

	Bahnanwendungen Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme Teil 2: Sicherheitsrelevante Kommunikation in offenen Übertragungssystemen Deutsche Fassung EN 50159-2:2001	<u>DIN</u> EN 50159-2
VDE	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Vorstand beschlossenen Genehmigungsverfahrens unter nebenstehenden Nummern in das VDE-Vorschriftenwerk aufgenommen und in der etz Elektrotechnische Zeitschrift bekannt gegeben worden.	Klassifikation VDE 0831 Teil 159-2
ICS 35.240.60; 45.020 Railway applications Communication, signalling and processing systems Part 2: Safety related communication in open transmission systems; German version EN 50159-2:2001 Applications ferroviaires Systèmes de signalisation, de télécommunication et de traitement Partie 2: Communication de sécurité sur des systèmes de transmission ouverts; Version allemande EN 50159-2:2001 Die Europäische Norm EN 50159-2:2001 hat den Status einer Deutschen Norm. Beginn der Gültigkeit Die EN 50159-2 wurde am 2000-01-01 angenommen. Nationales Vorwort Für die vorliegende Norm ist das nationale Arbeitsgremium UK 713.4 „Bahn-Signalanlagen“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE zuständig. Norm-Inhalt war veröffentlicht als E DIN EN 50159-2 (VDE 0831 Teil 159-2):1997-10. Fortsetzung Seite 2 und 46 Seiten EN DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Nationaler Anhang NA (informativ) Zusammenhang mit Europäischen und Internationalen Normen

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm oder andere Unterlage ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm oder anderen Unterlage.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm oder anderen Unterlage.

Der Zusammenhang der zitierten Normen und anderen Unterlagen mit den entsprechenden Deutschen Normen und anderen Unterlagen ist nachstehend wiedergegeben. Zum Zeitpunkt der Veröffentlichung dieser Norm oder anderen Unterlage waren die angegebenen Ausgaben gültig.

IEC hat 1997 die Benummerung der IEC-Publikationen geändert. Zu den bisher verwendeten Normnummern wird jeweils 60000 addiert. So ist zum Beispiel aus IEC 68 nun IEC 60068 geworden.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 50126:1999	–	DIN EN 50126 (VDE 0115 Teil 103):2000-03	VDE 0115 Teil 103
EN 50128:2001	–	DIN EN 50128 (VDE 0831 Teil 128):2001-xx	VDE 0831 Teil 128
EN 50129:1998-05	–	DIN V ENV 50129 (VDE V 0831 Teil 129):1999-07	VDE V 0831 Teil 129

Nationaler Anhang NB (informativ) Literaturhinweise

DIN EN 50126 (VDE 0115 Teil 103), *Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS)*; Deutsche Fassung EN 50126:1999

DIN EN 50128 (VDE 0831 Teil 128), *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme*; Deutsche Fassung EN 50128:2001

DIN V ENV 50129 (VDE V 0831 Teil 129), *Bahnanwendungen – Sicherheitsrelevante elektronische Systeme für Signaltechnik*; Deutsche Fassung ENV 50129:1998

Bahnanwendungen
Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme
Teil 2: Sicherheitsrelevante Kommunikation in offenen Übertragungssystemen

Railway applications
Communication, signalling and processing
systems
Part 2: Safety related communication in open
transmission systems

Applications ferroviaires
Systèmes de signalisation, de
télécommunication et de traitement
Partie 2: Communication de sécurité sur des
systèmes de transmission ouverts

Diese Europäische Norm wurde von CENELEC am 2000-01-01 angenommen. Die CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Zentralsekretariat oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien, der Tschechischen Republik und dem Vereinigten Königreich.

CENELEC

Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel

Vorwort

Diese Europäische Norm wurde von SC 9XA „Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme“ des Technischen Komitees TC 9X „Elektrische und elektronische Anwendungen für Bahnen“ ausgearbeitet.

Der Text des Norm-Entwurfs wurde der formellen Abstimmung unterworfen und von CENELEC als EN 50159-2 am 2000-01-01 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem die EN auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2001-10-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2003-01-01

Anhänge, die als „informativ“ bezeichnet sind, enthalten nur Informationen.
In dieser Norm sind die Anhänge A, B C und D informativ.

Inhalt	Seite
Einleitung.....	4
1 Anwendungsbereich	5
2 Normative Verweisungen.....	5
3 Begriffe.....	6
4 Referenzarchitektur.....	11
5 Bedrohungen auf das Übertragungssystem	13
6 Anforderungen an die Schutzmaßnahmen.....	14
6.1 Einleitung	14
6.2 Allgemeine Anforderungen	14
6.3 Spezifische Schutzmaßnahmen	15
7 Anwendbarkeit der Schutzmaßnahmen gegen die Bedrohungen.....	20
7.1 Einleitung	20
7.2 Bedrohungs-/Schutzmaßnahmenmatrix	20
7.3 Wahl und Gebrauch des Sicherheitscodes und der kryptographischen Techniken.....	21
Anhang A (informativ) Leitfaden für Schutzmaßnahmen.....	22
A.1 Anwendung von Zeitstempeln	22
A.2 Auswahl und Gebrauch von Sicherheitscodes und kryptographischen Techniken	24
Anhang B (informativ) Literaturhinweise.....	30
Anhang C (informativ) Leitfäden für den Gebrauch der Norm.....	31
C.1 Anwendungsbereich/Zweck.....	31
C.2 Klassifikation von Übertragungssystemen.....	31
C.3 Prozedur	33
C.4 Beispiel.....	34
Anhang D (informativ) Bedrohungen auf offene Übertragungssysteme.....	38
D.1 Systemsicht.....	38
D.2 Ableitung der grundsächlichen Nachrichtenfehler	39
D.3 Bedrohungen	40
D.4 Ein mögliches Verfahren zum Aufstellen des Sicherheitsnachweises	41
D.5 Schlussfolgerungen	45

Einleitung

Wenn ein sicherheitsrelevantes System die Übertragung von Informationen zwischen verschiedenen Standorten beinhaltet, dann nimmt das Kommunikationssystem einen integralen Bestandteil des sicherheitsrelevanten Systems ein, und es muss gezeigt werden, dass die Übertragung von Endeinrichtung zu Endeinrichtung in Übereinstimmung mit **ENV 50129** sicher ist.

Die Sicherheitsanforderungen für ein Datenkommunikationssystem hängen von seinen Eigenschaften ab, die bekannt oder unbekannt sein können. Um die Komplexität des Verfahrens zum Aufzeigen der Sicherheit des Systems zu verringern, sind zwei Klassen von Übertragungssystemen betrachtet worden. Die erste Klasse besteht aus einem System, über das der Entwickler des Sicherheitssystems einen gewissen Grad an Kontrolle hat. Dieses betrifft die geschlossenen Übertragungssysteme, deren Sicherheitsanforderungen in **EN 50159-1** definiert sind. Die zweite Klasse, genannt offenes Übertragungssystem, besteht aus all denjenigen Systemen, deren Eigenschaften unbekannt oder teilweise unbekannt sind. Diese Norm definiert die Sicherheitsanforderungen, die an die Übertragung über offene Übertragungssysteme gerichtet sind.

Das Übertragungssystem, das in dieser Norm betrachtet wird, muss im Allgemeinen keine besonderen Voraussetzungen erfüllen. Vom Standpunkt der Sicherheit aus gesehen wird ihm nicht oder nicht vollständig vertraut und es wird als „Black Box“ betrachtet.

Diese Norm steht in enger Beziehung zu **EN 50159-1** „Sicherheitsrelevante Kommunikation in geschlossenen Übertragungssystemen“ und zu **ENV 50129** „Sicherheitsrelevante elektronische Systeme für Signaltechnik“.

Diese Norm ist für Anforderungen bestimmt, die bei der Übertragung von sicherheitsrelevanter Information über offene Übertragungssysteme in Betracht gezogen werden müssen.

Mit Ziel auf eine allgemeine Zulassung und nicht für spezifische Anwendungen, ist die gegenseitige Anerkennung in der gleichen Weise gefordert wie für **ENV 50129** „Sicherheitsrelevante elektronische Systeme für Signaltechnik“.

1 Anwendungsbereich

Diese Europäische Norm ist für sicherheitsrelevante elektronische Systeme anwendbar, die ein offenes Übertragungssystem für Kommunikationszwecke nutzen. Sie liefert die grundlegenden Anforderungen, die benötigt werden, um die sicherheitsrelevante Übertragung zwischen den sicherheitsrelevanten Einrichtungen, die an offenen Übertragungssystemen angeschlossen sind, zu ermöglichen.

Diese Norm ist für die Sicherheitsanforderungsspezifikation von sicherheitsrelevanten Einrichtungen anwendbar, wenn diese an ein offenes Übertragungssystem angeschlossen sind, damit die zugewiesene Sicherheitsanforderungsstufe (SIL) erreicht wird.

Die Eigenschaften und das Verhalten des offenen Übertragungssystems werden nur für die Definition der Leistungsfähigkeit genutzt, jedoch nicht für die Sicherheit. Deshalb kann das offene Übertragungssystem vom Standpunkt der Sicherheit aus gesehen möglicherweise irgendwelche Eigenschaften haben wie unterschiedliche Übertragungswege, Speichern von Nachrichten, nicht autorisierter Zugriff und so weiter. Der Sicherheitsprozess darf sich nur auf die Eigenschaften verlassen, die im Sicherheitsnachweis angegeben sind.

Die Sicherheitsanforderungsspezifikation ist eine Voraussetzung für den Sicherheitsnachweis eines sicherheitsrelevanten elektronischen Systems, für das die geforderten Nachweise in der **ENV 50129** definiert sind. Der Nachweis des Sicherheitsmanagements und Qualitätsmanagements ist der **ENV 50129** zu entnehmen. Die Anforderungen an die Kommunikation für den Nachweis der funktionalen und technischen Sicherheit sind Gegenstand dieser Norm.

Diese Norm ist nicht für existierende Systeme anwendbar, die bereits vor der Freigabe dieser Norm akzeptiert worden sind.

Diese Norm legt nicht fest:

- das offene Übertragungssystem;
- an das offene Übertragungssystem angeschlossene Einrichtungen;
- Lösungen (z. B. für Interoperabilität);
- welche Arten von Daten sicherheitsrelevant sind und welche nicht.

2 Normative Verweisungen

Diese Europäische Norm enthält durch datierte oder undatierte Verweisungen Festlegungen aus anderen Publikationen. Diese normativen Verweisungen sind an den jeweiligen Stellen im Text zitiert und die Publikationen nachstehend aufgeführt. Bei datierten Verweisungen gehören spätere Änderungen oder Überarbeitungen dieser Publikationen nur zu diesem Entwurf einer Europäischen Norm, wenn sie durch Änderung oder Überarbeitung eingearbeitet sind. Bei undatierten Verweisungen gilt die letzte Ausgabe der in Bezug genommenen Publikation.

EN 50126, *Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS)*

EN 50128, *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und -überwachungssysteme*

ENV 50129, *Bahnanwendungen – Sicherheitsrelevante elektronische Systeme für Signaltechnik*

3 Begriffe

Für die Anwendung dieser Norm gelten die folgenden Begriffe:

3.1

Zugriffsschutz

Prozesse, die entwickelt wurden, um entweder innerhalb des *sicherheitsrelevanten* Systems des Nutzers oder innerhalb des *Übertragungssystems* *nichtautorisierten* Zugriff auf eine *Information* zu verhindern, damit sie nicht gelesen oder verändert werden kann

3.1.1

Hacker

Person, die absichtlich versucht, den *Zugriffsschutz* zu umgehen

3.2

Authentizität

Zustand, in dem eine *Information* als *gültig* erkannt wurde und in dem bekannt ist, dass sie von der angegebenen Quelle erzeugt wurde

3.3

Autorisation

formale Erlaubnis, ein Produkt oder einen Dienst innerhalb der spezifizierten Anwendungsgrenzen zu nutzen

3.3.1

nichtautorisierter Zugriff

Situation, in der auf eine *Nutzinformation* oder eine *Information* überhaupt innerhalb des *Übertragungssystems* durch *nichtautorisierte* Personen oder *Hacker* zugegriffen wird

3.3.2

Vertraulichkeit

Eigenschaft, dass *Informationen* für nichtautorisierte Einheiten nicht zugänglich gemacht werden

3.4

Prüfung (check)

Prozess, um die Gewissheit über den Zustand eines Systems zu vergrößern

3.4.1

Redundanzprüfung

Art von Prüfung, dass eine vordefinierte Beziehung zwischen redundanten Daten und den Nutzdaten innerhalb einer *Nachricht* besteht, um die *Integrität* einer Nachricht zu beweisen

3.5

kryptographische Techniken

aus Eingangsdaten werden Ausgangsdaten mittels eines Algorithmus und eines Schlüssels als Parameter berechnet. Bei Kenntnis der Ausgangsdaten ist es innerhalb einer vernünftigen Zeit unmöglich, die Eingangsdaten zu berechnen, ohne den Schlüssel zu kennen. Es ist ebenso unmöglich innerhalb einer vernünftigen Zeit, den Schlüssel aus den Ausgangsdaten abzuleiten, selbst wenn die Eingangsdaten bekannt sind.

3.6

Daten

Teil einer *Nachricht*, der ein Stück *Information* darstellt

3.6.1

Datenverfälschung

Veränderung von Daten

3.6.2

Nutzdaten

Daten ohne irgendwelche *zusätzlichen Daten*, die die Zustände oder Ereignisse des *Nutzerprozesses* darstellen. Im Falle der Kommunikation zwischen sicherheitsrelevanten Einrichtungen enthalten die Nutzdaten die *sicherheitsrelevanten Daten*

3.6.3

zusätzliche Daten

Daten, die ohne Nutzen des letztendlichen *Nutzerprozesses* sind, jedoch für Steuerungszwecke, Verfügbarkeit und Sicherheitszwecke genutzt werden

3.6.4

redundante Daten

zusätzliche Daten, die aus den *Nutzdaten* durch einen sicherheitsrelevanten Übertragungsprozess abgeleitet wurden

3.6.4.1

Sicherheitscode

redundante Daten, die in einer *sicherheitsrelevanten Nachricht* enthalten sind, um die Entdeckung von Datenverfälschungen durch den *sicherheitsrelevanten* Übertragungsprozess zu ermöglichen. Geeignete Codierungstechniken dürfen beinhalten:

3.6.4.1.1

nichtkryptographischer Sicherheitscode

redundante Daten, die auf nichtkryptographischen Funktionen basieren und die in einer sicherheitsrelevanten Nachricht enthalten sind, um die Entdeckung von Datenverfälschungen durch den sicherheitsrelevanten Übertragungsprozess zu erlauben

3.6.4.1.1.1

zyklische Codeprüfung (CRC)

CRC basiert auf zyklischen Codes und wird benutzt, um Nachrichten vor Datenverfälschungen zu schützen

3.6.4.1.2

kryptographischer Sicherheitscode

redundante Daten, die auf kryptographischen Funktionen basieren und in einer sicherheitsrelevanten Nachricht enthalten sind, um die Entdeckung von Datenverfälschungen und nichtautorisiertem Zugriff durch den sicherheitsrelevanten Übertragungsprozess zu erlauben

3.6.4.1.2.1

Nachrichtenauthentifizierungscode (MAC)

MAC ist eine *kryptographische* Funktion von der gesamten Nachricht und eines geheimen oder öffentlichen Schlüssels. Mit der gesamten Nachricht sind auch implizite Daten der Nachricht gemeint, die nicht zum Übertragungssystem gesendet werden

3.6.4.1.2.2

Manipulationsentdeckungscode (MDC)

MDC ist eine Funktion von der gesamten Nachricht, aber im Gegensatz zum *MAC* ist kein geheimer Schlüssel einbezogen worden. Mit der gesamten Nachricht sind auch implizite Daten der Nachricht gemeint, die nicht zum Übertragungssystem gesendet werden. Der MDC basiert oft auf einer Hash-Funktion

3.6.4.2

Sequenznummer

Sequenznummer ist als ein zusätzliches Datenfeld definiert, das eine Nummer enthält, die in vordefinierter Weise von *Nachricht* zu *Nachricht* wechselt

3.6.4.3

Zeitstempel

Zeitstempel ist eine Information, die vom Sender einer *Nachricht* hinzugefügt wird

3.6.4.3.1

relativer Zeitstempel

Zeitstempel ist als relativer Zeitstempel definiert, wenn er sich auf die lokale Uhr einer Einheit bezieht. Im Allgemeinen existieren keine Beziehungen zu den Uhren von anderen Einheiten

3.6.4.3.2

absoluter Zeitstempel

Zeitstempel ist als absoluter Zeitstempel definiert, wenn er sich auf eine globale Zeit bezieht, die für eine Gruppe von Einheiten aus einem Übertragungsnetzwerk gemeinsam ist

3.6.4.3.3

doppelter Zeitstempel

wenn zwei Einheiten ihre Zeitstempel austauschen und vergleichen, wird das doppelte Zeitstempel genannt. In diesem Fall sind die Zeitstempel in den Einheiten voneinander unabhängig

3.6.4.4

Quellen- und Zielbezeichner

jeder einzelnen Einheit ist ein Bezeichner zugeordnet. Dieser Bezeichner kann ein Name, eine Nummer oder ein willkürliches Bitmuster sein. Dieser Bezeichner wird für die sicherheitsrelevante Übertragung genutzt. Üblicherweise wird der Bezeichner den Nutzdaten hinzugefügt

3.7

Schutzmaßnahme (defence)

in die Konstruktion eines sicheren Kommunikationssystems eingebrachte Maßnahme, um besondere *Bedrohungen* abzuwehren

3.8

Fehlzustand (error)

Abweichung vom beabsichtigten Entwurf, die zu unerwünschtem Systemverhalten oder *Fehlfunktion/Ausfall* führen kann

3.9

Fehlfunktion/Ausfall (failure)

Abweichung vom spezifizierten Verhalten des Systems. Eine Fehlfunktion/Ausfall ist die Folge einer *Fehlerursache* oder eines *Fehlzustandes* im System

3.9.1

zufällige Fehlfunktion (random failure)

Fehlfunktion, die zeitlich zufällig erfolgt

3.9.2

systematische Fehlfunktion (systematic failure)

Fehlfunktion, die unter einer gewissen Kombination von Eingaben oder unter besonderen Umgebungsbedingungen wiederholbar eintritt

3.10

Ausfall/Fehlerursache (fault)

abnormaler Zustand, der zu einem Fehler oder einer Fehlfunktion/Ausfall in einem System führen kann. Eine Fehlerursache kann zufällig oder systematisch sein

3.10.1

Zufallsausfall (random fault)

Eintreten eines Ausfalls, das auf der Wahrscheinlichkeitstheorie und dem vorausgehenden funktionsfähigen Zustand beruht

3.10.2

systematischer Fehler (systematic fault)

Fehler in der Spezifikation, im Entwurf, in der Konstruktion, in der Installation, im Betrieb oder in der Instandhaltung eines Systems, eines Teilsystems oder einer Einrichtung

3.11

Gefährdung

Bedingung, die zu einem Unfall führen kann

3.11.1

Gefährdungsanalyse

Prozess zum Identifizieren der Gefährdungen, die ein Produkt oder dessen Verwendung verursachen kann

3.12

Information

Darstellung des Zustandes oder der Ereignisse eines *Prozesses* in der Form, wie es durch den Prozess verstanden wird

3.13

Integrität (integrity)

Zustand, in dem *Information* komplett und unverändert ist

3.14

Nachricht

Information, die von einem Sender (Datenquelle) zu einem oder mehreren Empfängern (Datensenke) übertragen wird

3.14.1

gültige Nachricht

Nachricht, deren Form in jeder Hinsicht den spezifizierten Anforderungen des Nutzers entspricht

3.14.2

Nachrichtenintegrität

Nachricht, in der *Information* vollständig und unverändert ist

3.14.3

authentische Nachricht

Nachricht, von deren *Information* bekannt ist, dass sie durch die angegebene Quelle erzeugt wurde

3.14.4

Nachrichtenstrom

geordnete Menge von Nachrichten

3.14.5

Nachrichtenverschlüsselung

Umformung von Bits innerhalb einer Nachricht unter Benutzung einer *kryptographischen Technik* im Zusammenwirken mit einem durch einen Schlüssel gesteuerten Algorithmus, um das zufällige Lesen von Daten zu erschweren. Sie liefert keinen Schutz gegen Datenverfälschungen

3.14.6

Antwortnachricht (feedback message)

Antwortnachricht ist definiert als eine Erwiderung des Empfängers an den Sender der Nachricht über einen Rückkanal

3.14.7

Nachrichtenhandling (message handling)

Prozesse außerhalb des unmittelbaren Einflusses des Nutzers, die in die Übertragung von Nachrichtenströmen zwischen den Teilnehmern eingefügt sind

3.14.8

Nachrichtenfehler (message errors)

Menge aller möglichen *Nachrichtenverfälschungs(failure)*arten, die zu potentiell gefährlichen Situationen oder zu einer Verringerung der Systemverfügbarkeit führen können. Es kann eine Anzahl von Ursachen für einen *Fehler(error)*typ existieren

3.14.8.1

wiederholte Nachricht

Art eines Nachrichtenfehlers, bei dem eine einzelne Nachricht mehr als einmal empfangen wurde

3.14.8.2

ausgelassene Nachricht

Art eines Nachrichtenfehlers, bei dem eine Nachricht aus dem Nachrichtenstrom entfernt wurde

3.14.8.3

eingefügte Nachricht

Art eines Nachrichtenfehlers, bei dem eine zusätzliche Nachricht in den Nachrichtenstrom eingefügt wurde

3.14.8.4

resequenzierte Nachricht

Art eines Nachrichtenfehlers, bei dem die Reihenfolge von Nachrichten in den Nachrichtenstrom verändert wurde

3.14.8.5

verfälschte Nachricht

Art eines Nachrichtenfehlers, bei dem eine Datenverfälschung entstanden ist

3.14.8.6

verzögerte Nachricht

Art eines Nachrichtenfehlers, bei dem eine Nachricht später als erwartet empfangen wurde

3.14.8.7

manipulierte Nachricht

Art einer eingefügten Nachricht, bei der eine nichtauthentische Nachricht so entworfen wurde, dass sie authentisch erscheint

3.15

Prozess

3.15.1

Nutzerprozess

Prozess innerhalb einer Anwendung, der direkt zu dem Verhalten beiträgt, wie es der Nutzer des Systems spezifiziert hat

3.15.2

Übertragungsprozess

Prozess innerhalb einer Anwendung, der nur zur Übertragung von Informationen zwischen den Nutzerprozessen beiträgt, aber nicht zu den Nutzerprozessen selbst

3.15.3

Zugriffsschutzprozess

Prozess innerhalb des Systems, der nur zum *Zugriffsschutz* von Informationen im System beiträgt, aber nicht zu den Nutzerprozessen oder Übertragungsprozessen selbst

3.16

Sicherheit (safety)

Freisein von nicht akzeptierbaren Risiken

3.16.1

sicherheitsrelevant/sicherheitsbezogen (safety-related)

trägt Verantwortung für die Sicherheit

3.16.2

Sicherheitsanforderungsstufe (safety integrity level) (**SIL**)

Zahl, die den erforderlichen Grad des Vertrauens anzeigt, mit dem ein System seine spezifizierten Sicherheitseigenschaften einhält

3.16.3

Sicherheitsnachweis (safety case)

dokumentierter Nachweis, dass ein Produkt die spezifizierten Sicherheitsanforderungen erfüllt

3.17

Übertragungssystem

von der Anwendung genutzter Dienst, um *Nachrichtenströme* zwischen einer Anzahl von Teilnehmern, die Quellen oder Senken von Informationen sein können, auszutauschen

3.17.1

geschlossenes Übertragungssystem

festgelegte Anzahl oder festgelegte Höchstanzahl von Teilnehmern, die über ein Übertragungssystem mit wohlbekannten und festgelegten Eigenschaften miteinander verbunden sind, und bei dem das Risiko von *nichtautorisiertem* Zugriff als vernachlässigbar betrachtet wurde

3.17.2

offenes Übertragungssystem

Übertragungssystem, welches für nicht bekannte Telekommunikationsdienste genutzt wird, mit einer unbekannten Anzahl von Teilnehmern, mit unbekannten und variablen Eigenschaften, denen nicht vertraut wird, und bei dem das Risiko von *nichtautorisiertem* Zugriff bewertet werden muss

3.18

Bedrohung

potentielle Verletzung der *Sicherheit* einschließlich des *Zugriffsschutzes* eines Kommunikationssystems

3.19

Rechtzeitigkeit

Zustand, in dem eine *Information* rechtzeitig entsprechend den Anforderungen verfügbar ist

3.20

Gültigkeit

Zustand, in dem in jeder Hinsicht den spezifizierten Anforderungen des Nutzers entsprochen wird

4 Referenzarchitektur

Diese Referenzarchitektur eines sicherheitsrelevanten Übertragungssystem basiert auf:

- dem nicht vertrauenswürdigen Übertragungssystem, welche internen Übertragungsschutzmechanismen auch immer enthalten sind;
- den sicherheitsrelevanten Übertragungsfunktionen;
- den sicherheitsrelevanten Zugriffsschutzfunktionen.

Für die Anwendung dieser Norm ist angenommen, dass das offene Übertragungssystem, das sich zwischen zwei oder mehr sicherheitsrelevanten Einrichtungen befinden kann, aus allem Möglichen besteht (Hardware, Software, Übertragungsmedien usw.).

Das offene Übertragungssystem kann einiges oder alles von folgenden Punkten enthalten:

- Elemente, die Daten lesen, speichern, verarbeiten oder weiter übertragen, und die von Nutzern des Übertragungssystems erzeugt und dargestellt werden mit einem dem Nutzer unbekannten Programm. Die Anzahl von Nutzern ist im Allgemeinen unbekannt; sicherheitsrelevante und nicht sicherheitsrelevante Einrichtungen und Einrichtungen, die nicht zu Bahnanwendungen gehören, können an das offene Übertragungssystem angeschlossen sein.

- Übertragungsmedien irgendeines Typs mit Übertragungseigenschaften und Anfälligkeit gegenüber externen Einflüssen, die für den Nutzer unbekannt sind.
- Netzwerksteuerungs- und Managementsysteme, die die Fähigkeit haben, die Leitwegzuteilung (und deren dynamischer Neufestlegung) von Nachrichten über jeden Pfad festzulegen mit Hilfe von einem oder mehreren Typen von Übertragungsmedien zwischen den Enden des offenen Übertragungssystems, und im Zusammenwirken mit einem dem Nutzer unbekannten Programm.

Das offene Übertragungssystem kann für Folgendes anfällig sein:

- Andere Nutzer des Übertragungssystems, die dem Entwickler des Steuerungs- und Überwachungssystems unbekannt sind, senden unbekannte Mengen an Informationen in unbekannten Formaten.
- Nutzer des Übertragungssystems, die versuchen könnten, Zugriff auf Daten von anderen Nutzern zu erlangen, um sie zu lesen und/oder um sie nachzuahmen, ohne dass eine Erlaubnis des Systemverwalters dazu vorliegt.
- Jede Art von zusätzlichen Bedrohungen auf die Integrität der sicherheitsrelevanten Daten.

Eine prinzipielle Struktur des sicherheitsrelevanten Systems unter Verwendung eines offenen Übertragungssystems ist in Bild 1 dargestellt. Das prinzipielle Modell einer sicherheitsrelevanten Nachricht ist in Bild 2 wiedergegeben.

Es dürfen den nicht vertrauenswürdigen Eigenschaften des offenen Übertragungssystems keine Sicherheitsanforderungen auferlegt werden. Die Sicherheitsaspekte sind durch die Anwendung von Sicherheitsprozeduren und Sicherheitscodes auf die sicherheitsrelevanten Übertragungsfunktionen zu berücksichtigen.

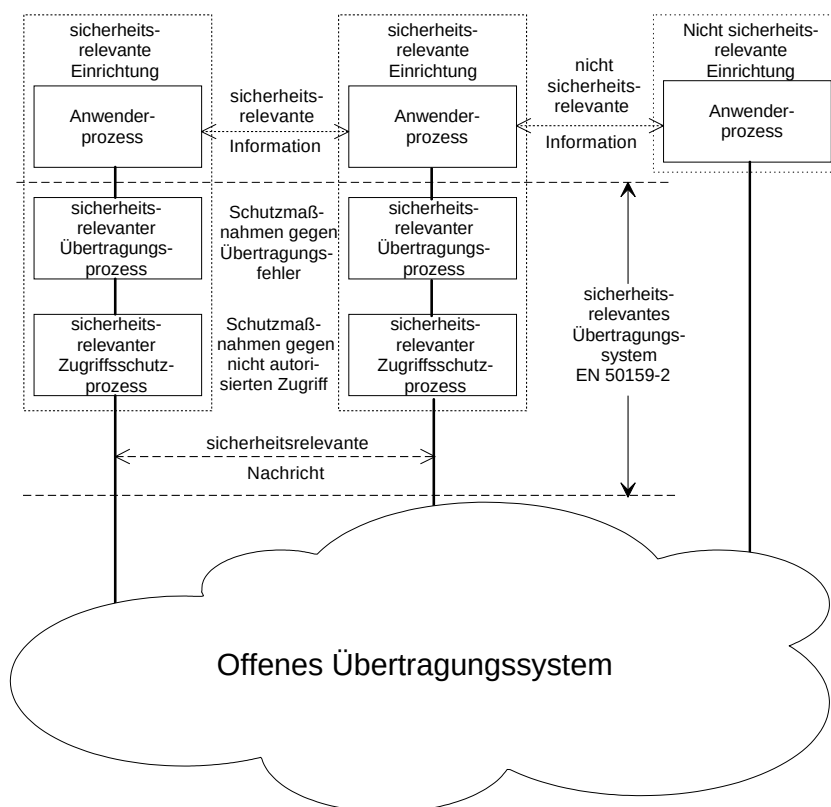


Bild 1 – Struktur des sicherheitsrelevanten Systems unter Verwendung eines nicht sicherheitsrelevanten Übertragungssystems

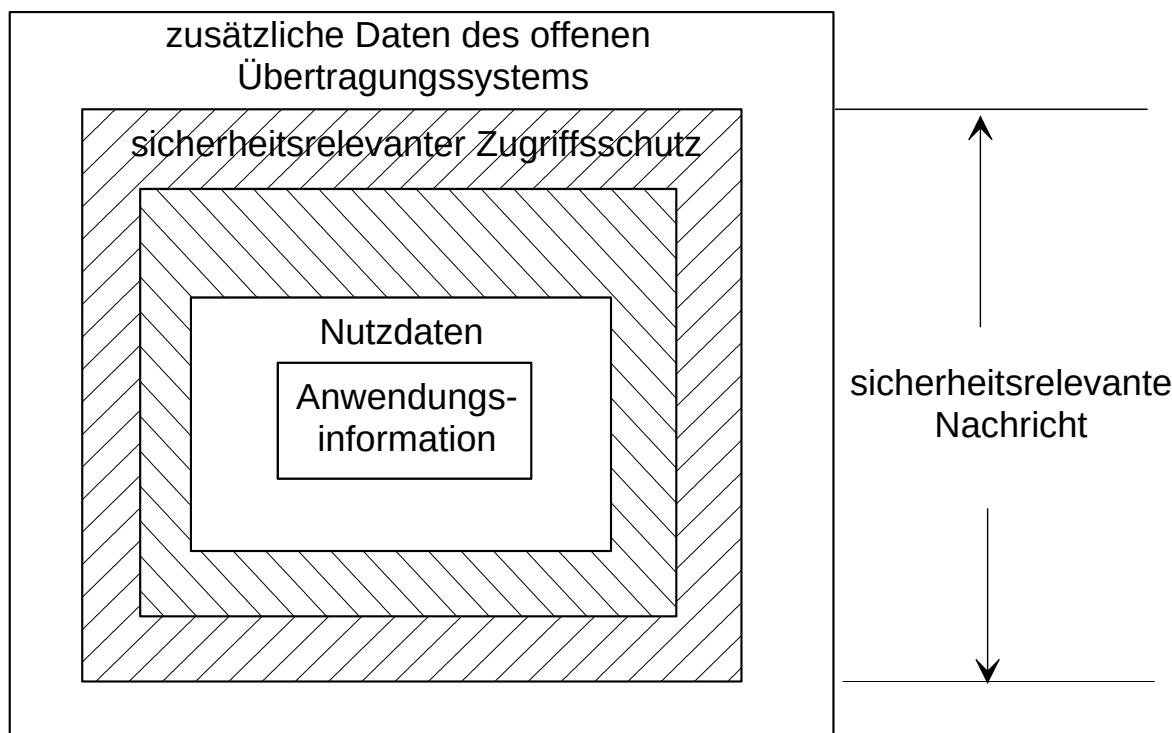


Bild 2 – Modell einer sicherheitsrelevanten Nachricht

5 Bedrohungen auf das Übertragungssystem

Nur Bedrohungen auf das Übertragungssystem selbst müssen betrachtet werden. Bedrohungen auf die sicherheitsrelevanten Einrichtungen müssen nach **ENV 50129** betrachtet werden.

Diese Norm bezieht sich auf Kommunikationen zwischen allgemeinen Anwendungen, die ein Übertragungssystem benutzen, dessen Eigenschaften (zumindest teilweise) unbekannt sind.

Es ist deshalb notwendig, eine Hauptgefährdung auf die Sicherheit zu definieren – unabhängig von der Funktionalität einer speziellen Anwendung und von den Charakteristiken des Netzwerkes. Die betreffende Definition heißt: „*Das Versagen, eine authentische (und konsequenterweise gültige) Nachricht beim Empfänger zu bekommen*“.

Mit Bezug auf den **Anhang D** ist eine Menge von möglichen grundsätzlichen Nachrichtenfehlern abgeleitet worden.

Die entsprechenden Bedrohungen sind:

- Wiederholung;
- Auslassung;
- Einfügung;
- Resequenzierung;
- Verfälschung;
- Verzögerung;
- Manipulation.

Das Erfüllen der Anforderungen dieser Norm gibt keinen Schutz gegen vorsätzlichen oder nicht vorsätzlichen Missbrauch seitens autorisierter Quellen. Der Sicherheitsnachweis muss diese Aspekte ansprechen.