören Gesichtspunkte, die sich auf die Funktionsfähigkeit (Zuverlässigkeit) auswirken, also etwa: Betriebsart, Beanspruchungsniveau, Umgebungsbedingungen und Instandhaltung, soweit zutreffend.

Anmerkung 2: Es wird üblicherweise davon ausgegangen, dass sich die Einheit zu Beginn des Zeitintervalls in einem wie geforderten funktionsfähigen Zustand befindet.

Anmerkung 3: Falls $t_1 = 0$ und $t_2 = t$, verkürzt sich $R(0,t)$ zu $R(t)$ und wird als Überlebenswahrscheinlichkeitsfunktion bezeichnet. Siehe IEC 61703, Mathematical expressions for reliability, availibility, maintainability and maintenance support terms zu weiteren Einzelheiten

Anmerkung 4: Siehe auch Funktionsfähigkeit, <einer Einheit> (192-01-24)“
[Quelle: IEV 192-05-05 [2]]

Überlebenswahrscheinlichkeitsfunktion $R(t)$ – reliability function
Wahrscheinlichkeit zur Funktionserfüllung bis zur Zeit t, wobei $R(t) = R(t_1, t_2)$ für $t_1 = 0$ und $t_2 = t$ [17]

4.5.3 Verteilungsfunktion der Klarzeit $F_U(t)$

Verteilungsfunktion der Klarzeit $F_U(t)$ – Up time distribution function
Funktion, die jedem Wert t die Wahrscheinlichkeit zuordnet, dass die Dauer eines Klarzeitintervalls kleiner oder gleich t ist [17]

4.5.4 Komplement der Verteilungsfunktion der Klarzeit $R_U(t)$/ Klarzeitüberlebensfunktion

Komplement der Verteilungsfunktion der Klarzeit $R_U(t)$/ Klarzeitüberlebensfunktion – complement of the up time distribution function
Funktion, die jedem Wert t die Wahrscheinlichkeit zuordnet, dass die Dauer eines Klarzeitintervalls größer t ist.

Anmerkung 1: $R_U(t) = 1 - F_U(t)$

Anmerkung 2 – falls die Dauern der Klarzeitintervalle exponentiell verteilt sind: $R_U(t) = e^{\frac{-t}{MUT}}$

wobei MUT die mittlere Klardauer ist. [17]

4.5.5 Ausfallrate

(Momentane) Ausfallrate – (Instantaneous) failure rate
„Grenzwert – falls er existiert – des Quotienten der bedingten Wahrscheinlichkeit, dass der Zeitpunkt des Ausfalls einer nicht instandsetzbaren Einheit in ein Zeitintervall (t, $t + \Delta t$) fällt, sofern Δt gegen Null geht, vorausgesetzt, dass sich der Ausfall nicht im Zeitintervall (0,t) ereignet hat.

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{1}{\Delta t} \frac{F(t+\Delta t) - F(t)}{R(t)} = \frac{f(t)}{R(t)} \quad (2)$$

Hierbei sind $F(t)$ und $f(t)$ jeweils die Verteilungsfunktion bzw. die Wahrscheinlichkeitsdichte zum Ausfallzeitpunkt und $R(t)$ ist die Überlebenswahrscheinlichkeitsfunktion $R(t_1, t_2)$ bei $R(t) = R(0,t)$

Anmerkung: Zur Bezeichnung der Ausfallrate werden im Englischen weitere Benennungen verwendet: ‚hazard function', ‚hazard rate' und ‚force of morality'"
[Quelle: IEV 192-05-06 [2]]

Mittlere Ausfallrate – Mean/Average failure rate
„Mittelwert der momentanen Ausfallrate während eines gegebenen Zeitintervalls (t_1, t_2)
[Quelle: IEV 192-05-07 [2]]

$$\bar{\lambda}(t_1, t_2) = \frac{1}{t_1 - t_2} \int_{t_1}^{t_2} \lambda(t) dt \qquad (3)$$

4.5.6 Mittlere Betriebszeit bis zum Ausfall

Mittlere Betriebszeit bis zum Ausfall –
Mean operating time to failure (*MTTF*)
„Erwartungswert der Verteilung der Dauern bis zum Ausfall

Anmerkung 1: Im Falle von nicht instandsetzbaren Einheiten mit exponentiell verteilter Dauer bis zum Ausfall (d. h. konstanter Ausfallrate) ist die *MTTF* numerisch gleich dem Reziprokwert der Ausfallrate. Das ist auch für reparierbare Einheiten zutreffend, wenn sie nach ihrer Wiederherstellung als „so-gut-wie-neu" (en: as-good-as-new) betrachtet werden können.

Anmerkung 2: Siehe auch Betriebszeit bis zum Ausfall (IEV 192-05-01 [2])"
[Quelle: IEV 192-05-11 [2]]

4.5.7 Mittlere Betriebszeit zwischen Ausfällen

Mittlere Betriebszeit zwischen Ausfällen –
Mean operating time between failures (*MTBF, MOTBF*)
„Erwartungswert der Verteilung der Betriebszeit zwischen Ausfällen

Anmerkung: Der Begriff „mittlere Betriebszeit zwischen Ausfällen" sollte nur auf instandsetzbare Einheiten angewendet werden."
[Quelle: IEV 192-05-13 [2]]

4.5.8 Mittlere Klardauer

Mittlere Klardauer – Mean up time (*MUT*)
„Erwartungswert der Verteilung der Dauern der Klarzeitintervalle"
[Quelle: IEV 192-08-09 [2]]

4.5.9 Mittlere Unklardauer

Mittlere Unklardauer – Mean down time (*MDT*)
„Erwartungswert der Verteilung der Dauern der Unklarzeitintervalle"
[Quelle: IEV 192-08-10 [2]]

4.6 Fazit

Mit den in diesem Kapitel beschriebenen Begriffen lässt sich Abbildung 1 konkretisieren. Abbildung 7 zeigt die Zuordnung einer Auswahl der Leistungsmerkmale, Kenngrößen und Maßgrößen der Zuverlässigkeit in Anlehnung an [18] S. 91.

Zuverlässigkeit			
Leistungsmerkmale	Verfügbarkeit	Funktionsfähigkeit	Wiederherstellbarkeit
	Sicherheit	Selbstwiederherstellbarkeit	Dienstgüte
Allgemeine Zuverlässigkeits-kenngrößen	Klarzeit	Unklarzeit	BZ bis zum ersten Ausfall
	Betriebszeit bis zum Ausfall		Betriebszeit zwischen Ausfällen
	Ausfallabstand		Wiederanlaufzeit
Allgemeine wahrscheinlichkeits-theoretische Maßgrößen	Mittlere BZ bis zum Ausfall		Mittlere BZ zwischen Ausfällen
	Überlebenswahrscheinlichkeit		momentane Ausfallrate
	mittlere Ausfallrate	mittlere Klardauer	mittlere Unklardauer

BZ - Betriebszeit; AZ – Anzahl; N - Nachrichten

Abbildung 7: Leistungsmerkmale, Zuverlässigkeitskenngrößen und Maßgrößen der Zuverlässigkeit

5 Betrachtungsraum industrielle Funkkommunikation

5.1 Betrachtungsraum

Um den Zuverlässigkeitsbegriff auf die drahtlose Kommunikation in der Industrie anzuwenden, soll die Definition des Betrachtungsraumes der industriellen Funkkommunikation nach [20] zugrunde gelegt werden (siehe Abbildung 8).

Ausgangspunkt ist, dass zwischen örtlich verteilten Anwendungsfunktionen einer industriellen Automatisierungsanwendung Nachrichten zu übertragen sind. Dafür werden die Nachrichten an einer Schnittstelle zwischen Anwendungssystem und Funkkommunikationssystem ausgetauscht. Diese Schnittstelle heißt Bezugsschnittstelle, da sich geforderte und zugesicherte Werte für Kenngrößen, die die Verhaltenseigenschaften der Funkkommunikation beschreiben, auf diese Schnittstelle beziehen. Zu diesen Kenngrößen gehören Zuverlässigkeitskenngrößen der industriellen Funkkommunikation, die in Anlehnung an die in Kapitel 4 aufgeführten Kenngrößen in Kapitel 6 für eine logische Verbindung definiert werden.

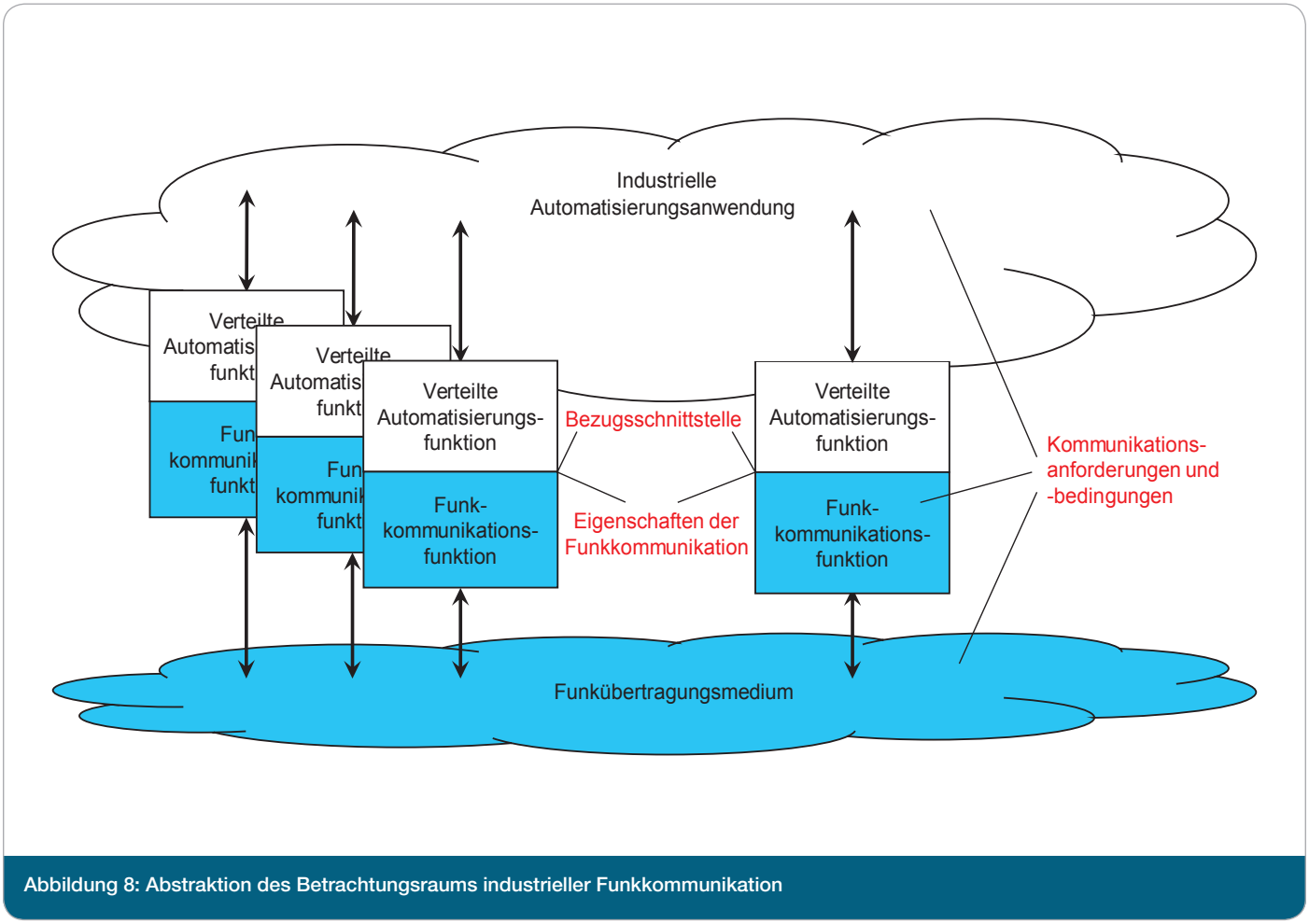


Abbildung 8: Abstraktion des Betrachtungsraums industrieller Funkkommunikation

Die Bedingungen, die das Verhalten der Funkkommunikation beeinflussen, werden bestimmt von

- Kommunikationsanforderungen der Anwendung (z. B. Länge der Nachricht),
- Eigenschaften des Kommunikationssystems (z. B. Ausgangsleistung eines Senders) und
- Übertragungsbedingungen des Mediums (z. B. Signaländerung durch Mehrwegeausbreitung).

Der in Abbildung 8 dargestellte Betrachtungsraum repräsentiert die allgemeine Sicht eines Industrieanwenders von Funkkommunikationssystemen.

Soll eine Zuverlässigkeitsbewertung vorgenommen werden, sind, gemäß der Definition des Zuverlässigkeitsbegriffs, eine Betrachtungseinheit, deren Funktion und die Bedingungen zu spezifizieren, unter denen die Funktion zu erbringen ist. Dementsprechend werden diese Aspekte im Folgenden für relevante Betrachtungseinheiten diskutiert.

Allgemeine Anforderungen an das Zeit- und Fehlerverhalten eines Kommunikationssystems aus Anwendungssicht beziehen sich meist auf eine sogenannte Ende-zu-Ende-Verbindung. Dabei wird angenommen, dass das Verhalten dieser Verbindung repräsentativ für das gesamte Kommunikationssystem und für den gesamten Umfang der Anwendung ist. Je nach Zielstellung oder Kontext kann diese Annahme zu falschen Schlussfolgerungen oder zu Missverständnissen führen. Deshalb sollen nachfolgend für die Zuverlässigkeitsbewertung relevante Betrachtungseinheiten diskutiert werden.

5.2 Logische Verbindung

5.2.1 Wesen und Funktion

Ausgehend von der oben erwähnten allgemeinen Herangehensweise kann die logische Verbindung als eine mögliche Betrachtungseinheit im Betrachtungsraum angesehen werden (siehe Abbildung 9). Es handelt sich dabei um die Verbindung zwischen einem logischen Endpunkt in einem Quellgerät und einem logischen Endpunkt in einem in einem Zielgerät. Logische Endpunkte sind Elemente der Bezugsschnittstelle, die jeweils mehrere logische Endpunkte zusammenfassen kann. Das Wesen dieser Betrachtungseinheit ist der Bezug zur Anwendung und die Kapselung der Datenübertragung.

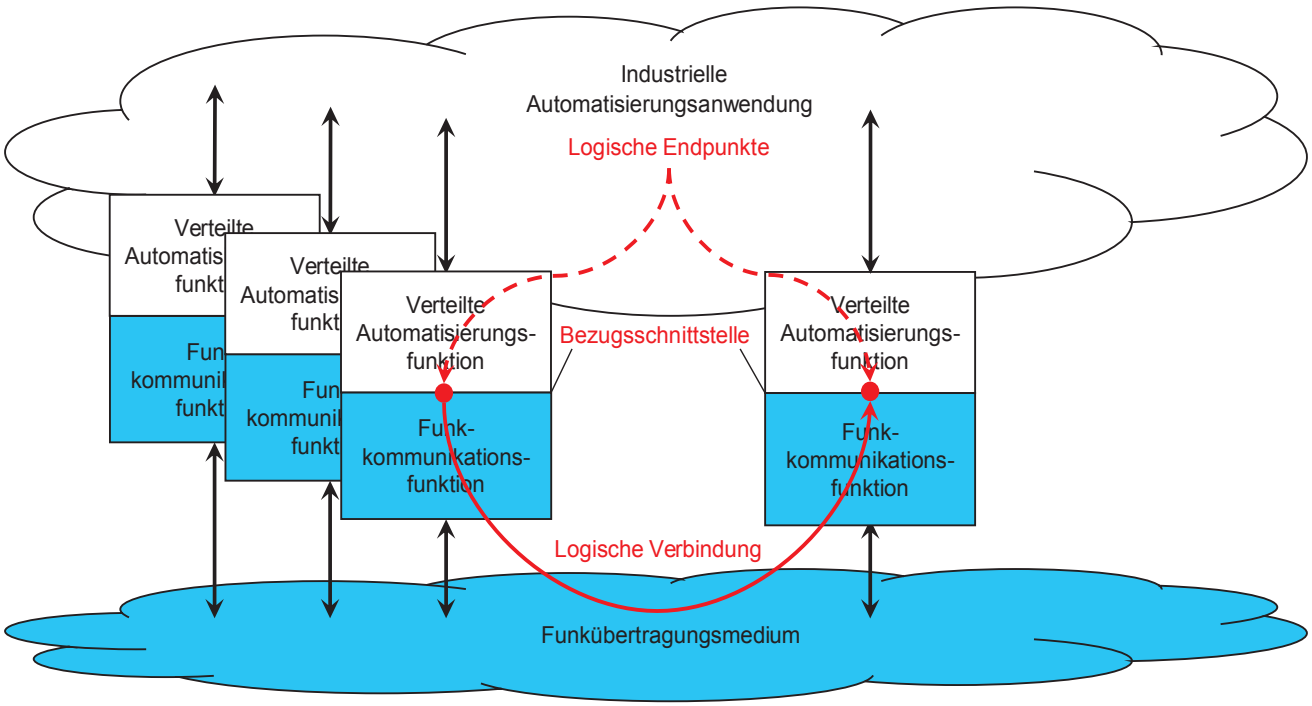


Abbildung 9: Logische Verbindung im Betrachtungsraum

Die bestimmungsgemäße Funktion der logischen Verbindung ist der Transport einer Folge von Nachrichten von einem logischen Quellendpunkt zum korrekten logischen Zielendpunkt. Dabei wird jede Nachricht in eine Form gewandelt, die eine fehlerfreie Übertragung ermöglicht. Die Übertragung schließt Verfahren ein, z. B. Wiederholungen, um die bestimmungsgemäße Funktion zu erfüllen. Nach der Übertragung erfolgt eine erneute Wandlung in eine für die Anwendung nutzbare Form. Die Nachricht soll innerhalb eines definierten Zeitraums unverfälscht am Ziel zur Verfügung stehen. Die Nachrichtenfolge am Ziel soll der Folge an der Quelle entsprechen.

Die zur Erfüllung dieser Aufgabe notwendigen Funktionseinheiten sind in Abbildung 10 dargestellt.

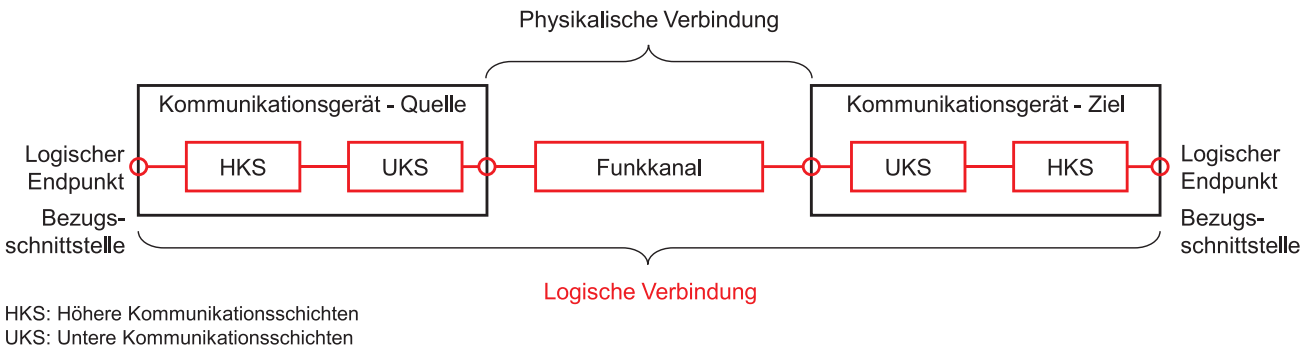


Abbildung 10: Betrachtungseinheit „Logischen Verbindung“

Die geforderte Funktion kann durch verschiedene Einflüsse beeinträchtigt sein, was zu Kommunikationsfehlern führen kann. Solche Einflüsse sind beispielsweise in [20] und [21] beschrieben. Das Auftreten eines Fehlers beeinflusst die Werte der relevanten Zuverlässigkeitskenngrößen der logischen Verbindung.

5.2.2 Nachrichtentransformation

Aus Implementierungssicht lassen sich Kommunikationsschichten und Schnittstellen in Geräten kaum einheitlich identifizieren, z. B. mit Bezug auf das Open Systems Interconnection (*OSI*) Model. Allerdings sind Implementierungen von Kommunikationsfunktionen meist in eine höhere Kommunikationsschicht (*HKS*) und eine untere Kommunikationsschicht (*UKS*) aufgeteilt, die von Implementierung zu Implementierung unterschiedliche Teile des *OSI* Referenzmodells beinhalten können. Für die weiteren Betrachtungen wird deshalb eine generische Implementierungssicht mit *HKS* und *UKS* zugrunde gelegt.

Die zur bestimmungsgemäßen Funktion einer logischen Verbindung zu übertragenden Nachrichten werden durch bedeutungstragende Zeichenfolgen beschrieben. Eine solche Zeichenfolge wird als Nutzdaten an der Referenzschnittstelle zur Übertragung übergeben. Wenn die Anzahl der Zeichen einer Nachricht zu groß ist, um mit einem Mal übertragen zu werden, kann die Nachricht für die Übertragung in mehrere Pakete aufgeteilt werden (Fragmentierung). Die Pakete werden anschließend von einer höheren Kommunikationsschicht (*HKS*) zu einer unteren Kommunikationsschicht (*UKS*) übergeben (Abbildung 11). Dort wird ein Bitstrom erzeugt der an die Bitübertragungsschicht (*PS*) übergeben wird. Von der Bitübertragungsschicht des Quellgerätes wird entsprechend dem Bitstrom ein Signalstrom zum Zielgerät übertragen. Im Zielgerät wird von der Bitübertragungsschicht der empfangenen Signalstrom in ein Bitstrom gewandelt, der an die untere Kommunikationsschicht übergeben wird. Hier werden Pakete zusammengestellt, die von der unteren Kommunikationsschicht zu höheren Kommunikationsschicht übergeben und dort zur Nachricht zusammengefasst wird. Durch geeignete Mechanismen (Bestätigung, parallele Übertragung durch anderen Kommunikationskanal/-medium, mehrfaches Übertragen eines identischen Pakets usw.) kann bei einem Verlust eines Pakets die Wahrscheinlichkeit erhöht werden, dass die Nachricht die Anwendung korrekt erreicht. In Abbildung 11 ist eine Nachrichtenübertragung mit drei Paketen inklusive Bestätigung dargestellt. Wird keine Bestätigung im geforderten Zeitintervall empfangen (Paket 2), wird das Paket erneut gesendet.

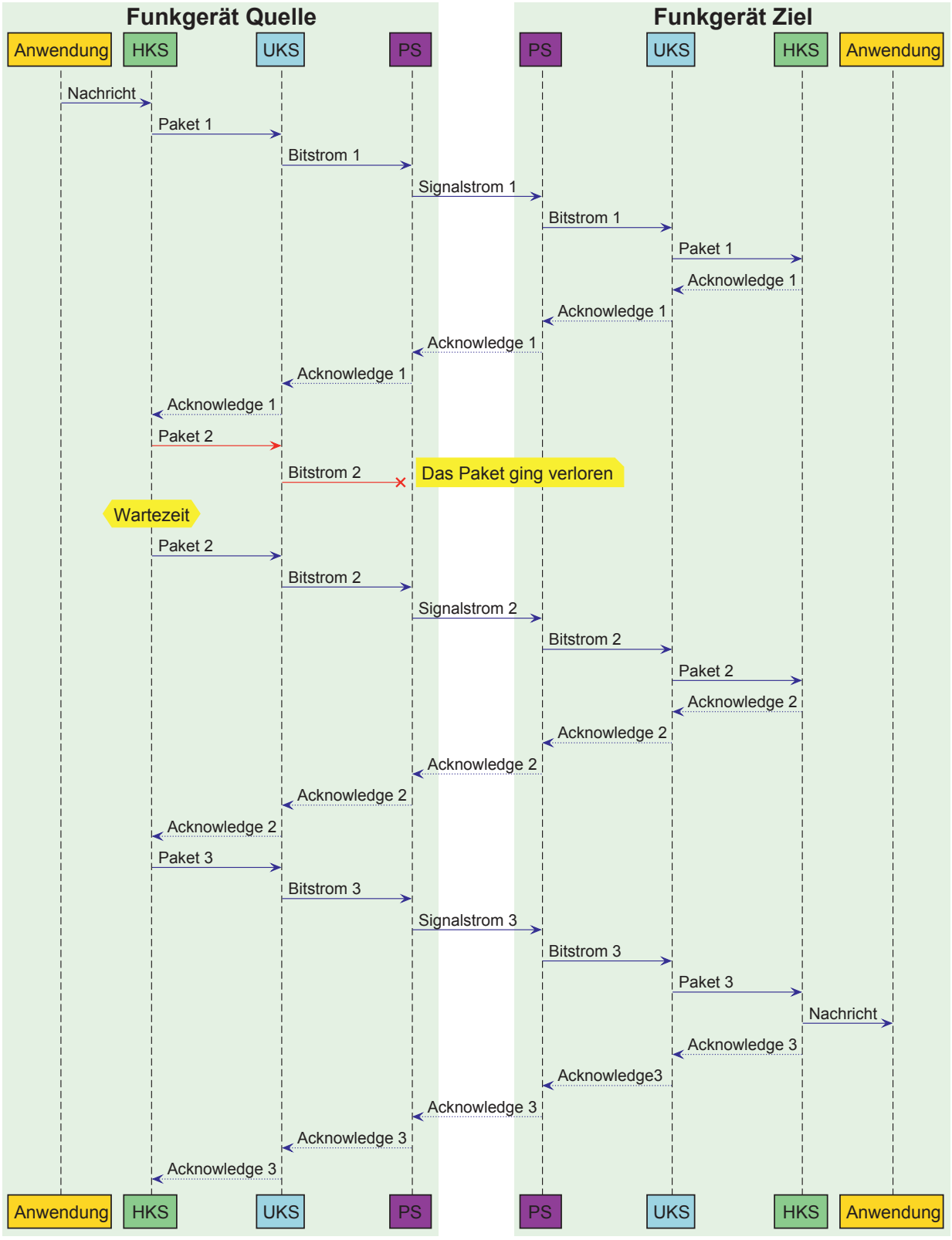


Abbildung 11: Übertragung einer Nachricht als Pakete und Bitströme

Der Verlust eines Paketes ist also nicht in jedem Fall mit dem Verlust einer Nachricht gleichzusetzen.

Dieses Dokument fokussiert auf die anwendungsbezogenen Nachrichten. Zur besseren Einordnung befinden sich auf Pakete bezogene Definitionen in der Anlage.

5.2.3 Kommunikationsfehler

In IEC/EN 61784-3-3 [11] sind wesentliche Kommunikationsfehler beschrieben, die für Anwendungen mit funktionalen Sicherheitsanforderungen zu erkennen sind. Die Beschreibung dieser Kommunikationsfehler bezieht sich auf Feldbusse. Allerdings sind diese Fehler auch für andere Kommunikationssysteme gültig.

Verfälschung

„Durch Fehler in einem Busteilnehmer oder durch Fehler auf dem Übertragungsmedium oder durch Nachrichtenstörung werden Nachrichten verfälscht.

Anmerkung 1: Nachrichtenfehler während der Übertragung sind übliche Vorgänge in jedem Kommunikationssystem; solche Ereignisse werden auf Empfängerseite mit hoher Wahrscheinlichkeit durch Hash-Funktionen entdeckt und die jeweilige Nachricht wird nicht ausgewertet.

Anmerkung 2: Die meisten Kommunikationssysteme sehen Protokolle zur Nachrichtenwiederherstellung nach Fehlern vor. Bevor nicht Wiederherstellungs- oder Wiederholungsprozeduren fehlgeschlagen sind oder nicht zur Anwendung gekommen sind, sollten solche Nachrichten daher nicht unter „Verlust“ eingeordnet werden.

Anmerkung 3: Wenn die Wiederherstellungs- oder Wiederholungsprozeduren länger als eine festgesetzte Frist benötigen, dann ist eine Nachricht unter ‚unzulässige Verzögerung‘ einzuordnen.

Anmerkung 4: In dem sehr unwahrscheinlichen Fall, dass mehrere Fehler zu einer neuen Nachricht mit korrekter Struktur (zum Beispiel Adressierung, Länge, Hash-Funktion wie CRC, usw.) führen, wird diese Nachricht akzeptiert und weiter verarbeitet. Auswertungen auf Basis der laufenden Nummer oder eines Zeitstempels können dann zu Einordnungen führen wie ‚Unbeabsichtigte Wiederholung‘, ‚Falsche Reihenfolge‘, ‚Unzulässige Verzögerung‘ oder ‚Einfügung‘.“ [11]

Unbeabsichtigte Wiederholung

„Durch Fehler, Störung oder Störbeeinflussung werden alte, nicht aktuelle Nachrichten zur falschen Zeit wiederholt.

Anmerkung 1: Wiederholung durch den Sender ist eine übliche Prozedur, wenn eine erwartete Bestätigung/Antwort von der Zielstation nicht eingetroffen ist, oder falls eine Empfangsstation das Fehlen einer Nachricht feststellt und um erneute Sendung nachfragt.

In einigen Fällen kann das Aufdecken einer fehlenden Antwort und das erneute Senden mit geringem Verzug und ohne Verlust der Reihenfolge erfolgen. In anderen Fällen tritt die Wiederholung zu einem späteren Zeitpunkt auf und kommt nicht in der richtigen Nachrichtenreihenfolge an.

Anmerkung 2: Einige Feldbusse benutzen Redundanz, um die gleiche Nachricht mehrfach oder auf mehreren Wegen zu senden und somit die Wahrscheinlichkeit für ihren einwandfreien Empfang zu erhöhen.“ [11]

Falsche Abfolge

„Durch Fehler, Störung oder Störbeeinflussung ist die den Nachrichten einer bestimmten Quelle zugeordnete Abfolge (zum Beispiel über natürliche Zahl, Zeitreferenz) falsch.

Anmerkung 1: Feldbussysteme können Elemente beinhalten, die Nachrichten speichern (zum Beispiel FIFOs in Switches, Bridges, Routern) oder sie können Protokolle nutzen, die die Abfolge verändern (zum Beispiel dadurch, dass hochpriore Nachrichten niederpriore Nachrichten überholen).

Anmerkung 2: Wenn mehrere Abfolgen aktiv sind, beispielsweise in Nachrichten von unterschiedlichen Quellen oder Meldungen von unterschiedlichen Objekttypen, dann werden diese Abfolgen getrennt überwacht und Fehler für jede Abfolge gemeldet.“ [11]

Verlust

„Durch Fehler, Störung oder Störbeeinflussung wird eine Nachricht nicht empfangen oder nicht quittiert.“ [11]

Inakzeptable Verzögerung

„Nachrichten können über ihr zulässiges Empfangszeitfenster hinaus verzögert sein, zum Beispiel durch Fehler im Übertragungsmedium, durch überlastete Übertragungsstrecken, durch Störbeeinflussung oder durch Teilnehmer, die Nachrichten in einer Weise versenden, dass Dienste verzögert oder verweigert werden (zum Beispiel FIFOs in Switches, Bridges, Router).

Anmerkung: In unterlagerten Feldbussen mit planmäßigen oder zyklischen Abfragen können Nachrichtenfehler auf folgende verschiedene Weise behoben werden:

a) sofortige Wiederholung;
b) Wiederholung in der verbleibenden Zeit am Ende des Zyklus;
c) Betrachten der Nachricht als verloren und Warten auf den nächsten Zyklus mit Empfang des folgenden Wertes.

Im Fall a) werden sämtliche nachfolgenden Nachrichten in diesem Zyklus geringfügig verzögert, während in Fall b) nur die erneut gesendete Nachricht verzögert wird.

Fälle a) und b) werden üblicherweise nicht unter „Unzulässige Verzögerung“ eingeordnet.

Fall c) würde als „Unzulässige Verzögerung“ eingeordnet werden, es sei denn, die Zykluszeit ist kurz genug, um sicherzustellen, dass Verzögerungen zwischen Zyklen unwesentlich sind und der nächste zyklische Wert als Ersatz für den verfehlten Vorgängerwert akzeptiert werden kann.“ [11]

Maskerade

„Durch eine Störung oder Störbeeinflussung wird eine Nachricht eingefügt, die von einer scheinbar zulässigen Quelle stammt, so dass eine nicht-sicherheitsrelevante Nachricht von einem sicherheitsrelevanten Teilnehmer empfangen werden kann, der sie als sicherheitsrelevant behandelt.

Anmerkung: Kommunikationssysteme für sicherheitsrelevante Anwendungen können zusätzliche Prüfungen zur Aufdeckung einer Maskerade einsetzen, wie autorisierte Quellenkennungen und Passphrasen oder Kryptografie.“ [11]

Einfügung

„Durch eine Störung oder Störbeeinflussung wird eine Nachricht eingefügt, die sich auf eine unerwartete oder unbekannte Quelle bezieht.

Anmerkung: Diese Nachrichten sind zusätzlich im erwarteten Nachrichtenstrom vorhanden und können wegen der nicht erwarteten Quellen nicht als ‚Korrekt‘, ‚Unbeabsichtigte Wiederholung‘ oder ‚Falsche Abfolge‘ eingeordnet werden.“ [11]

Adressierung

„Durch eine Störung oder Störbeeinflussung wird eine sicherheitsrelevante Nachricht an den falschen sicherheitsrelevanten Teilnehmer gesandt, der dann den Empfang als korrekt behandelt.“ [11]

5.3 Kommunikationsgerät

Die Kommunikationsgeräte bestimmen wesentlich die Funktion und damit die Zuverlässigkeit der logischen Verbindung (Abbildung 12). Werden Kommunikationsgeräte als Betrachtungseinheit der Zuverlässigkeitsbewertung herangezogen, stehen die Methoden und Algorithmen sowie deren Implementierungen im Fokus. Die Funktion der Kommunikationsgeräte ist die korrekte Sendung bzw. der korrekte Empfang von Nachrichtenfolgen. Die in den Kommunikationsgeräten implementierten Methoden und Algorithmen sollen die bei der Nachrichtenübertragung vorliegenden Übertragungsbedingungen bestmöglich berücksichtigen und dabei die Anforderungen an die Nachrichtenübertragung bestmöglich erfüllen. Im Kontext der Forschungsausschreibung ZDKI stellt die Erforschung entsprechender drahtloser Übertragungsmethoden für die industrielle Automatisierung den Schwerpunkt der Teilprojekte dar.

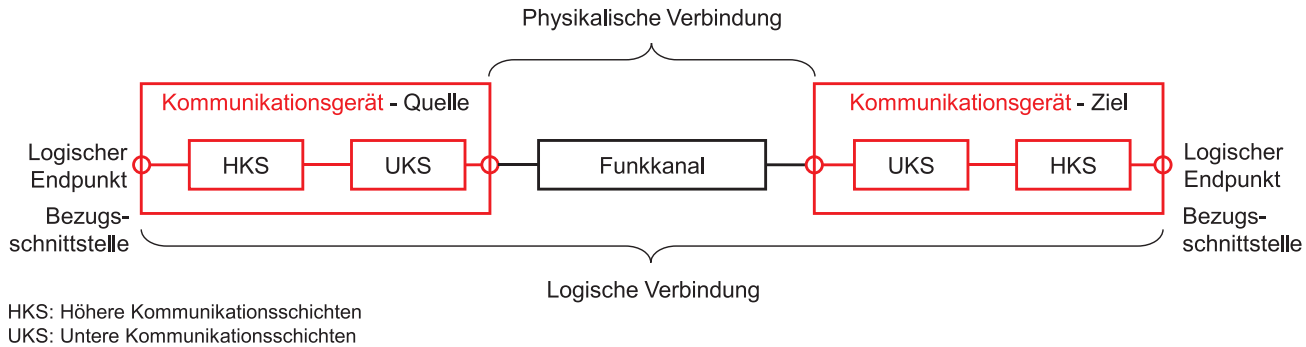


Abbildung 12: Betrachtungseinheit „Kommunikationsgerät“

Neben den Methoden und Algorithmen selbst, ist auch deren Implementierung in Hard- und Software von Bedeutung. Dabei können nachfolgend aufgeführte Fehler die Zuverlässigkeit beeinflussen.

Hardware-Fehler

Hardware-Fehler bezeichnen den Ausfall oder die Störung der Funktion von elektrischen, elektronischen und programmierbaren Bauelementen. Diese werden durch physikalische und chemische Prozesse, die in der Umwelt oder im System ständig ablaufen verursacht. Entspricht die Funktion eines Bauelementes nicht mehr der Spezifikation, so wird es in der Regel als unbrauchbar und damit als ausgefallen gewertet.

In Abhängigkeit von der Ursache, dem Umfang und der Geschwindigkeit des Auftretens wird unterschieden zwischen:

- Zufälligen Ausfall und deterministischem Ausfall
- Totalausfall und Teilausfall
- Sprungausfall und Driftausfall, Ermüdungsausfall

Hardware-Fehler können beispielsweise durch

- Schlechte Verarbeitung,
- Bauteile minderer Qualität,
- Alterung,
- Überlastung (z. B. Taktfrequenz, Spannung oder Strom),
- Hohe oder tiefe Temperaturen,
- Häufiger Temperaturwechsel,
- Stöße, Beschleunigung, Vibration,
- elektrische, magnetische oder elektromagnetische Felder,
- kosmische Strahlung und
- radioaktive Strahlung

verursacht werden.

Im Kontext der Forschungsausschreibung ZDKI stehen auch Schaltungstechnische Aspekte im Fokus, die Fehlfunktionen minimieren sollen.

Software-Fehler oder Programmfehler

Software-Fehler oder Programmfehler bezeichnen ein Fehlverhalten von Rechnerprogrammen. Es werden folgende Arten von Software-Fehlern unterschieden:

- Syntaxfehler
  sind Verstöße gegen die grammatischen Regeln der benutzten Programmiersprache. Ein Syntaxfehler verhindert die Kompilierung des fehlerhaften Programms. Syntaxfehler sind i.d.R. zur Laufzeit nicht von Interesse, es sei denn, es wird eine Programmiersprache verwendet, die das Programm sequenziell interpretiert.
- Laufzeitfehler
  bezeichnet alle Arten von Fehlern, die während der Programmabarbeitung auftreten, z. B. Überschreitung des Wertebereichs oder falsche Datentypen von Variablen bei der Eingabe, wenn die Überprüfung fehlt oder es wird eine falsche Version des Betriebssystems verwendet.
- Logische Fehler
  treten bei falschen Ansatz oder falschem Algorithmus auf.
- Designfehler
  sind Fehler im Grundkonzept, die durch Annahme falscher Anforderungen oder fehlerhaften Software-Design hervorgerufen werden.
- Fehler als Folge physikalischer Betriebsbedingungen
  Elektromagnetische Felder, Strahlen, mechanische Belastungen, Temperaturschwankungen usw. können auch bei Systemen, die innerhalb der Spezifikation arbeiten zu Fehlern führen. Ein Beispiel hierfür ist, dass ein oder mehrere Bits in einem Speicher auf Grund der genannten Einflüsse ihren Zustand wechseln.

Betrachtungen zu Software- und Hardwarefehlern finden sich z. B. in IEC 62439 [22], die darüber hinaus Redundanzkonzepte in Industrial Ethernet Netzwerken behandelt, oder in IEC 62673 [23], in der eine allgemeine Methodik zur Zuverlässigkeitsbeurteilung und -sicherung von Kommunikationsnetzen über den Lebenszyklus beschrieben ist.

Im Kontext der Forschungsausschreibung ZDKI stehen Verfahren zur zuverlässigen Softwareentwicklung nicht im Fokus.

5.4 Physikalische Verbindung

Die physikalische Verbindung stellt bei der drahtlosen Übertragung eine besondere Herausforderung dar. Die Einsatzumgebung hat einen großen Einfluss auf die Zuverlässigkeitskenngrößen. Unterschieden wird in passive Einflüsse (das abgestrahlte Signal wird auf dem Weg zum Empfänger beeinflusst) und aktive Einflüsse (zusätzliche Signale beeinträchtigen die Erkennung des Nutzsignals am Empfänger). Zu den passiven Einflüssen gehört die Entfernung (entfernungsabhängige Dämpfung des Signals), metallische Hindernisse (Reflexion, Beugung, Brechung des Signals), dielektrische Hindernisse (Dämpfung des Signals) oder starker Regen-/Nebel (Absorption des Signals). Aktive Einflüsse ergeben sich aus Sendern elektromagnetischer Wellen im Umfeld. Passive und aktive Einflüsse werden als Störung bezeichnet. Diese Störungen wirken auf die physikalische Verbindung und können Ursache für Übertragungsfehler sein.

Die Zuverlässigkeitsbewertung der physikalischen Verbindung beschreibt die Bedingungen, die der Entwicklung von Kommunikationsmethoden und algorithmen zugrunde gelegt werden können. Die Funktion der physikalischen Verbindung ist die fehlerfreie Signalübertragung zwischen dem physikalischen Endpunkt der Quelle und dem physikalischen Endpunkt des Ziels (siehe Abbildung 13). Durch die Änderung einer Bedingung z. B. das Auftreten eines Störsignals, störende Gegenstände oder eine plötzliche Änderung der Wetterlage wird die Übertragung auf dem Funkübertragungsmedium beeinflusst. Die Bedingungen können sich dabei sehr schnell, sehr umfangreich und kaum vorhersehbar ändern. Die dadurch auftretenden Übertragungsfehler haben ihre Ursache in der Änderungen der Signalparameter, so dass durch die Algorithmen und deren Implementierung am Ziel der Informationsgehalt nicht fehlerfrei wiederhergestellt werden kann.

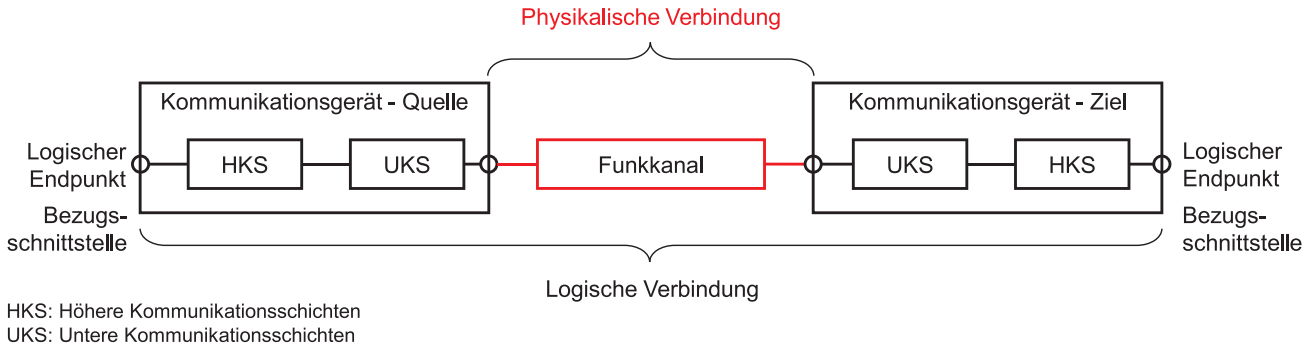


Abbildung 13: Betrachtungseinheit „Physikalische Verbindung“

Im Kontext der Forschungsausschreibung ZDKI wird dem Funkkanal besondere Aufmerksamkeit gewidmet. Es werden die spezifischen Einflüsse des Funkkanals auf die Zuverlässigkeit untersucht (passive Umgebungseinflüsse) aber auch der Aspekt der Koexistenz von Funkanwendungen. Auf Basis dieser Untersuchungsergebnisse können entsprechende Verfahren und Algorithmen für eine zuverlässige Funkkommunikation entwickelt werden.

5.5 Kommunikationssystem

Das Kommunikationssystem als Betrachtungseinheit stellt sich als Menge logischer Verbindungen dar, deren Nachrichtenübertragungen von einer Menge von Funkgeräten über ein oder mehrere Medien realisiert wird (Abbildung 14). Die bereitzustellende Funktion des Kommunikationssystems besteht darin, für alle logischen Verbindungen der örtlich verteilten Anwendung Folgen von Nachrichten zu übertragen. Diese Funktion ist über eine definierte Zeitdauer, die Betriebszeit der Automatisierungsanwendung, zu erbringen.

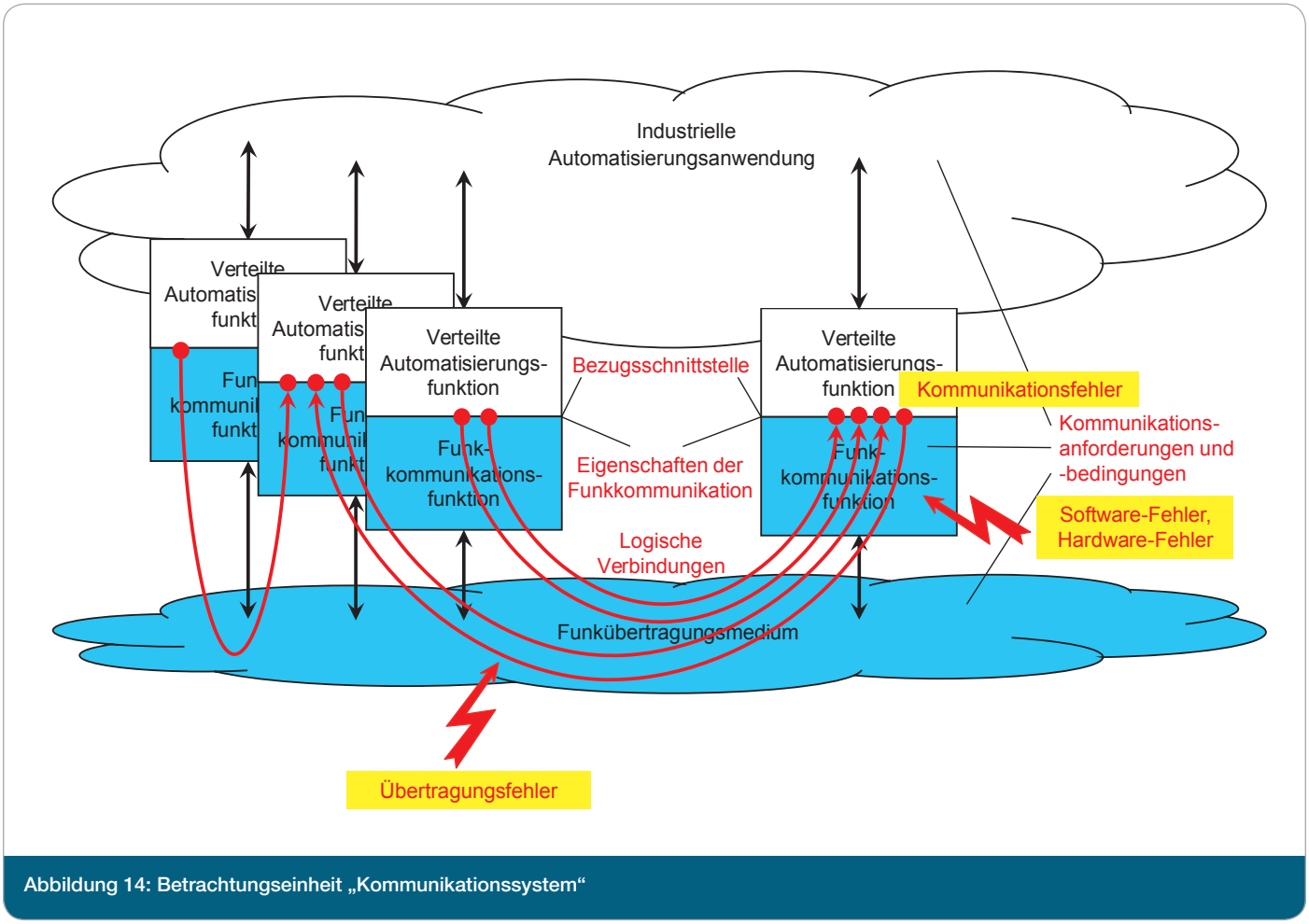


Abbildung 14: Betrachtungseinheit „Kommunikationssystem“

Es sind die Anforderungen aller logischen Verbindungen zu erfüllen. Diese Anforderungen sowie die Bedingungen können sehr unterschiedlich sein. Deshalb können sich die Funktionen (Dienste und Protokolle) für einzelne logische Verbindungen auch unterscheiden. Trotz dieser Unterschiede teilen sich logische Verbindungen zum Teil Kommunikationsgeräte und Medien. Das führt zu Wechselwirkungen, die bei den bisher diskutierten Betrachtungseinheiten nicht berücksichtigt sind. Demzufolge eignet sich das gesamte Kommunikationssystem als Betrachtungseinheit zur Zuverlässigkeitsbewertung für die Untersuchung von System- und Anwendungsaspekten.

In Abbildung 14 sind auch die bereits diskutierten Fehler bei der Nachrichtenübertragung dargestellt. Die Systembetrachtung offenbart bestehende Wechselwirkungen. Anlass für eine Fehlfunktion kann die Änderung einer Bedingung sein, z. B. das Auftreten eines Störsignals oder die Vergrößerung des Abstandes zwischen Funkgeräten. Ursachen dafür, dass sich diese Änderung als Fehlfunktion manifestiert, können fehlende Robustheit, unzureichende Verfahren oder fehlerhafte Implementierungen sein. Dabei kann der Anlass bei einer logischen Verbindung aufgetreten sein, sich aber bei einer anderen als Kommunikationsfehler darstellen.

Im Kontext der Forschungsausschreibung ZDKI ist die Zuverlässigkeitsbewertung des Gesamtsystems zum Teil Inhalt der Betrachtungen.

5.6 Funktionsbeeinflussende Bedingungen

Die für die Zuverlässigkeitsbewertung erforderliche quantitative Berücksichtigung der Bedingungen ist nicht Gegenstand dieses Dokumentes. Dafür wird auf die in [19] beschriebenen anwendungsspezifischen, funkgeräte- und -systemspezifischen sowie umgebungsspezifischen Einflussgrößen der Funkkommunikation verwiesen.

5.7 Fazit

Der Bewertung der zuverlässigen drahtlosen Kommunikation in der Industrie können verschiedene Betrachtungseinheiten zugrunde gelegt werden. In Tabelle 1 ist zusammengefasst für welche Aufgaben in ZDKI die Zuverlässigkeitsbewertung welcher Betrachtungseinheit geeignet ist. Außerdem ist aufgeführt, welche Fachgruppe des BZKI sich diesen Aufgaben widmet. Die Fachgruppe „Anwendungen, Anforderungen und Validierung“ schafft, z. B. mit diesem Dokument, die Voraussetzung für eine ZDKI einheitliche Herangehensweise bei der Zuverlässigkeitsbewertung. Die Fachgruppe „Standardisierung, Interoperabilität und Best Practices“ strebt die Verankerung und Harmonisierung dieser Sichtweise der Zuverlässigkeitsbewertung in Richtlinien und Normen an.

Betrachtungseinheit	Relevanz	BZKI Fachgruppe
Kommunikationssystem	Systemintegrator, Betreiber: Aufdeckung von systembezogenen Fehlerursachen Entwickler: Entwicklung von Konzepten zur Optimierung der Zuverlässigkeit	Implementierung, Integration und Roadmaps
Logische Verbindung	Betreiber, Dienstleister: Aufdeckung von Fehlerursachen Entwickler: Entwicklung von Konzepten zu deren Erkennung und zur Vermeidung von Fehlerauswirkungen	Koexistenz, Architektur und Schnittstelle Implementierung, Integration und Roadmaps Safety and Security
Kommunikationsgerät	Hersteller, Entwickler: Entwicklung von Methoden und Algorithmen für zuverlässige Sendung und Empfang von Nachrichten Entwickler: Hardwareentwicklung Hersteller: Herstellungsprozess	Radio Air Interface Implementierung, Integration und Roadmaps
Physikalische Verbindung	Entwickler: Charakterisierung der passiven und aktiven Umgebungseinflüsse zur Berücksichtigung bei der Entwicklung von Konzepten und Lösungen Betreiber, Dienstleister: Charakterisierung der passiven und aktiven Umgebungseinflüsse zur Berücksichtigung bei der Fehlersuche	Koexistenz, Architektur und Schnittstelle Radio Air Interface

Tabelle 1: Betrachtungseinheiten der Zuverlässigkeitsbewertung im ZDKI

Bei der Anwendung der in Kapitel 4 beschrieben Leistungsmerkmale, Kenn- und Maßgrößen zur Bewertung der Zuverlässigkeit stellt man fest, dass je nach Betrachtungseinheit verschiedene Merkmale und Kenngrößen sinnvoll sind. Im folgenden Kapitel wird eine Zuordnung vorgenommen.

6 Leistungsmerkmale, Kenn- und Maßgrößen zur Bewertung der Zuverlässigkeit einer logischen Verbindung

6.1 Relevante Leistungsmerkmale

Die in Abschnitt 4.2 definierten Leistungsmerkmale sind in Tabelle 2 aufgelistet und bezüglich der Relevanz für die Beurteilung einer Kommunikationsverbindung bewertet. Die Merkmale Haltbarkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft werden dabei meist nicht berücksichtigt. Der Fokus liegt auf der Übertragungsstrecke. Ist die Übertragungsstrecke nicht funktionsfähig, ist der Grund dafür meistens eine Störung. Nach dieser Störung ist die Funktionsfähigkeit in der Regel (selbst-)wiederherstellbar. Dass die Informationssicherheit ein relevantes Leistungsmerkmal ist steht außer Frage. Die funktionale Sicherheit wird in Kapitel 8 gesondert betrachtet.

In den folgenden Abschnitten werden Kenngrößen und deren wahrscheinlichkeitstheoretischen Maßgrößen mit Bezug auf eine logische Kommunikationsverbindung diskutiert.

IEV Nummer	Benennung DE	Benennung ENG	Relevant für logische Verbindung
192-01-23	Verfügbarkeit	Availability	Ja
192-01-24	Funktionsfähigkeit	Reliability	Ja
192-01-25	Wiederherstellbarkeit	Recoverability	Ja
192-01-26	Selbst-Wiederherstellbarkeit	Self-recoverability	Ja
192-01-27	Instandhaltbarkeit	Maintainability	Nein
192-01-29	Instandhaltungsbereitschaft	Maintenance support performance	Nein
192-01-21	Haltbarkeit	Durability	Nein
351-57-05	Sicherheit	Safety	Ja
–	Informationssicherheit	Information Security	Ja
351-57-06	Funktionale Sicherheit	Functional safety	Ja
715-07-14	Dienstgüte	Quality of service	Ja

Tabelle 2: Übersicht über Leistungsmerkmale der Zuverlässigkeit für eine logische Verbindung

6.2 Kenngrößen und deren wahrscheinlichkeitstheoretischen Maßgrößen

6.2.1 Klarzeitintervall

Im Klarzustand einer logischen Verbindung kann jederzeit eine Nachricht vom logischen Endpunkt der Quelle zum logischen Endpunkt des Ziels übertragen werden. Das Klarzeitintervall beginnt mit einem expliziten oder impliziten Verbindungsaufbau und endet mit dem Ausfall der Verbindung bzw. mit dem Verbindungsabbau aufgrund eines Fehlers. Dabei ist zu beachten, dass das messbare Klarzeitintervall vom tatsächlichen abweichen kann. Der Grund dafür ist, dass der Klarzustand anhand der korrekt empfangenen oder inkorrekten bzw. verlorenen Nachrichten ermittelt wird. In Abbildung 15 ist gezeigt, dass der Beginn eines Klarzeitintervalls erst durch die erste erfolgreich empfangene Nachricht festgestellt wird. Das Ende des Klarzeitintervalls ist in Abbildung 15 durch einen Nachrichtenverlust dargestellt. Das heißt, eine erwartete Nachricht wurde nicht innerhalb der geforderten Zeitgrenze korrekt empfangen.

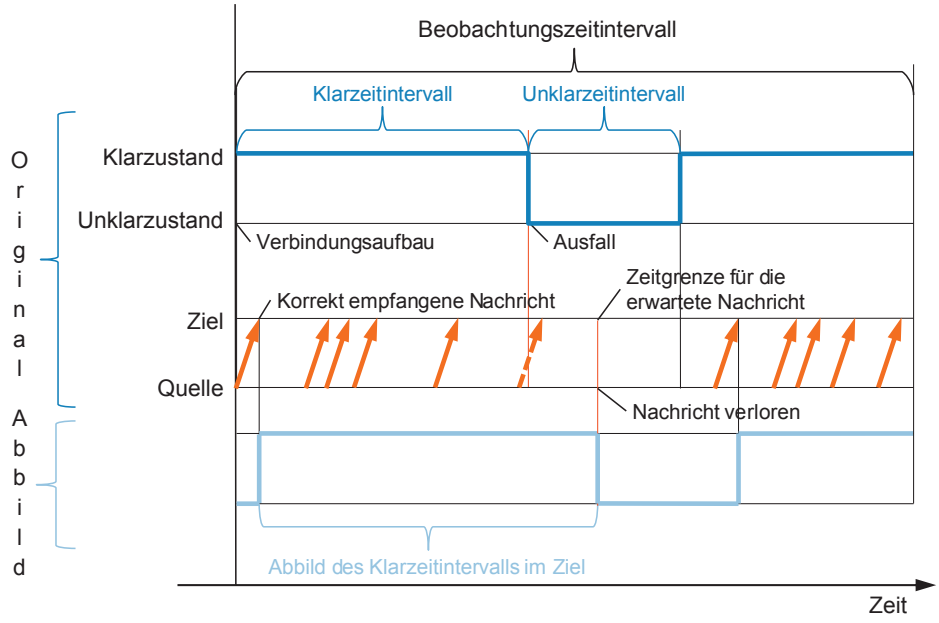


Abbildung 15: Klarzeitintervall einer logischen Verbindung

Wie in Abbildung 15 dargestellt, kann es innerhalb eines Beobachtungsintervalls, beispielsweise eines Produktionszeitraums, mehrere Klarzeitintervall geben, die durch Unklarzeitintervalle nach Ausfall voneinander getrennt sind.

Laut Definition wird für die Analyse des Klarzeitintervalls der Erwartungswert innerhalb eines Beobachtungsintervalls berechnet. Bei einer statistischen Auswertung entspricht der geschätzte Erwartungswert dem arithmetischen Mittelwert. Somit ist die mittlere Klardauer (Mean Up Time – MUT), die Summe der Klarzeitintervalle t_U geteilt durch die Anzahl der Klarzeitintervalle n, gemäß Gleichung (4).

$$\overline{t_U} = \frac{1}{n}\sum_{i=1}^{n} t_{Ui} = MUT \qquad (4)$$

6.2.2 Betriebszeitintervall

Eine logische Verbindung ist in Betrieb, wenn sie durch einen expliziten oder impliziten Verbindungsaufbau eingerichtet wurde. Erfolgt der Abbau der Verbindung durch einen Fehler, ist das Betriebszeitintervall identisch mit dem Klarzeitintervall gemäß Abschnitt 6.2.1 (siehe Abbildung 16). Wird die Verbindung gezielt abgebaut ist die logische Verbindung als Betrachtungseinheit nicht mehr existent und benötigt keine weitere Bewertung. Das heißt, der in Abbildung 2 aufgeführte und in Abbildung 4 und folgende dargestellte Wartezustand und die damit verbundene Wartezeit ist für die logische Verbindung nicht relevant.

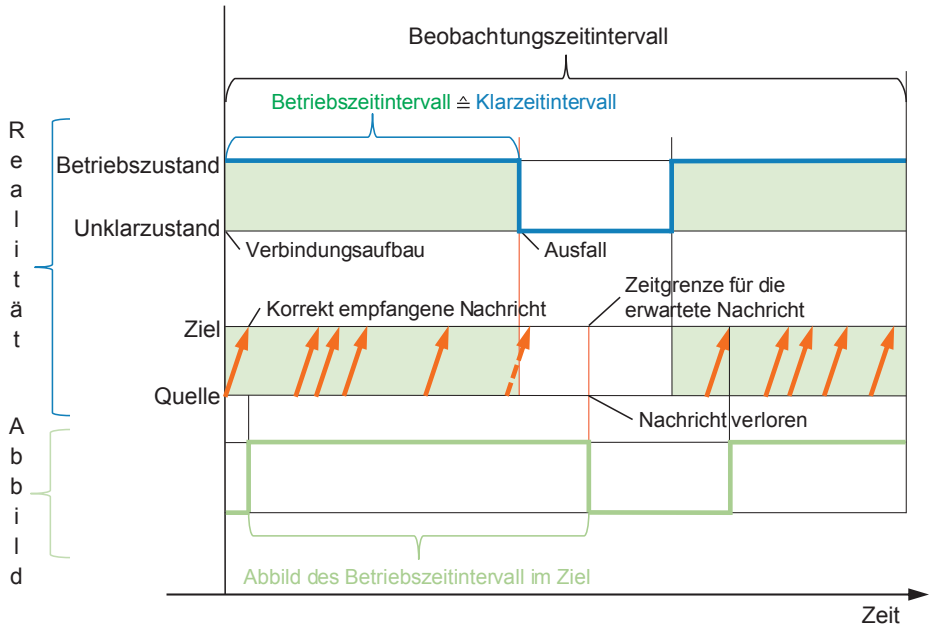


Abbildung 16: Betriebszeitintervall einer logischen Verbindung

6.2.3 Unklarzeitintervall

Das Unklarzeitintervall beginnt mit dem Ausfall der logischen Verbindung und endet mit deren Wiederherstellung. Der Ausfall kann anhand der ersten inkorrekten Nachricht mithilfe der in Abschnitt 6.2.12 beschriebenen Kriterien festgestellt werden. Das Abbild des Unklarzeitintervalls, kann wiederum, wie in Abbildung 17 dargestellt, vom tatsächlichen Unklarzeitintervall abweichen. Der Klarzustand wird durch den Empfang der ersten korrekten Nachricht identifiziert.

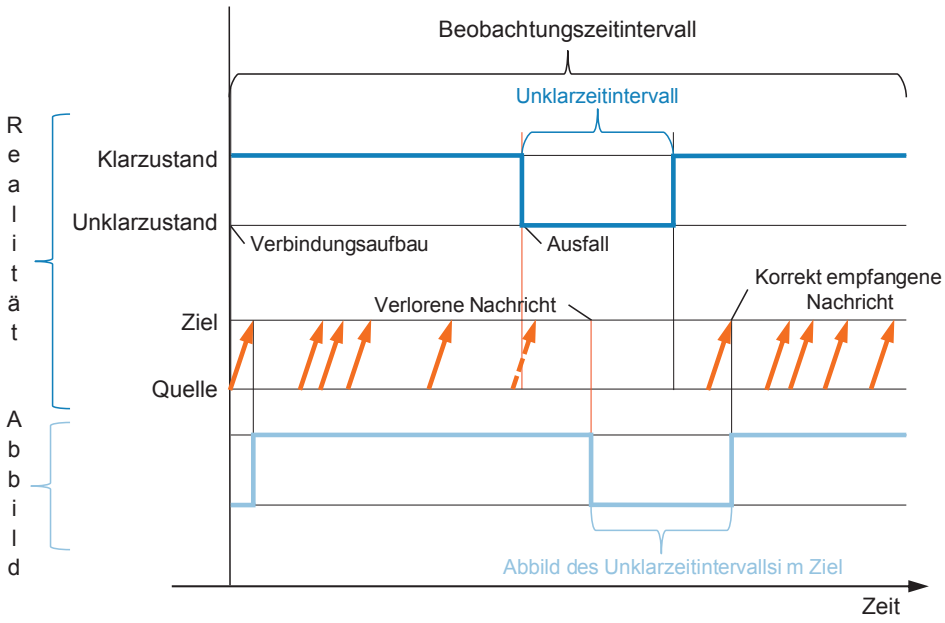


Abbildung 17: Unklarzeitintervall einer logischen Verbindung

Die Länge des Abbildes des Unklarzeitintervalls kann genutzt werden, um Maßnahmen für den Schutz von Mensch, Maschine oder Produkt durch die Anwendung abzuleiten.

Laut Definition wird für die Analyse des Unklarzeitintervalls der Erwartungswert berechnet. Bei einer statistischen Auswertung entspricht der geschätzte Erwartungswert dem arithmetischen Mittelwert. Somit kann die mittlere Unklardauer (MDT), durch die Summe der Unklarzeitintervalle t_D geteilt durch die Anzahl der Klarzeitintervalle n, gemäß Gleichung (5) ermittelt werden.

$$\overline{t_D} = \frac{1}{n} \sum_{i=1}^{n} t_{Di} = MDT \qquad (5)$$

6.2.4 Betriebszeit bis zum Ausfall

Die Betriebszeit bis zum Ausfall einer logischen Verbindung entspricht der Summe aller Betriebszeitintervalle, für die Verbindung gezielt abgebaut wurde, zuzüglich der Betriebszeit, die durch den ersten Ausfall beendet wurde (Gleichung (6)).

$$t_{FF} = \sum_{i=1}^{n} t_{OPi} = TTF \text{ mit } n\text{: erstes durch Ausfall beendetes Betriebszeitintervall} \qquad (6)$$

In Abbildung 18 sind zwei Betriebszeitintervalle dargestellt, wobei das erste Intervall durch einen Verbindungsabbau beendet wurde, das zweite Intervall durch den Empfang einer inkorrekten Nachricht.

Die Betriebszeit bis zum Ausfall ist eine Zuverlässigkeitskenngröße für die Bewertung der Alterung einer Betrachtungseinheit, die zum Ausfall führt. Mit Bezug zur logischen Verbindung betrifft das die genutzten Betriebsmittel (z. B. Funkgerät), nicht aber die Übertragungsstrecke.

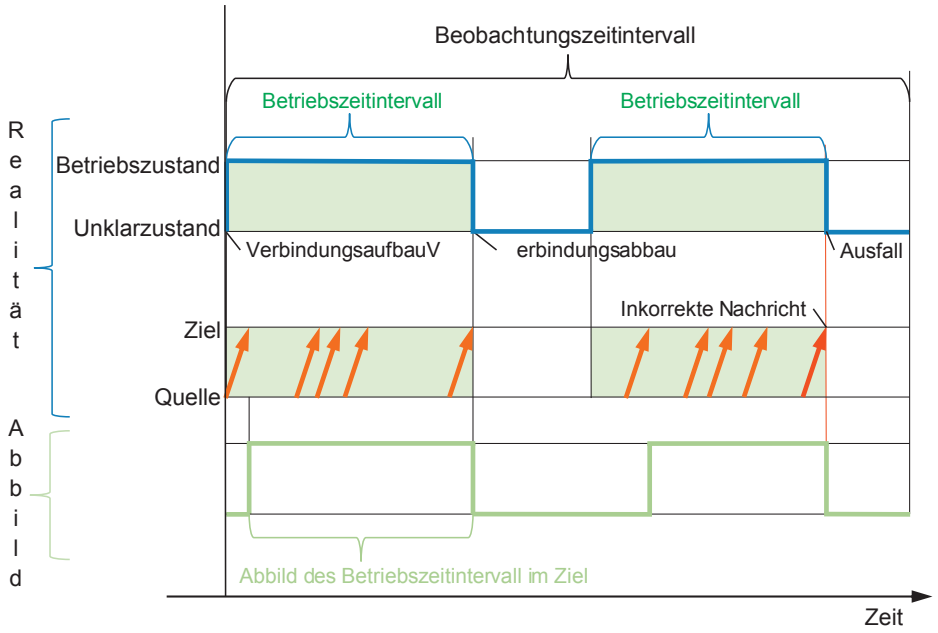


Abbildung 18: Betriebszeit bis zum Ausfall einer logischen Verbindung

6.2.5 Ausfallabstand

Der Ausfallabstand einer logischen Verbindung ergibt sich aus der Dauer zwischen zwei Ausfällen. Er umfasst also ein Unklarzeitintervall mit mindestens einer inkorrekten oder verlorenen Nachricht und ein Klarzeitintervall bzw. Betriebszeitintervall in dem mindestens eine Nachricht übertragen wurde. In Abbildung 19 ist zu erkennen, dass sich der Ausfallabstand der logischen Verbindung und der messbarer Ausfallabstand unterscheiden.

Laut Definition wird für die Analyse des Ausfallabstands der Erwartungswert berechnet. Bei einer statistischen Auswertung entspricht der geschätzte Erwartungswert dem arithmetischen Mittelwert. Somit können die einzelnen Ausfallabstände, durch die Summe der Unklarzeitintervalle t_D und dem darauf folgenden Klarzeitintervall t_U geteilt durch die Anzahl der Klarzeitintervalle n, gemäß Gleichung (7) ermittelt werden.

$$\bar{t}_G = \frac{1}{n}\sum_{i=1}^{n}(t_{Di} + t_{Ui}) \qquad (7)$$

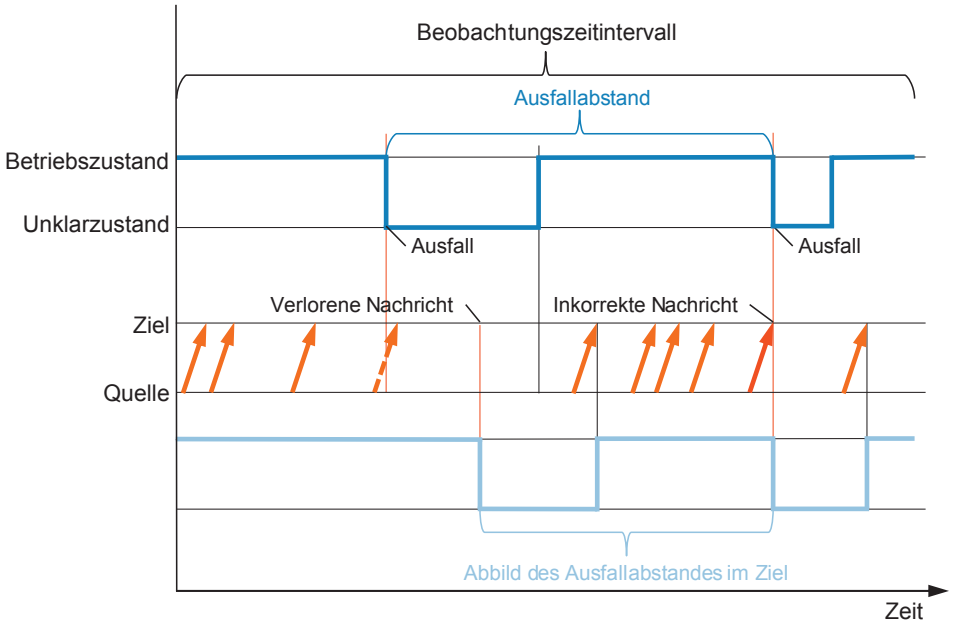


Abbildung 19: Ausfallabstand einer logischen Verbindung

6.2.6 Betriebszeit zwischen Ausfällen

Die Betriebszeit zwischen Ausfällen einer logischen Verbindung ist die Summe der Betriebszeitintervalle zwischen zwei aufeinanderfolgenden Ausfällen. Gemäß Gleichung (8) entspricht das bei einer logischen Verbindung auch der Summe der Klarzeitintervalle zwischen den Ausfällen.

$$t_{OP} = \sum_{i=1}^{n} t_{OPi} = \sum_{i=1}^{n} t_{Ui} = T(O)BF \qquad (8)$$

$$mit\ n\text{: }erstes\ durch\ Ausfall\ beendetes\ Betriebszeitintervall\ nach\ einem\ Ausfall$$

Als wahrscheinlichkeitstheoretische Maßgröße wird häufig der arithmetische Mittelwert der Betriebszeit zwischen Ausfällen ($MTBF$) gemäß Gleichung (9) zur Bewertung der Zuverlässigkeit verwendet.

$$\bar{t}_{OP} = \frac{1}{n}\sum_{i=1}^{n} t_{OPi} = \frac{1}{n}\sum_{i=1}^{n} t_{Ui} = M(O)TBF \qquad (9)$$

6.2.7 Wiederanlaufzeit

Die Wiederanlaufzeit wird definiert als die Zeitspanne zwischen dem Verlassen des Störzustandes und dem korrekten Empfang einer Nachricht am Ziel.

Für die Wiederanlaufzeit werden die gleichen wahrscheinlichkeitstheoretischen Maßgrößen herangezogen wie für die Übertragungszeit (siehe Abschnitt 6.2.7), Modalwert und Perzentilwert P95.

6.2.8 Übertragungszeit

Die Übertragungszeit (Transmission Time) ist eine grundlegende Kenngröße, die zur Bewertung von Verfügbarkeit und Echtzeitfähigkeit einer Funklösung herangezogen werden kann. Dabei ist von Interesse wie lange die Übertragung einer Nachricht von der Quelle (z. B. einem Sensor) bis zum Ziel (z. B. eine Steuerung) dauert. Ein einheitliches Verständnis dieser Zeitspanne erfordert die genaue Festlegung des Starts dieser Übertragung und deren Ende. Gemäß [24] ist die Übertragungszeit der Zeitabschnitt von der Übergabe des ersten atomaren Bestandteils einer Nachricht, der Nutzdaten (Bit, Oktett), an der Schnittstelle zwischen Anwendung und Funkkommunikation eine Quelle und der Übergabe des letzten atomaren Bestandteils derselben Nachricht an der Schnittstelle zwischen Funkkommunikation und Anwendung eines Ziels (siehe Abbildung 20). Die Art der Schnittstelle zwischen Funkkommunikation und Anwendung sowie deren Charakteristik ist bei der Veröffentlichung der Kenngrößenwerte immer mit anzugeben, da es keine einheitliche Bezugsschnittstelle gibt.

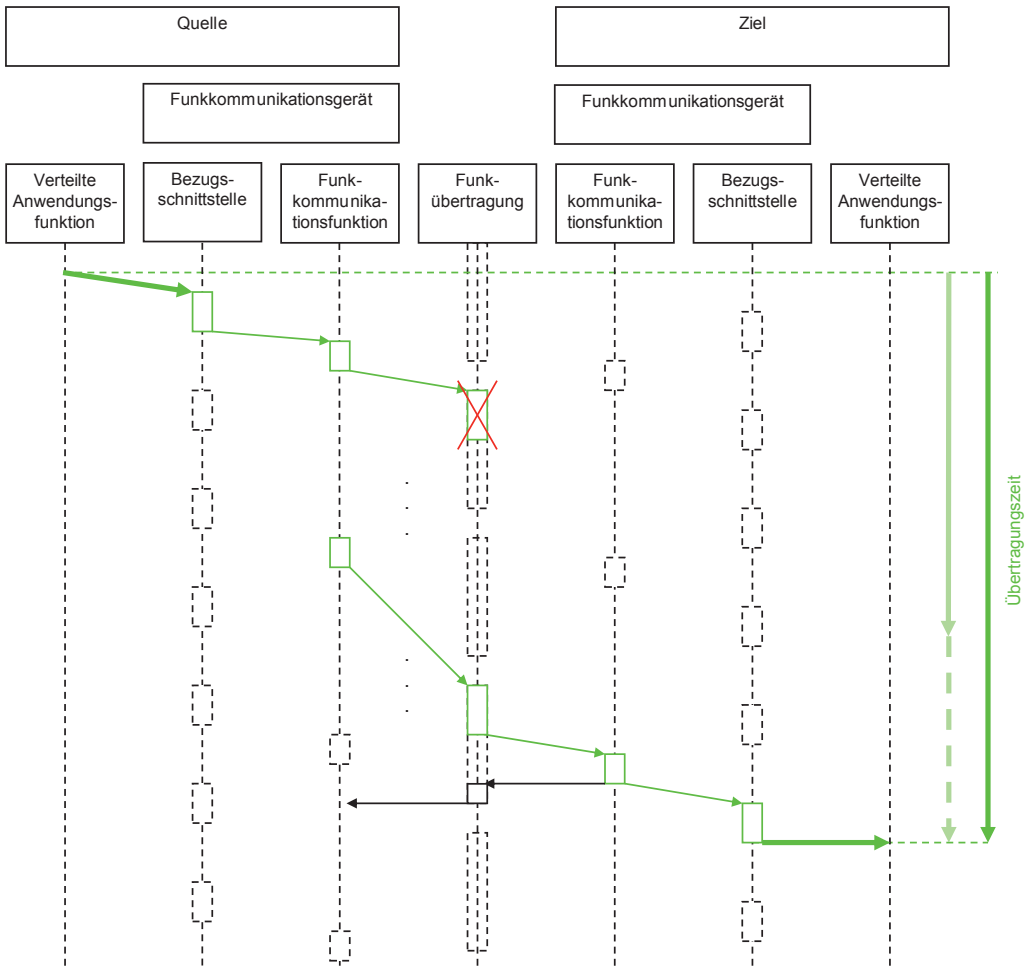


Abbildung 20: Definition der Übertragungszeit

Die Übertragungszeit eignet sich als Kenngröße der Echtzeitfähigkeit besonders für Anwendungen mit aperiodischem Kommunikationsbedarf. Unabhängig vom zeitlichen Abstand zweier Übertragungen kann der Zeitpunkt der Bereitstellung der Nutzdaten am Ziel bewertet werden. Außerdem wird die Übertragungszeit zur Bewertung der Zuverlässigkeit herangezogen.

Wie in Abbildung 20 dargestellt, schwanken die Werte der Übertragungszeit. Zu den Ursachen gehört, dass auf die Bereitschaft zur Datenübernahme oder auf den Zeitschlitz für den Mediumzugriff (jeweils durch ein gestricheltes Rechteck dargestellt) gewartet werden muss. Die Übertragungszeit kann einen Minimalwert nicht unterschreiten, nimmt meist aber einen Wert in dessen Nähe ein. Deshalb ist der Wert

der am häufigsten auftritt, der Modalwert, für die Bewertung des Zentrums am Besten geeignet. Ein sinnvoller Streuungsparameter der Übertragungszeit ist das Perzentil P95, der Wert für 95 % aller Übertragungen. Der Maximalwert der Übertragungszeit kann Zehnerpotenzen größer sein als der Modalwert und ist deshalb als Parameter zur Bewertung ungeeignet.

6.2.9 Aktualisierungszeit

Die Aktualisierungszeit (Update time) entspricht im Idealfall dem Sendezeitabstand von Nachrichten einer logischen Verbindung. Das heißt, die übertragenen Nutzdaten einer Nachricht werden an der Bezugsschnittstelle des Ziels in denselben zeitlichen Abständen übernommen, wie sie an der Bezugsschnittstelle einer Quelle übergeben wurden. Die Aktualisierungszeit ist definiert als der Zeitabschnitt von der Übergabe des letzten atomaren Bestandteils der Nutzdaten einer Quelle an der Bezugsschnittstelle eines Ziels bis zur Übergabe des letzten atomaren Bestandteils der unmittelbar nachfolgend übertragenen Nutzdaten der gleichen Quelle einer logischen Verbindung. In Abbildung 21 ist dargestellt, dass Information zum Teil nur zu bestimmten Zeiten bzw. in bestimmten Zeitintervallen weiter gegeben werden können. Daraus ergeben sich die Differenzen zwischen Sendezeitabstand und Aktualisierungszeit.

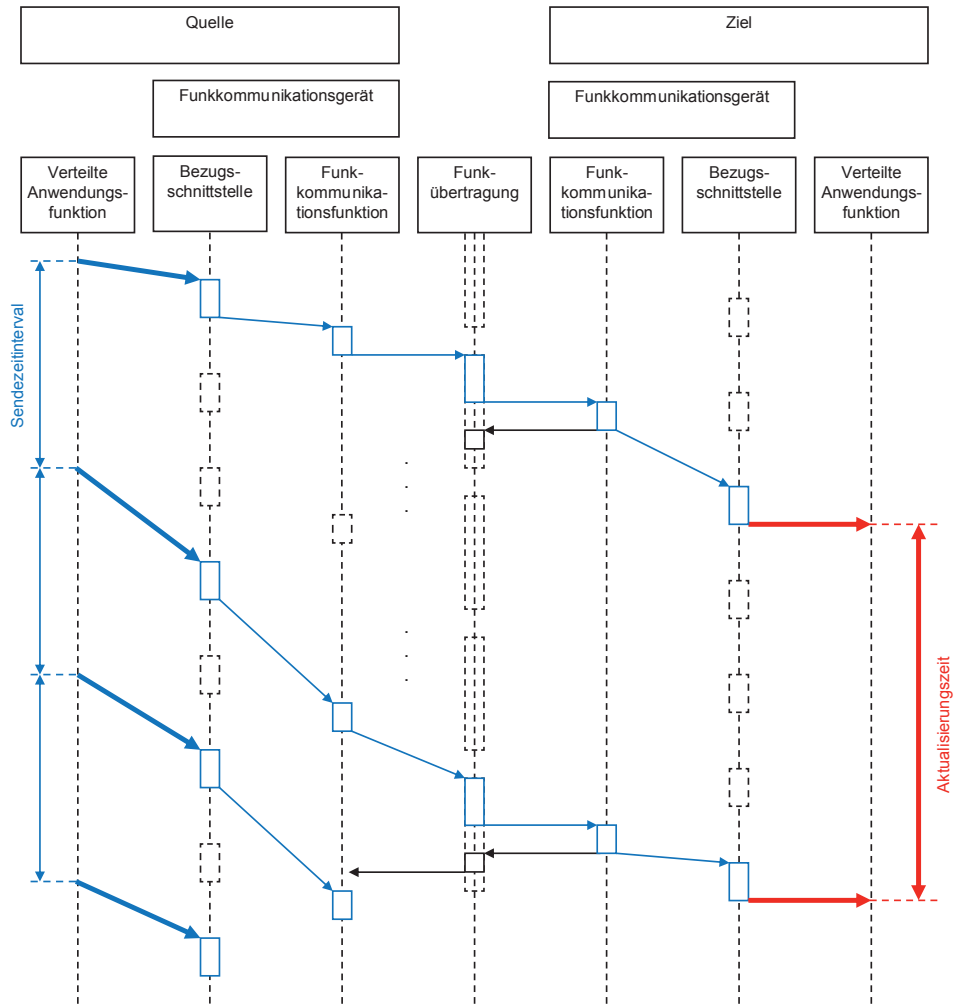


Abbildung 21: Definition der Aktualisierungszeit

Die Aktualisierungszeit ist besonders für die Bewertung der Rechtzeitigkeit und des Determinismus von Anwendungen mit periodischem Kommunikationsbedarf geeignet [1]. Aussagefähige wahrscheinlichkeitstheoretische Maßgrößen für die Aktualisierungszeit sind der arithmetische Mittelwert und die Standardabweichung.

6.2.10 Antwortzeit

Die Antwortzeit (Response time) bezieht sich auf die Übertragung einer Anforderungsnachricht und der zugehörigen Antwortnachricht. Sie beinhaltet neben der Zeit für den Transport der Nachrichten auch die Zeit zur Erstellung der Antwortnachricht. Die Antwortzeit ist der Zeitabschnitt von der Übergabe des ersten atomaren Bestandteils der Anforderungsnachricht an der Bezugsschnittstelle bis zur Übergabe des letzten atomaren Bestandteils der zugehörigen Antwortnachricht an derselben Bezugsschnittstelle.

Für die Antwortzeit werden die gleichen wahrscheinlichkeitstheoretische Maßgrößen herangezogen wie für die Übertragungszeit, Modalwert und Perzentilwert P95.

6.2.11 Anzahl korrekt empfangener Nachrichten

Eine Nachricht Me_{Rxi} gilt zunächst als empfangen, wenn es an der Bezugsschnittelle des Ziels an die Anwendung übergeben wurde.

Die Anzahl empfangener Nachrichten (Number of recieved messages: N_{RM}) ergibt sich aus:

$$N_{RM} = \sum_{i=1}^{n} Me_{Rxi} \tag{10}$$

Da es allerdings zu Verfälschungen des Inhalts und zu Wiederholungen der Übertragung kommen kann, die nicht durch die Fehlersicherungsmechanismen der Funklösung identifiziert bzw. beseitigt werden, sind die empfangenen Daten daraufhin zu prüfen. Außerdem gehört die Rechtzeitigkeit zu den Bedingungen einer korrekt empfangenen Nachricht. Deshalb werden bei der nachfolgend aufgeführten Bestimmung der korrekt empfangenen Nachrichten der Dateninhalt (Data content: Co), die Reihenfolge (Sequence number: SN), die Übertragungszeit $t_T(Me_{Rxi})$ und die Adressen (Address: Ad) berücksichtigt.

$$N_{Rx} = \sum_{i=1}^{n} c(Me_{Rxi}) \tag{11}$$

$$mit \begin{cases} c(Me_{Rxi}) = 1, wenn\ Co(Me_{Rxi}) = Co(Me_{Txi}) \wedge SN(Me_{Rxi}) > SN(Me_{Rxi-1}) \wedge t_T(Me_{Rxi}) \leq T_{Tmax} \\ \wedge\ Ad_{SCR}(Me_{Rxi}) = Ad_{SCR}\ \wedge\ Ad_{DST}(Me_{Rxi}) = Ad_{DST} \\ c(Me_{Rxi}) = 0, sonst \end{cases}$$

N_{Rx} bezeichnet demzufolge die Anzahl korrekt empfangener Nachrichten, für die gilt:

- Der Inhalt der empfangenen Daten $Co(Me_{Rxi})$ stimmt nach einem Bitvergleich mit dem Inhalt der gesendeten Daten $Co(Me_{Txi})$ überein. Es liegen keine Bitfehler bzw. Symbolfehler vor. Die Korrektheit (correctness) einer empfangenen Nachricht ist mit $c(Me_{Rxi})$ bezeichnet. Eine einfache CRC-Prüfung ist dafür nicht ausreichend.
- Die laufende Nummer der empfangenen Nachrichten $SN(Me_{Rxi})$ muss größer als die laufende Nummer der vorherigen empfangenen Nachricht $SN(Me_{Rxi-1})$ sein. Überholte Nachrichten werden somit als inkorrekt gewertet.
- Der Wert der Übertragungszeit $t_T(Me_{Rxi})$ muss kleiner sein, als ein vorgegebener Grenzwert T_{Tmax}
- Die Adresse der Quelle $Ad_{SCR}(Me_{Rxi})$ in der Nachricht muss der Quelladresse der logischen Verbindung entsprechen. Über welche Parameter (Knotenadressen, Port, Endpunkt) die Adresse definiert wird, hängt von der jeweiligen Anforderung ab.

- Die Adresse des Ziels $Ad_{DST}(Me_{Rxi})$ in der Nachricht muss dem Ziel der logischen Verbindung entsprechen. Über welche Parameter (Knotenadressen, Port, Endpunkt) die Adresse definiert wird, hängt von der jeweiligen Anforderung ab.

Je nach Anforderungen kann die Formel angepasst bzw. erweitert (z. B. Aktualisierungszeit) werden. Wird eine Nachricht korrekt empfangen ist das System im Klarzustand.

6.2.12 Anzahl inkorrekt empfangener Nachrichten

Im Rahmen dieser Betrachtung gilt eine empfangene Nachricht Me_{Rxi} als inkorrekt, wenn deren Übertragungszeitwert $t_T(Me_{Rxi})$ über einem definierten Maximalwert T_{Tmax} liegt oder wenn der Dateninhalt am Ziel nicht dem an der Quelle entspricht. Des Weiteren wird bei Nachrichtenvertauschungen die verspätete Nachricht als inkorrekt gewertet, selbst wenn sie den Maximalwert T_{Tmax} nicht überschritten hat. Analog zu den korrekt empfangenen Nachrichten sind Dateninhalt, Reihenfolge, die Adresse einer empfangenen Nachricht zu berücksichtigen.

Die Anzahl inkorrekter Nachrichten (Number of false messages: N_{Fx}) ergibt sich damit wie folgt:

$$N_{Fx} = \sum_{i=1}^{n} f(Me_{Rxi}) \qquad (12)$$

$$mit \begin{cases} f(Me_{Rxi}) = 1, wenn\ Co(Me_{Rxi}) \neq Co(Me_{Txi}) \vee SN(Me_{Rxi}) \leq SN(Me_{Rxi-1}) \vee t_T(Me_{Rxi}) > T_{Tmax} \\ \vee\ Ad_{SCR}(Me_{Rxi}) \neq Ad_{SCR} \vee Ad_{DST}(Me_{Rxi}) \neq Ad_{DST} \\ f(Me_{Rxi}) = 0, sonst \end{cases}$$

$f(Me_{Rxi})$bezeichnet eine inkorrekte Nachricht. N_{Fx} bezeichnet die Anzahl inkorrekter Nachrichten, für die gilt:

- Der Inhalt der empfangenen Daten $Co(Me_{Rxi})$ stimmt nach einem Bitvergleich nicht mit dem Inhalt der gesendeten Daten $Co(Me_{Txi})$ überein. Es liegen Bitfehler bzw. Symbolfehler vor.
- Die laufende Nummer der empfangenen Nachricht $SN(Me_{Rxi})$ ist kleiner oder gleich der laufenden Nummer der vorherigen empfangenen Nachricht $SN(Me_{Rxi-1})$. Überholte Nachrichten werden somit als inkorrekt gewertet.
- Der Wert der Übertragungszeit $t_T(Me_{Rxi})$ ist größer oder gleich dem vorgegebenen Grenzwert T_{Tmax}.
- Die Adresse der Quelle $Ad_{SCR}(Me_{Rxi})$ in der Nachricht entspricht nicht der Quelladresse der logischen Verbindung. Über welche Parameter (Knotenadressen, Port, Endpunkt) die Adresse definiert wird, hängt von der jeweiligen Anforderung ab.
- Die Adresse des Ziels $Ad_{DST}(Me_{Rxi})$ in der Nachricht entspricht nicht der Zieladresse der logischen Verbindung. Über welche Parameter (Knotenadressen, Port, Endpunkt) die Adresse definiert wird, hängt von der jeweiligen Anforderung ab.

Je nach Anforderungen kann die Formel angepasst bzw. erweitert (z. B. Aktualisierungszeit) werden.

6.2.13 Anzahl empfangener Nachrichten unrechtmäßiger Herkunft

Es ist möglich, dass Nachrichten empfangen wurden, die nicht für das Ziel bestimmt waren. Sie stammen zum Beispiel von einer nicht zulässigen Quelle oder die Quelle war zwar zulässig, aber die Nachricht war für ein anderes Ziel bestimmt. In Abbildung 22 ist der Empfang von Nachrichten unrechtmäßiger Herkunft schematisch dargestellt.

Eine Nachricht kann mutwillig an den Empfänger gesendet (Angreifer) oder zufällig empfangen (Quelle 2) werden. In beiden Fällen ist es wichtig, dass die Nachricht als falsch erkannt und nicht berücksichtigt wird, damit die Anwendung falsche Daten nicht interpretiert und verarbeitet. Bei periodischer Übertragung zählt mindestens der Sendezeit-

abstand (transfer interval) in dem die Nachricht unrechtmäßiger Herkunft empfangen wurde als inkorrekt. Im Allgemeinen kann es bei der Verarbeitung dieser Nachrichten zu Überschreibungen korrekter Nachrichten oder blockieren des Empfangens von korrekten Nachrichten kommen.

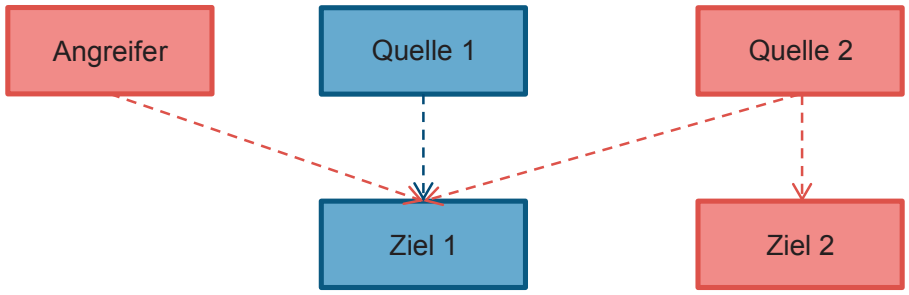


Abbildung 22: Empfangen einer Nachricht unrechtmäßiger Herkunft

Die Anzahl empfangener Nachrichten unrechtmäßiger Herkunft (Number of alien messages: N_{AN}) ergibt sich wie folgt:

$$N_{AN} = \sum_{i=1}^{n} a(Me_{Rxi}) \; mit \begin{cases} a(Me_{Rxi}) = 1, \; wenn \; Ad_{SCR}(Me_{Rxi}) \neq Ad_{SCR} \vee Ad_{DST}(Me_{Rxi}) \neq Ad_{DST} \\ a(Me_{Rxi}) = 0, sonst \end{cases} \quad (13)$$

$a(Me_{Rxi})$ bezeichnet die unrechtmäßige Herkunft einer Nachricht. N_{AN} bezeichnet die Anzahl empfangener Nachrichten unrechtmäßiger Herkunft (alien message), für die gilt:

- Die Adresse der Quelle $Ad_{SCR}(Me_{Rxi})$ in der Nachricht entspricht nicht der Quelladresse der logischen Verbindung.
- Die Adresse des Ziels $Ad_{DST}(Me_{Rxi})$ in der Nachricht entspricht nicht der Zieladresse der logischen Verbindung.

6.2.14 Anzahl verlorener Nachrichten

Eine Nachricht gilt als verloren, wenn an der Bezugsschnittelle der Quelle übergebene Nutzdaten nicht korrekt an der Bezugsschnittelle des Ziels übergeben werden. Dabei ist zu berücksichtigen, dass an der Bezugsschnittelle des Ziels ggf. auch Nachrichten unrechtmäßiger Herkunft (N_{AN}) übergeben werden. Es ist also in diesem Fall zu berücksichtigen, dass mehr Nachrichten ausgewertet werden als von der Quelle der logischen Verbindung gesendet wurden.

Die Anzahl verlorener Nachrichten (Number of lost messages: N_{LM}) ergibt sich somit aus der Differenz der gesendeten Nachrichten (Number of transmitted messages: N_{Tx}) sowie der empfangenen Nachrichten unrechtmäßigen Herkunft (N_{AN}) und den Nachrichten, die korrekt (N_{Rx}) und inkorrekt (N_{Fx}) empfangen wurden.

$$N_{LM} = N_{Tx} + N_{AN} - (N_{Rx} + N_{Fx}) \quad (14)$$

Um die verschiedenen Arten von Nachrichten besser differenzieren zu können, ist ein Beispiel in Abbildung 23 dargestellt. Q1 ist die rechtmäßige Quelle der logischen Verbindung, Q2 eine unrechtmäßige Quelle und Z ist das Ziel der logischen Verbindung. Q1 sendet 14 Nachrichten ($N_{Tx}=14$), Q2 sendet 2 Nachrichten. Das Ziel empfängt 15 Nachrichten.

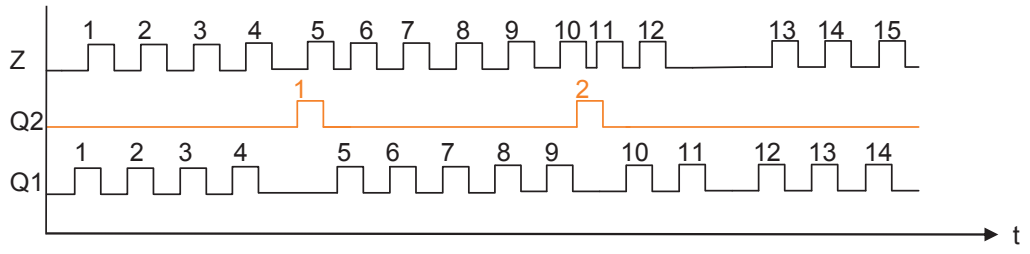


Abbildung 23: Beispiel: Nachrichten vor der Auswertung

Die 15 empfangenen Nachrichten werden ausgewertet. Davon seien, wie in Abbildung 24 dargestellt, 10 korrekt empfangene Nachrichten, 5 inkorrekt empfangene Nachrichten und 2 empfangene Nachrichten unrechtmäßiger Herkunft (Quelle Q2). Die empfangenen Nachrichten unrechtmäßiger Herkunft sind gemäß Abschnitt 6.2.12 Bestandteil von inkorrekt empfangenen Nachrichten.

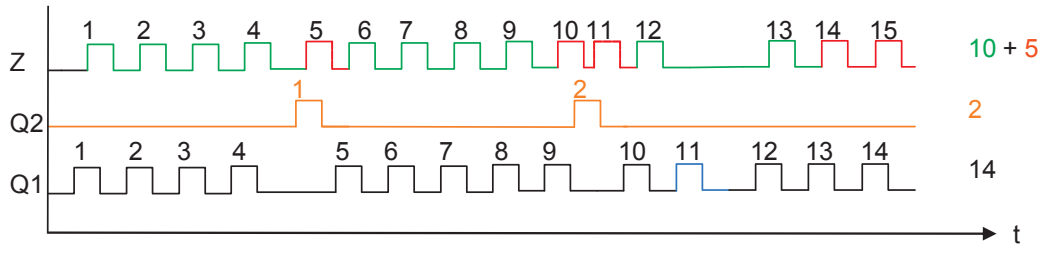


Abbildung 24: Beispiel: Nachrichten nach der Auswertung

$$N_{LM} = N_{Tx} - N_{Rx} - N_{Fx} + N_{AN} = 14 + 2 - (10 + 5) = 1 \quad (15)$$

Die Beispielrechnung in Gleichung (15) verdeutlicht, dass die Menge der empfangenen Nachrichten unrechtmäßiger Herkunft eine Teilmenge der inkorrekt empfangenen Nachrichten ist (Abbildung 25).

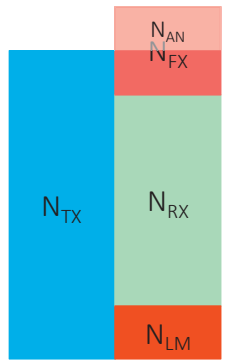


Abbildung 25: Mengen gesendeter, empfangener und verlorener Nachrichten

6.2.15 Ausfallrate

Die Ausfallrate λ, wird manchmal auch als Fehlerrate bezeichnet. Sie kann herangezogen werden, um zu bewerten, wie oft die logische Verbindung in einer Zeiteinheit ausfällt.

Als wahrscheinlichkeitstheoretische Maßgröße kann die mittlere Ausfallrate genutzt werden, die gemäß Gleichung (16) dem Reziproken der mittleren Betriebszeit zwischen Ausfällen entspricht.

$$\overline{\lambda} = \frac{1}{MTBF} \tag{16}$$

6.2.16 Nachrichtenfehlerquote

Die Nachrichtenfehlerquote (message error ratio: *MER*) ergibt sich aus dem Verhältnis der inkorrekt empfangenen Nachrichten N_{Fx} und den gesendeten Nachrichten N_{Tx}.

$$MER = \frac{N_{Fx}}{N_{Tx}} \tag{17}$$

Die Nachrichtenfehlerwahrscheinlichkeit ist die Wahrscheinlichkeit, dass die empfangene Nachricht, im Vergleich mit der entsprechenden gesendeten Nachricht, fehlerbehaftet und somit inkorrekt ist.

6.2.17 Nachrichtenverlustquote

Die Nachrichtenverlustquote (Message Loss Rate – *MLR*) ist gemäß [2] IEV 371-08-07 das Verhältnis der Anzahl der verlorenen Nachrichten zur Gesamtzahl der gesendeten Nachrichten.

$$MLR = \frac{N_{LM}}{N_{Tx}} \tag{18}$$

6.2.18 Restfehlerquote

Die Restfehlerquote (Residual Error Rate – *RER*) ist nach [2] IEV 371-08-05 das Verhältnis der Anzahl unerkannter fehlerhafter Nachrichten zur Gesamtzahl der gesendeten Nachrichten.

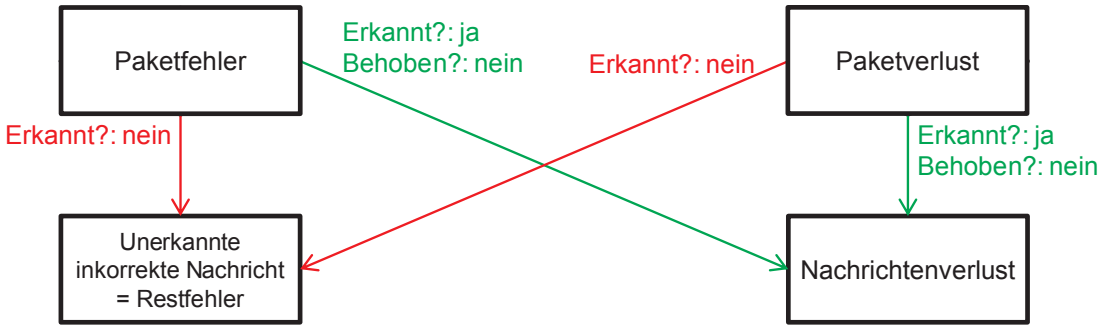


Abbildung 26: Auswirkungen von Paketfehler und Paketverlust

In Abbildung 26 sind mögliche Auswirkungen von Paketfehlern und Paketverlusten aufgezeigt. Es wird unterschieden ob sie erkannt bzw. behoben werden. Es sollen hier vier Fälle unterschieden werden.

Im ersten Fall wird der Paketfehler nicht erkannt. Dies führt zu einer inkorrekten Nachricht die direkt an die Applikation weitergegeben wird. Diese unerkannte inkorrekte Nachricht ist ein Restfehler (vgl. Definition Restfehlerquote [2] – IEV 371-08-05, 721-08-56). Somit ergibt sich, dass in der vorliegenden Betrachtungsweise die Nachrichtenfehlerquote der Restfehlerquote entspricht.

Im zweiten Fall wird ein Paketfehler erkannt, kann aber nicht behoben werden. Dies hat zur Folge, dass die Nachricht nicht zusammengefügt werden kann. Es folgt ein Nachrichtenverlust.

Im dritten Fall wird ein Paketverlust nicht erkannt. Dies führt zu einem Nachrichtenfehler. Die Nachricht wird in den oberen Kommunikationsschichten unvollständig zusammengefügt und direkt an die Applikation weitergegeben. Diese unerkannte inkorrekte Nachricht ist ein Restfehler.

Im vierten Fall wird ein Paketverlust erkannt, kann aber nicht behoben werden. Dies hat zur Folge, dass die Nachricht nicht zusammengefügt werden kann. Es folgt ein Nachrichtenverlust.

Werden Paketfehler oder Paketverlust erkannt und behoben, entsteht weder ein Nachrichtenverlust, noch ein Nachrichtenfehler. Die Sicherheits- und Rekonstruktionsmechanismen haben gegriffen und es sind keine negativen Auswirkungen für den Nachrichteninhalt aufgetreten. Aus diesem Grund ist der Fall nicht im Bild dargestellt.

In [2] IEV 721-08-56 ist für die Restfehlerquote synonym die Restfehlerhäufigkeit definiert als Verhältnis der Anzahl Bits, Einheitsschnittstelle, Zeichen oder Blöcke, die unrichtig empfangen und unerkannt oder unkorrigiert durch die Fehlerminderungseinrichtungen bleiben, zur Gesamtzahl der entsprechenden gesendeten Elemente.

6.3 Leistungsmerkmale

6.3.1 Verfügbarkeit

Gemäß der Definition (Abschnitt 4.1) ist die Verfügbarkeit (Availability: A) ein Maß für die Fähigkeit einer Einheit, während eines gegebenen Zeitintervalls in einem wie geforderten funktionsfähigen Zustand zu sein. Angewandt auf die Funktion einer logischen Verbindung ist die Verfügbarkeit das Verhältnis der Klarzeit (Uptime: t_U) zu einem Betrachtungszeitraum (Observation time: t_O):

$$A = \frac{1}{t_O} \sum_{i=1}^{t_O} t_U \qquad (19)$$

Unter der Annahme, dass die Quelle im Betrachtungszeitraum t_O eine Anzahl Nachrichten (Number of transmitted messages: N_{Tx}) periodisch mit einem Sendezeitabstand (Transfer interval: t_{TI}) versendet und dass die Funklösung für jede empfangene Nachricht für die Zeit des Sendezeitabstandes als korrekt empfangene Nachricht (N_{Rx}-Kapitel 6.2.11) gilt, kann die Verfügbarkeit wie folgt bestimmt werden:

$$A = \frac{N_{Rx} t_{TI}}{N_{Tx} t_{TI}} = \frac{N_{Rx}}{N_{Tx}} \qquad (20)$$

Aus Sicht der Applikation sind aufgeführte Kenngrößen zur Bewertung der Zuverlässigkeit relevant, die in Richtlinienblatt 4 der VDI/VDE-Richtlinie 2185 [1] definiert sind.

6.3.2 Funktionsfähigkeit

Auf den ersten Blick gibt es keinen Unterschied zwischen den Begriffen Verfügbarkeit (Kapitel 4.1) und Funktionsfähigkeit (Kapitel 4.2.2). Gemäß Definition der Verfügbarkeit ist die Funktionsfähigkeit aber nur ein Merkmal der Verfügbarkeit. Zur Bewertung der Verfügbarkeit sind zusätzlich die Merkmale zu betrachten, die die Vermeidung von Ausfällen (Instandhaltbarkeit) oder die Wiederherstellung der Funktion (Wiederherstellbarkeit) beschreiben. Deshalb muss eine funktionsfähige Kommunikationsverbindung nicht zwangsläufig auch eine hohe Verfügbarkeit haben.

In Abbildung 27 a ist die Betriebszeit zwischen zwei Ausfällen im Mittel hoch gegenüber Abbildung 27 b. Das heißt, die Funktionsfähigkeit ist in Abbildung 27 a größer. Eine Kommunikationsverbindung ist umso funktionsfähiger, je seltener Ausfälle auftreten. Über die Länge der Unterbrechung der Funktion sagt der Begriff Funktionsfähigkeit nichts aus.

Die akkumulierte Funktionsfähigkeit ist in Abbildung 27b höher als in Abbildung 27a und somit ist das Verhältnis zwischen Klarzeitintervall und Beobachtungszeit in Abbildung 27 b günstiger. Das heißt, die Verfügbarkeit ist in Abbildung 27 b größer. Allerdings sind die Betriebszeiten zwischen den Fehlern (TBF – Abschnitt 4.3.7) in Abbildung 27a länger, aber auch die Ausfallzeiten.

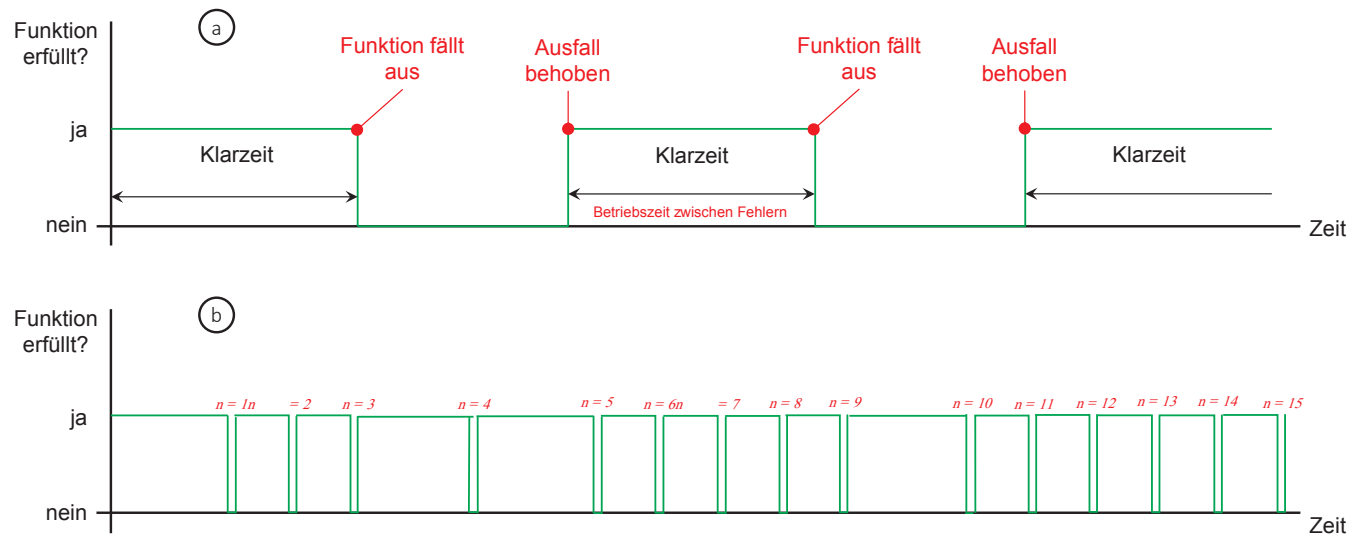


Abbildung 27: Unterschied zwischen hoher Funktionsfähigkeit (a) und hoher Verfügbarkeit (b)

6.4 Fazit

In Abbildung 28 ist die Gliederung nach relevanten Leistungsmerkmalen, Kenngrößen und Maßgrößen der Zuverlässigkeit in Anlehnung an [18] S.91 erfolgt und in Hinblick auf die Funkkommunikation erweitert.

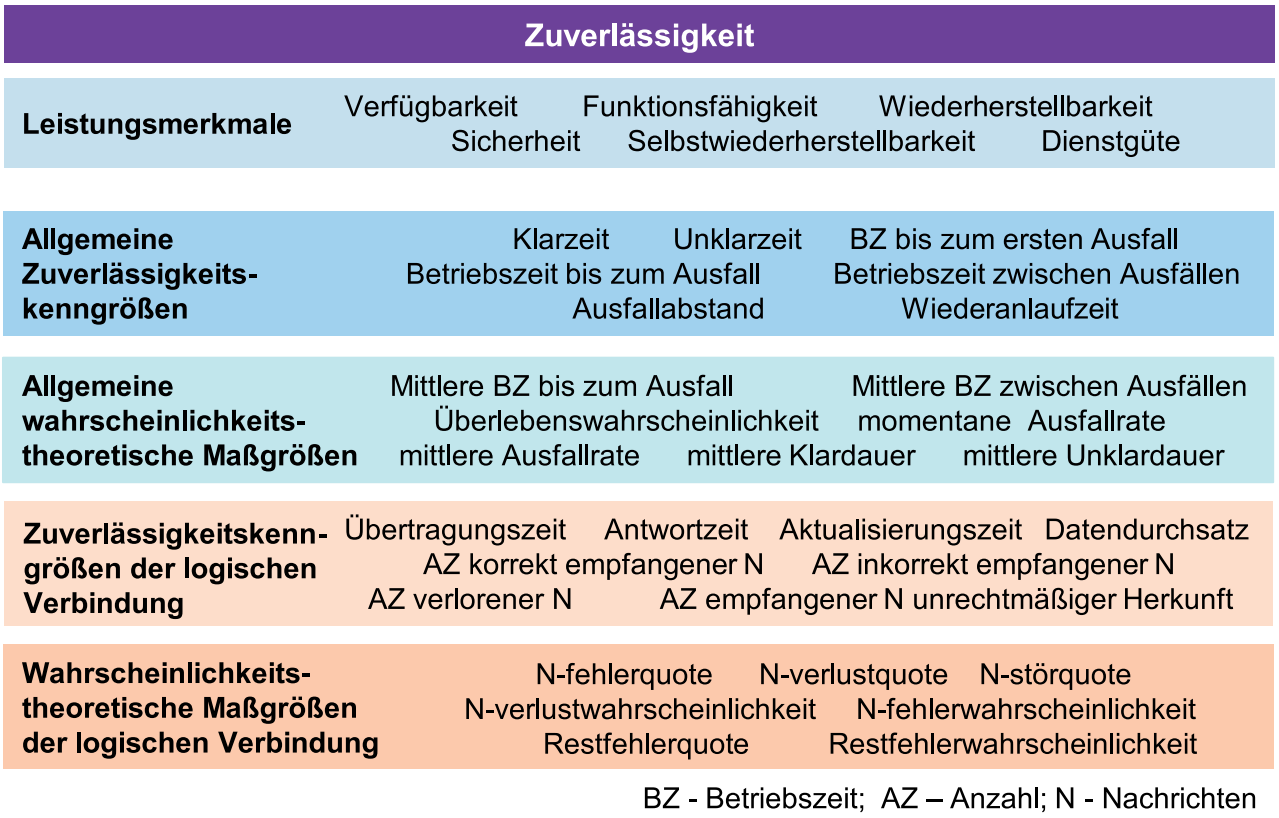


Abbildung 28: Zuverlässigkeit, Leistungsmerkmale, Zuverlässigkeitskenngrößen und Maßgrößen

Die allgemeinen Zuverlässigkeitskenngrößen – im Besonderen die Klarzeit und Unklarzeit – stehen im Mittelpunkt. Sie sind die Grundlage zum einen zur Berechnung einzelner Leistungsmerkmale zum anderen für die allgemeinen wahrscheinlichkeitstheoretischen Maßgrößen (kurz: allgemeine Maßgrößen). Die Zuverlässigkeitskenngrößen der logischen Verbindung, wie zum Beispiel die Anzahl korrekt oder inkorrekt empfangener Nachrichten, werden übertragender Maßen auch Klarzeit und Unklarzeit zugeordnet. Wird eine Nachricht korrekt empfangen, befindet sich das System im Klarzustand. Das System verbleibt solange im Klarzustand wie Nachrichten korrekt empfangen werden (Klarzeit). Werden Nachrichten inkorrekt empfangen oder gehen gar verloren, befindet sich das System im Unklarzustand und zwar solange bis Nachrichten wieder korrekt empfangen werden. Die Anzahl korrekt empfangener Nachrichten kann sich also über den gesamten betrachteten Zeitraum beziehen (Bezug zur Verfügbarkeit) oder auf ein Klarzeitintervall zwischen Ausfällen (Bezug zur Betriebszeit zwischen Ausfällen). Diese Klarzeitintervalle können wiederum gemittelt werden (Bezug zur mittleren Betriebszeit zwischen Ausfällen). Aus den Zuverlässigkeitskenngrößen der logischen Verbindung können dementsprechend über die allgemeinen Zuverlässigkeitskenngrößen Leistungsmerkmale und allgemeine Maßgrößen berechnet werden. Außerdem dienen die Zuverlässigkeitskenngrößen der logischen Verbindung noch zur Berechnung einiger wahrscheinlichkeitstheoretischen Maßgrößen der logischen Verbindung, wie Nachrichtenverlustquote, -fehlerquote, oder -störquote. Die Wahrscheinlichkeiten beruhen nur auf theoretischen Berechnungen, deshalb stehen diese Einzeln und in keiner Abhängigkeit von anderen Größen.

In der jeweiligen Gruppe stehen die Größen natürlich auch im Zusammenhang. Zum Beispiel bei den allgemeinen Zuverlässigkeitskenngrößen ist die Zeit zwischen den Ausfällen (bei periodischen Systemen) gleich der Klarzeit. Ein anderes Beispiel ist die Wiederanlaufzeit, sie ist Bestandteil der Unklarzeit. Die mittleren Zeiten (Gruppe der allgemeinen Maßgrößen) werden aus ihren zugehörigen Kenngrößen berechnet. Aus der $MTBF$ kann man dann die Ausfallrate λ und aus dieser wiederum die Überlebenswahrscheinlichkeitsfunktion $R(t)$ berechnen.

7 Leistungsmerkmale, Kenn- und Maßgrößen zur Bewertung der Zuverlässigkeit der anderen Betrachtungseinheiten

7.1 Allgemeines

Die Betrachtungen aus Kapitel 6 können auch für die anderen in Kapitel 5 diskutierten Betrachtungseinheiten vorgenommen werden. Im folgende wird sich auf einige wenige Aspekte beschränkt.

7.2 Kommunikationsgerät

7.2.1 Allgemeines

In Tabelle 3 werden die Leistungsmerkmale der Zuverlässigkeit für ein Kommunikationsgerät bewertet.

IEV Nummer	Benennung DE	Benennung ENG	Relevant für Kommunikationsgerät
192-01-23	Verfügbarkeit	Availability	Ja
192-01-24	Funktionsfähigkeit	Reliability	Ja
192-01-25	Wiederherstellbarkeit	Recoverability	Ja
192-01-26	Selbstwiederherstellbarkeit	Self-recoverability	Ja
192-01-27	Instandhaltbarkeit	Maintainability	Ja
192-01-29	Instandhaltungsbereitschaft	Maintenance support performance	Ja
192-01-21	Haltbarkeit	Durability	Ja
351-57-05	Sicherheit	Safety	Ja
–	Informationssicherheit	Information Security	Ja
351-57-06	Funktionale Sicherheit	Functional safety	Ja
715-07-14	Dienstgüte	Quality of service	Ja

Tabelle 3: Übersicht über Leistungsmerkmale der Zuverlässigkeit für ein Kommunikationsgerät

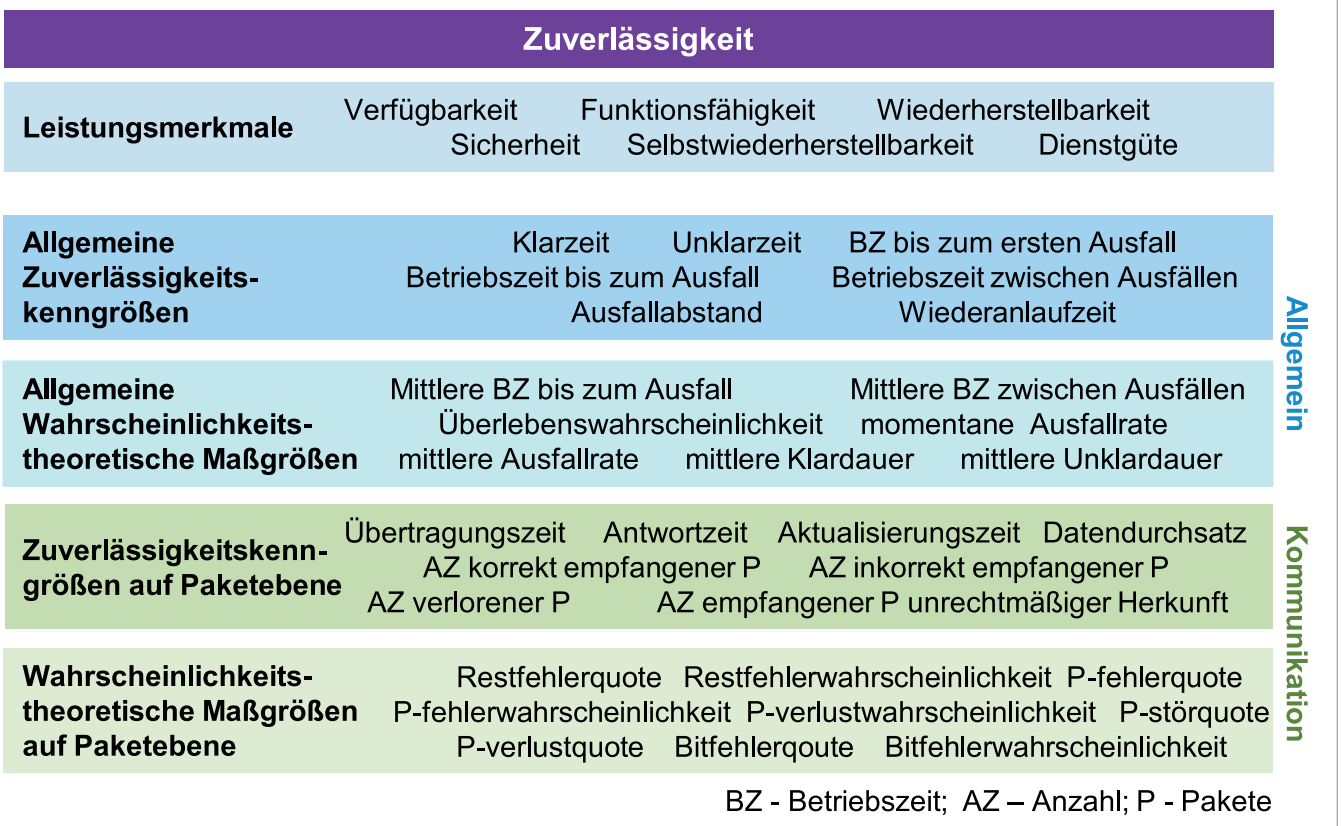


Abbildung 29: Zuverlässigkeit, Leistungsmerkmale, Zuverlässigkeitskenngrößen und Maßgrößen

Auf der Ebene der Kommunikationsgeräte der unteren Kommunikationsschichten sprechen wir bei der Übertragung von Pakten und nicht wie bei der logischen Verbindung von Nachrichten. Die entsprechenden Kenn- und Maßgrößen sind zur Vollständigkeit in Abbildung 29 aufgeführt, stehen aber nicht im Fokus der Bewertung.

Des Weiteren gibt es Kenngrößen die Aussagen zu Instandhaltung, Instandhaltungsbereitschaft und zur Hard- und Softwareperformance treffen. Bei den Betrachtungen stehen diese Kenngrößen nicht im Fokus und werden deshalb an dieser Stelle nicht weiter ausgeführt.

7.2.2 Anzahl korrekt empfangener Pakete

Ein Paket P_{Ri} gilt zunächst als empfangen, wenn es an der Bezugsschnittelle des Ziels an höhere Kommunikationsschichten übergeben wurde. Die Anzahl empfangener Pakete (Number of recieved packages: N_{RP}) ergibt sich aus:

$$N_{RP} = \sum_{i=1}^{n} P_{Ri} \qquad (21)$$

Da es allerdings zu Verfälschungen des Inhalts und zu Wiederholungen der Übertragung kommen kann, die nicht durch die Fehlersicherungsmechanismen der Funklösung identifiziert und beseitigt werden, sind die empfangenen Daten daraufhin zu prüfen. Außerdem gehört die Rechtzeitigkeit zu den Bedingungen einer korrekt empfangener Pakete. Deshalb werden bei der nachfolgend aufgeführten Bestimmung der korrekt empfangenen Pakete der Dateninhalt (Data content: Co), die Reihenfolge (Sequence number: SN), die Übertragungszeit $t_T(P_{Ri})$ und die Adresse der Geräte (Address: Ad) berücksichtigt.

$$N_{RCP} = \sum_{i=1}^{n} c(P_{Ri}) \tag{22}$$

$$mit \begin{cases} c(P_{Ri}) = 1, wenn\ Co(P_{Ri}) = Co(P_{Ri}) \wedge SN(P_{Ri}) > SN(P_{Ri-1}) \wedge t_T(P_{Ri}) \leq T_{Tmax} \\ \wedge\ Ad_{SCR}(P_{Ri}) \in A\ \wedge\ Ad_{DST}(P_{Ri}) \in B \\ c(P_{Ri}) = 0, sonst \end{cases}$$

N_{RCP} bezeichnet demzufolge die Anzahl korrekt empfangener Pakete, für die gilt:

- Der Inhalt der empfangenen Daten $Co(P_{Ri})$ stimmt nach einem Bitvergleich mit dem Inhalt der gesendeten Daten $Co(P_{Ri})$ überein. Es liegen keine Bitfehler bzw. Symbolfehler vor. Die Korrektheit (correctness) einer empfangenen Nachricht ist mit $c(P_{Ri})$ bezeichnet. Eine CRC-Prüfung ist dafür nicht ausreichend.
- Die laufende Nummer der empfangenen Nachrichten $SN(P_{Ri})$ muss mit größer als die laufende Nummer der vorherigen empfangenen Nachricht $SN(P_{Ri-1})$ sein. Überholte Nachrichten werden somit als Verlust gewertet.
- Der Wert der Übertragungszeit $t_T(P_{Ri})$ muss kleiner sein, als ein vorgegebener Grenzwert T_{Tmax}
- Die Adresse der Quelle $Ad_{SCR}(P_{Ri})$ in der Nachricht muss Bestandteil der Menge A der erlaubten Quellen sein. Über welche Parameter (Knotenadressen, Port, Endpunkt) die Adresse definiert wird, hängt von der jeweiligen Anforderung ab.
- Die Adresse des Ziels $Ad_{DST}(P_{Ri})$ in der Nachricht muss Bestandteil der Menge B der erlaubten Ziele sein. Über welche Parameter (Knotenadressen, Port, Endpunkt) die Adresse definiert wird, hängt von der jeweiligen Anforderung ab.

Dies stellt den allgemeinen Fall von mehreren Zielen und Quellen dar. Je nach Anforderungen kann die Formel angepasst bzw. erweitert (Aktualisierungszeit, Jitter) werden.

Die Formel lässt sich vereinfachen, wenn nur eine Quelle und ein Ziel vorhanden ist.

$$N_{RCP} = \sum_{i=1}^{n} c(P_{Ri}) \tag{23}$$

$$mit \begin{cases} c(P_{Ri}) = 1, wenn\ Co(P_{Ri}) = Co(P_{Ri}) \wedge SN(P_{Ri}) > SN(P_{Ri-1}) \wedge t_T(P_{Ri}) \leq T_{Tmax} \\ c(P_{Ri}) = 0, sonst \end{cases}$$

7.2.3 Anzahl inkorrekt empfangener Pakete

Im Rahmen dieser Betrachtung gilt eine empfangenes Paket P_{Ri} als inkorrekt, wenn dessen Übertragungszeitwert $t_T(P_{Ri})$ über einem definierten Maximalwert T_{Tmax} liegt oder wenn der Dateninhalt am Ziel nicht dem an der Quelle entspricht. Des Weiteren wird bei Paketvertauschungen das verspätete Paket als inkorrekt gewertet, selbst wenn es den Maximalwert T_{Tmax} nicht überschritten hat. Analog zu den korrekt empfangenen Paketen sind Dateninhalt, Reihenfolge und die Adresse der Geräte eines empfangenen Paketes zu berücksichtigen.

Die Anzahl inkorrekt empfangener Pakete (Number of false packages: N_{FP}) ergibt sich damit wie folgt:

$$N_{RFP} = \sum_{i=1}^{n} f(P_{Ri}) \tag{24}$$

$$mit \begin{cases} f(P_{Ri}) = 1, wenn\ Co(P_{Ri}) \neq Co(P_{Ri}) \vee SN(P_{Ri}) \leq SN(P_{Ri-1}) \vee t_T(P_{Ri}) > T_{Tmax} \\ \vee\ Ad_{SCR}(P_{Ri}) \notin A \vee Ad_{DST}(P_{Ri}) \notin B \\ f(P_{Ri}) = 0, sonst \end{cases}$$

N_{RFP} bezeichnet die Anzahl inkorrekter Pakete, für die gilt:

- Der Inhalt der empfangenen Daten $Co(P_{Ri})$ stimmt nach einem Bitvergleich nicht mit dem Inhalt der gesendeten Daten $Co(P_{Ri})$ überein. Es liegen Bitfehler bzw. Symbolfehler vor.
- Die laufende Nummer des empfangenen Paketes $SN(P_{Ri})$ ist kleiner oder gleich der laufende Nummer der vorherigen empfangenen Paketes $SN(P_{Ri-1})$. Überholte Pakete werden somit als Verlust gewertet.
- Der Wert der Übertragungszeit $t_T(P_{Ri})$ ist größer oder gleich dem vorgegebenen Grenzwert T_{Tmax}
- Die Adresse der Quelle $Ad_{SCR}(P_{Ri})$ in den Paketen ist kein Element der Menge A der erlaubten Quellen. Über welche Parameter (Knotenadressen, Port, Endpunkt) die Adresse definiert wird, hängt von der jeweiligen Anforderung ab.
- Die Adresse des Ziels $Ad_{DST}(P_{Ri})$ in dem Paket ist kein Element der Menge B der erlaubten Ziele. Über welche Parameter (Knotenadressen, Port, Endpunkt) die Adresse definiert wird, hängt von der jeweiligen Anforderung ab.

Dies stellt den allgemeinen Fall von mehreren Quellen und Zielen dar. Je nach Anforderungen kann die Formel angepasst bzw. erweitert (Aktualisierungszeit, Jitter) werden.

Die Formel lässt sich analog zu den korrekt empfangenen Paketen vereinfachen, wenn nur eine Quelle und ein Ziel vorhanden sind.

$$N_{RFP} = \sum_{i=1}^{n} f(P_{Ri}) \tag{25}$$

$$mit \begin{cases} f(P_{Ri}) = 1, Co(P_{Ri}) \neq Co(P_{Ri}) \vee SN(P_{Ri}) \leq SN(P_{Ri-1}) \vee t_T(P_{Ri}) > T_{Tmax} \\ f(P_{Ri}) = 0, sonst \end{cases}$$

7.2.4 Anzahl empfangener Pakete unrechtmäßiger Herkunft

Es ist möglich, dass Pakete empfangen wurden, die nicht für das Ziel bestimmt waren. Sie stammen zum Beispiel von einer nicht zulässigen Quelle oder die Quelle war zwar zulässig, aber das Paket war für einen anderes Ziel bestimmt. Eine Paket kann mutwillig eingefügt oder zufällig empfangen werden. In beiden Fällen ist es wichtig, dass das Paket als falsch erkannt und nicht berücksichtigt wird, damit falsche Daten nicht interpretiert und verarbeitet werden.

Die Anzahl empfangener Pakete unrechtmäßiger Herkunft (Number of alien packages: N_{ANP}) ergibt sich wie folgt:

$$N_{ANP} = \sum_{i=1}^{n} a(P_{Ri}) \; mit \begin{cases} a(P_{Ri}) = 1, wenn \; Ad_{SCR}(P_{Ri}) \notin A \; \vee \; Ad_{DST}(P_{Ri}) \notin B \\ a(P_{Ri}) = 0, sonst \end{cases} \quad (26)$$

$a(P_{Ri})$ bezeichnet die unrechtmäßige Herkunft eines Paketes. N_{ANP} bezeichnet demzufolge die Anzahl empfangener Nachrichten unrechtmäßiger Herkunft (alien packet), für die gilt:

- Die Adresse der Quelle $Ad_{SCR}(P_{Ri})$ in der Nachricht ist kein Element der Menge A der erlaubten Quellen.
- Die Adresse des Ziels $Ad_{DST}(P_{Ri})$ in der Nachricht ist kein Element der Menge B der erlaubten Ziele.

7.2.5 Anzahl verlorener Pakete

Ein Paket gilt als verloren, wenn an der Bezugsschnittelle der Quelle übergebene Nutzdaten nicht an der Bezugsschnittelle des Ziels übergeben werden. Die Anzahl der verlorenen Pakete (number of lost packages: N_{LP}) ergibt sich aus der Differenz der gesendeten Pakete (Number of transmitted packages: N_{TP}) sowie der empfangenen Pakete unrechtmäßigen Herkunft (N_{ANP}) und den korrekt und inkorrekt empfangenen Paketen (N_{RCP}, N_{RFP}).

$$N_{LP} = N_{TP} - N_{RCP} - N_{RFP} + N_{ANP} \quad (27)$$

Für den vereinfachten Fall, wenn nur eine Quelle und ein Ziel sind, gilt:

$$N_{LP} = N_{TP} - N_{RP} \quad (28)$$

Die Anzahl der den verlorenen Pakete N_{LP} ergibt sich aus den gesendeten Paketen (N_{TP}) und den empfangenen Paketen N_{RP}.

7.2.6 Paketfehlerquote und Paketfehlerwahrscheinlichkeit

Als Kriterium für die Qualität einer Übertragungsstrecke wird gelegentlich die Paketfehlerwahrscheinlichkeit angegeben, die sich aus der Bitfehlerwahrscheinlichkeit (p) und der Länge der Pakete (L) wie folgt berechnen lässt.

$$\mathrm{p}_E = 1 - (1 - \mathrm{p})^L \tag{29}$$

In der Praxis werden Paketfehlerwahrscheinlichkeit und Paketfehlerquote (PER) sowie Bitfehlerwahrscheinlichkeit und Bitfehlerquote (BER) häufig gleichgesetzt. Generell gilt: Die Wahrscheinlichkeiten sind theoretische Werte, die Quoten können durch Messwerte ermittelt werden.

Die Paketfehlerquote ergibt sich aus der Division der inkorrekt empfangenen Pakete N_{RFP} und den gesendeten Paketen N_{TP}.

$$\mathrm{PER} = \frac{N_{RFP}}{N_{TP}} \tag{30}$$

Im Gegensatz zu den Quoten beschreiben die Wahrscheinlichkeiten eine durch theoretische Überlegungen berechnete Wahrscheinlichkeit für das Auftreten eines Bit- bzw. Paketfehlers. Diese Berechnungen von Paketfehler- und Bitfehlerwahrscheinlichkeiten sind i.d.R. nur für idealisierte Szenarien möglich. Sie werden häufig verwendet, um Grenzen der Leistungsfähigkeit von nachrichtentechnischen Systemen zu bestimmen.

7.2.7 Paketverlustquote

Die Paketverlustquote (ratio of packet loss: RPL) ist das Verhältnis der Anzahl der verlorenen Pakete zur Gesamtzahl der gesendeten Pakete.

$$\mathrm{RPL} = \frac{N_{LM}}{N_{Tx}} \tag{31}$$

7.2.8 Paketstörquote

Die Paketstörquote (ratio of packet interference: RPI) ist das Verhältnis der Anzahl empfangener Pakete unrechtmäßiger Herkunft zur Gesamtzahl der gesendeten Pakete.

Die Paketstörquote ist ein Maß für die Belastung des Ziels durch empfange Pakete unrechtmäßiger Herkunft sein. Es werden Beeinträchtigungen abgeleitet.

$$\mathrm{RPI} = \frac{N_{AP}}{N_{TP}} \tag{32}$$

7.3 Physikalische Verbindung

In Tabelle 4 werden die Leistungsmerkmale der Zuverlässigkeit für eine physikalische Verbindung bewertet.

IEV Nummer	Benennung DE	Benennung ENG	Relevant für physikalische Verbindung
192-01-23	Verfügbarkeit	Availability	Ja
192-01-24	Funktionsfähigkeit	Reliability	Ja
192-01-25	Wiederherstellbarkeit	Recoverability	Ja
192-01-26	Selbstwiederherstellbarkeit	Self-recoverability	Ja
192-01-27	Instandhaltbarkeit	Maintainability	Nein
192-01-29	Instandhaltungsbereitschaft	Maintenance support performance	Nein
192-01-21	Haltbarkeit	Durability	Nein
351-57-05	Sicherheit	Safety	Ja
–	Informationssicherheit	Information Security	Ja
351-57-06	Funktionale Sicherheit	Functional safety	Nein
715-07-14	Dienstgüte	Quality of service	Ja

Tabelle 4: Übersicht über Leistungsmerkmale der Zuverlässigkeit für eine physikalische Verbindung

Relevante Kenngrößen für die physikalische Verbindung sind zum Beispiel Bitfehlerquote, Bitfehlerwahrscheinlichkeit und Symbolfehlerwahrscheinlichkeit. Diese Kenngrößen sind für die logische Verbindung nicht relevant, da Bitfehler durch Mechanismen bei der Zusammenfügung zu einem Paket beseitigt werden. Durch diese Mechanismen sollten trotz Bitfehler die Pakete korrekt empfangen werden können. Der Vollständigkeit halber sind im Folgenden die Definitionen aufgeführt.

Bitfehlerquote, bit error rate (*BER*) ([2] – IEV 371-08-01)
„Verhältnis der Anzahl invertiert empfangener Bits zur Gesamtzahl der gesendeten Bits“

Bitfehlerquote, Bitfehlerrate (*veraltet*) ([2] – IEV 704-18-04)
„Fehlerquote für ein Binärsignal“

Bitfehlerwahrscheinlichkeit ([2] – IEV 371-08-02)
„Wahrscheinlichkeit, dass ein empfangenes Bit im Vergleich zum entsprechenden gesendeten Bit invertiert ist“

7.4 Kommunikationssystem

Das Kommunikationssystem umfasst mehrere logische Verbindungen mit eventuell unterschiedlichen Anforderungen der einzelnen Kenngrößen wie zum Beispiel der Übertragungszeit oder dem Datendurchsatz. Wichtige Kenngrößen für das Kommunikationssystem sind das Klar- und Unklarzeitintervall des Systems, die Überlebensfähigkeit des Systems (einfach, zweifach, n-fach zusammenhängend) [25] bzw. generell die Zusammenhänge zwischen Komponenten- und Systemzustände bezüglich Redundanz.

Leistungsmerkmale (Tabelle 5) wie Verfügbarkeit und Wiederherstellbarkeit des Kommunikationssystems sind wie auch bei der logischen Verbindung von hoher Relevanz. Die gesamtheitliche Bewertung der funktionalen Sicherheit von Kommunikationssysteme ist bisher nicht möglich.

IEV Nummer	Benennung DE	Benennung ENG	Relevant für Kommunikationssystem
192-01-23	Verfügbarkeit	Availability	Ja
192-01-24	Funktionsfähigkeit	Reliability	Ja
192-01-25	Wiederherstellbarkeit	Recoverability	Ja
192-01-26	Selbstwiederherstellbarkeit	Self-recoverability	Ja
192-01-27	Instandhaltbarkeit	Maintainability	Ja
192-01-29	Instandhaltungsbereitschaft	Maintenance support performance	Ja
192-01-21	Haltbarkeit	Durability	Ja
351-57-05	Sicherheit	Safety	Ja
–	Informationssicherheit	Information Security	Ja
351-57-06	Funktionale Sicherheit	Functional safety	Nein
715-07-14	Dienstgüte	Quality of service	Ja

Tabelle 5: Übersicht über Leistungsmerkmale der Zuverlässigkeit für ein Kommunikationssystem

8 Zuverlässigkeitsbetrachtungen am Beispiel funktionaler Sicherheit

8.1 Motivation

Die Zuverlässigkeit industrieller Kommunikationssysteme wird insbesondere für funktional sichere (Safety) Anwendungen betrachtet. Zur Bewertung und Prüfung der Zuverlässigkeit verwendet man zuvor beschriebene wahrscheinlichkeitstheoretische Maßgrößen. Dieses Anwendungsfeld ist somit ein Beispiel für deren praktische Verwendung.

8.2 Prinzipien für Sicherheitskommunikationssysteme

Sicherheitskommunikationssysteme basieren heute zumeist auf dem Black-Channel-Prinzip, bei dem zwischen der Sicherheitsanwendung und einem nichtsicheren Kommunikationskanal ein Sicherheitsprotokoll integriert wird. Diese Sicherheitskommunikationsschicht entspricht dem Sicherheitsniveau des sicherheitsrelevanten Systems und erkennt oder beherrscht die Übertragungsfehler des darunterliegenden Kommunikationskanals (Black Channel). In Tabelle 6 aus [26] sind Maßnahmen zur Erkennung von Kommunikationsfehlern genannt, die in der Sicherheitskommunikationsschicht integriert sind. Jede Sicherheitsmaßnahme kann zur Erkennung eines oder mehrerer Fehler führen.

Fehler	Maßnahmenkatalog							
	Laufende Nummer	Zeitstem-spelung	Zeiter-wartung	Verbindungs-erkennung	Empfangs-bestätigung (Echo)	Datensicherung	Redundanz mit Kreuzvergleich	Unterschiedliche Datensicherung SR-NSR
Verfälschung					x	x	Nur für serielle Busse	
Unbeabsichtigte Wiederholung	x	x					x	
Falsche Abfolge	x	x					x	
Verlust	x				x		x	
Inakzeptable Verzögerung		x	x					
Einfügung	x			x	x		x	
Maskerade				x	x			x
Falsche Adressierung				x				

Tabelle 6: Überblick von Maßnahmen zur Erkennung von Kommunikationsfehlern [26]

Durch Verwendung dieser Sicherheitskommunikationsschicht lassen sich somit komplexe Kommunikationsverfahren wie Ethernet- und Funk-basierte Protokolle oder auch Netzübergänge zwischen Teilsystemen und Rückwandbussen verwenden, ohne dass dafür die Einhaltung von Sicherheitsnormen wie der IEC 61508 nachzuweisen ist. Allerdings werden dann auch die im Kommunikationskanal bereits enthaltenen Maßnahmen (CRC, Zeitüberwachung etc.) bei der Sicherheitsbewertung nicht berücksichtigt. Mit den zusätzlichen evtl. redundanten Maßnahmen gehen Nachteile im Zeitverhalten der Kommunikationsverbindung einher, die bei der Anwendung des sogenannten White Channel Prinzip verringert bzw. vermieden werden können. Im Gegensatz zum Black Channel Prinzip muss der komplette Kommunikationskanal (Hardware, Software, Netzkomponenten) nach IEC 61508 entworfen, implementiert und geprüft werden, sofern Sicherheitsfunktionen direkt im Kommunikationskanal implementiert oder die enthaltenen Maßnahmen bei der Sicherheitsbewertung berücksichtigt werden sollen [27]. Die zuvor beschriebenen Maßgrößen können bei der Bewertung und Prüfung helfen.

8.3 Sicherheits-Integritätslevel

Zur Bewertung der Zuverlässigkeit des gesamten Systems werden Ausfallwahrscheinlichkeiten bzw. Ausfallraten genutzt. Entsprechend dieser Ausfallwahrscheinlichkeiten können die Systeme, wie in Tabelle 7 aufgeführt, unterschiedliche Safety Integrity Level (*SIL*) erreichen.

Sicherheits-Integritätslevel (*SIL*)	Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (Wahrscheinlichkeit eines gefahrbringenden Fehlers pro Stunde (*PFH*))
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Tabelle 7: Sicherheits-Integritätslevel: Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben wird [28]

Dabei ist zu beachten, dass eine logische Verbindung des sicheren Kommunikationskanals nicht mehr als 1 % der Maximalwerte von PFH_d des Ziel-*SIL* benötigen soll (siehe Abbildung 30).

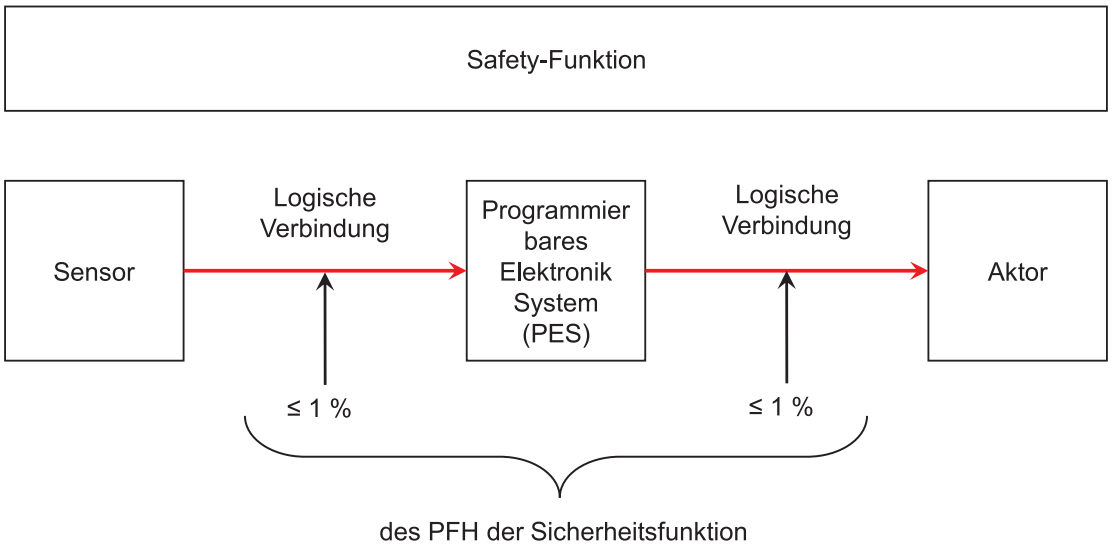


Abbildung 30: Funktional sichere Kommunikation als Teil einer Safety-Funktion

Soll beispielsweise die Sicherungsfunktion *SIL2* mit einer PFH_d von 10^{-6} erreichen, so darf die Ausfallrate an den Endpunkten der logischen Verbindung 10^{-8} nicht überschreiten.

8.4 Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde

Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde, average frequency of a dangerous failure per hour (*PFH*) (Übersetzung aus IEC 61508-4 3.6.19 [29])

Wahrscheinlichkeit eines gefährlichen Ausfalls eines E/E/PE sicherheitsrelevanten Systems die spezifizierte Sicherheitsfunktion über eine gegebene Zeitdauer auszuführen [...]

Anmerkung 3: Wenn das E/E/PE sicherheitsrelevante System, die letzte Sicherheitsschicht ist, *PFH* sollte von seiner Ausfallwahrscheinlichkeit $F(T)=1-R(t)$ berechnet werden (siehe Ausfallrate). Wenn es nicht das letzte sicherheitsrelevante System ist, dann sollte der *PFH* von der Nichtverfügbarkeit $U(t)$ berechnet werden […]. Approximierte *PFH*'s sind gegeben durch $\frac{F(T)}{T}$ und $\frac{1}{MFFT}$ oder $\frac{1}{MTBF}$ […].

9 Zusammenfassung

Eine einfache Formel zur quantitativen Bestimmung der Zuverlässigkeit gibt es nicht!

Prinzipiell können die Definitionen der Zuverlässigkeit in zwei Gruppen eingeteilt werden:

1. Zuverlässigkeit wird als Oberbegriff definiert, zu dem Verfügbarkeit, Funktionsfähigkeit, Instandhaltbarkeit usw. gehören.
2. Zuverlässigkeit wird als Funktionszuverlässigkeit angesehen, das heißt eine Funktion wird über eine bestimmte Zeit erfüllt.

Es ist unter anderem Ziel die verschiedenen Begrifflichkeiten, die mit der Zuverlässigkeit einhergehen, zusammenzutragen und einzuordnen, um das Verständnis und die Kommunikation zwischen Zuverlässigkeitstechnikern, Kommunikationstechnikern und Anwendern zu erleichtern.

Mögliche Arten an Kommunikationsfehlern werden erläutert und Maßnahmen zu deren Erkennung aufgezeigt.

Die Merkmale und Größen helfen sowohl Teile des Systems, wie die Kommunikationsstrecke als auch das gesamte System inklusive Hardware und Softwarekomponenten für quantitative Betrachtungen zu bewerten.

Eine unverzichtbare Größe zur Bewertung der Zuverlässigkeit ist die Verfügbarkeit. Diese beinhaltet die Funktionsfähigkeit und lässt sich aus den Klar- und Unklarzeiten (Up time und Down time) berechnen.

Eine weitere wichtige Größe ist die Mittlere Betriebszeit zwischen Ausfällen (*MTBF*). Durch ermitteln der *MTBF* ist es bei konstanten Anforderungen und Bedingungen möglich festzustellen, wie sich bestimmte Sicherungsmaßnahmen der Kommunikationsverbindungen auswirken. Damit kann dieser Wert nützliche Hinweise bei der Entwicklung oder Installation von Funklösungen bieten. Eine im Betrieb ermittelte *MTBF* kann ein Indikator für Änderungen an der Zuverlässigkeit der Übertragung sein und somit für Statusmeldungen oder Diagnosezwecke verwendet werden. Die Ausfallrate ist das Reziproke vom *MTBF* und kann unter Berücksichtigung der Ausfallraten von weiteren Komponenten zur Bewertung des Gesamtsystems herangezogen werden.

Für die Zuverlässigkeit in der Funkkommunikation ist es wichtig, den Betrachtungsraum zu benennen sowie auf welche Art der Sendung, Pakete oder Nachrichten (anwendungsbezogen) Bezug genommen wird. In diesem Dokument steht die logische Verbindung zwischen zwei Anwendungen als Betrachtungsraum im Vordergrund, somit die Übertragung der Nachricht. Bei der Übertragung von Paketen gibt es verschiedenste Mechanismen um Fehler und Verluste zu beheben, so dass die Nachricht ungeachtet dessen korrekt an der Anwendung empfangen werden kann. Der Verlust eines Paketes ist nicht zwangsläufig gleichbedeutend mit dem Verlust einer Nachricht!

In Bezug auf die Nachricht, können die Kenngrößen und Maßgrößen – immer abhängig von den Anforderungen des jeweiligen Systems – unterschiedliche Prioritäten einnehmen. Etablierte Größen sind:

- Übertragungszeit
- Aktualisierungszeit
- Antwortzeit
- Anzahl verlorener Nachrichten
- Nachrichtenverlustquote (Nachrichtenverlustrate veraltet)
- Restfehlerquote

Die Restfehlerquote stellte eine wichtige Rolle dar, weil sie das Verhältnis zwischen unerkannten fehlerhaften Nachrichten und der Gesamtzahl der gesendeten Nachrichten aufzeigt. Das heißt, sie ist ein Indikator dafür, wie die Mechanismen zur korrekten und sicheren Datenübertragung greifen.

Mathematische Zusammenhänge zwischen den Kenngrößen und Parameter zur Bewertung der Zuverlässigkeit werden aufgezeigt.

Es sei darauf verwiesen, dass die Zuverlässigkeitsbewertung nicht nur der Planung von Funktionseinheiten (Software, Hardware, Verbindungen, Systemen) dient. Eine standardisierte Zuverlässigkeitsbewertung ist die Grundlage für die Entwicklung von Verfahren, die Änderungen der Zuverlässigkeit im Betrieb erkennen und rechtzeitig vor dem Ausfall reagieren. Solche resilienten Kommunikationssysteme und deren Funktionsbausteine erfordern weitere Forschungsinitiativen (siehe auch [30]).

10 Quellen

[1] VDI/VDE: Funkgestützte Kommunikation in der Automatisierungstechnik, VDI/VDE Richtlinie 2185, Blatt 1

[2] DKE: DKE Wörterbuch, Internetseite, https://www2.dke.de/de/Online-Service/DKE-IEV/Seiten/IEV-Woerterbuch.aspx, 2016

[3] Industialradio: Glossar: http://industrialradio.de/Menu/Home/Glossar, 2016

[4] http://wirtschaftslexikon.gabler.de/Definition/quote.html, Mai 2017

[5] Plakos: Zuverlässigkeit - Bedeutung, Definition und Sprüche, Internet, https://zuverlaessigkeit.plakos.de/, 2016

[6] VDI: Zuverlässigkeitsmanagement, VDI 4003, Juli 2005

[7] DIN: Zuverlässigkeit; Begriffe, DIN 40 041, Dez. 1990

[8] J. Franz: Vorlesungen über Zuverlässigkeit und Statistik bei reparierbaren Systemen, Dresdner Schriften zur Mathematischen Stochastik, Technische Universität Dresden, 2016

[9] H. Bartsch: Definition Technische Zuverlässigkeit, Internet, http://www.heinz-bartsch.de/TZ-1.PDF, 2016

[10] IEC: International electrotechnical vocabulary - Part 192: Dependability, 2015

[11] EN: Industrielle Kommunikationsnetze - Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilfestlegungen, IEC 61784-3-3:2016

[12] Wikipedia: Zuverlässigkeit (Telekommunikation), Internetseite, https://de.wikipedia.org/wiki/Zuverl%C3%A4ssigkeit_(Telekommunikation), 2016

[13] ITU-R, Rec. ITU-R P.842-2: Computation of reliability and compatibility of HF radio systems

[14] ITU-T, Series Y: Global Information Infrastructure terminology: Terms and definitions, Y101, 03/2000

[15] ETSI EG 202 009-1: User Group; Quality of telecom services; Part 1, 01/2007

[16] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on New Services and Markets Technology Enablers - Critical Communications; Stage 1 (Release 14), Juni 2016

[17] DIN EN 61703:2002; Mathematische Ausdrücke für Begriffe der Funktionsfähigkeit, Verfügbarkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft

[18] IEC 61703:2016; MATHEMATICAL EXPRESSIONS FOR RELIABILITY, AVAILABILITY, MAINTAINABILITY AND MAINTENANCE SUPPORT TERMS

[19] ITU-T E.800 ITU-T (09/08) „Definitions of terms related to quality of service“

[20] Lutz Rauchhaupt, Elke Hintze, André Gnad: Über die Bewertung der Zuverlässigkeit industrieller Funklösungen - Teil 1 Theoretische Grundlagen, atp 49 Heft 3, S. 38, 2007

[21] L. Rauchhaupt, D. Schulze, A. Gnad: Anforderungsprofile im ZDKI Aspekte der Zuverlässigkeitsbewertung in ZDKI, Fachgruppe 1 „Anwendungen, Anforderungen und Validierung“ im BMBF-Förderprogramm „IKT 2020 - Zuverlässige drahtlose Kommunikation in der Industrie“ (BZKI), 2016

[22] IEC: Industrial communication networks - High availability automation networks - Part 1: General concepts and calculation methods, IEC 62439-1

[23] IEC: Methodology for communication network dependability assessment and assurance, IEC 62673, 2013

[24] IEC: Industrial communication networks - Wireless communication networks - Part 2: Coexistence management, IEC 62657-2

[25] D. Reichelt, F. Rothlauf; Verfahren zur Berechnung der Zuverlässigkeit von Kommunikationsnetzwerken – Eine Studie zu exakten und approximativen Verfahren; 2004; Working Paper

[26] IEC: Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions, IEC 61784-3

[27] E. Hintze, L. Rauchhaupt: Funktionale Sicherheit im Kontext von IIoT, Computer & Automation Sonderheft Safety & Security, S3-2016, S. 26ff, Juli 2016

[28] IEC: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements, IEC 61508-1 Ed. 2.0, 2010

[29] IEC: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations, IEC 61508-4 Ed. 2.0, 2010

[30] VDE Positionspapier „Resiliente Netze mit Funkzugang“ 20.03.2017

[31] Peterson, W. Wesley: Error-Correction Codes, 2nd Edition 1981, MIT-Press

[32] DIN: Internationales Elektrotechnisches Wörterbuch - Teil 351: Leittechnik, DIN IEC 60050

[33] DIN: Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS); Deutsche Fassung EN 50126:1999

[34] IEC: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3, IEC 61508-6 Ed. 2.0, 2010

[35] VDI/VDE: Funkgestützte Kommunikation in der Automatisierungstechnik, VDI/VDE Richtlinie 2185, Blatt 2

[36] H.–T. Hannen: Beitrag zur Analyse sicherer Kommunikationsprotokolle im industriellen Einsatz, Dissertation, Universität Kassel, 2012

[37] P.-W. Gräber, Automatisierungstechnik in der Wasserwirtschaft, 2009, Vorlesungsskript Kapitel 6 Messfehler

[38] Grundlagen der Statistik; http://www.statistics4u.info/fundstat_germ/ee_precision_accuracy.html Januar 2017

[39] IEC: Industrial communication networks - Wireless communication networks - Part 1: Wireless communication requirements and spectrum considerations, IEC TS 62657-1:2014

[40] NIST Special Publication 800-53 „Security and Privacy Controls for Federal Information Systems and Organizations“, National Institute of Standards and Technology, U.S. Department of Commerce

[41] ISO/IEC 2382-14:1997 Information technology –Vocabulary—Part 14: Reliability, maintainability and availability, 1997

Impressum

BZKI | Begleitforschung zur
zuverlässigen, drahtlosen
Kommunikation in der Industrie
Fachgruppe 1

Ansprechpartner

ifak – Institut für Automation und
Kommunikation e.V. Magdeburg
Werner-Heisenberg-Str. 1
39106 Magdeburg

Sarah Willmann
E-Mail: sarah.willmann@ifak.eu

INDUSTRIAL RADIO.DE®