electrosuisse

Schweizer Norm
Norme Suisse
Norma Svizzera

Fachbereich Elektrotechnik

EN 50159

EINGETRAGENE NORM DER SCHWEIZERISCHEN NORMENVEREINIGUNG SNV

NORME ENREGISTREE DE L'ASSOCIATION SUISSE DE NORMALISATION

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante Kommunikation in Übertragungssystemen

Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité sur des systèmes de transmission

Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

Diese Norm ist die deutsche Fassung EN 50159:2010

Die Europäische Norm EN 50159:2010 hat den Status einer Schweizer Norm.
Sie gilt in der Schweiz als anerkannte Regel der Technik.

Die EN 50159:2010 gilt seit: 01.09.2010.

Für die vorliegende Norm ist das Schweizerische Elektrotechnische Komitee (CES), Technisches Komitee 9 - Elektrische und elektronische Anwendungen für Bahnen - zuständig.

Referenznummer / No. de référence

SNEN 50159:2010(D)

Herausgeber / Vertrieb Editeur / Distributeur

Electrosuisse
Luppmenstrasse 1, CH-8320 Fehraltorf

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN 50159

September 2010

ICS 35.240.60; 45.020

Ersatz für EN 50159-1:2001, EN 50159-2:2001

Deutsche Fassung

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante Kommunikation in Übertragungssystemen

Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité sur des systèmes de transmission

Diese Europäische Norm wurde von CENELEC am 2010-09-01 angenommen. 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, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brüssel

Ref. Nr. EN 50159:2010 D

Vorwort

Diese Europäischen Norm wurde vom SC 9XA „Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme“ des Technischen Komitees CENELEC/TC 9X „Elektrische und elektronische Anwendungen für Bahnen“ ausgearbeitet. Sie wurde der formellen Abstimmung unterworfen und von CENELEC am 2010-09-01 als EN 50159 angenommen.

Dieses Dokument ersetzt EN 50159-1:2001 und EN 50159-2:2001.

Die Inhalte beider Normen wurden zusammengeführt; der informative Anhang E stellt eine Zuordnung zwischen diesen früheren Ausgaben und dem jetzigen Dokument dar.

Diese Europäischen Norm steht in enger Beziehung zu EN 50129:2003.

Zu beachten ist die Möglichkeit, dass einige Elemente dieses Dokuments Gegenstand von Patentrechten sein können. CEN und CENELEC sind nicht verantwortlich, einige oder alle dieser Patentrechte zu identifizieren.

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)	2011-09-01
– spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen	(dow)	2013-09-01

Dieser Entwurf einer Europäischen Norm wurde unter einem Mandat erstellt, das von der Europäischen Kommission und der Europäischen Freihandelszone an CENELEC gegeben wurde. Diese Europäische Norm deckt grundlegende Anforderungen der EG-Richtlinien 96/48/EG (HSR), umgestaltet durch die EG-Richtlinie 2008/57/EG (RAIL) ab. Siehe Anhang ZZ.

Inhalt

Seite

Bilder

Tabellen

Einleitung

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

Das in dieser Norm betrachtete Übertragungssystem, das dem Transfer von Information zwischen verschiedenen Stellen dient, muss im allgemeinen keine besonderen Voraussetzungen erfüllen. Vom Standpunkt der Sicherheit aus gesehen wird ihm nicht vertraut, oder nicht vollständig vertraut.

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

Obwohl die RAM Aspekte in dieser Norm nicht betrachtet werden, wird empfohlen, sich vor Augen zu halten, dass sie einen wichtigen Aspekt der Gesamtsicherheit darstellen.

Die Sicherheitsanforderungen hängen von den Eigenschaften des Übertragungssystems ab. Um die Komplexität der Vorgehensweise für den Nachweis der Sicherheit des Systems zu reduzieren, wurden Übertragungssysteme in drei Kategorien unterteilt.

– Kategorie 1 besteht aus Systemen, die unter der Kontrolle des Designers sind und die während ihres Lebenszyklussees unveränderlich bleiben.
– Kategorie 2 besteht aus Systemen, die teilweise unbekannt sind und auch nicht unveränderlich bleiben, bei denen jedoch nicht autorisierter Zugriff ausgeschlossen werden kann.
– Kategorie 3 besteht aus Systemen, die nicht unter Kontrolle des Designers sind, d. h. dass nicht autorisierter Zugriff berücksichtigt werden muss.

Die erste Kategorie wurde durch EN 50159-1:2001 abgedeckt, die anderen durch EN 50159-2:2001.

Wenn sicherheitsrelevante Kommunikationssysteme, die entsprechend den vorherigen Normen zugelassen worden sind, Gegenstand von Wartung und/oder Erweiterungen sind, kann der informative Anhang E zum Zwecke der Rückverfolgbarkeit von (Unter)Abschnitten dieser Norm zu (Unter)Abschnitten der früheren Normenreihe benutz werden.

1 Anwendungsbereich

Diese Europäische Norm ist für sicherheitsrelevante elektronische Systeme anwendbar, die zu digitalen Kommunikationszwecken ein Übertragungssystem benutzen, das nicht notwendigerweise für sicherheitsrelevante Anwendungen entworfen worden ist und das

– unter der Kontrolle des Designers ist und während des Lebenszyklussees unveränderlich bleibt, oder

– teilweise unbekannt ist und auch nicht unveränderlich bleibt, bei dem jedoch nicht autorisierter Zugriff ausgeschlossen werden kann, oder

– nicht unter Kontrolle des Designers ist und nicht autorisierter Zugriff auch berücksichtigt werden muss.

An das Übertragungssystem können sowohl sicherheitsrelevante, als auch nicht sicherheitsrelevante Einrichtungen angeschlossen sein.

Diese Norm liefert die grundlegenden Anforderungen, die für die sicherheitsrelevante Kommunikation zwischen den an ein Übertragungssystem angeschlossenen, sicherheitsrelevanten Einrichtungen benötigt werden.

Diese Norm ist für die Sicherheitsanforderungsspezifikation der and das Übertragungssystem angeschlossenen sicherheitsrelevanten Einrichtungen anwendbar, um die zugeordneten Anforderungen der Sicherheitsintegrität zu erreichen.

Sicherheitsanforderungen sind im allgemeinen in sicherheitsrelevanten Einrichtungen implementiert, die entsprechend der EN 50129 entwickelt wurden. In bestimmten Fällen können diese Anforderungen in anderen Einrichtungen des Übertragungssystems implementiert sein, solange Kontrolle durch Sicherheitsmaßnahmen besteht, um der zugeordneten Anforderung and die Sicherheitsintegrität nachzukommen.

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

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

Diese Europäische Norm legt nicht fest:

– das Übertragungssystem,

– an das Übertragungssystem angeschlossene Einrichtungen,

– Lösungen (z. B. für Interoperabilität),

– welche Arten von Daten sicherheitsrelevant sind und welche nicht.

Ein sicherheitsrelevantes Gerät, das an ein offenes Übertragungssystem angeschlossen ist, kann Gegenstand von vielerlei unterschiedlichen IT Sicherheitsbedrohungen sein, gegen die ein generelles Programm definiert werden muss, das Management, technische und betriebliche Aspekte umfassen muss.

In dieser Europäischen Norm werden jedoch, soweit IT Sicherheit betroffen ist, nur absichtliche Angriffen mit Hilfe von Telegrammen auf sicherheitsrelevante Anwendungen berücksichtigt.

Diese Europäische Norm umfasst nicht allgemeine Sachverhalte der IT Sicherheit und im besonderen nicht Sachverhalte der IT Sicherheit in Bezug auf

– Sicherstellung von Vertraulichkeit von sicherheitsrelevanter Information,

– Verhinderung der Überlastung des Übertragungssystems.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

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

EN 50129:2003, *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik*

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1.1
absoluter Zeitstempel
Zeitstempel, bezogen auf eine globale Zeit, die für eine Gruppe von Einheiten aus einem Übertragungssystem gemeinsam ist

3.1.2
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

3.1.3
zusätzliche Daten
Daten, die ohne Nutzen des letztendlichen Nutzerprozesses sind, jedoch für Steuerungszwecke, Verfügbarkeit und Sicherheitszwecke genutzt werden

3.1.4
authentische Nachricht
Nachricht, von deren Information bekannt ist, dass sie durch die angegebene Quelle erzeugt wurde

3.1.5
Authentizität
Zustand, in dem eine Information als gültig erkannt wurde und in dem bekannt ist, dass sie von der angegebenen Quelle erzeugt wurde

3.1.6
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 wird

3.1.7
Kommunikation
Transfer von Information zwischen Anwendungen

3.1.8
Vertraulichkeit
Eigenschaft, dass Informationen für nichtautorisierte Einheiten nicht zugänglich gemacht werden

3.1.9
verfälschte Nachricht
Art eines Nachrichtenfehlers, bei dem eine Datenverfälschung entstanden ist

3.1.10
kryptographische Techniken
aus Eingangsdaten werden Ausgangsdaten mittels eines Algorithmus und einem Schlüssel als Parameter berechnet

ANMERKUNG Es ist unmöglich innerhalb einer vernünftigen Zeit, durch Kenntnis der Ausgangsdaten, 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.

3.1.11
zyklische Redundanzprüfung
CRC (en: Cyclic Redundancy Check)
zyklischer Code, der benutzt wird, um Nachrichten vor Datenverfälschungen zu schützen

3.1.12
Daten
Teil einer Nachricht, der ein Stück Information darstellt (siehe auch Nutzdaten, zusätzliche Daten, redundante Daten)

3.1.13
Datenverfälschung
Veränderung von Daten

3.1.14
Schutzmaßnahme
(en: defence)
in das Design eines sicherheitsrelevanten Kommunikationssystems eingebrachte Maßnahme, um bestimmte Bedrohungen abzuwehren

3.1.15
verzögerte Nachricht
Art eines Nachrichtenfehlers, bei dem eine Nachricht später als beabsichtigt empfangen wurde

3.1.16
ausgelassene Nachricht
Art eines Nachrichtenfehlers, bei dem eine Nachricht aus dem Nachrichtenstrom entfernt wurde

3.1.17
doppelter Zeitstempel
wenn zwei Einheiten ihre Zeitstempel austauschen und vergleichen, wird das doppelter Zeitstempel genannt. In diesem Fall sind die Zeitstempel in den Einheiten voneinander unabhängig.

3.1.18
Fehler
(en: error)
Abweichung vom beabsichtigten Design, die zu unerwünschtem Systemverhalten oder Fehlfunktion/Ausfall führen kann

3.1.19
Ausfall
(en: failure)
Abweichung vom spezifizierten Verhalten des Systems

ANMERKUNG Ein Ausfall ist die Folge eines Fehlzustandes oder eines Fehlers im System.

3.1.20
Fehlzustand
(en: fault)
abnormaler Zustand, der zu einem Fehler oder einem Ausfall in einem System führen kann

ANMERKUNG Ein Fehlzustand kann zufällig oder systematisch sein.

3.1.21
Antwortnachricht
(en: feedback message)
Antwortnachricht ist definiert als eine Erwiderung des Empfängers an den Sender über einen Rückkanal

3.1.22
Hacker
Person, die absichtlich versucht, den Zugriffsschutz zu umgehen

3.1.23
Gefährdung
(en: hazard)
Bedingung, die zu einem Unfall führen kann

3.1.24
Gefährdungsanalyse
Prozess zur Identifikation der Gefährdungen und analysieren ihrer Ursachen, und der Herleitung von Anforderungen, um die Wahrscheinlichkeit und Konsequenzen von Gefährdungen auf ein akzeptiertes Niveau zu begrenzen

3.1.25
eingeschlossene Daten
implizite Daten
zusätzliche Daten, die nicht übertragen werden, aber dem Sender und Empfänger bekannt sind

3.1.26
Information
Darstellung des Zustandes oder der Ereignisse eines Prozesses in der Form, wie es durch den Prozess verstanden wird

3.1.27
eingefügte Nachricht
Art eines Nachrichtenfehlers, bei dem eine zusätzliche Nachricht in den Nachrichtenstrom eingefügt wurde

3.1.28
Integrität
Zustand, in dem Information komplett und unverändert ist

3.1.29
Manipulationsentdeckungscode
MDC
Funktion von der gesamten Nachricht, ohne geheimen Schlüssel

ANMERKUNG Im Gegensatz zum MAC ist kein geheimer Schlüssel einbezogen. 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.

3.1.30
manipulierte Nachricht
(en: masqueraded message)
Art einer eingefügten Nachricht, bei der eine nichtauthentische Nachricht so entworfen wurde, dass sie authentisch erscheint

3.1.31
Nachricht
Information, die von einem Sender (Datenquelle) zu einem oder mehreren Empfängern (Datensenke) übertragen wird

3.1.32
Nachrichten – Authentifizierungscode
MAC
kryptographische Funktion von der gesamten Nachricht und eines geheimen oder öffentlichen Schlüssels

ANMERKUNG Mit der gesamten Nachricht sind auch implizite Daten der Nachricht gemeint, die nicht zum Übertragungssystem gesendet werden.

3.1.33
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.

3.1.34
Nachrichtenfehler
(en: message error)
Menge aller möglichen Nachrichtenverfälschungs(failure)arten, die zu potenziell gefährlichen Situationen oder zu einer Verringerung der Systemverfügbarkeit führen können. Es kann eine Anzahl von Ursachen für einen Fehler(error)typ existieren.

3.1.35
Nachrichtenintegrität
Nachricht, in der Information vollständig und unverändert ist

3.1.36
Nachrichtenstrom
geordnete Menge von Nachrichten

3.1.37
nicht kryptographischer Sicherheitscode
redundante Daten, die auf nicht kryptographischen Funktionen basieren und die in einer sicherheitsrelevanten Nachricht enthalten sind, um die Entdeckung von Datenverfälschung durch die sicherheitsrelevante Übertragungsfunktion zu erlauben

3.1.38
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 welches das Potenzial zu nichtautorisiertem Zugriff hat

3.1.39
zufällige Fehlfunktion
(en: random failure)
Fehlfunktion, die zeitlich zufällig erfolgt

3.1.40
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

3.1.41
redundante Daten
zusätzliche Daten, die aus den Nutzdaten durch eine sicherheitsrelevante Übertragungsfunktion abgeleitet wurden

3.1.42
relativer Zeitstempel
Zeitstempel ist als relativer Zeitstempel definiert, wenn er sich auf die lokale Uhr einer Einheit bezieht. Im allgemeinem existieren keine Beziehungen zu den Uhren von anderen Einheiten.

3.1.43
wiederholte Nachricht
Art eines Nachrichtenfehlers, bei dem eine einzelne Nachricht mehr als einmal empfangen wurde

3.1.44
resequenzierte Nachricht
Art eines Nachrichtenfehlers, bei dem die Reihenfolge von Nachrichten in dem Nachrichtenstrom verändert wurde

3.1.45
sicherer Zustand
(en: safe fall back state)
sicherer Zustand einer sicherheitsrelevanten Einrichtung als eine Abweichung vom fehlerfreien Zustand als Resultat einer Sicherheitsreaktion, die zu einer reduzierten Funktionalität der sicherheitsrelevanten und möglicherweise nicht sicherheitsrelevanten Funktionen führt

3.1.46
Sicherheit
Freisein von nicht akzeptierbaren Risiken

3.1.47
Sicherheitsnachweis
(en: safety case)
dokumentierter Nachweis, dass ein Produkt die spezifizierten Sicherheitsanforderungen erfüllt

3.1.48
Sicherheitscode
redundante Daten, die der Nachricht hinzugefügt werden, um durch sicherheitsrelevante Übertragungsfunktion die Entdeckung von Datenverfälschungen zu ermöglichen

3.1.49
Sicherheitsanforderungsstufe
(en: safety integrity level, SIL)
Zahl, die den erforderlichen Grad des Vertrauens anzeigt, mit dem ein System seine spezifizierten Sicherheitseigenschaften in Bezug auf systematische Fehler einhält

3.1.50
Sicherheitsreaktion
ein sicherheitsrelevanter Schutz, der durch den Sicherheitsprozess als Antwort auf ein Ereignis (wie ein Ausfall des Übertragungssystems) ausgelöst wird, der zum sicheren Zustand der Einrichtung führen kann

3.1.51
sicherheitsrelevant
trägt Verantwortung für die Sicherheit

3.1.52
sicherheitsrelevante Übertragungsfunktion
Funktion, die in der sicherheitsrelevanten Einrichtung enthalten ist, um Authentizität, Integrität, zeitliche Richtigkeit und Sequenz von Daten sicherzustellen

3.1.53
Sequenznummer
Sequenznummer ist als ein zusätzliches Datenfeld definiert, das eine Nummer enthält, die in vordefinierter Weise von Nachricht zu Nachricht wechselt

3.1.54
Quellen- und Zielbezeichner
Bezeichner, der jeder Einheit zugeordnet ist. Dieser Bezeichner kann ein Name, eine Nummer oder ein willkürliches Bitmuster sein. Dieser Bezeichner wird für die sicherheitsrelevante Kommunikation genutzt. Üblicherweise wird der Bezeichner den Nutzdaten hinzugefügt.

3.1.55
systematische Fehlfunktion
Fehlfunktion, die unter einer gewissen Kombination von Eingaben oder unter besonderen Umgebungsbedingungen wiederholbar eintritt

3.1.56
Bedrohung
potentielle Verletzung der Sicherheit

3.1.57
Zeitstempel
vom Sender einer Nachricht hinzugefügte, die Übertragungszeit betreffende Information

3.1.58
Rechtzeitigkeit
Zustand, in dem eine Information rechtzeitig entsprechend den Anforderungen verfügbar ist

3.1.59
Übertragungscode
redundante Information, hinzugefügt zu der sicheren und nichtsicheren Nachricht des nicht sicherheitsrelevanten Übertragungssystems, um die Integrität der Nachricht während der Übertragung sicherzustellen

3.1.60
Übertragungssystem
ein von der Anwendung genutzter Dienst, um Nachrichtenströme zwischen einer Anzahl von Teilnehmern, die Quellen oder Senken von Information sein können, auszutauschen

3.1.61
vertrauenswürdig
hat Eigenschaften, die benutzt werden, um den Nachweis der Sicherheit zu unterstützen

3.1.62
nichtautorisierter Zugriff
Situation, in der auf eine Nutzinformation oder eine Information überhaupt innerhalb des Übertragungssystems durch nichtautorisierte Personen oder Hacker zugegriffen und/oder die geändert wird

3.1.63
Nutzdaten
(en: user data)
Daten, die die Zustände oder Ereignisse eines Sicherheitsprozesses darstellen ohne zusätzliche Daten. Im Falle der Kommunikation zwischen sicherheitsrelevanten Einrichtungen enthalten die Nutzdaten sicherheitsrelevante Daten.

3.1.64
gültige Nachricht
Nachricht, deren Form in jeder Hinsicht den spezifizierten Anforderungen des Nutzers entspricht

3.1.65
Gültigkeit
Zustand, in dem in jeder Hinsicht den spezifizierten Anforderungen des Nutzers entsprochen wird

3.2 Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Abkürzungen.

BCH	Bose, Ray-Chaudhuri, Hocquenghem Code
B.M.E.	Grundsätzliche Nachrichtenfehler *(en: Basic Message Errors)*
BSC	Binärer Symmetrischer Kanal *(en: Binary Symmetric Channel)*
CAN	Controller Area Network
CRC	Cyclic Redundancy Check
EC	Europäische Gemeinschaft *(en: European Community)*
ECB	Electronic Code Book mode
EMI	Elektromagnetische Interferenz *(en: Electromagnetic Interference)*
FTA	Fehlerbaumanalyse *(en: Fault Tree Analysis)*
GPRS	General Packet Radio Service
GSM-R	Global System for Mobile communication – Railways
H.E.	Gefährliches Ereignis *(en: Hazardous Event)*
HW	Hardware
IT	Informations-Technologie *(en: Information Technology)*
LAN	Lokales Netzwerk *(en: Local Area Network)*
MAC	Nachrichten – Authentifizierungscode *(en: Message Authentification Code)*
MDC	Manipulationsentdeckungscode *(en: Manipulation Detection Code)*
MD4, MD5	Message Digest algorithms
M.H.	Hauptgefährdung *(en: Main Hazard)*
MTBF	Mittlere Zeit zwischen Fehlern *(en: Mean Time Between Failures)*
MVB	Multi-purpose Vehicle Bus
PROFIBUS	Process Field Bus
QSC	q-nary Symmetric Channel
RAMS	Zuverlässigkeit, Verfügbarkeit, Wartbarkeit und Sicherheit *(en: Reliability, Availability, Maintainability and Safety)*
SIL	Sicherheitsanforderungsstufe *(en: Safety Integrity Level)*
SR	Sicherheitsrelevant *(en: Safety-Related)*
SRS	Sicherheitsanforderungsspezifikation *(en: Safety Requirement Specification)*
SW	Software
TX	Übertragung
UTC	Allgemeine kodierte Zeit *(en: Universal Coordinated Time)*
WAN	Weitverkehrsnetzwerk *(en: Wide Area Network)*
Wi-Fi	Wireless Fidelity

4 Referenzarchitektur

Diese Europäische Norm definiert die Sicherheitsanforderungen für die sichere Kommunikation zwischen sicherheitsrelevanten Einrichtungen über ein Übertragungssystem, das entweder geschlossen, oder offen sein kann. Sowohl sicherheitsrelevante, als auch nicht sicherheitsrelevante Einrichtungen können an das Übertragungssystem angeschlossen sein. Dieser Abschnitt beschreibt mögliche Konfigurationen von sicherheitsrelevanter Kommunikation in Übertragungssystemen, einschließlich der Definition der beteiligten funktionalen Blöcke. Die durch diese Blöcke zu erfüllenden besonderen Anforderungen sind in den folgenden Abschnitten spezifiziert.

Eine kombinierte Sicht – offenes und geschlossenes Übertragungssystem – der grundlegenden Architektur ist in Bild 1 dargestellt, wo alle Kommunikationselemente entsprechend ihres Informationsflusses verbunden sind, um sicherheitsrelevante Information zwischen sicherheitsrelevanten Einrichtungen auszutauschen. Die Referenzarchitektur zeigt auch eine nicht sicherheitsrelevantes Schnittstelle, die nicht immer vorhanden ist. Eine typische Nutzung könnte für Diagnose Nachrichten sein, die zu einem Diagnose Zentrum geleitet werden.

Neben der Quelle und Senke der sicherheitsrelevanten Kommunikation befasst sich die Referenzarchitektur mit einem sicherheitsrelevanten Kommunikationssystem, das aufgeteilt werden kann in

– sicherheitsrelevante Übertragungsfunktionen, eingebettete in sicherheitsrelevanten Einrichtungen. Diese Funktionen stellen Authentizität, Integrität, Rechtzeitigkeit und Sequenz von Daten sicher;

– sicherheitsrelevante kryptographische Techniken, die die sicherheitsrelevante Nachricht schützen. Diese können entweder durch Einbettung in sicherheitsrelevanten Einrichtungen realisiert werden, oder außerhalb von sicherheitsrelevanten Einrichtungen, aber geprüft durch Sicherheitstechniken. Diese Techniken schützen die sicherheitsrelevante Nachricht in einem Kategorie 3 Übertragungssystem und werden bei Kategorie 1 oder 2 Übertragungssystemen nicht benötigt;

– ein nicht sicherheitsrelevantes, offenes oder geschlossenes Übertragungssystem, das selbst Übertragungsschutzfunktionen und/oder Zugriffsschutzfunktionen enthalten kann.

Die Merkmale von geschlossenen Übertragungssystemen (Kategorie 1) sind folgende:

– die Anzahl der anschließbaren Einrichtungen – sicherheitsrelevant oder auch nicht – an das Übertragungssystem ist bekannt und fixiert;

– das Risiko von nicht autorisiertem Zugriff wird als vernachlässigbar erachtet;

– die physikalischen Eigenschaften des Übertragungssystems (z. B. Übertragungsmedium, Umweltbedingungen entsprechend Design-Hypothesen, usw.) sind fixiert und bleiben während der Lebenszyklussees des Systems unverändert.

Das offene Übertragungssystem (Kategorie 2 und/oder 3) kann einiges oder alles von folgenden Punkten enthalten:

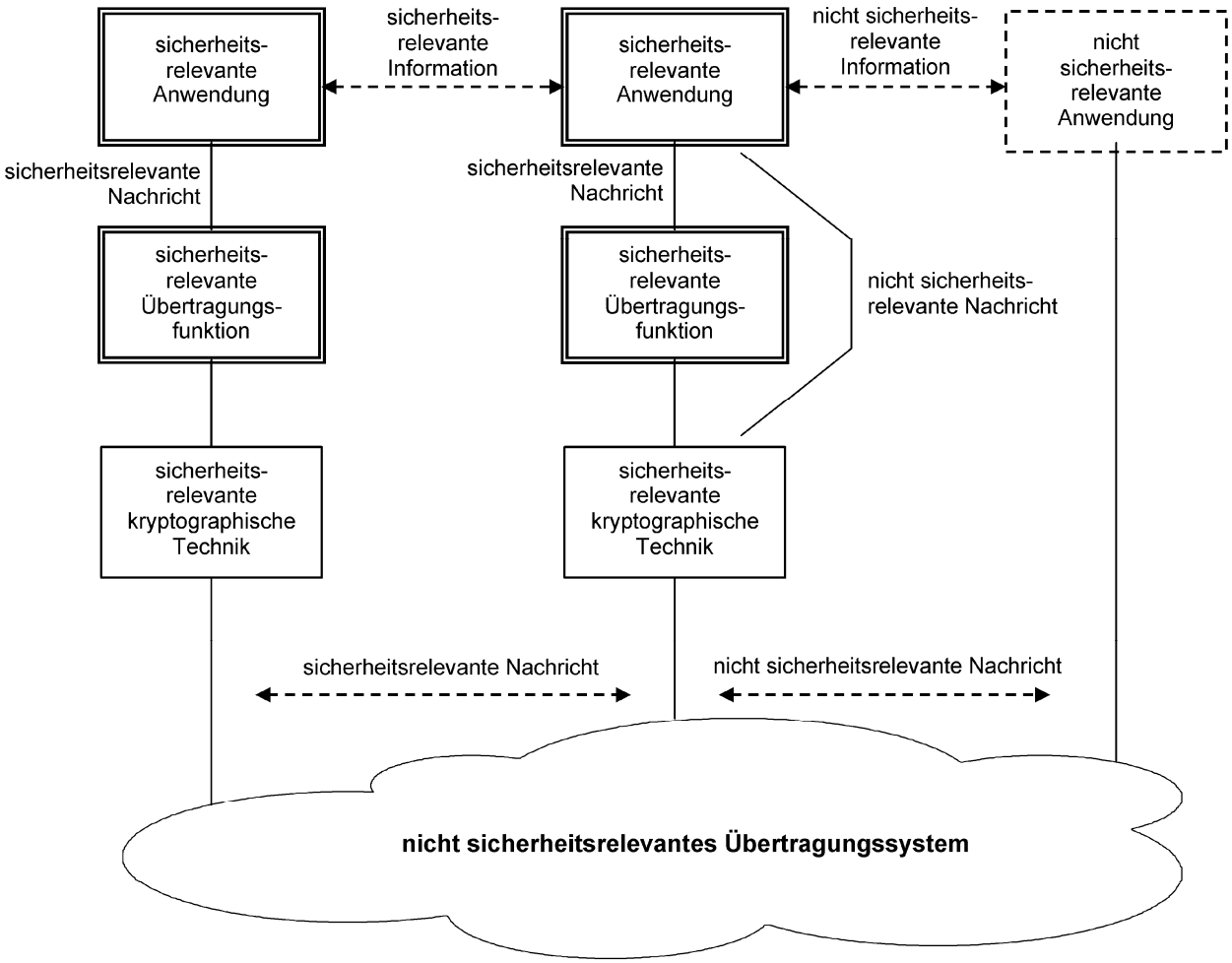
– Elemente, die Daten lesen, speichern, verarbeiten oder weiter übertragen, und die von Nutzern des Übertragungssystems erzeugt und dargestellt werden mit einem dem Nutzer unbekanntem Programm. Die Anzahl von Nutzern ist im allgemeinem unbekannt; sicherheitsrelevante und nicht sicherheitsrelevante Einrichtungen 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 unbekanntem Programm;

– andere Nutzer des Übertragungssystems, die dem Designer der sicherheitsrelevanten Anwendung unbekannt sind, senden unbekannte Mengen an Informationen in unbekannten Formaten.

Das offenen Übertragungssystem der Kategorie 3 kann Gegenstand von nicht autorisiertem, böswilligem Zugriff auf das Übertragungssystem sein.



Implementiert in sicherheitsrelevanter Einrichtung entsprechend EN 50129

Implementiert für Kategorie 3 Übertragungssysteme in:

– sicherheitsrelevanter Einrichtung entsprechend EN 50129, oder
– nicht sicherheitsrelevanter Einrichtung, geprüft durch sicherheitsrelevante Techniken

Implementiert in:

– nicht sicherheitsrelevanter Einrichtung, oder
– sicherheitsrelevanter Einrichtung (Schnittstelle zwischen sicherheitsrelevanten und nicht sicherheitsrelevanten Funktionen, bewertet nach EN 50129)

Bild 1 – Referenzarchitektur für sicherheitsrelevante Kommunikation

Die Referenzarchitektur beabsichtigt nicht Implementierungen einzuschränken; unterschiedliche Strukturen sind möglich, siehe Beispiele im informativen Anhang C und im besonderen Abschnitt C.5 für nicht sicherheitsrelevante Nachrichten.

5 Bedrohungen auf das Übertragungssystem

Die Hauptgefährdung für eine sicherheitsrelevante Kommunikation ist: „Das Versagen, eine gültige Nachricht bezogen auf Authentizität, Integrität, Sequenz und zeitliche Richtigkeit am empfangenden Ende zu bekommen“. Diese Norm berücksichtigt Bedrohungen auf diese Nachrichtenmerkmale, die vom Übertragungssystem kommen. Bedrohungen auf die sicherheitsrelevanten Einrichtungen müssen entsprechend EN 50129 beachtet werden.

Die Einhaltung der Anforderungen dieser Norm bietet jedoch keinen Schutz gegen beabsichtigten oder nicht beabsichtigten Missbrauch von autorisierten Quellen. Es ist notwendig, im Sicherheitsnachweis diese Aspekte zu berücksichtigen.

Weitere Informationen mit Leitfäden für die Bedrohungsanalyse und den Sicherheitsnachweis sind im informativen Anhang A enthalten. Es muss betont werden, dass für jedes Projekt eine Analyse gemacht werden muss, denn obwohl die Methode für Nachrichtenfehler des Anhangs A eingeschlossen sein kann, muss das nicht von selbst notwendigerweise komplett sein.

Identifizierte gefährliche Ereignisse können folgendes einschließen:

– systematische Fehler;
– Drahtbruch;
– Verkabelungsfehler;
– Falschausrichtung von Antennen;
– Verlust der Leistung;
– zufällige HW Fehler und Alterung;
– menschliche Fehler;
– Instandhaltungsfehler;
– EMI;
– Übersprechen;
– thermisches Rauschen;
– Schwundeffekte;
– Überlastung des Übertragungssystems;
– magnetischer Sturm;
– Feuer;
– Erdbeben;
– Blitz

ebenso absichtlich veranlasste Ereignisse, wie

– anzapfen der Leitung,
– Zerstörung, oder nicht autorisierte Änderung der HW,
– nicht autorisierte Änderung der SW,
– abhören von Leitungen,
– Übertragung von nicht autorisierten Nachrichten.

Doch, obwohl ein weiter Bereich von gefährlichen Ereignissen existieren kann, die grundsätzlichen Nachrichtenfehler, die die Bedrohungen für das Übertragungssystem bilden, sind eine von den folgenden:

– Wiederholung;
– Auslassung;
– Einfügung;
– Resequenzierung;
– Verfälschung;

– Verzögerung;
– Manipulation.

Tabelle A.1 geht darauf ein, welche Bedrohungen auf das Übertragungssystem durch jede Art eines gefährlichen Ereignisses verursacht werden können. Nach Identifizierung der gefährlichen Ereignisse, die für ein bestimmtes System auftreten können und vor denen nicht durch andere Mittel geschützt ist, kann die Tabelle als Leitlinie benutzt werden, um die für das System zu berücksichtigten Bedrohungen zu identifizieren.

Tabelle A.1 einhält keine Wahrscheinlichkeiten der Ereignisse, dies muss Teil der Bedrohungsanalyse sein.

6 Klassifikation von Übertragungssystemen

6.1 Allgemeines

Dieser Abschnitt definiert den Prozess, der für die Klassifikation aller Übertragungssysteme anzuwenden ist. Hierbei werden die für solche Systeme relevanten Bedrohungen identifiziert, die die Auswahl der Schutzmaßnahmen beeinflussen, die in die Sicherheitsanwendungen einzubeziehen sind.

6.2 Allgemeine Aspekte der Klassifikation

Es gibt viele Faktoren, die die Bedrohungen auf ein sicherheitsrelevantes Übertragungssystem beeinflussen können.

Zum Beispiel ist es möglich, dass von Signalsystemnutzern Übertragungsdienste von privaten oder öffentlichen Diensterbringern bezogen werden. Unter solchen Dienstverträgen kann die Verantwortung des Diensterbringers für die garantierte Leistungsfähigkeit des Übertragungssystems begrenzt sein.

Deshalb hängt die Bedeutung der Bedrohungen (und demzufolge die Anforderungen an die Schutzmaßnahmen) von dem Ausmaß der Kontrolle ab, die über das Übertragungsnetzwerk ausgeübt wird, bei Einbeziehung folgender Punkte:

– die technischen Eigenschaften des Systems einschließlich der Garantien der Zuverlässigkeit und Verfügbarkeit des Systems, des Ausmaßes von Datenspeicherung innerhalb des Systems (welches die Verzögerung oder die Resequenzierung von Nachrichten beeinflussen kann);
– die Beständigkeit der Leistungsmerkmale des Systems über der Lebensdauer (z. B. Netzwerkänderungen und Änderungen in der Nutzerbasis), und der Auswirkung von Verkehrslasten durch andere Nutzer;
– Zugriff auf das System abhängig davon, ob das Netzwerk privat oder öffentlich ist, der Grad der vom Operator ausgeübten Zugriffskontrolle über andere Nutzer, die Möglichkeit des Missbrauchs des Systems durch andere Nutzer, und der Zugriff von Instandhaltungspersonal, um das System zu re- konfigurieren oder Zugriff auf das Übertragungsmedium selbst zu erlangen.

Unter Beachtung dieser Sachverhalte können drei Kategorien von Übertragungssystemen definiert werden.

6.3 Kriterien für die Klassifizierung von Übertragungssystemen

6.3.1 Kriterien für Kategorie 1 Übertragungssysteme

Ein Übertragungssystem kann als Kategorie 1 angesehen werden, wenn folgende Vorbedingungen erfüllt sind.

Pr1 Die Anzahl der anschließbaren Einrichtungen – sicherheitsrelevant oder auch nicht – an das Übertragungssystem muss bekannt und festgelegt sein. Da die sicherheitsrelevante Kommunikation von diesem Parameter abhängt, muss die maximale Anzahl der Teilnehmer, die miteinander kommunizieren dürfen, in der Sicherheitsanforderungsspezifikation als Vorbedingung genannt sein. Die Konfiguration des Systems muss in dem Sicherheitsnachweis definiert/eingeschlossen sein. Jeder nachfolgenden Änderung an dieser Konfiguration muss eine Nachprüfung ihrer Auswirkung auf den Sicherheitsnachweis vorangehen.

Pr2 Die Eigenschaften des Übertragungssystems (z. B. Übertragungsmedium, „worst case"- Umweltbedingungen, etc.) sind bekannt und festgelegt. Sie müssen während der gesamten Einsatzdauer des Systems beibehalten bleiben. Falls wichtige, im Sicherheitsnachweis benutzte Parameter geändert werden sollen, müssen alle sicherheitsrelevanten Aspekte nachgeprüft werden.

Pr3 Das Risiko eines nicht autorisierten Zugriffs auf das Übertragungssystem muss vernachlässigbar sein.

Wenn ein Übertragungssystem alle die obigen Vorbedingungen erfüllt, darf es als Kategorie 1 und als ein geschlossenes System angesehen werden, und, falls das so ist, muss es den Regeln eines, im allgemeinen reduzierten Satzes von Prozessen und Anforderungen des Abschnitts 7 folgen.

6.3.2 Kriterien für Kategorie 2 Übertragungssysteme

Wenn ein Übertragungssystem die Vorbedingungen 1 oder 2 (Pr1 oder Pr2) in 6.3.1 nicht erfüllt, aber die Vorbedingung 3 (Pr3) erfüllt, muss es als Kategorie 2 und als ein offenes System angesehen werden und es muss mit einem umfassenderen Satz von Prozessen und Anforderungen des Abschnitts 7 bemessen werden.

6.3.3 Kriterien für Kategorie 3 Übertragungssysteme

Wenn ein Übertragungssystem die Vorbedingung 3 (Pr3) in 6.3.1 nicht erfüllt, muss es als Kategorie 3 und als ein offenes System angesehen werden und es muss mit dem vollen Satz von Prozessen und Anforderungen des Abschnitts 7 bemessen werden.

6.4 Beziehung zwischen Übertragungssystemen und den Bedrohungen

Die Bedeutsamkeit der Bedrohung auf das sicherheitsrelevante Kommunikationssystem muss entsprechend dem Grad der durch den Benutzer ausgeübten Kontrolle über das Übertragungssystem bewertet werden.

Die in Abschnitt 5 identifizierten Bedrohungen sind für alle Übertragungssystemkategorien anwendbar, mit der Ausnahme von Manipulation, die nur für offene Übertragungssystem anwendbar ist.

In Anhang B ist ein Beispiel der Klassifikation von Übertragungssystemen in Tabelle B.1 dargestellt und in Tabelle B.2 ein Beispiel der Zuordnung Bedrohung/Kategorie.

Die Anwendbarkeit des Abschnitts 7 hängt von der Kategorie des Übertragungssystems ab.

7 Anforderungen an die Schutzmaßnahmen

7.1 Einführung

In der Vergangenheit sind gewisse Techniken in Datenübertragungssystemen (nicht sicherheitsrelevant, sicherheitsrelevant) genutzt worden. Diese Techniken stellen eine „Bibliothek" von möglichen Verfahren dar, die für den Entwickler des Steuerungs- und Überwachungssystems verfügbar sind, um einen Schutz gegen jede einzelne der oben genannten Bedrohungen bereitzustellen.

Um das Risiko zu reduzieren, das von den im vorigen Abschnitt genannten Bedrohungen ausgeht, müssen die folgenden elementaren Sicherheitsdienste in Betracht gezogen werden und in dem für die Anwendung erforderlichen Umfang, sowohl für offene als auch für geschlossene Übertragungssysteme eingesetzt werden:

– Nachrichtenauthentizität;
– Nachrichtenintegrität;
– Rechtzeitigkeit der Nachrichten;
– Nachrichtensequenz.

Die folgende Menge bekannter Schutzmaßnahmen werden umrissen:

a) Sequenznummer;

b) Zeitstempel;

c) Zeitüberwachung (time out);

d) Quellen- und Zielbezeichner;

e) Rücknachricht;

f) Identifikationsprozedur;

g) Sicherheitscode;

h) kryptographische Techniken.

Eine Anzahl, die Architektur betreffenden Sachverhalte müssen durch die jeweilige Anwendung berücksichtigt und im Sicherheitsnachweis rechtfertigt werden, z. B.:

– Bedingungen zur Inanspruchnahme und zum Erhalt der Übereinstimmung mit den Vorbedingungen der Kategorie 1, oder 2 Übertragungssysteme;

– Kriterien für die Abschottung zwischen Übertragungssystemen unterschiedlicher Kategorie;

– Robustheit der Übertragungssystems gegen Verweigerung des Dienstes als Folge von Überlaufangriffen, z. B. Bedarf an Zugangsschutz.

Mit Referenz auf h), der Anwendungsbereich dieser Norm schließt allgemeine IT Sicherheitsangelegenheiten aus:

– nur Angriffe während des betrieblichen Einsatzes werden berücksichtigt;

– nur Angriffe anhand von Nachrichten auf die sicherheitsrelevante Anwendung werden hier angesprochen.

Ein vollständiges Verfahren zum Zugriffsschutz sollte jedoch berücksichtigen

– Verfahrens- und Instandhaltungsaspekte des Zugriffsschutzes,

– Angreifbarkeit der Software, die nicht Teil der sicherheitsrelevanten Anwendung ist,

– Vertraulichkeit der Information.

7.2 Allgemeine Anforderungen

7.2.1 Es müssen adäquate Schutzmaßnahmen zur Verfügung gestellt werden, gegen alle identifizierten Bedrohungen auf die Sicherheit der Systeme, die ein offenes, oder geschlossenes Übertragungssystem benutzen. Alle nicht anzunehmenden Bedrohungen müssen rechtfertigt und im Sicherheitsnachweis aufgezeichnet werden. Anhang A enthält eine Liste möglicher Bedrohungen, die als Leitfaden benutzt werden kann.

7.2.2 Im Falle einer Kommunikation zwischen sicherheitsrelevanten und nicht sicherheitsrelevanten Anwendungen über das selbe Übertragungssystem gelten folgende Anforderungen:

– für die Sicherheitsschutzmaßnahmen in den sicherheitsrelevanten Einrichtungen muss gezeigt werden, dass sie von den Schutzmaßnahmen der nicht sicherheitsrelevanten Funktionen funktional unabhängig sind;

– die sicherheitsrelevanten und nicht sicherheitsrelevanten Nachrichten müssen unterschiedliche Strukturen aufweisen, indem ein Sicherheitscode bei den sicherheitsrelevanten Nachrichten angewendet wird. Dieser Sicherheitscode muss die Fähigkeit besitzen, das System entsprechend der Sicherheitsanforderungsstufe zu schützen (siehe 7.3.7), sodass sich eine nicht sicherheitsrelevante Nachricht nicht in eine sicherheitsrelevante Nachricht verändern kann.

7.2.3 In den detaillierten Anforderungen an die für die Anwendung benötigten Schutzmaßnahmen sind zu berücksichtigen:

– das Ausmaß des Risikos (Häufigkeit/Folgen) für jede einzelne Bedrohung; und

– die·Sicherheitsanforderungsstufe (SIL) der Daten und des betroffenen Prozesses.

Anhang C gibt Hinweise für die Auswahl von zur Zeit bekannten Techniken, um die Bedrohungen abzuwehren. Die Angaben zur Wirksamkeit in diesem Anhang sollten sorgfältig betrachtet werden, wenn die Schutzmaßnahme ausgewählt wird.

7.2.4 Die Anforderungen an die benötigten Schutzmaßnahmen müssen in der Systemanforderungsspezifikation und in der Systemsicherheitsanforderungsspezifikation der Anwendung enthalten sein, und sie müssen im Teil „Funktionsnachweis“ des Sicherheitsnachweises der Anwendung berücksichtigt werden.

7.2.5 Alle Schutzmaßnahmen müssen entsprechend den Anforderungen nach EN 50129 implementiert werden. Das bedeutet, dass die Schutzmaßnahmen

– komplett innerhalb der sicherheitsrelevanten Übertragungseinrichtungen des Systems implementiert sein müssen (mit der möglichen Ausnahme von einigen kryptographischen Architekturen, siehe 7.3.8 und Abschnitt C.2),

– von den benutzten Schichten des nicht sicherheitsrelevanten Übertragungssystems funktional unabhängig sein müssen.

7.2.6 In den folgenden Abschnitten sind verbindliche Anforderungen für die speziellen Schutzmaßnahmen vorgegeben. Sie gelten, wenn die spezielle Schutzmaßnahme genutzt wird.

7.2.7 Andere als die in dieser Norm beschriebenen Schutzmaßnahmen dürfen benutzt werden, sofern der Sicherheitsnachweis eine Analyse ihrer Wirksamkeit gegen die Bedrohungen enthält.

7.2.8 Der Nachweis der funktionalen und technischen Sicherheit muss nach dem gleichen Prozess erfolgen, wie in EN 50129 spezifiziert, einschließlich

– einem umfassenden Fehlermodell,

– einer funktionalen Spezifikation, basierend auf der Analyse des umfassenden Fehlermodells,

– Analyse jeder in der sicherheitsrelevanten Kommunikation benutzten Schutzmaßnahme,

– der Sicherheitsreaktion für den Fall eines entdeckten Übertragungsfehlers,

– der Anforderungsspezifikation an die Sicherheitsintegrität und SIL Zuweisung.

7.2.9 7.3 definiert einen umfassenden Satz von Schutzmaßnahmen. Für Kategorie 1 Übertragungssysteme reicht jedoch der folgende reduzierte Satz, dennoch unter Beibehaltung der elementaren Sicherheitsdienste:

– Quellen und/oder Zielbezeichner (im Fall von mehr als einem Sender und/oder mehr als einem Empfänger);

– Sequenznummer und/oder Zeitstempel in dem von der Anwendung benötigten Umfang; und

– ein Sicherheitscode.

7.3 Spezifische Schutzmaßnahmen

Die folgenden Abschnitte enthalten kurze Einführungen und die Anforderungen für spezifische Schutzmaßnahmen, die entweder für sich allein oder kombiniert gegen einzelne oder mehrere Bedrohungen wirksam sind. Alle oben genannten allgemeinen Anforderungen müssen erfüllt werden.

Detailliertere Beschreibungen von Schutzmaßnahmen und ihre Beziehung zu allen möglichen Bedrohungen sind im informativen Anhang C angegeben.

7.3.1 Sequenznummer

7.3.1.1 Einführung

Sequenznummerierung erfolgt durch Hinzufügung einer laufenden Nummer (genannt Sequenznummer) zu jeder einzelnen Nachricht, die zwischen einem Sender und einem Empfänger ausgetauscht wird. Dieses gestattet dem Empfänger, die Folge der vom Sender bereitgestellten Nachrichten zu prüfen.

7.3.1.2 Anforderungen

Der Sicherheitsnachweis muss aufzeigen, dass folgende Punkte im Hinblick auf die Sicherheitsanforderungsstufe des Prozesses und die Art des sicherheitsrelevanten Prozesses angemessen gelöst sind:

– die Länge der Sequenznummer;

– die Vorkehrungen zur Initialisierung und Überlauf der Sequenznummer;

– die Vorkehrungen zur Wiederherstellung nach einer Unterbrechung der Nachrichtensequenz.

7.3.2 Zeitstempel

7.3.2.1 Einführung

Wenn eine Einheit eine Information empfängt, ist die Bedeutung der Information oft zeitbezogen. Der Grad von Abhängigkeit zwischen Information und Zeit kann sich von Anwendung zu Anwendung unterscheiden. In gewissen Fällen kann eine veraltete Information nutzlos und harmlos sein, und in anderen Fällen kann sie eine potentielle Gefahr für den Nutzer darstellen. Die Lösungen können sich in Abhängigkeit von dem zeitlichen Verhalten der Prozesse, die Informationen austauschen (zyklisch, ereignisgesteuert usw.), unterscheiden.

Eine Lösung, die die Beziehungen zwischen Zeit und Informationen abdeckt, ist die Hinzufügung von Zeitstempeln zu den Informationen. Diese Art von Information kann anstelle der Sequenznummern oder kombiniert mit ihnen – abhängig von den Anwendungsanforderungen – genutzt werden. Abschnitt C.1 zeigt den unterschiedlichen Gebrauch von Zeitstempeln und deren Eigenschaften.

7.3.2.2 Anforderungen

Der Sicherheitsnachweis muss aufzeigen, dass folgende Punkte im Hinblick auf die Sicherheitsanforderungsstufe des Prozesses und die Art des sicherheitsrelevanten Prozesses angemessen gelöst sind:

– der Wert des Zeitinkrements;

– die Genauigkeit des Zeitinkrements;

– die Größe des Zeitgebers;

– der absolute Wert der Zeitgeber (z. B. UTC (allgemeine koordinierte Zeit) oder einer anderen globalen Zeit);

– der Synchronismus der Zeitgeber in den verschiedenen Einheiten;

– die Zeitverzögerung zwischen der Erzeugung der Information und Addition des Zeitstempels auf ihr;

– die Zeitverzögerung zwischen der Prüfung des Zeitstempels und Nutzung der Information.

7.3.3 Zeitüberwachung

7.3.3.1 Einführung

Bei (typischerweise zyklischen) Übertragungen kann der Empfänger prüfen, ob die Verzögerung zwischen zwei Nachrichten eine vordefinierte, erlaubte Höchstzeit überschreitet. Falls dies der Fall ist, muss ein Fehler angenommen werden.

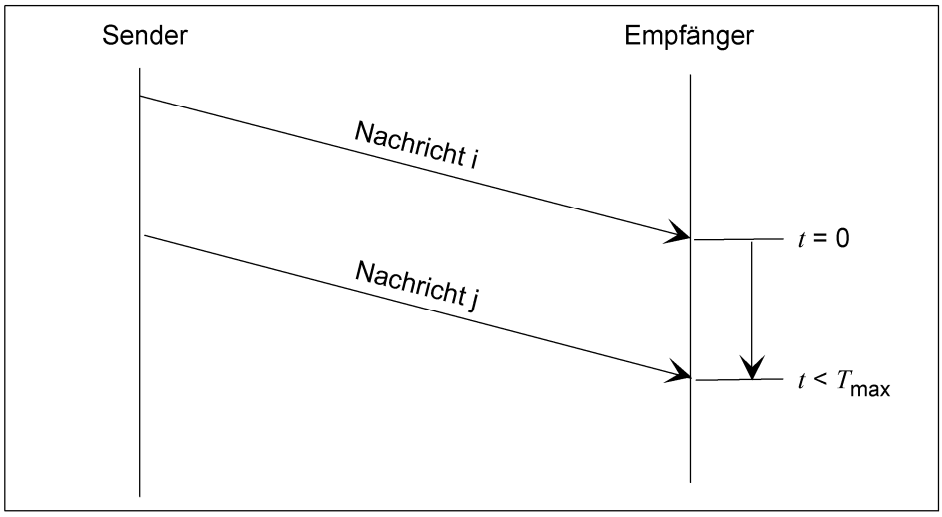


Bild 2 – Zyklische Übertragung von Nachrichten

Die Überwachung kann durch den Sender durchgeführt werden, falls ein Rückkanal zur Verfügung steht. Beim Senden der Nachricht i startet der Sender einen Zeitgeber. Der Empfänger der Nachricht i antwortet mit einer Bestätigungsnachricht j bezogen auf die empfangene Nachricht i. Wenn der Sender die entsprechende Bestätigungsnachricht j nicht innerhalb einer vorgegeben Zeit empfängt, muss ein Fehler angenommen werden.

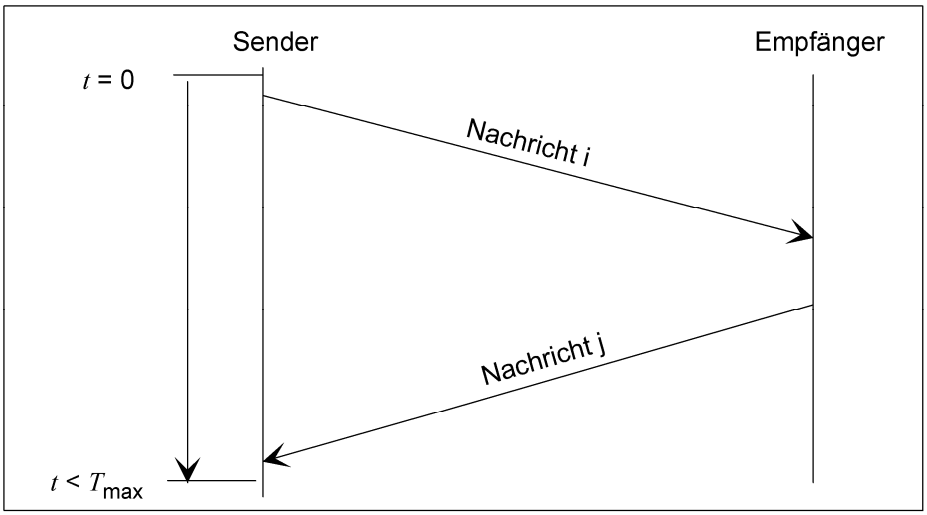


Bild 3 – Bidirektionale Übertragung von Nachrichten

7.3.3.2 Anforderungen

Der Sicherheitsnachweis muss aufzeigen, dass folgende Punkte im Hinblick auf die Sicherheitsanforderungsstufe des Prozesses und die Art des sicherheitsrelevanten Prozesses angemessen gelöst sind:

– die akzeptierbare Verzögerung;

– die Genauigkeit der Zeitüberwachung.

7.3.4 Quellen- und Zielbezeichner

7.3.4.1 Einführung

Bei Kommunikationsprozessen zwischen vielen Teilnehmern benötigen diese adäquate Mittel, um die Quelle aller empfangenen Informationen zu prüfen, bevor diese genutzt werden. Die Nachrichten müssen zusätzliche Daten enthalten, um dieses zu ermöglichen.

Die Nachrichten können einen einzigartigen Quellenbezeichner oder einen einzigartigen Zielbezeichner oder beides enthalten. Die Wahl hängt von der sicherheitsrelevanten Anwendung ab. Diese Bezeichner werden von den sicherheitsrelevanten Übertragungsfunktionen der Anwendung hinzugefügt.

– Die Einfügung eines Quellenbezeichners kann es den Nutzern der Nachrichten ermöglichen zu prüfen, ob die Nachrichten von der beabsichtigten Quelle stammen, ohne der Notwendigkeit eines Dialoges zwischen den Nutzern. Dies kann z. B. in unidirektionalen oder Broadcast – Kommunikationssystemen hilfreich sein.
– Die Einfügung eines Zielbezeichners kann es den Nutzern der Nachrichten ermöglichen zu prüfen, ob die Nachrichten für sie bestimmt sind, ohne der Notwendigkeit eines Dialoges zwischen den Nutzern. Dies kann z. B. in unidirektionalen oder Broadcast – Kommunikationssystemen hilfreich sein. Man kann Zielbezeichner wählen, um einzelne Ziele oder Gruppen von Nutzern zu identifizieren.

7.3.4.2 Anforderungen

Der Sicherheitsnachweis muss aufzeigen, dass folgende Punkte im Hinblick auf die Sicherheitsanforderungsstufe des Prozesses und die Art des sicherheitsrelevanten Prozesses angemessen gelöst sind:

– die Einzigartigkeit der Bezeichner für die Einheiten im gesamten Übertragungssystem;
– die Größe des Bezeichnerdatenfeldes.

7.3.5 Rücknachricht

7.3.5.1 Einführung

Dort, wo ein geeigneter Übertragungskanal verfügbar ist, kann eine Rücknachricht vom Empfänger der sicherheitskritischen Information an den Sender gesendet werden. Der Inhalt dieser Rücknachricht kann folgendes umfassen:

– vom Inhalt der Originalnachricht abgeleitete Daten, entweder in identischer oder in veränderter Form;
– vom Empfänger hinzugefügte Daten, die von seiner eigenen lokalen Information abgeleitet wurden;
– zusätzliche Daten für sicherheitsrelevante Sicherheits- oder Informationssicherheitszwecke.

Die Verwendung einer solchen Rücknachricht kann zur Sicherheit des Prozesses in verschiedenster Weise beitragen:

– durch die Bereitstellung einer positiven Bestätigung des Empfangs von gültigen und rechtzeitigen Nachrichten;
– durch die Bereitstellung einer positiven Bestätigung des Empfangs von gestörten Nachrichten, um eine geeignete Aktion zu unternehmen;
– durch die Bestätigung der Identität der Empfangseinrichtung;
– zur Erleichterung der Synchronisation von Uhren in den Sende- und Empfangseinrichtungen;
– zur Erleichterung von dynamischen Prüfprozeduren zwischen den Teilnehmern.

7.3.5.2 Anforderungen

Die Existenz eines Rückkanals verhilft nicht von sich heraus zu einer Schutzmaßnahme gegen irgendeine identifizierte Bedrohung. Es handelt sich um einen Mechanismus, der auf Anwendungsebene andere Schutzmaßnahmen ermöglicht. Deswegen gibt es keine spezifischen Sicherheitsanforderungen für einen solchen Rückkanal.

7.3.6 Identifikationsprozedur

7.3.6.1 Einführung

Der vorangegangene Abschnitt deckt die Anforderungen an die zu identifizierenden Einheiten ab.

Offene Übertragungssysteme können zusätzlich das Risiko einbringen, dass Nachrichten von anderen (unbekannten) Nutzern mit Originalinformationen von einer beabsichtigten Quelle verwechselt werden (eine Form von manipulierter Nachricht).

Eine geeignet entworfene Identifikationsprozedur innerhalb des sicherheitsrelevanten Prozesses kann diese Bedrohung abwehren.

Es kann zwischen zwei Arten von Identifikationsprozeduren unterschieden werden:

– bidirektionale Identifikation
  Wo ein Rückkanal verfügbar ist, kann der Austausch von Einheitenbezeichner zwischen den Sendern und Empfängern der Informationen zusätzliche Sicherheit bieten, dass die Kommunikation tatsächlich zwischen den beabsichtigten Teilnehmern geschieht.
– dynamische Identifikationsprozedur
  Der dynamische Austausch von Informationen zwischen Sender und Empfänger - einschließlich der Umwandlung und Rücknachricht der empfangenen Information zu dem Sender - kann die Sicherheit bieten, dass die Kommunikationsteilnehmer nicht nur behaupten, die korrekte Identität zu besitzen, sondern sich auch in der erwarteten Art verhalten. Dieser Typ der dynamischen Identifikationsprozedur kann dazu verwendet werden, die Übertragung der Information zwischen sicherheitsrelevanten Prozessen einzuleiten und/oder sie kann während der Informationsübertragung selbst verwendet werden.

7.3.6.2 Anforderungen

Die Identifikationsprozedur stellt einen Teil des sicherheitsrelevanten Anwendungsprozesses dar. Die detaillierten Anforderungen müssen in der Sicherheitsanforderungsspezifikation definiert werden.

7.3.7 Sicherheitscode

7.3.7.1 Einführung

In Übertragungssystemen werden im allgemeinen Übertragungscodes benutzt, um Bit- und/oder Büschelfehler zu entdecken, und/oder um die Übertragungsqualität durch Fehlerkorrekturmaßnahmen zu erhöhen. Obschon diese Übertragungscodes sehr effizient sein können, können sie wegen Hardware Defekten, externen Einflüssen, oder systematischen Fehlern ausfallen.

Der sicherheitsrelevante Prozess darf sich aus Sicht der Sicherheit nicht auf solche Übertragungscodes verlassen. Deshalb ist zusätzlich ein Sicherheitscode unter Kontrolle des sicherheitsrelevanten Prozesses erforderlich, um Nachrichtenverfälschungen zu entdecken.

Der Sicherheitsnachweis muss aufzeigen, dass folgende Punkte im Hinblick auf die geforderte Sicherheitsanforderungsstufe und den Charakter der sicherheitsrelevanten Funktionen angemessen gelöst sind:

– die Fähigkeit, erwartete systematische Nachrichtenverfälschungen zu entdecken;
– die Wahrscheinlichkeit, zufällige Nachrichtenverfälschungen zu entdecken.

ANMERKUNG Der Sicherheitscode kann eine Kombination verschiedener Codes sein, z. B. ein linearer Code kombiniert mit einem konstanten Wert.

Abschnitt C.3 enthält eine Anleitung zur Auswahl von Sicherheitscodes.

7.3.7.2 Anforderungen

7.3.7.2.1 Der Sicherheitscode muss ungleich dem Übertragungscode sein. Diese Ungleichheit kann erreicht werden entweder durch:

– die Anwendung eines ungleichen Algorithmus;

– die Anwendung ungleicher Konfigurationsparameter (z. B. Polynome) für denselben Algorithmus. Falls beide Codes auf einem CRC basieren, müssen die Polynome unterschiedlich sein. Wenn beide Polynome gemeinsame Faktoren haben, muss ihr Beitrag zur Leistungsfähigkeit des Sicherheitscodes in der Sicherheitsanalyse vernachlässigt werden.

ANMERKUNG Im Fall eines geschlossenen Übertragungssystems kann der Designer einfach einen Sicherheitscode wählen, der ungleich dem Übertragungscode ist, weil er volle Kenntnis über das Übertragungssystem hat. Im Fall eines offenen Übertragungssystems kann die Anforderung durch einen Sicherheitscode erfüllt werden, der nicht in kommerziellen Übertragungssystemen verwendet wird.

7.3.7.2.2 Der Sicherheitscode muss entdecken

– Übertragungsfehler, z. B. verursacht durch EMI,

– systematische Fehler, verursacht durch Hardwarefehler innerhalb des nicht sicherheitsrelevanten Übertragungssystems.

ANMERKUNG Fehler, die den Sicherheitscode nachahmen, können nicht adäquat entdeckt werden. Deshalb muss der Sicherheitscode komplexer, als die erwarteten Fehler sein. Infolgedessen kann angenommen werden, dass ein Hardwarefehler im nicht sicherheitsrelevanten Übertragungssystem keinen gültigen Sicherheitscode generieren kann.

7.3.7.2.3 Um die geforderte Sicherheitsanforderungsstufe zu erfüllen, ist es notwendig, dass der Sicherheitscode hinreichend komplex ist, z. B. basierend auf einem CRC, um typische Ausfälle und Fehler zu entdecken und zu behandeln. Die Analyse muss mindestens umfassen:

– unterbrochene Übertragungsleitung;

– alle Bits sind logisch 0;

– alle Bits sind logisch 1;

– Nachricht ist invertiert;

– Synchronisationsschlupf (im Fall von serieller Übertragung);

– zufällige Fehler;

– Bündelfehler;

– systematische Fehler, z. B. sich wiederholende Fehlermuster;

– Kombinationen des obigen.

7.3.7.2.4 Die wahrscheinlichkeitstheoretische Analyse der Leistungsfähigkeit des Sicherheitscodes muss kompatibel mit dem Sicherheitsziel sein. Ein Modell der Ausfallarten muss erstellt werden und alle Annahmen, die für die Berechung gemacht wurden, müssen verifiziert und validiert werden.

Die Wahrscheinlichkeit von unentdeckten Fehlern bei linearen Codes wird oft durch Anwendung des Modells des binären symmetrischen Kanals (BSC) berechnet (siehe Abschnitt C.4). Falls ein nicht binärer Code benutzt wird, kann der *„q-nary“* symmetrische Kanal QSC geeigneter sein. Diese Norm empfiehlt, diese Wahrscheinlichkeit auf den durch diese Modelle berechneten ungünstigsten Wert zu begrenzen.

ANMERKUNG Der BSC ist gut geeignet für zufällige Fehler, wie durch EMI verursacht. Aber einfache zufällige Fehler werden üblicherweise durch das nicht sicherheitsrelevante Übertragungssystems beseitigt. Deshalb sind normalerweise viele Bits in der sicherheitsrelevanten Nachricht gestört, falls ein Fehler durch den Sicherheitscode entdeckt wird. Weil für diese Fälle keine einfachen Modelle verfügbar sind, empfiehlt diese Norm, keine niedrigeren Wahrscheinlichkeiten für unentdeckte Fehler zu benutzen, als den durch die Anwendung des BSC erreichten ungünstigsten Wert für Bitfehlerraten kleiner als ein halb (siehe Abschnitt C.4).

Ein Beispiel eines vereinfachten Modells für ein geschlossenes Übertragungssystems ist in Abschnitt C.4 (informativ) vorgegeben.

7.3.8 Kryptographische Techniken

7.3.8.1 Einführung

Kryptographische Techniken können benutzt werden, wenn böswillige Angriffe innerhalb des offenen Übertragungssystems nicht ausgeschlossen werden können.

Das ist gewöhnlich der Fall, wenn die sicherheitsrelevante Kommunikation ein

– öffentliches Netzwerk;
– Funkübertragungssystem;
– ein Übertragungssystem mit Anschlüssen an öffentliche Netzwerke

benutzt.

Gegen vorsätzliche Angriffe mittels Nachrichten auf sicherheitsrelevante Anwendungen, muss die sicherheitsrelevante Nachricht durch kryptographische Techniken geschützt werden.

Diese Anforderung, die der Vermeidung von Manipulation von nicht autorisierten Sendern dient, kann durch eine der folgenden Lösungen erfüllt werden:

1) Nutzung eines Sicherheitscodes, der kryptographischen Schutz bietet;
2) Verschlüsselung der Nachricht, nach Anwendung des Sicherheitscodes;
3) Hinzufügung eines kryptographischen Codes zum Sicherheitscode.

Diese Techniken können mit Sicherheitscodierungsverfahren kombiniert werden oder separat eingesetzt werden. Anhang C zeigt einige mögliche Lösungen.

Kryptographische Techniken beinhalten den Gebrauch von Schlüsseln und Algorithmen. Der Wirksamkeitsgrad hängt von der Stärke der Algorithmen und der Geheimhaltung der Schlüssel ab. Die Geheimhaltung eines Schlüssels hängt von seiner Länge und seinem Management ab.

7.3.8.2 Anforderungen

Der Sicherheitsnachweis muss aufzeigen, dass folgende Punkte im Hinblick auf die Sicherheitsanforderungsstufe des Prozesses und die Art des sicherheitsrelevanten Prozesses angemessen gelöst sind:

– technische Auswahl der kryptographischen Techniken, einschließlich
  – Leistungsfähigkeit des Verschlüsselungsalgorithmus (z. B. symmetrisch, oder asymmetrisch),
  – Schlüsseleigenschaften (z. B. unveränderlich, oder sitzungsbasiert),
  – Rechtfertigung der gewählten Schlüssellänge,
  – Häufigkeit des Schlüsselwechsels,
  – physikalische Speicherung der Schlüssel,
– technische Auswahl von kryptographischen Architekturen, einschließlich
  – Prüfung der korrekten Funktion (vor und während der Betriebsphase) der kryptographischen Prozesse, wenn diese außerhalb der sicherheitsrelevanten Anwendung implementiert sind,
– Managementaktivitäten, einschließlich
  – Erzeugung, Speicherung, Verteilung und Vernichtung der vertraulichen Schlüssel,
  – Management der Einrichtungen,
  – Überprüfungsprozesse für die Angemessenheit der kryptographischen Techniken in Bezug auf Risiken von böswilligen Angriffen.

Der kryptographische Algorithmus muss auf alle Nutzdaten angewendet werden und kann auf zusätzliche Daten, die nicht übertragen werden, jedoch dem Sender und Empfänger bekannt sind (implizite Daten), angewendet werden.

Es müssen vernünftige Annahmen über das Wesen, die Motivation und die finanziellen und technischen Mittel eines potentiellen Hackers beschrieben werden, die auch Entwicklungen (sowohl technische, wie Anstieg der Computerleistung, der Kostenverringerung von schnellen Prozessoren, der Ausbreitung des Wissen über Algorithmen, als auch „soziale“, wie wirtschaftliche Konflikte, ein Anstieg des Vandalismus, ...) in Betracht ziehen, die während der Lebenszeit des Systems erwartet werden können.

Für das Schlüsselmanagement werden genormte Techniken (z. B. entsprechend ISO/IEC 11770) dringend empfohlen.

7.4 Anwendbarkeit der Schutzmaßnahmen

7.4.1 Einführung

Die in 7.3 dargelegten Schutzmaßnahmen können auf die in Abschnitt 5 definierte Menge von möglichen Bedrohungen bezogen werden. Jede Schutzmaßnahme kann gegen eine oder mehrere Bedrohungen für die Übertragung Schutz bieten. In dem Sicherheitsnachweis muss gezeigt werden, dass mindestens eine entsprechende Schutzmaßnahme oder eine Kombination von Schutzmaßnahmen gegenüber jeder definierten möglichen Bedrohung vorhanden ist.

7.4.2 Bedrohungs-/Schutzmaßnahmenmatrix

Die X in Tabelle 1 zeigen, dass die Schutzmaßnahme einen Schutz gegen die entsprechende Bedrohung sicherstellen kann. Die Schutzmaßnahmen in Tabelle 1 können in Übereinstimmung mit 7.2.7 erweitert werden.

Tabelle 1 – Bedrohungs-/Schutzmaßnahmenmatrix

Bedrohung	Schutzmaßnahme							
	Sequenz-Nummer	Zeit-Stempel	Zeit-Überwachung	Quellen- und Ziel-Bezeichner	Rück-Nachricht	Identifikations-Prozedur	Sicherheits-Code	Kryptographische Techniken
Wiederholung	X	X						
Auslassung	X							
Einfügung	X			X [a]	X [b]	X [b]		
Resequenzierung	X	X						
Verfälschung							X [c]	X
Verzögerung		X	X					
Manipulation					X [b]	X [b]		X [c]

[a] Nur anwendbar auf Quellenbezeichner.
Wird nur Einfügung von ungültigen Quellen entdecken.
Falls wegen unbekannten Nutzern keine eindeutigen Bezeichner festgelegt werden können, muss eine kryptographische Technik angewendet werden, siehe 7.3.8.

[b] Anwendungsabhängig.

[c] Siehe 7.4.3 und Abschnitt C.2.

7.4.3 Wahl und Gebrauch von Sicherheitscodes und kryptographischen Techniken

Die Wahl des Sicherheitscodes und der kryptographischen Techniken muss von folgenden Gesichtspunkten bestimmt sein:

– ob nicht autorisierter Zugriff ausgeschlossen werden kann oder nicht;

– der Typ des vorgeschlagenen kryptographischen Codes;

– ob der sicherheitsrelevante Zugriffsschutzprozess vom sicherheitsrelevanten Prozess separiert ist oder nicht.

Abschnitt C.2 liefert Hinweise zu diesen Punkten.

Anhang A
(informativ)

Bedrohungen auf offene Übertragungssysteme

A.1 Systemsicht

Die Bedrohungen der über die Verbindung gesendeten Nachrichten durch das Steuerungs- und Schutzsystem entstehen als Resultat von möglichen Änderungen in den Leistungsmerkmalen der Verbindung, die entweder unter normalen Bedingungen entstehen können (d. h. ohne Fehlfunktionen) oder unter anormalen Bedingungen (d. h. durch vorangegangene Fehlfunktionen des Übertragungssystems).

Das angesetzte Verfahren für die Ableitung der Menge an Bedrohungen ist durch die Aufspaltung der Gefährdungsanalyse, die in der Form eines Baumes (siehe Bild A.1) erstellt wurde, auf drei unterschiedliche Ebenen durchgeführt worden:

– die Benutzerebene;

– die Netzwerkebene;

– die externe Umgebung.

Diese Ebenen folgen einer „Top down“ – Vorgehensweise, beginnend von der Hauptgefährdung *(main hazard)* (M.H.), die als „das Versagen, eine korrekte Nachricht am Empfängerende, im Sinne von Authentizität, Integrität, Sequenz und zeitlicher Richtigkeit zu erhalten“ definiert ist.

Durch die Analyse des möglichen Verhaltens der Nachrichten, die auf der Empfängerseite beobachtet werden, sind die potentiellen Grundgefährdungen *(basic hazards)* herausgestellt, und es wird eine Menge von grundsätzlichen Nachrichtenfehlern *(basic message errors)* (B.M.E.) beschrieben, die als Klassifikation aller möglichen Nachrichtenverfälschungsarten beabsichtigt ist.

Die Ableitung der korrespondierenden Bedrohungen, die als Formen von Netzwerkfehlfunktionen (d. h. die vom Standpunkt des Netzwerks gesehenen grundsätzlichen Nachrichtenfehler) zu verstehen sind, ist dann eindeutig. Die Bedrohung ist die Einheit, die eine für die Sicherheit gefährliche Situation erzeugt (d. h. sie kann zu einem Unfall führen), und sie ist deswegen eine Ursache (auf der Netzwerkebene) für einen möglichen grundsätzlichen Nachrichtenfehler. Deswegen ist die Beziehung Bedrohung – grundsätzlicher Nachrichtenfehler konsequenterweise 1:1.

Umgekehrt kann eine Bedrohung durch eine Anzahl von Ursachen erzeugt werden, die gefährliche Ereignisse *(hazardous events* (H.E.)) genannt werden. Diese können sowohl auf der Netzwerkebene als auch in der externen Umgebung gegenwärtig sein. Dasselbe gefährliche Ereignis kann offensichtlich auf verschiedene Bedrohungen bezogen sein.

Die Aufspaltung der Analyse auf unterschiedliche Ebenen ermöglicht auch (mindestens) drei Ebenen von Schutzmaßnahmen:

a) eine auf der System/Nutzer-Anwendungsebene, die die Implementierung des Systems behandelt – unabhängig vom Übertragungsfeld. Ein Beispiel ist Auslassung, die ungefährlich sein kann, wenn das System in einer Weise entworfen wurde, dass ausgelassene Nachrichten keine Gefährdung darstellen;

b) eine, die logische Struktur der Nachricht betreffende; zum Beispiel alle möglichen Codes, die auf die Nachricht angewendet werden können, oder spezifische Gegenmaßnahmen wie Sequenznummer, Zeitstempel usw.;

c) eine auf physikalischer Ebene; ein Beispiel ist Abschirmung, um Verfälschung aufgrund von elektromagnetischen Einflüssen zu vermeiden.

Dieser Anhang wird diesen Punkt nicht weiter behandeln, da er nur erwähnt wurde mit der Absicht, ein Gesamtbild der verwendeten Methodik zu liefern.

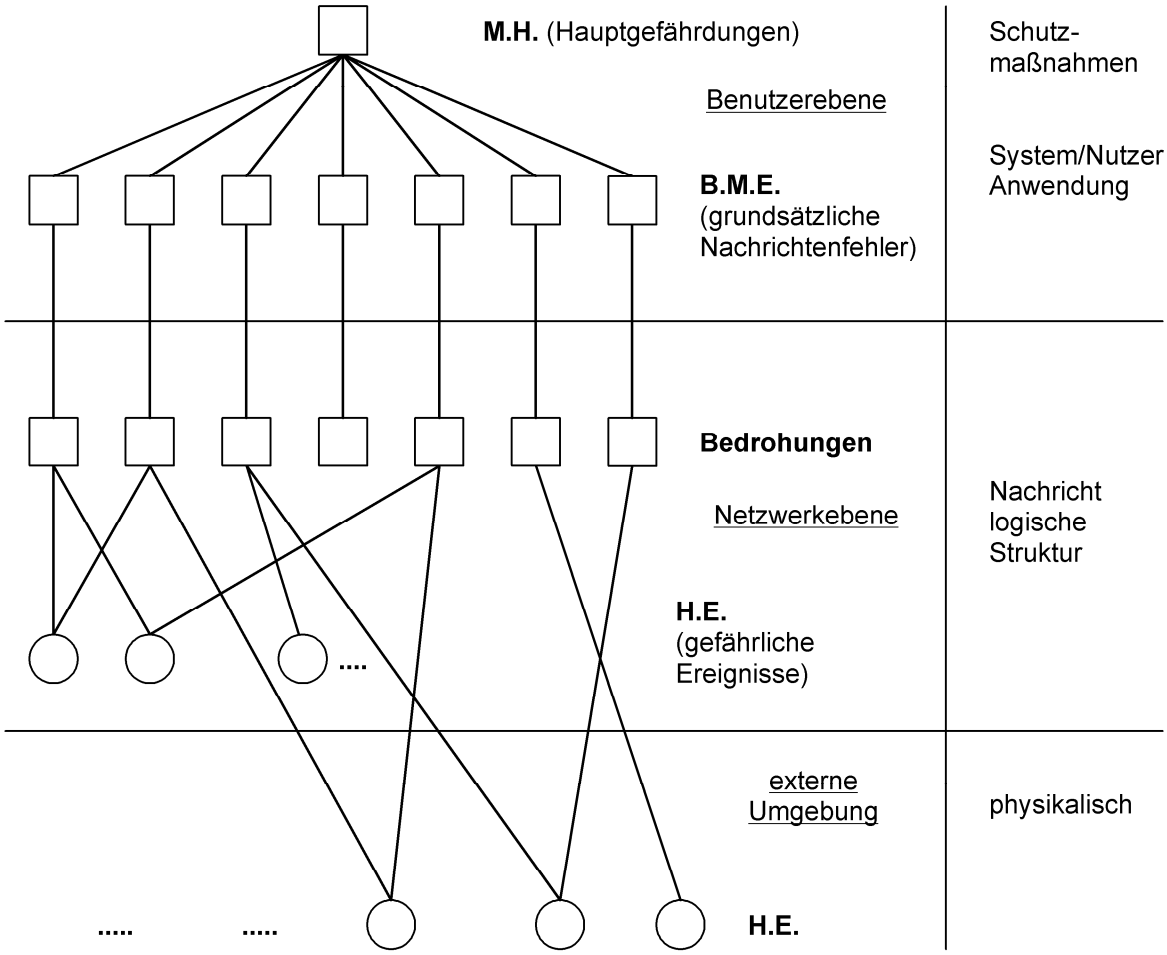


Bild A.1 – Gefährdungsbaum

A.2 Ableitung der grundsätzlichen Nachrichtenfehler

Die Nachricht ist der Hauptgegenstand der gesamten Analyse. Deswegen ist der Kommunikationsprozess aus der Sicht des Empfängers untersucht worden. Eine Nachricht kann definiert werden als *„durch eine Quelle erzeugte Nutzinformation, die innerhalb einer Zeit Δt – vom Beginn der Übertragung an gerechnet – ausgeliefert werden soll“.*

Die Integrität des Nachrichtenstroms ist die hauptsächliche Betrachtung beim identifizieren der Gefährdungen, die beim Übertragen einer sicherheitsrelevanten Kommunikation über ein offenes Übertragungssystem auftreten können.

Ein „Nachrichtenstrom“ ist als eine geordnete Menge von Nachrichten definiert, und er ist für jedes Zeitfenster und jeden Empfänger einmalig, falls keine Fehlfunktionen, Angriffe oder falsche Betriebsweisen auftreten.

Der tatsächlich empfangene Nachrichtenstrom kann aus einer Anzahl von Gründen sich von dem erwarteten unterscheiden. Drei besondere Unterklassen sind spezifiziert (Grundgefährdungen):

– mehr Nachrichten empfangen als erwartet;
– weniger Nachrichten empfangen als erwartet;
– dieselbe Anzahl von Nachrichten empfangen wie erwartet.

Mehr Nachrichten empfangen als erwartet

In diesem Fall sind eine oder mehrere Nachrichten wiederholt worden, oder es wurde eine externe Nachricht auf der Strecke eingefügt. Der grundsächliche Nachrichtenfehler ist daher *wiederholte, eingefügte Nachricht*.

Weniger Nachrichten empfangen als erwartet

In diesem Fall sind eine oder mehrere Nachrichten ausgelassen worden. Der grundsächliche Nachrichtenfehler heißt daher *ausgelassene Nachricht*.

Dieselbe Anzahl von erwarteten und empfangenen Nachrichten

In diesem Fall können verschiedene Möglichkeiten auftreten:

– alle Nachrichten im Strom sind im Inhalt und in der Übertragungszeit korrekt, jedoch ist die Sequenz verkehrt: Resequenzierung ist aufgetreten;

– eine Nachricht brauchte mehr Zeit als die Nennzeit Δt, um den Empfänger zu erreichen: Verzögerung ist aufgetreten;

– die Nachricht wurde verändert: Verfälschung ist aufgetreten;

– der Empfänger glaubt, dass der Absender der Nachricht ein anderer als der wirkliche ist: Manipulation ist aufgetreten.

In den letzten beiden Unterfällen wurde die Integrität einer einzelnen Nachricht betrachtet. Die grundsächlichen Nachrichtenfehler sind *resequenzierte, verzögerte, verfälschte, manipulierte Nachricht*.

Die folgende Menge von grundsächlichen Nachrichtenfehlern wurde daher identifiziert:

– wiederholte Nachricht;

– ausgelassene Nachricht;

– eingefügte Nachricht;

– resequenzierte Nachricht;

– verfälschte Nachricht;

– verzögerte Nachricht;

– manipulierte Nachricht.

Die oben definierten grundsächlichen Nachrichtenfehler schließen sich gegenseitig nicht aus. Es ist möglich, dass mehrere Nachrichten in einem Strom oder auch eine einzelne Nachricht mit mehr als einer Fehlerart beeinträchtigt wurden.

A.3 Bedrohungen

Nachdem die Definition der grundsächlichen Nachrichtenfehler in Abschnitt A.2 spezifiziert wurde, ist die Ableitung der zugehörigen Bedrohungen einfach.

Angenommen wird, dass A, B und C drei autorisierte Parteien sind, die sicherheitsrelevante Nachrichten kommunizieren, während X der Angreifer ist.

Es muss beachtet werden, dass Zufalls- und systematische HW/SW-Fehler ebenso in der Liste der Bedrohungen zu berücksichtigen sind. Die folgenden Erklärungen sind nur Beispiele und deswegen nicht umfassend.

A.3.1 Wiederholung

– X kopiert eine Nachricht [„Höchstgeschwindigkeit: 250 km/h“] und spielt sie in einer ungeeigneten Situation ein [während der Zug in einer Langsamfahrstelle ist],

oder

– infolge einer Hardwarefehlfunktion wiederholt das nicht sichere Übertragungssystem eine alte Nachricht.

A.3.2 Auslassung

– X löscht die Nachricht heraus [X löscht die Nachricht „Nothalt“ oder „Höchstgeschwindigkeit: 250 km/h“],

oder

– eine Nachricht wurde aufgrund einer Hardwarefehlfunktion gelöscht.

A.3.3 Einfügung

– X fügt eine Nachricht ein [„Höchstgeschwindigkeit: 250 km/h“],

oder

– ein autorisierter dritter Teilnehmer C fügt unabsichtlich eine Nachricht in den Informationsfluss von A nach B ein (oder dasselbe passiert wegen eines Netzwerkfehlers).

A.3.4 Resequenzierung

– X ändert absichtlich die Folge von Nachrichten für B (z. B. durch Verzögerung einer Nachricht oder indem er eine Nachricht zwingt, einen anderen Weg durch das Netzwerk zu nehmen),

oder

– wegen einer Hardwarefehlfunktion wurde die Nachrichtenreihenfolge geändert.

A.3.5 Verfälschung

– die Nachricht ist zufälligerweise in eine andere, formal korrekte Nachricht verändert worden (z. B. durch EMI),

oder

– X verändert die Nachricht [„Höchstgeschwindigkeit: 30 km/h“ in „Höchstgeschwindigkeit: 250 km/h“] in einer plausiblen Weise, so dass A und/oder B diese Modifikation nicht entdecken können.

A.3.6 Verzögerung

– das Übertragungssystem ist durch den üblichen Nachrichtenverkehr überlastet (z. B. aufgrund eines falschen Entwurfes oder einer zufällig hohen Verkehrslast),

oder

– X erzeugt eine Überlast in dem Übertragungssystem durch Erzeugung von Scheinnachrichten, so dass der Dienst verzögert oder gestoppt wird.

A.3.7 Manipulation

– A und B möchten sensible Daten austauschen;

und

– X gibt gegenüber A vor, B zu sein, oder B gegenüber A zu sein (oder beides), um Zugriff auf die sensiblen Daten zu erlangen, oder um als legaler Nutzer des Systems betrachtet zu werden.

A.4 Ein mögliches Verfahren zum Aufstellen des Sicherheitsnachweises

Das Verfahren, das hier vorgestellt wird, ist ein Beispiel, und es ist nicht das einzige, das verfolgt werden kann. Eine komplette Gefährdungsanalyse erfordert tiefe Kenntnis der ihr zugehörigen Anwendung, um eine geeignete Risikobewertung durchzuführen.

A.4.1 Strukturierte Verfahren für eine Identifikation der Gefährdungsereignisse

Im folgenden beginnt die Analyse bei der Betrachtung, dass der untersuchte Fall damit zu tun hat, dass eine externe Umgebung auf ein Netzwerk einwirkt. Diese beiden Einheiten sind in Untereinheiten gegliedert (in Bild A.2 unterstrichen), die als die Ursachen von möglichen Gefährdungsereignissen auf das analysierte System betrachtet werden können. Die Einheit „Netzwerk“ ist entsprechend den verschiedenen Schritten seines Lebenszyklus unterteilt, während die Aufteilung der Einheit „Externe Umgebung“ ihre zwei möglichen Merkmale - die physikalischen und die menschlichen - berücksichtigt.

Die Blätter des Baumes in Bild A.2 stellen die Ursachen für Gefährdungen dar. Für jede Ursache werden die zugehörigen Gefährdungsereignisse ausgewiesen. Diese Vorgehensweise macht es auch leichter, die einmal definierte Wahrscheinlichkeit für eine einzelne Ursache der Wahrscheinlichkeit für jedes erzeugte gefährliche Ereignis zuzuordnen.

Im folgenden wird jede Ursache in eine Anzahl von gefährlichen Ereignissen aufgespaltet, wobei diese Aufspaltung nicht erschöpfend ist. Während der Gefährdungsanalyse könnten einige andere gefährliche Ereignisse, - abhängig von der speziellen Anwendung - in Betracht gezogen werden.

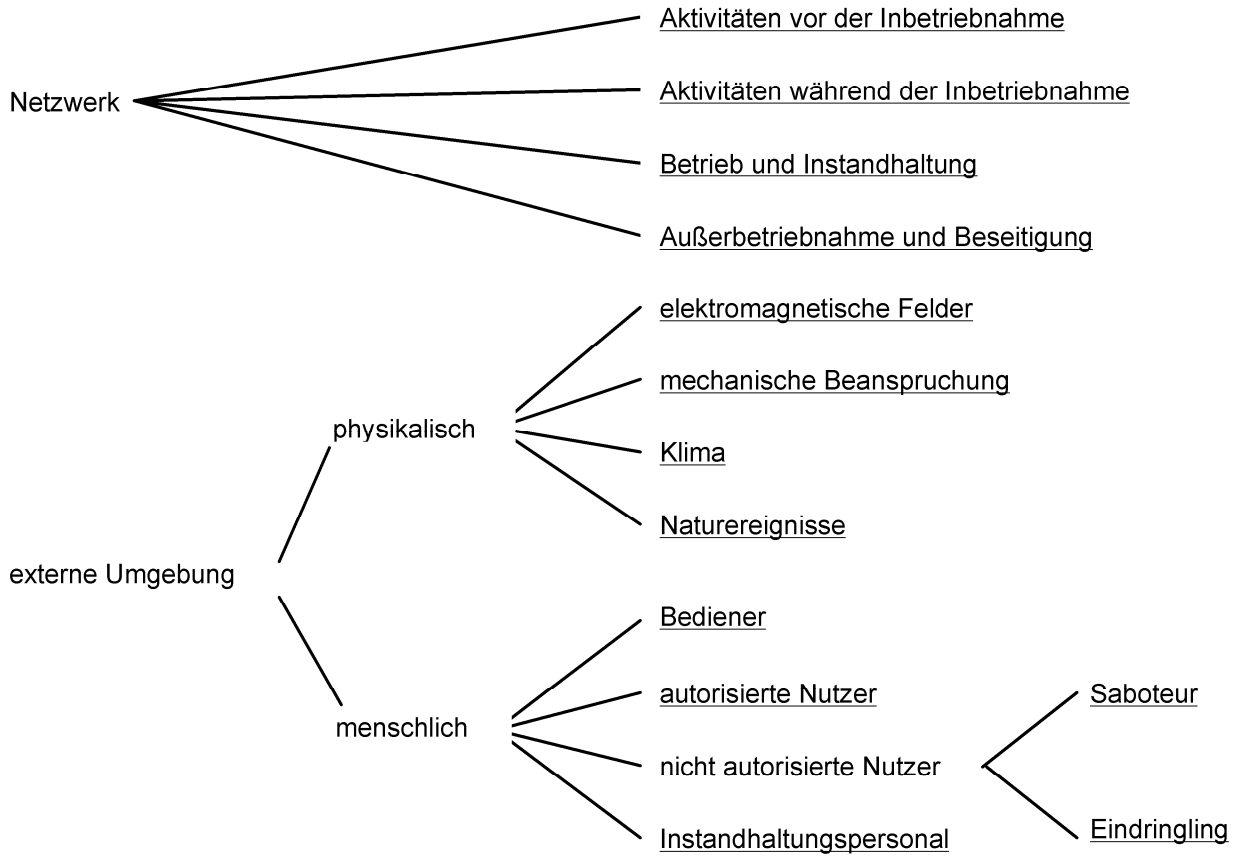


Bild A.2 – Ursachen von Bedrohungen

A.4.1.1 Netzwerk

Die Phasen des Lebenszyklus eines Netzwerks können entsprechend EN 50126 definiert werden. Sie können für den Anwendungsbereich dieses Anhangs (d. h. Feststellung von gefährlichen Ereignissen, die als ”Fehler” in jeder Phase entstehen können) in folgender Weise gruppiert werden:

– Konzept, Systemdefinition und Anwendungsbedingung, Risikoanalyse, Systemanforderungen, Zuteilung der Systemanforderungen, Entwurf und Implementierung, Herstellung: Alle diese Phasen sind auf Aktivitäten vor der Inbetriebnahme bezogen;

– Installation, Systemvalidation und Systemakzeptanz: Diese sind auf die Inbetriebnahme des Systems bezogen;

– Betrieb und Instandhaltung;

– Außerbetriebnahme und Beseitigung.

A.4.1.1.1 Aktivitäten vor Inbetriebnahme

Fehler während dieser Phase können zu folgendem führen:

– systematische HW-Fehler;

– systematische SW-Fehler.

A.4.1.1.2 Aktivitäten während der Inbetriebnahme

Fehler während dieser Phase können zu folgendem führen:

– Übersprechen;
– Drahtbruch;
– Falschausrichtung von Antennen;
– Kabelfehler.

A.4.1.1.3 Betrieb und Instandhaltung

Während dieser Lebensphase können gefährliche Ereignisse sowohl durch den Leistungsverlust der Systemkomponenten auftreten, als auch durch Fehler während einer Reparatur und/oder Änderung:

– Verlust der Leistung;
– zufällige HW-Ausfälle;
– Alterung der HW.

A.4.1.1.4 Instandhaltung

– Benutzung unkalibrierter Instrumente;
– Benutzung ungeeigneter Instrumente;
– fehlerhafter HW-Ersatz;
– fehlerhafte SW-Erneuerung oder –Austausch.

A.4.1.1.5 Modifikation

– Schwundeffekte;
– menschliche Fehler [1)].

A.4.1.1.6 Außerbetriebnahme und Beseitigung

Es wird nicht erwartet, dass während dieser Phase des Lebenszyklus eines Netzwerkes gefährliche Ereignisse in Bezug auf Kommunikationsfehler entstehen können.

A.4.1.2 Externe Umgebung

A.4.1.2.1 Elektromagnetische Felder

– EMI;
– Übersprechen (mit externen Kabeln oder Funkverbindungen).

A.4.1.2.2 Mechanische Beanspruchung

– Zufällige HW-Ausfälle;
– Alterung der HW.

A.4.1.2.3 Klima

– Thermisches Rauschen;
– Alterung der HW;
– zufällige HW-Ausfälle;
– Schwundeffekte.

---

1) Sie hängen von der Art der speziellen Anwendung ab und können deswegen auf dieser Ebene der Analyse nicht spezifiziert werden.

A.4.1.2.4 Naturereignisse

– Magnetischer Sturm;
– Feuer;
– Erdbeben;
– Blitz.

A.4.1.2.5 Bediener

– Menschliche Fehler [1)].

A.4.1.2.6 Autorisierte Benutzer

– Menschliche Fehler [1)];
– Überlastung des Übertragungssystems.

A.4.1.2.7 Instandhaltungspersonal

– Benutzung unkalibrierter Instrumente;
– Benutzung ungeeigneter Instrumente;
– fehlerhafter HW-Ersatz;
– menschliche Fehler [1)];
– fehlerhafte SW-Erneuerung, oder Austausch.

A.4.1.2.8 Saboteuer [2)]

– Anzapfen der Leitung;
– HW-Zerstörung oder Unterbrechung;
– nicht autorisierte SW-Modifikationen.

A.4.1.2.9 Eindringling [2)]

– Abhören der Leitung;
– Übertragung nicht autorisierter Nachrichten.

A.4.2 Beziehung zwischen gefährlichen Ereignissen und Bedrohungen

Unter Verweis auf Abschnitt A.1 kann jede Bedrohung als eine Reihe von gefährlichen Ereignissen gesehen werden, die sie erzeugt. Ausgehend von den im letzten Unterabschnitt identifizierten gefährlichen Ereignissen besteht der nächste Schritt in der Aufstellung der Beziehung zwischen ihnen und den in Abschnitt A.3 beschriebenen Bedrohungen durch Verwendung eines „Bottom Up“ – Verfahren [3)]. Das Ziel ist nachzuweisen, dass keine zusätzliche Bedrohung gefunden wird, um die Gültigkeit des durchgeführten Verfahrens zu beweisen. Die Beziehung Bedrohung - gefährliche Ereignisse kann durch die Tabelle A.1 dargestellt werden.

Wie man sehen kann, ist keine zusätzliche Bedrohung entdeckt worden, nachdem jedes gefährliche Ereignis analysiert wurde. Dieses beweist die Tatsache, dass die Liste aus Abschnitt A.3 umfassend ist.

(Es muss klar sein, dass die obige Tabelle für jedes gefährliche Ereignis nur die primären Effekte betrachtet, d. h. es können andere Beziehungen festgestellt werden).

---

2) Der Unterschied zwischen einem Saboteur und einem Eindringling ist der, dass der erste keine Rücksicht darauf nimmt, was auf der Leitung passiert. Sein Ziel ist allein, das Netzwerk zu verändern. Der zweite ändert nicht das Netzwerk, sondern er benutzt es, um Vorteile daraus zu ziehen.

3) Allgemein gesprochen muss eine solches „Bottom Up“-Verfahren während der Sicherheitsnachweisanalyse angewendet werden, um die Bedrohungen zu beurteilen, die durch die gefährliche Ereignisse (H.E.) in Bezug auf die spezielle Anwendung verursacht werden.

A.5 Schlussfolgerung

Es sind zwei unterschiedliche Verfahren für die Ableitung der Menge von möglichen Bedrohungen auf eine sicherheitsrelevante Übertragung in einem offenem Kommunikationssystem ausgewiesen worden. Das erste ist ein „Top Down"-Verfahren, die von der Hauptgefährdung ausgeht und mit der Klassifizierung aller möglichen gefährlichen Ereignisse, die zu einer Gefährdung führen, endet. Das zweite beginnt bei der Definition von zwei Haupteinheiten des betrachteten Systems (d. h. Netzwerk und externe Umgebung), um alle möglichen Ursachen von gefährlichen Ereignissen bezogen auf das System zu klassifizieren. Diese Ereignisse beziehen sich auf die Bedrohung(en), die sie erzeugt haben.

Die zwei Analysen konvergieren zu derselben Menge an Bedrohungen und beweisen deswegen die Gültigkeit dieser Arbeit.

Tabelle A.1 – Beziehung zwischen gefährlichen Ereignissen und Bedrohungen

Gefährliche Ereignisse	Bedrohungen						
	Wiederholung	Auslassung	Einfügung	Resequenzierung	Verfälschung	Verzögerung	Manipulation
Systematische HW Fehler	X	X	X	X	X	X	
Systematische SW Fehler	X	X	X	X	X	X	
Übersprechen		X	X		X		
Drahtbruch		X			X	X	
Antennenfehlausrichtung		X			X		
Kabelfehler		X	X		X	X	
Zufällige HW Fehler	X	X	X	X	X	X	
HW-Alterung	X	X	X	X	X	X	
Benutzung unkalibrierter Instrumente	X	X	X	X	X	X	
Benutzung ungeeigneter Instrumente	X	X	X	X	X	X	
Fehlerhafter HW-Ersatz	X	X	X	X	X	X	
Schwundeffekte		X		X	X	X	
EMI		X			X		
Menschliche Fehler	X	X	X	X	X	X	
Thermisches Rauschen		X			X		
Magnetischer Sturm		X			X	X	
Feuer		X			X	X	
Erdbeben		X			X	X	
Blitz		X			X	X	
Überlastung des Übertragungssystems		X				X	
Anzapfen	X	X	X	X	X	X	
HW Zerstörung		X			X	X	
Nicht autorisierte SW Modifikationen	X	X	X	X	X	X	X [a]
Übertragung nicht autorisierter. Nachrichten	X		X				X [a]
Abhören [b]							

[a] In diesem Fall ist die Nachricht von vornherein betrügerisch; es wird eine starke Abwehrmaßnahme benötigt, z. B. die Verwendung eines Schlüssels.

[b] Nicht autorisiertes Abhören von sicherheitsrelevanten Nachrichten wird nicht direkt als gefährliches Ereignis berücksichtigt; die Gefährdung der Systemsicherheit entsteht durch „Übertragung von nicht autorisieren Nachrichten", resultierend von nicht autorisiertem Abhören. Vertraulichkeit von Anwenderdaten ist eine separate Systemanforderung außerhalb des Anwendungsbereichs dieser Norm.

Anhang B
(informativ)

Kategorien von Übertragungssystemen

B.1 Kategorien von Übertragungssystemen

6.3 dieser Norm identifiziert drei Kategorien von Übertragungssystemen:

– Kategorie 1 – Geschlossene Übertragungssysteme, wo alle wesentlichen Eigenschaften des Systems unter Kontrolle des sicherheitsrelevanten Systemdesigners sind und ein vereinfachter Satz von Sicherheitsanforderungen definiert werden kann;

– Kategorie 2 – Offene Übertragungssysteme, wo das Risiko von böswilligen Angriffen als vernachlässigbar betrachtet werden kann, obwohl die Übertragung nicht voll unter Kontrolle des sicherheitsrelevanten Systemdesigners ist;

– Kategorie 3 – Offene Übertragungssysteme, wo es die Möglichkeit für böswillige Angriffe gibt und kryptographische Schutzmaßnahmen erforderlich sind.

Die folgende Tabelle B.1 gibt einige weitere Hinweise, wie derzeitige Übertragungssysteme, auf die man in sicherheitsrelevanten Anwendungen stoßen kann, sich auf die drei Kategorien beziehen, auf Basis der Eigenschaften der von ihnen benutzten Technologie und Schlüsselmerkmale ihrer Konfiguration.

Es ist nicht möglich, zu rein hypothetischen Beispielen präzise zu sein, aber die in der Tabelle aufgelisteten Haupteigenschaften können Anwender dieser Norm anleiten, um festzulegen, ob ein bestimmtes System zum Zwecke der Analyse als Kategorie 1, 2 oder 3 betrachtet werden kann.

Tabelle B.1 – Kategorien von Übertragungssystemen

Kategorie	Haupteigenschaften	Beispielhafte Übertragungssysteme
Kategorie 1	Entworfen für eine bekannte maximale Anzahl von Teilnehmern. Alle Eigenschaften des Übertragungssystems sind bekannt und invariable während der Lebensdauer des Systems. Vernachlässigbare Chance für nicht autorisiertem Zugriff.	Übertragung über einen geschlossenen Luftspalt (z. B. Balise zu Zugantenne). Geschützter serieller Bus innerhalb des sicherheitsrelevanten Systems (z. B. PROFIBUS, CAN, MVB (multi purpose vehicle bus defined by IEC)). Industrie Standard LAN, das verschiedene Einrichtungen verbindet (sicherheitsrelevant und nicht sicherheitsrelevant) innerhalb eines einzelnen Systems, das die Vorbedingungen erfüllen und beibehalten muss.

Tabelle B.1 – Kategorien von Übertragungssystemen *(fortgesetzt)*

Kategorie	Haupteigenschaften	Beispielhafte Übertragungssysteme
Kategorie 2	Eigenschaften sind unbekannt, teilweise unbekannt, oder variable während der Lebensdauer des Systems. Begrenzte Erweiterungsmöglichkeit für Nutzergruppen. Bekannte Nutzergruppe, oder -gruppen Vernachlässigbare Chance für nicht autorisiertem Zugriff (Netzwerken wird vertraut) Gelegentliche Nutzung von nicht sicherheitsrelevanten Netzwerken.	Geschützter serieller Bus innerhalb des sicherheitsrelevanten Systems (z. B. PROFIBUS, MVB), aber mit der Möglichkeit, dass das Übertragungssystem während der Lebensdauer re-konfiguriert, oder durch ein anderes Übertragungssystem ersetzt werden kann. Industrie Standard LAN, das verschiedene Systeme verbindet (sicherheitsrelevant und nicht sicherheitsrelevant) innerhalb eines kontrollieren und begrenzten Bereichs. WAN, das die Eisenbahnen betreiben und das unterschiedliche Systeme (sicherheitsrelevant und nicht sicherheitsrelevant) in verschiedenen Stellen verbindet. Geschaltete Verbindungen in öffentlichen Netzwerken, gelegentlich genutzt zu unvorhersagbaren Zeiten (Verbindungsaufbau zur Ferndiagnose eines Stellwerksystems). Geleaste permanente Punkt zu Punkt Verbindungen in öffentlichen Telefon Netzwerken. Funkübertragungssystem mit begrenztem Zugang (z. B. Nutzung von Wellenleitern, oder Schlitzkabeln mit einer Verbindungsbeschränkung, die nur einem in sich geschlossenen Sendeempfänger den Empfang ermöglicht; oder Nutzung eines proprietären Modulationsschemas, das es unmöglich macht, dieses mit einem handelsüblichen, oder erschwinglichen Laborgerät zu reproduzieren).
Kategorie 3	Eigenschaften sind unbekannt, teilweise unbekannt, oder variable während der Lebensdauer des Systems. Unbekannte vielfache Nutzergruppen. Maßgebliche Chance für nicht autorisierten Zugriff.	Paket-orientierter Datendienst in öffentlichen Netzwerken. Internet. Verbindungs-orientierter Funk Datendienst (z. B. GSM-R). Paket-orientierter Funk Datendienst (z. B. GPRS). Nahbereichsfunk (e.g. Wi-fi). Funkübertragungssysteme ohne Einschränkungen.

B.2 Beziehung zwischen der Kategorie des Übertragungssystems und Bedrohungen

Die folgende Tabelle B.2 stellt eine grobe Zuordnung der Bedrohungen zu jeder der oben definierten Kategorien von Übertragungssystem dar.

Tabelle B.2 – Beziehung Bedrohung/Kategorie

Kategorie	Wiederholung	Auslassung	Einfügung	Resequenzierung	Verfälschung	Verzögerung	Manipulation
Kat. 1	+	+	+	+	++	+	–
Kat. 2	++	++	++	+	++	++	–
Kat. 3	++	++	++	++	++	++	++

Legende

– Bedrohung kann vernachlässigt werden.

\+ Bedrohung existent, jedoch seltene, schwache Gegenmaßnahme ausreichend.

++ Bedrohung existent, starke Gegenmaßnahme erforderlich.

ANMERKUNG Diese Matrix ist nur eine Anleitung – es wird immer eine Analyse notwendig sein, um festzulegen, ob Gegenmaßnahmen und in welchem Maß erforderlich sind. Jede Bedrohung wird vom Netzwerktyp, von der Applikation und der Konfiguration abhängig sein.

Auf dieser allgemeinen Ebene ist es unmöglich, entsprechend der Kategorie des Übertragungssystems den für jede Bedrohung benötigten SIL der Schutzmaßnahmen zuzuordnen; es ist wesentlich, die entsprechende Anwendung zu analysieren, um die SIL zuzuordnen.

Anhang C
(informativ)

Leitfaden für Schutzmaßnahmen

C.1 Anwendung von Zeitstempeln

Ein Zeitstempel kann für unterschiedliche Zwecke genutzt werden.

a) Um den Zeitpunkt eines Ereignisses in einer Einheit zu anzugeben, der für den die Information empfangenden Prozess von Wichtigkeit ist. Ereignisse können zu einander zeitbezogen sein. Wenn die Zeiten und Werte für eine Folge von Ereignissen bekannt sind, ist es möglich, zwischen den Werten zu interpolieren und die Genauigkeit der berechneten Werte (z. B. für Geschwindigkeit, Beschleunigung) zu erhöhen. Übertragungsverzögerungen kann man in den Griff bekommen.

   Randbedingungen:

   – die Zeiten in den Einheiten müssen synchronisiert werden, wenn ein absoluter Zeitstempel genutzt wird. Jede Einheit benötigt einen sicheren Zeitprüfungsmechanismus und einen Abgleich auf die globale Zeit. Die Netzwerkverzögerungen haben einen Einfluss auf den globalen Zeitverteilmechanismus, die Gültigkeit der Informationen und die Prozessleistungsfähigkeit;

   – das Fehlen von Nachrichten wird nicht entdeckt, falls kein Kommunikationsdialog zur Verfügung steht.

b) Um Ereignisfolgen zu ordnen, die durch den Empfänger geprüft werden können.

   Randbedingungen:

   – wenn die Zeitgranularität zu grob ist, können die Sequenzeigenschaften von Ereignissen unbestimmt sein. In solchen Fällen können die Informationen mit Sequenznummern ergänzt werden;

   – die Reihenfolge von Nachrichten wird durch die für die Nachrichten benutzten Übertragungswege und die Zeitverzögerungen im Netzwerk beeinflusst;

   – das Fehlen von Nachrichten wird nicht entdeckt, falls kein Kommunikationsdialog zur Verfügung steht.

c) Um die Zeit zwischen zwei empfangenen Ereignissen zu messen, die von einer Einheit als Folge von Nachrichten gesendet werden. Dadurch wird auch geprüft, dass Ereignisse nicht verzögert sind.

   Falls eine Information von einer Einheit (A) wiederholt durch eine andere Einheit (B) angefordert wird, erhält die letztgenannte die Information über die lokale Uhrzeit des Partners aus den Zeitstempeln. Diese Information kann auf seine eigene Uhrzeit bezogen werden, wobei die Übertragungsverzögerung in Betracht gezogen wird. Eine logische Uhrzeit ist aus der logischen Uhrzeit von Einheit (B) erzeugt worden.

   Randbedingung:

   – die logische Uhr wird durch schwankende Zeitverzögerungen im Netzwerk und bei der Bearbeitung in Einheit (A) beeinflusst.

d) Um die Gültigkeit der Information von Einheit (A) zu prüfen, indem eine Rücksendung des Zeitstempels angefordert wird, der von Einheit (B) in der vorangegangenen Nachricht an Einheit (A) gesandt wurde. Dieses stellt eine spezifische Antwort (Identität) sicher und überprüft auch die vorgegebene Zeit für die Schleife. Eine in der Einheit (B) erstellte und zeitüberwachte Sequenznummer (oder Marke) erfüllt die gleiche Aufgabe. Es wird keine globale Zeit benötigt (außer wenn andere Anwendungen das fordern).

   Der Empfänger entdeckt den Verlust von Informationen durch Verwendung einer Zeitüberwachung.

   Randbedingungen:

   – die Prozedur sollte Unterbrechungen aufgrund von Initialisierung oder Fehlerbedingungen behandeln;

   – die Prozedur garantiert nicht die Authentifizierung der Nachrichten.

e) Um eine Prozedur, die doppelter Zeitstempel [A155] genannt wird, zu erzeugen. Diese Prozedur beinhaltet die Eigenschaften einer Kombination der Fälle b), c) und d). Die doppelte Zeitstempelprozedur erlaubt asynchrone Uhren in den Einheiten und vermeidet deshalb die Probleme, die mit dem Aufrechterhalten der globalen Zeit in den Einheiten verbunden sind. Das Verfahren kann genutzt werden für

   – die Erzeugung einer logischen Uhr aus der lokalen Uhr des Partners und für relative Zeitstempel von der eigenen lokalen Uhr (und der Organisation der Uhrensynchronisation zwischen den beiden Einheiten),
   – den Bezug der Ereignisse zu den relativen Zeitstempeln unter Einbeziehung der Netzwerkverzögerung,
   – die Überprüfung der korrekten Reihenfolge von Nachrichten,
   – die Überprüfung der Uhr des Partners, um die Richtigkeit der eigenen Uhr zu bestätigen (anwendungsabhängig).

   Die Kommunikation ist für einen Zweipartner-Dialog oder für eine Master/Slave - Beziehung gültig. Das letztgenannte lässt sich besser für Zwecke der zyklischen Übertragung anwenden als das Zeitstempeln einzelner Ereignisse, bei dem die Zeit für eine Einzelfunktion wichtig ist.

   Randbedingungen:

   – wenn die Zeitgranularität zu grob ist, können die Sequenzeigenschaften von Ereignissen unbestimmt sein. In solchen Fällen sollten die Informationen mit Sequenznummern ergänzt werden;
   – doppeltes Zeitstempeln könnte erfordern, dass die Gesamtverzögerungszeit der Übertragung (Hinweg und Rückweg) bekannt ist, wenn die Anwendung den obigen Fall a) betrachtet.

Es sind näher ausgearbeitete Verfahren als die doppelten Zeitstempel erdacht worden, die das Ordnen von Ereignissen erlauben, die in mehr als zwei Systemen auftreten [TBaum].

C.2 Auswahl und Gebrauch von Sicherheitscodes und kryptographischen Techniken

Obwohl das Übertragungssystem unbekannt oder variabel während seiner Lebenszeit sein könnte, kann man in den meisten Fällen entscheiden, ob böswillige Angriffe auf sicherheitsrelevante Nachrichten ausgeschlossen werden können oder nicht. Diese Unterscheidung ist sehr nützlich, da im Falle der Möglichkeit dieser böswilligen Angriffe kryptographische Mechanismen mit geheimen Schlüsseln gefordert sind. Es wird empfohlen, diese Unterscheidung in einem frühen Stadium zu treffen, um die Menge der sicherheitsrelevanten Funktionen zu begrenzen. Falls die Möglichkeit des nichtautorisierten Zugriffs besteht, kann eine separate Zugriffsschutzebene angewendet werden (Typ B0 oder B1), oder der Schutz wird durch die sicherheitsrelevante Übertragungsfunktion unter Verwendung kryptographischer Mechanismen sichergestellt (Typ A1) und in diesem Fall wird der Begriff „kryptographischer Sicherheitscode“ im folgenden Text verwendet.

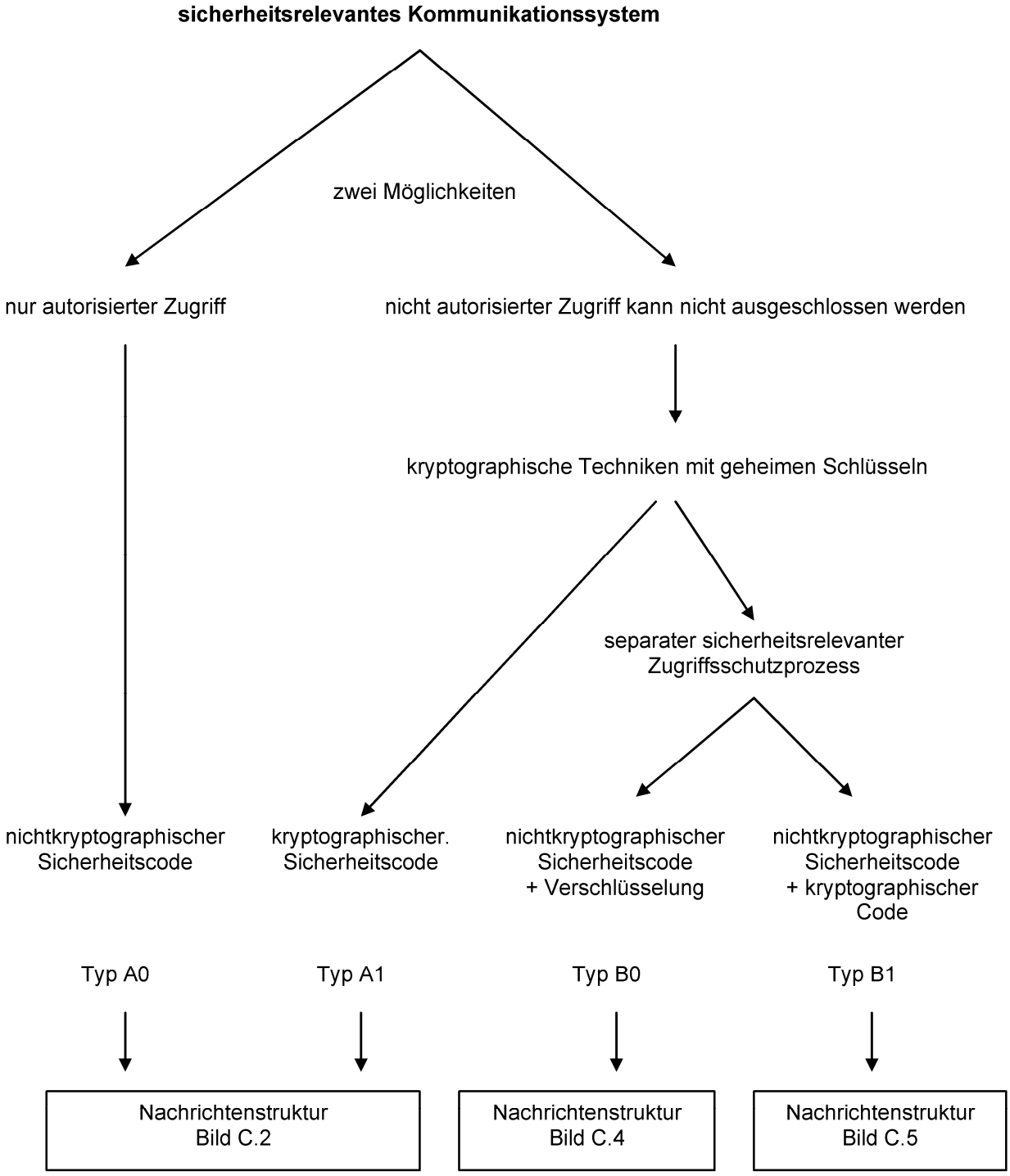


Bild C.1 – Klassifikation des sicherheitsrelevanten Kommunikationssystems

Die Prinzipien der Nachrichtenstrukturen für Nachrichtentypen A0 und A1 sind in Bild C.2 dargestellt.

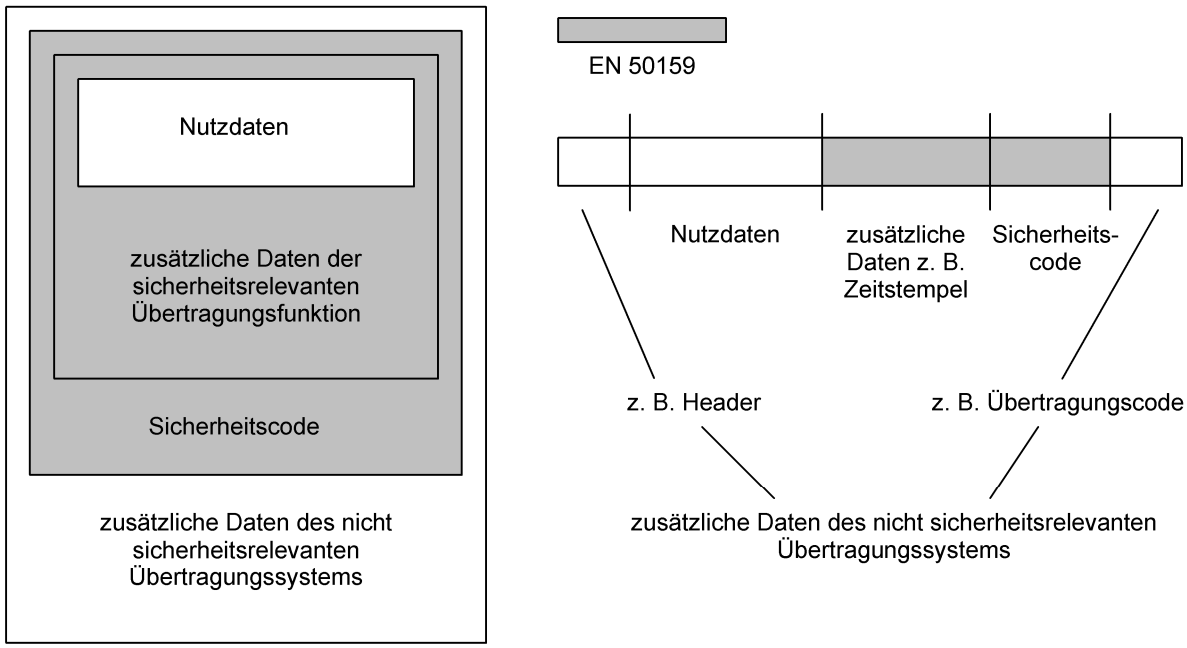


Bild C.2 – Modell der Nachrichtendarstellung innerhalb des Übertragungssystems (Typ A0, A1)

Separate Zugriffsschutzebenen sind in jenen Fällen nützlich, wo Gruppen von sicherheitsrelevanten Computern, die an ein lokales Netzwerk (LAN) angeschlossen sind, über offene Übertragungssysteme zu kommunizieren haben (siehe Bild C.3). Eine implizite Annahme hinter dem in Bild C.3 dargestellten Modell ist, dass LANs als Kategorie 2 klassifiziert werden können. Die kryptographische Hardware und Software kann an den Eintrittspunkten zum offenem Übertragungssystem konzentriert werden. Andere Schnittstellen zum offenen Übertragungssystem sollten ausgeschlossen werden. Die kryptographischen Funktionen können mit Gateway-Funktionen kombiniert werden, die gewöhnlich erforderlich sind, wenn z. B. ein LAN an ein Weitverkehrsnetzwerk (WAN) angeschlossen wird.

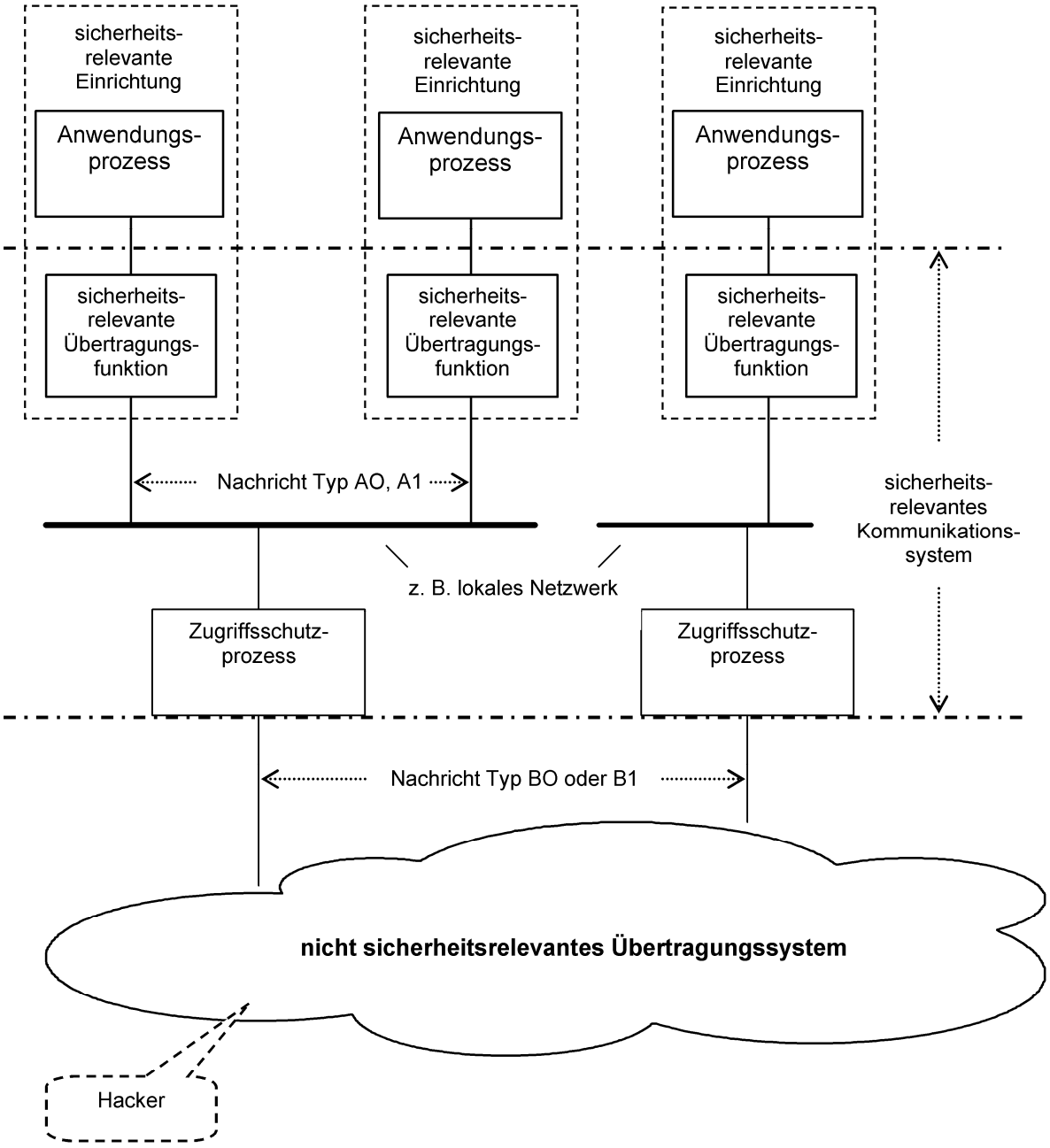


Bild C.3 – Verwendung einer unabhängigen Zugriffsschutzebene

Der Zugriffsschutzprozess kann auf unterschiedliche Arten durchgeführt werden:

a) Verschlüsselung der Nachrichten;

b) Hinzufügung eines kryptographischen Codes.

In beiden Fällen wird ein Sicherheitscode erzeugt, bevor eine sicherheitsrelevante Nachricht an die Zugriffsschutzebene gesendet wird. Die die Zugriffsschutzebene enthaltende Einrichtung muss nicht in sich selbst sicher sein, siehe die allgemeinen Anforderungen in 7.2. Es ist zu beachten, dass Fehlfunktionen des Zugriffsschutzprozesses betrachtet werden sollen.

Die prinzipiellen Nachrichtenstrukturen für Nachrichtentypen B0 und B1 sind in den Bildern C.4 und C.5 dargestellt.

Diese Beispiele zeigen die Anwendung des kryptographischen Schutzes direkt nach dem Sicherheitscode. In anderen Beispielen kann er auf niedrigeren Ebenen angewendet werden (Transport- oder Netzwerkebene).

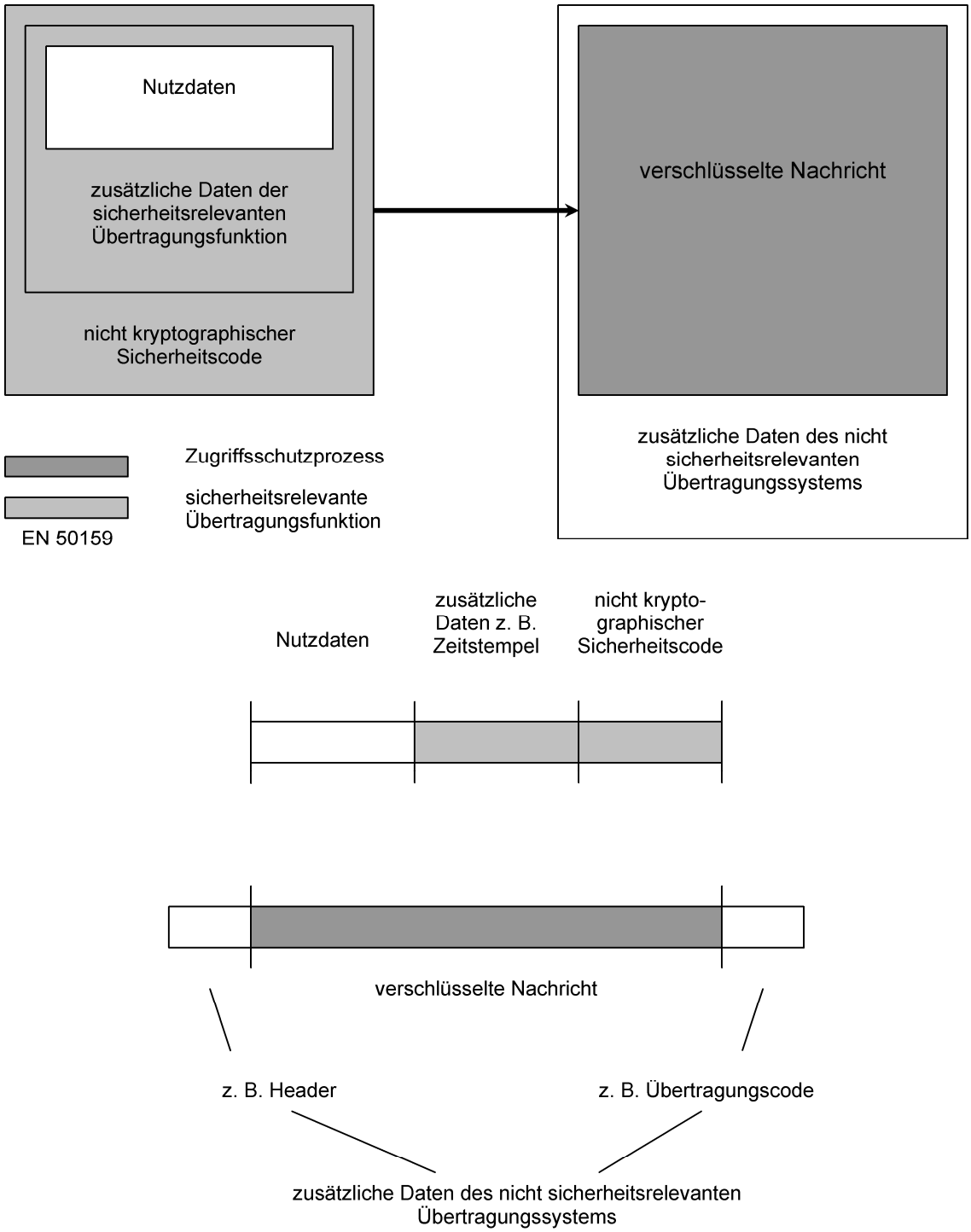


Bild C.4 – Modell der Nachrichtendarstellung innerhalb des Übertragungssystems (Typ B0)

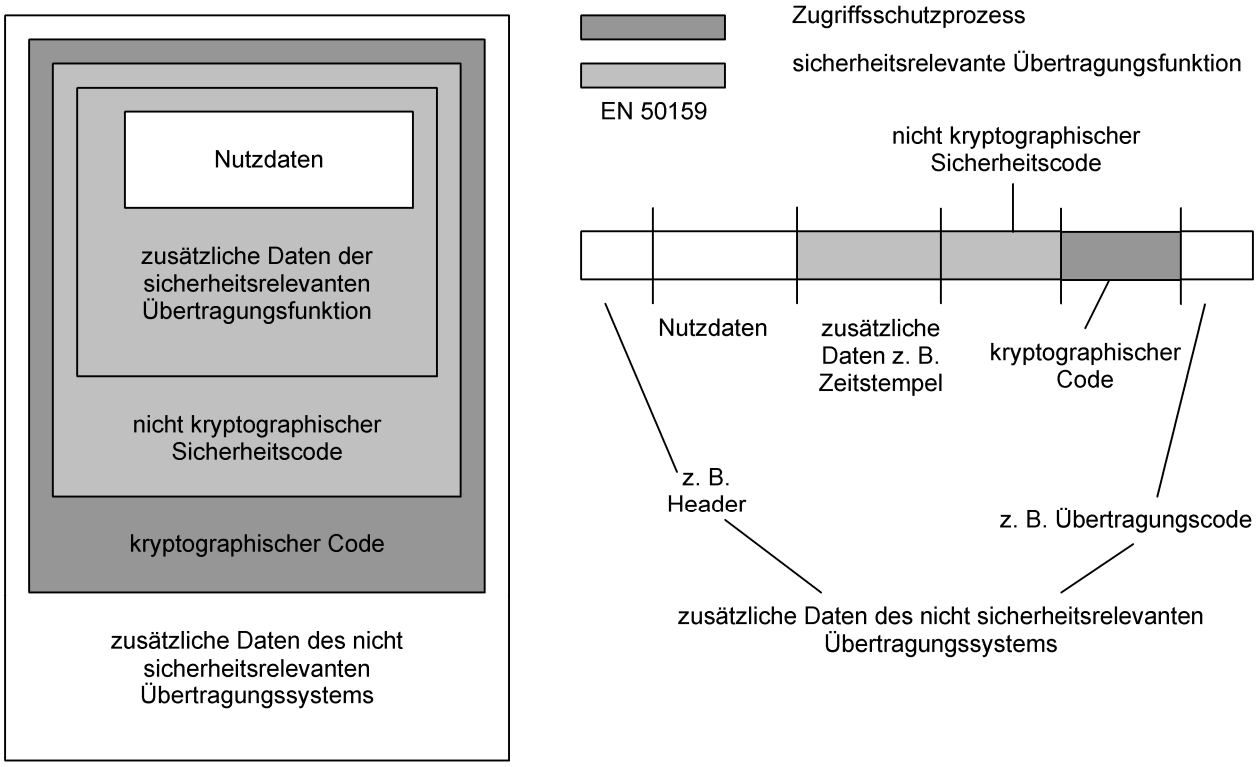


Bild C.5 – Modell der Nachrichtendarstellung innerhalb des Übertragungssystems (Typ B1)

C.3 Sicherheitscode

Die geforderten Eigenschaften des Sicherheitscodes hängen von den Charakteristiken des Übertragungssystems und der Architektur des sicherheitsrelevanten Kommunikationssystems ab (siehe Bild C.1).

Wenn nichtautorisierter Zugriff auf das Übertragungssystem ausgeschlossen werden kann, muss der Sicherheitscode alle Arten von zufälligen und systematischen Bitfehlern entdecken. Es ist zu beachten, dass das Übertragungssystem gewöhnlich seine Nachrichten mit seinem eigenen Übertragungscode schützt, der bereits so entworfen wurde, dass eine definierte Qualität und Bitfehlerrate erreicht wird. Deshalb war, falls das Übertragungssystem eine ungültige Nachricht liefert, entweder die Störung auf dem Übertragungskanal so groß, dass der Übertragungscode versagte, oder es ist ein Ausfall aufgetreten. In jedem dieser Fälle sollte berücksichtigt werden, dass restliche Bitfehler nicht zufällig sind und ein beliebiges Hamminggewicht haben können [Peterson].

Wenn nichtautorisierter Zugriff nicht ausgeschlossen werden kann, können zwar böswillige Angriffe nicht verhindert werden, sie können jedoch entdeckt und unschädlich gemacht werden. Der übliche Weg, um böswilligen Angriffen zu begegnen, ist die Anwendung kryptographischer Algorithmen mit mindestens einem geheimen Schlüssel. Der Sicherheitscode selbst kann auf solchen Algorithmen basieren, oder es kann eine unabhängige Zugriffsschutzebene mit kryptographischen Funktionen implementiert werden. Im letztgenannten Fall kann der Sicherheitscode auch Fehlfunktionen der Zugriffsschutzeinrichtung entdecken.

C.3.1 Wichtigste Blockcodes

Die folgenden Unterabschnitte beschreiben kurz einige Codes und deren Haupteigenschaften. Siehe [Peterson] für mehr Details.

C.3.1.1 Lineare Blockcodes

Ein Blockcode ist dann und nur dann linear, wenn die Summe beliebiger Codewörter wieder ein Codewort ergibt.

Die meisten für Fehlererkennungszwecke verwendeten Codes sind lineare binäre Codes. Ebenso werden auch nicht binäre Codes, wie z. B. Reed-Solomon-Codes, verwendet. Die Codes können ausgezeichnet zufällige Bitfehler und Büschelfehler bekämpfen. Die Codes können mit einer spezifischen Mindest-Hammingdistanz d entworfen werden. Das bedeutet, dass Fehler bis zu *d-1* falscher Symbole vollständig entdeckt werden. Aufgrund ihrer Linearität können die Codes auf ihre Fähigkeit zur Entdeckung von systematischen Übertragungsfehlern getestet werden.

Nützliche Modelle sind der binäre symmetrische Kanal (BSC) und der q-nary symmetrische Kanal (QSC). Die Codes können auch auf die Erkennung von systematischen Übertragungsfehlern getestet werden.

C.3.1.2 Zyklische Blockcodes

Ein linearer Blockcode ist zyklisch, wenn jedes zyklische Schieben eines Codewortes wieder ein Codewort ergibt. Ein zyklischer Code kann durch Polynome beschrieben werden. Die Mathematik der Codes kann z. B. in [Peterson] gefunden werden.

Die Codes können ausgezeichnet zufällige Bitfehler und Büschelfehler bekämpfen. Die Codes können mit einer spezifischen Mindest-Hammingdistanz *d* entworfen werden. Die Codes können auch auf ihre Fähigkeit zur Entdeckung von systematischen Fehlern geprüft werden. Ein zyklischer Code mit *c* redundanten Symbolen entdeckt alle Bündelfehler bis zu einer Länge von *c*.

In gewissen Anwendungen kann die zyklische Natur der Codes dazu ausgenutzt werden, um die Gefahr einer falschen Codewortsynchronisation zu vermeiden. Um dies zu erreichen, ist es notwendig, den Code zu erweitern, aber am Ende führt dies zu einem besseren Ergebnis als Systeme, die auf getrennten Synchronisationszeichen beruhen.

C.3.1.3 Hash-Blockcodes

Hashfunktionen können linear oder nichtlinear sein. Am wichtigsten sind die nichtlinearen Einwegfunktionen, die Eingangsdaten in einen „Fingerabdruck“ komprimieren. Wegen ihrer Nichtlinearität kann – abgesehen von wenigen trivialen Fällen – keine Mindest-Hammingdistanz abgeleitet werden. Trotzdem ist die Fehlerentdeckungsfähigkeit für gute Hashcodes groß. Ein einzelner Bitwechsel in den Eingangsdaten führt im Mittel zum Wechsel der Hälfte der Bits im Hashwert. Bei gegebenem Hashwert ist es rein rechnerisch nicht ausführbar, Eingangsdaten zu finden, die zu diesem Hashwert führen (Einweg-Eigenschaft), und es ist bei gegebenen Eingangsdaten rein rechnerisch nicht ausführbar, andere Eingangsdaten zu finden, die zu demselben Hashwert führen (Kollisionseigenschaft für schwache Hashfunktionen). Eine weitere Eigenschaft ist es, dass es rein rechnerisch nicht ausführbar ist, irgendwelche zwei Sätze von Eingangsdaten zu finden, die zu diesem Hashwert führen (Kollisionseigenschaft für starke Hashfunktionen).

Die Norm ISO/IEC 10118-1 definiert in allgemeiner Weise Hashcodes für Informationssicherheitszwecke. Die Norm ISO/IEC 10118-2 beschreibt Hashcodes, die einen *n*-Bit Blockverschlüsselungsalgorithmus ohne Anwendung eines Schlüssels benutzen. Auch kann ein MAC als Hashcode genutzt werden, jedoch ist in diesem Fall ein Schlüssel erforderlich.

Eine gute Software-Leistungsfähigkeit kann mit dem öffentlich allgemein verfügbaren „message digest“ – Algorithmen MD4 und MD5 [Rivest] erreicht werden, welche Klassen vom MDC sind. Es sind keine hohen Anforderungen an das Kollisionskriterium gestellt, da böswillige Attacken durch andere Mittel abgewehrt werden. Das bedeutet, dass entweder ein kryptographischer Blockcode (MAC) benutzt wird, oder ein kryptographischer Schutz wird über die gesamte sicherheitsrelevante Nachricht einschließlich des Hashwertes angewendet.

C.3.1.4 Digitale Signaturen

Eine Anzahl von Bits abhängig von allen Bits der Eingangsdaten (Nutzerdaten und zusätzliche Daten) und genauso von einem geheimen Schlüssel. Ihre Korrektheit kann durch Verwendung eines öffentlichen Schlüssels nachgewiesen werden [Davies].

C.3.1.5 Kryptographische Blockcodes

Kryptographische Blockcodes sind eine Art von nichtlinearen Hashblockcode, die auf kryptographischen Algorithmen basieren. Der Vorteil ist, dass sie gegen böswillige Attacken schützen können, falls sie auf Schlüsseln basieren. Der bekannteste Code ist der Nachrichtenauthentifizierungscode MAC, der in ISO/IEC 9797-1 und ISO/IEC 9797-2 genormt ist.

C.3.2 Empfehlungen für die Anwendung von Sicherheitscodes

Beispiele für die Bewertung diverser grundlegender Techniken sind in Tabelle C.1 angegeben.

Tabelle C.1 – Bewertung von Sicherheitskodierungsmechanismen [4)]

Typ [a]	Referenz, siehe Abschnitt 2 und Literaturhinweise	Typ des sicherheitsrelevanten Kommunikationssystems, siehe Bild C.1			
		A0	**A1**	**B0** [b]	**B1** [b]
CRC [c]	[Peterson]	R	US [d]	– [e]	R
MAC [c]	ISO/IEC 9797-1 & 2	R	HR	R	R
Hash code [c]	ISO/IEC 10118-2	R	US [d]	HR	HR
Digitale Signatur [c]	ISO/IEC 9796-2 & 3	R	R	R	R

Legende

HR Dieses Symbol bedeutet, dass die Technik für diese Architektur dringend empfohlen wird. Wenn diese Technik nicht benutzt wird, dann sollte der Grund des Nichtbenutzens im technischen Sicherheitsbericht begründet werden.

R Dieses Symbol bedeutet, dass die Technik für diese Architektur empfohlen wird. Es ist ein niedrigerer Empfehlungsgrad als HR.

– Dieses Symbol bedeutet, dass für die Technik oder Maßnahme keine Empfehlung dafür oder dagegen ausgesprochen wird.

US Dieses Symbol bedeutet, dass diese Technik ungeeignet in dieser Systemkategorie ist.

a Andere Sicherheitsmaßnahmen sind möglich, aber hier nicht betrachtet.

b Nur nicht-kryptographischer Sicherheitscode. Kryptographische Techniken separat zu betrachten.

c Die Fehlererkennungsfähigkeiten sind für die gleiche Anzahl von Redundanzbits ähnlich.

d Geheimer Schlüssel gefordert, kann mit dieser Technik nicht erreicht werden.

e Falls Stromverschlüsselungstechniken verwendet werden, dann ist die Anwendung eines CRC als Sicherheitscode ungeeignet. Andernfalls kann ein Angreifer eine sicherheitsrelevante Nachricht mit einem gültigen CRC durch Zufügen einer beliebigen Nachricht mit einem gültigem CRC zu der stromverschlüsselten Nachricht erzeugen, ohne den Schlüssel zu brechen.

Obwohl die Kenntnis der Fehlercharakteristiken eines speziellen Kanals die Möglichkeit eröffnen kann, einige Arten von Fehlern außer Acht lassen zu können, und um daher eine höhere Leistungsfähigkeit zu beanspruchen, darf in einem offenem Kanal (schwarzer Kanal) keine solche Kenntnis vorausgesetzt werden. In diesem Szenario wäre der Zufallscode (random code) die ideale Lösung. Deshalb sollte für die geforderte Wahrscheinlichkeit eines unentdeckten Fehlers p_{UE} des Sicherheitscodes nie ein kleinerer Wert beansprucht werden als die Leistungsfähigkeit des Zufallscodes. Dieser beträgt $p_{UE} = 2^{-c}$, wobei c die Anzahl der Redundanzbits bedeutet.

4) Wo mehr als ein Sicherheitscodierungsmechanismus empfohlen wird, sollte eine geeignete Kombination einer oder mehrerer Mechanismen ausgewählt werden.

C.3.3 Kryptographische Techniken

Wenn Verschlüsselungstechniken benutzt werden, werden genormte Betriebsarten, z. B. entsprechend ISO/IEC 10116 empfohlen. Diese Norm empfiehlt nicht die Betriebsart Elektronisches Codebuch (Electronic Codebook mode (ECB)) für Eingangslängen, die die Blocklänge des Verschlüsselungsalgorithmus überschreiten. Kryptographische Algorithmen können entsprechend den Regeln der Internationalen Norm ISO/IEC 9979 registriert werden, aber die Registrierung selbst garantiert nicht die Stärke des Algorithmus.

Gut bekannte und gut geprüfte Algorithmen wie [AES] werden empfohlen.

C.4 Länge des Sicherheitscodes

Dieser Anhang ist nur für Kategorie 1, d. h. geschlossene Übertragungssysteme anwendbar, weil die vorgegebenen Formeln auf spezifischen Prämissen des Übertragungssystems beruhen.

Tatsächlich verlässt sich das hier beschriebene Modell teilweise auf die Fehlererkennungs- und Management Mechanismen des Übertragungssystems. Normalerweise entdeckt der Fehlererkennungsmechanismus des Übertragungssystems unter fehlerfreien Bedingungen alle Übertragungsfehler und wirk diesen entgegen. In diesem Fall wird der Sicherheitscode keinerlei Fehler entdecken. Nichtsdestotrotz kann das Übertragungssystem selbst, oder sein Fehlererkennungsmechanismus wegen Hardwarefehlern ausfallen, oder einige Übertragungsfehler sind so hoch, dass sie nicht entdeckt werden. In all diesem Fällen hat der Sicherheitscode solche Fehler zu erkennen.

Wenn dieses Modelle benutzt wird, führt das zu kleineren Sicherheitsintegritätsanforderungen für den Sicherheitscode, im Vergleich zu Modellen, die die Fehlererkennungsfähigkeiten der Übertragungssystems vernachlässigen. Demgegenüber ist das Übertragungssystem nun fixiert und kann nicht durch ein anderes ausgetauscht werden, ohne den Sicherheitsnachweis anzupassen. Dieses Modell kann (und sollte falls notwendig) für Systeme modifiziert werden, bei denen ihre Fehlererkennungsmechanismen, oder der Einfluss der Hardware Ausfallraten ignoriert werden.

Dieser Anhang stellt einfache Gleichungen für die Berechnung der Länge des Sicherheitscodes zur Verfügung. Die Erfüllung der gegebenen Anforderungen stellt das Erreichen des Sicherheitszieles sicher.

Das Basismodell für die Berechnung der Länge des Sicherheitscodes zeigt das Bild C.6.

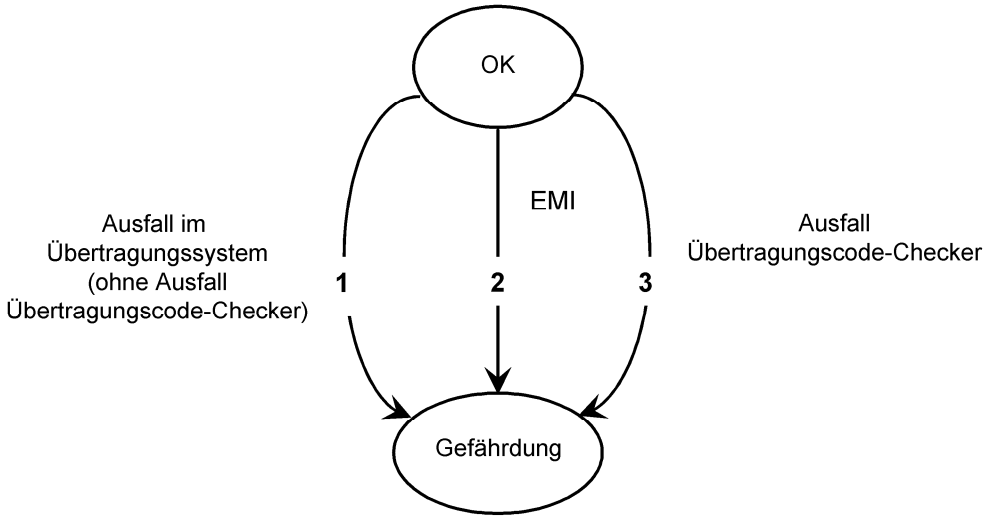


Bild C.6 – Grundlegendes Fehlermodell

Es gibt drei Wege, die zu einer Gefährdung führen können:

1. die Übertragungshardware fällt aus, so dass die Nachrichten verfälscht werden;
2. aufgrund von EMI treten Bitfehler auf, die nicht vom Übertragungscode entdeckt wurden;
3. ein Ausfall des Übertragungscodecheckers tritt auf, so dass jede verfälschte Nachricht vom nicht sicherheitsrelevanten Übertragungssystem zu der sicherheitsrelevanten Einrichtung durchgeleitet werden kann.

Die folgenden Definitionen gelten:

R_{H} Ziel-Gefährdungsrate des vollständigen Übertragungssystems

R_{H1} Gefährdungsrate durch Hardware Ausfälle ohne Übertragungcode-Checker

R_{H2} Gefährdungsrate durch EMI

R_{H3} Gefährdungsrate des Übertragungscode-Checkers

R_{HW} Hardware-Ausfallrate des nicht sicherheitsrelevanten Übertragungssystems

p_{US} Restfehlerwahrscheinlichkeit durch die Wirksamkeit des Sicherheitscodes

p_{UT} Restfehlerwahrscheinlichkeit durch die Wirksamkeit des Übertragungscodes

ANMERKUNG Wenn das nicht sicherheitsrelevante Übertragungssystem keinen Übertragungscode-mechanismus beinhaltet, dann muss p_{UT} = 1 angenommen werden.

f_{M} Maximale Frequenz von Nachrichten auf einen Empfänger bezogen

f_{W} Frequenz von verfälschten Nachrichten

T Zeitspanne, für die gilt: Wird mehr als eine definierte Anzahl von verfälschten Nachrichten innerhalb dieser Zeit empfangen, wird der sichere Zustand eingenommen

k_1 Faktor für Hardwareausfälle einschließlich einer Sicherheitsspanne

k_2 Faktor, der den Prozentsatz von Hardwareausfällen beschreibt, die zu einer nicht entdeckten Unwirksamkeit des Übertragungscodecheckers führen

m Sicherheitsfaktor, der in k_1 eingerechnet wird

n Anzahl von aufeinander folgenden verfälschten Nachrichten bis der sichere Zustand erreicht wird

Mit diesen Definitionen müssen folgende Gleichungen bewertet werden:

$$R_{HW} \times p_{US} \times k_1 = R_{H1} \quad (1)$$

$$p_{UT} \times p_{US} \times f_{W} = R_{H2}^{5)} \quad (2)$$

$$k_2 \times p_{US} \times \frac{1}{T} = R_{H3} \quad (3)$$

5) Dies bedeutet, dass der Sicherheitscode und der Übertragungscode unabhängig sind. Dies kann schwer zu überprüfen sein. Ein konservativerer Versuch ist, sich nur auf den Sicherheitscode zu verlassen.

Die Summe aller drei Raten darf R_H nicht überschreiten:

$$R_{H1} + R_{H2} + R_{H3} \leq R_H$$

Da nicht angenommen werden kann, dass der Ausfall zufällig ist, ist es notwendig, eine Sicherheitsspanne m im Faktor k_1 zu berücksichtigen. Der Faktor k_1 sollte entsprechend der folgenden Gleichung berechnet werden:

$$k_1 \geq n \times m$$

Der Faktor m repräsentiert die Sicherheitsspanne mit $m \geq 5$.

Die maximale Frequenz von verfälschten Nachrichten f_W muss folgendermaßen abgeschätzt werden

– entweder durch die „worst case"-Abschätzung $f_W = f_M$,

– oder durch eine Begrenzung der maximalen Rate von verfälschten Nachrichten oder der Anzahl von verfälschten Nachrichten, wo sichere Zähler und/oder Zeitgeber implementiert sind. Falls mehr als eine verfälschte Nachricht innerhalb einer definierten Zeitspanne empfangen wurde, sollte die sichere Kommunikation abgebrochen und der sichere Zustand eingenommen werden. Eine mathematische Ableitung beweist, dass eine gewisse Grenze nicht überschritten werden kann.

Bei zyklischen Übertragungen ist die Frequenz f_M genau definiert. Im Falle von nichtzyklischen Übertragungen muss die maximal mögliche Frequenz genommen werden.

Wenn propere oder „gute" CRC [6)] genommen werden, darf der maximale Wert von p_{UT} abgeschätzt werden als

$$p_{UT} = 2^{-b}$$

wobei b die Anzahl der Redundanzbits bezeichnet.

Wenn andere Codes genutzt werden, z. B. die Kombination zweier Codes, dann sollte die „worst case"-Blockfehlerwahrscheinlichkeit unter Zugrundelegen des Modells des „binär symmetrischen Kanals" [7)] genommen werden.

Der Faktor k_2 ist schwierig abzuschätzen. Wenn eine periodische Prüfung des korrekten Arbeitens des Übertragungscode-Checkers möglich ist, kann der Faktor k_2 vernachlässigt werden.

6) „Properness" bedeutet, dass die Beziehung zwischen Bitfehlerwahrscheinlichkeit (weniger als ein halb) und Restfehlerwahrscheinlichkeit monoton ist. „Goodness" bedeutet, dass die Restfehlerwahrscheinlichkeit ihr absolutes Maximum bei einer Bitfehlerwahrscheinlichkeit von ein halb hat. Siehe z. B. Wolf, J. K., Michelson, A. M. und Levesque, A. H.: „On the probability of undetected error for linear block codes", IEEE COM-30, 1982, 317-324; Dodunekova R., Dodunekov S. M.: „Sufficient conditions for good and proper detecting codes", IEEE Trans. Inform. Theory, vol. 43. pp. 2023-2026, Nov. 1997.

7) Binär symmetrischer Kanal: Mit der Wahrscheinlichkeit p ist ein empfangenes Bit verfälscht (0 → 1 und 1 → 0). Jedes Bit ist unabhängig von jedem anderen.

Ohne irgendwelche Rechtfertigungen sollte k_2 = 1 verwendet werden.

ANMERKUNG Die folgende Ableitung ist lediglich zur Information gegeben:

– Wenn ein Hardwarefehler auftritt, wird in nur 1 von 10 000 Fällen der Übertragungscode-Checker unerkannt versagen.

– In diesem Fall dauert dieser Zustand (ohne EMI)

$$T = MTBF_{HW} = \frac{1}{R_{HW}}$$

Man beachte, dass bereits ein geringes Absinken der Übertragungsqualität üblicherweise zum sicheren Zustand führt, so dass diese Abschätzung als sehr pessimistisch eingeschätzt werden kann.

Unter diesen Annahmen kann der Wert $k_2 = 10^{-4}$ genommen werden.

Gleichung (3) führt zu einem minimalen Zeitintervall, in dem nur eine Verfälschung, die vom Sicherheitscode entdeckt wird, erlaubt ist. Wenn ein solcher Mechanismus nicht verwendet wird, muss der sichere Zustand unmittelbar nach dem ersten entdeckten Fehler eingeleitet werden, andernfalls müssen andere Maßnahmen gegen mögliche Fehlerbedingungen eingeführt wurden.

Die maximale Restfehlerwahrscheinlichkeit eines Sicherheitscode mit c Stellen sollte abgeschätzt werden als:

$$p_{US} = 2^{-c}.$$

Diese Formel kann als grobe Abschätzung der Restfehlerwahrscheinlichkeit angesetzt werden. Sie ist für eine große Klasse von Codes (Hamming Codes, einige BCH Codes, kryptographische Codes, etc.) unter realistischen Annahmen gültig. Trotzdem muss der Anwender zeigen, dass die „properness“ oder „goodness“ [6)] des gewählte Code erfüllt ist.

Durch Wiederholung jeder Nachricht und der Konsistenzprüfung zweier gegenseitig unabhängigen Nachrichten kann der Wert von c mindestens halbiert werden. Tatsächlich kann man eine gewisse weitere Verbesserung erzielen, aber um aufwendige mathematische Berechnungen zu vermeiden, sollte die gegebene pessimistische Abschätzung die Grenze sein.

ANMERKUNG Dieser Mechanismus verlässt sich auf die Tatsache, dass gleichartig wirkende Ausfälle, die beide Nachrichten betreffen vernachlässigbar sind.

C.5 Kommunikation zwischen sicherheitsrelevanten und nicht sicherheitsrelevanten Anwendungen

Ein Beispiel der Kommunikation zwischen nicht sicherheitsrelevanten Anwendungen und sicherheitsrelevanten Anwendungen ist in Bild C.7 dargestellt.

Innerhalb gesicherten Netzwerken (Kategorie 1 und 2) können nicht sicherheitsrelevante Anwendungen über dasselbe, von sicherheitsrelevanten Anwendungen benutzte Übertragungsmedium kommunizieren. Anforderungen dazu siehe 7.2.

In diesem Beispiel ist die nicht sicherheitsrelevante Nachricht auch durch kryptographische Technik geschützt, wenn sie ein Kategorie 3 Übertragungssystem passiert.

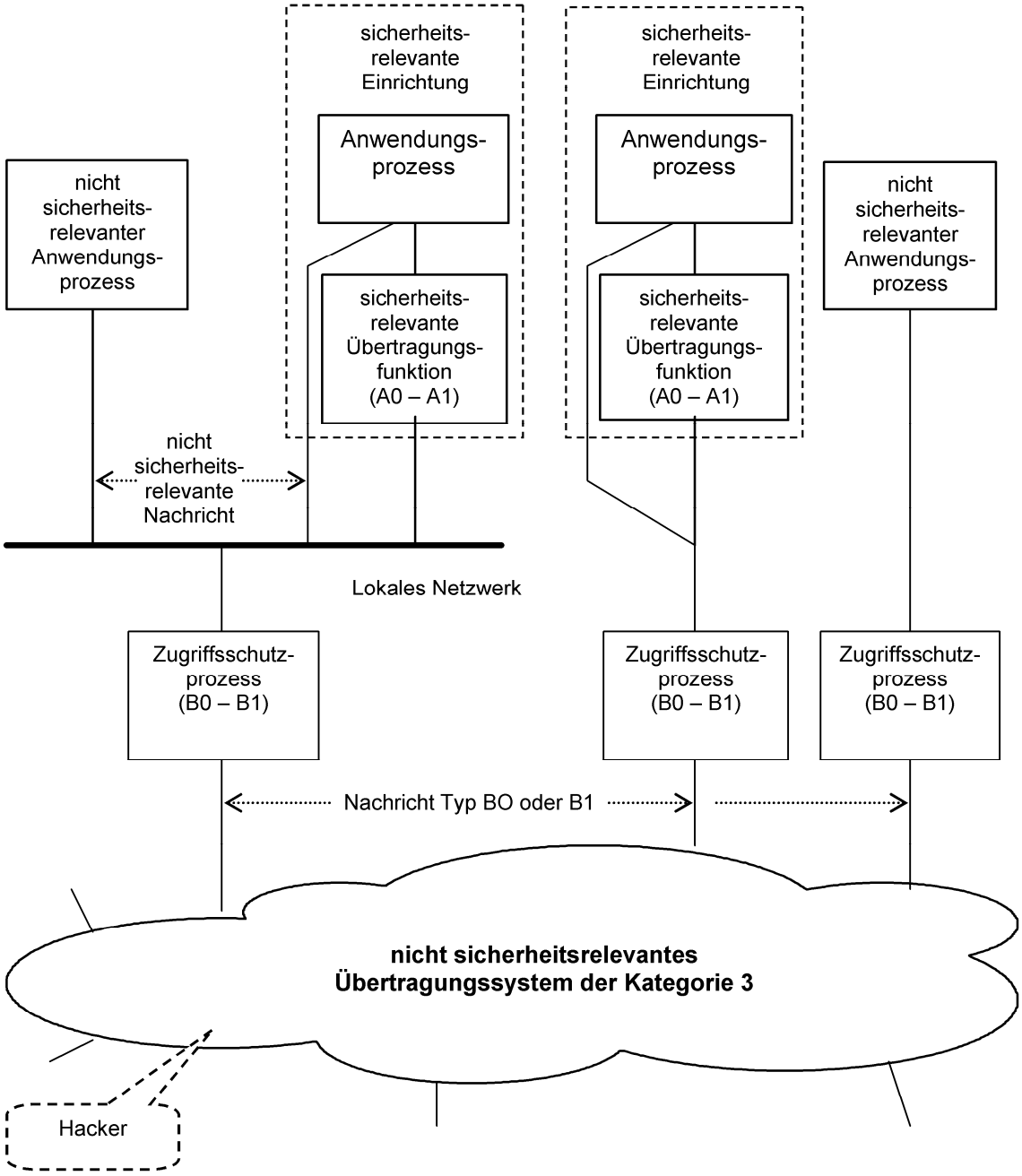


Bild C.7 – Kommunikation zwischen nicht sicherheitsrelevanten und sicherheitsrelevanten Anwendungen

Anhang D
(informativ)

Leitfäden für den Gebrauch der Norm

D.1 Prozedur

Eine Anzahl von unterschiedlichen Schritten können herausgefunden werden, um die System-Entwurfsaktivitäten auszuführen, die durch die EN 50129 abgedeckt sind.

Diese Schritte sind:

Anwendung
↓
Gefährdungsanalyse
↓
Risikoreduktion
↓
Zuordnung SIL und quantitative Ziele
↓
Sicherheitsanforderungsspezifikationen

Jeder dieser Schritte ist in den folgenden Abschnitten in detaillierterer Weise beschrieben:

D.1.1 Anwendung

Der Systementwickler muss die Anwendung des Übertragungssystems verstehen. Die Datenflüsse, Datentypen und die Häufigkeit und Art der Aktualisierung (z. B. periodisch oder ereignisgesteuert) beeinflussen im gesamtem die zu treffenden Entscheidungen für den Entwurf des Übertragungssystems. Das globale Sicherheitsziel (Rate oder durch qualitative Parameter und nichtfunktionale Parameter) des Systems muss ebenso definiert werden (durch den Nutzer oder die Sicherheitsbehörde).

D.1.2 Gefährdungsanalyse

Eine qualitative Gefährdungsanalyse des Systems (wie nach EN 50126 gefordert) muss die Top-Gefährdung(en) identifizieren, die als Ergebnis von Fehlfunktionen der Sender- und Empfängereinrichtung oder der Übertragungsverbindung selbst entstehen können. Diese Analyse muss die betriebsmäßigen oder anderer externer Bedingungen berücksichtigen, die das System einer Gefährdung aussetzen könnten. Für jede dieser Bedrohung an das System kann die Möglichkeit der Einführung einer Schutzmaßnahme in den Systementwurf mit eingeschlossen werden.

D.1.3 Risikoreduktion

Ausgehend vom globalen quantitativen Systemsicherheitsziel und der qualitativen Gefährdungsanalyse kann der Systementwickler Sicherheitsziele zu jeder identifizierten Bedrohung zuordnen. Die Zuordnung zu solchen Zielen kann iterativ sein, beginnend mit einer vereinfachten Zuordnung und Verfeinerung in einer detaillierteren Analyse und Abwägen der verschiedenen Fälle. Das Ausmaß der von jeder Schutzmaßnahme benötigten Risikoreduktion kann bestimmt werden, indem die quantitativen Werte über das Auftreten der externen Bedingungen, die das System zur Gefährdung führen, genutzt werden.

D.1.4 Zuordnung der SIL und quantitativen Ziele

Abhängig vom Ausmaß der für jede Schutzmaßnahme benötigten Risikoreduktion können unter Benutzung der in EN 50129 definierten Prozeduren SILs zugeordnet werden. Kennt man die SIL, kann man eine geeignete Entwurfstechnik für die entsprechende Schutzmaßnahme auswählen.

Ausgehend von der quantifizierten Gefährdungsrate (wrong side failure rate) für die Schutzmaßnahme können die Hardwareentwurfstechniken unter Verwendung der Tabellen aus EN 50129 gewählt werden, und man kann die Rate des Auftretens von gefährlichen Fehlfunktionen aufgrund von Zufallsausfällen berechnen.

D.1.5 Sicherheitsanforderungsspezifikation (SRS)

Die SIL für die Implementierung der für den sicheren Betrieb des Systems als erforderlich identifizierten Schutzmaßnahmen und die quantifizierten Sicherheitsziele müssen in der System – SRS dokumentiert werden.

D.2 Beispiele

Das folgende Beispiel zeigt lediglich einige grundlegenden Prinzipien dieser Prozedur. Es war nicht beabsichtigt, ein komplettes, in allen Details korrektes Beispiel zu beschreiben.

D.2.1 Anwendung

In einer Nebenbahnstrecke werden Fahrbefehle als Nachrichten über ein öffentliches Funkübertragungssystem zu den Zügen gesendet.

Für das System ist ein globales Sicherheitsziel von 10^{-x} je Stunde definiert.

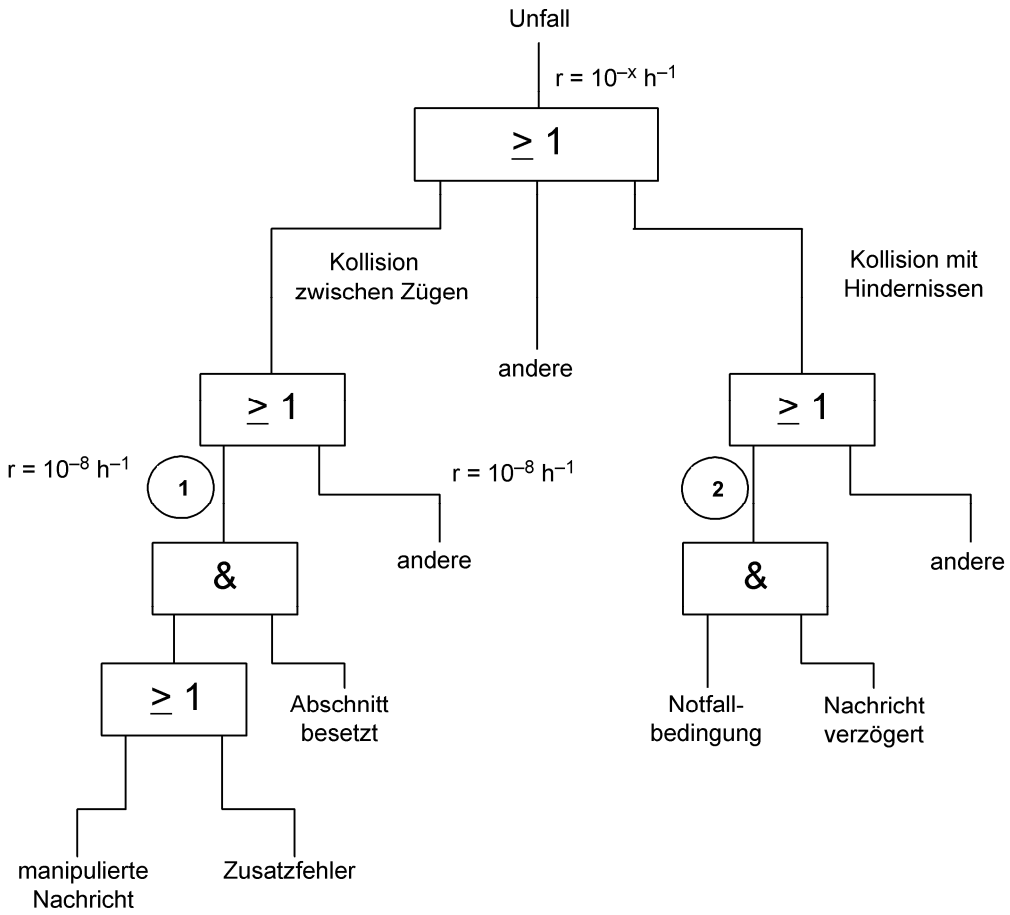
D.2.2 Gefährdungsanalyse

Zwei besondere Gefährdungen können identifiziert werden (unter anderen, hier nicht betrachteten):

a) der Empfang einer nicht korrekten (unerkannt verfälschten) Nachricht an Bord eines Zuges könnte dazu führen, dass der Zug in einen besetzten Abschnitt einfährt und mit einem anderen Zug kollidiert;

b) eine Verzögerung beim Empfang einer Nothaltnachricht könnte dazu führen, dass der Zug mit einem Hindernis auf der Stecke kollidiert.

Dieses ist in einem Fehlerbaum (Bild D.1) als ein Beispiel für die Durchführung der Gefährdungsanalyse dargestellt.



Legende

≥ 1	ODER Gatter
&	UND Gatter
1	Fehlerbaum für Fall 1 (siehe Bild D.2)
2	Fehlerbaum für Fall 2 (siehe Bild D.3)
r	tolerierbare Gefährdungsrate

ANMERKUNG Bevorzugte Symbole entsprechend EN 61025.

Bild D.1 – Fehlerbaum für die Gefährdung „Unfall“

Das globale Systemsicherheitsziel von 10^{-x} je Stunde ist so aufgeteilt, dass für die Fälle 1 und 2 (z. B.) 10^{-8} je Stunde zugeordnet wurden.

Die Fälle 1 und 2 werden nun im Detail betrachtet.

D.2.3 Fall 1

D.2.3.1 Risikoreduktion

Wenn eine Nachricht zu einem Zug wegen Zufallsfehler verfälscht ist, kann sie einem Zug erlauben, in einen besetzten Abschnitt einzufahren und mit einem anderen Zug zusammenzustoßen.

Zusätzlich könnte vorsätzlich versucht werden, eine nicht korrekte Nachricht in das System einzuschleusen (z. B. durch einen Hacker).

Angenommen wird nun, dass die Wahrscheinlichkeit für einen besetzten Abschnitt mit 10^{-1} eingeschätzt wurde.

In dieser Norm wird vorgeschlagen, einen der Nutzinformation hinzugefügten Sicherheitscode als mögliche Schutzmaßnahme gegen Nachrichtenverfälschung anzuwenden.

Die Einführung dieser Schutzmaßnahme in den diesen Fall betreffenden Teil des Fehlerbaums liefert die Resultate im folgenden Bild D.2:

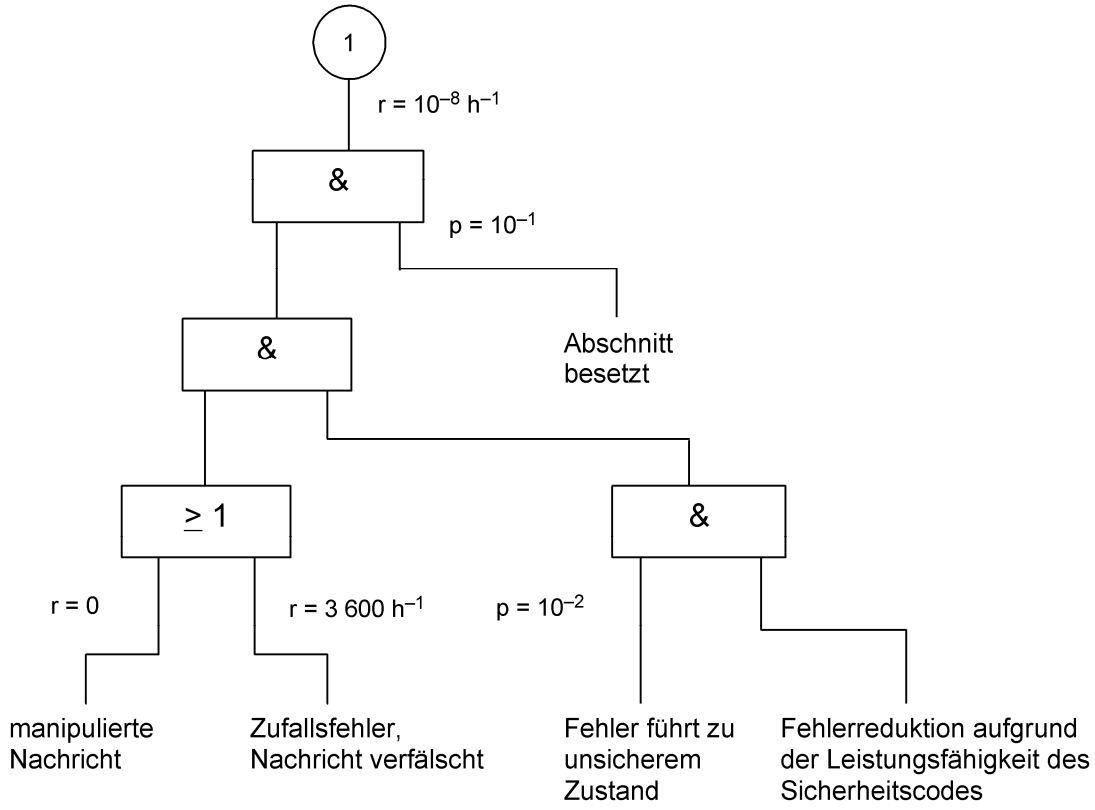


Bild D.2 – Fehlerbaum für Fall 1

Beim Betrachten der quantitativen Sicherheitsziele muss angenommen werden, dass in einem offenem System jede Nachricht verfälscht sein kann (d. h. Wahrscheinlichkeit = 1). Trotzdem würde nicht jede verfälschte Nachricht den Zug dazu berechtigen, in den speziellen Abschnitt einzufahren. Mit der Annahme, dass diese Wahrscheinlichkeit 10^{-2} beträgt, und mit der Annahme, dass Nachrichten mit der Länge von 100 Bit zum Zug über einen Kanal mit der Bitrate von 100 Bit/s (d. h. 3 600 Nachrichten je Stunde) gesendet werden, dann ist deutlich, dass der Sicherheitscode für die Nachricht eine Wahrscheinlichkeit für einen unentdeckten Fehler von weniger als 3×10^{-9} je Nachricht garantieren muss, bzw. darf die Häufigkeit dieser Ereignisse 10^{-5} h^{-1} nicht überschreiten.

D.2.3.2 SIL-Zuweisung und quantifizierter Zielwert

Nach EN 50129 kann eine SIL für die Implementierung der Funktion „Berechnung des Sicherheitscodes“ abgeleitet werden. Diese SIL könnte kleiner als für das gesamte Systemelement ”sicherheitsrelevantes Kommunikationssystem” sein.

Der Systementwickler muss einen Sicherheitscode mit einer ausreichenden Länge auswählen, um die geforderte Leistungsfähigkeit zu erreichen.

In dieser Norm wird vorgeschlagen, dass es notwendig ist, die Möglichkeit von absichtlichen Versuchen zu betrachten, falsche Nachrichten im offenem Übertragungssystem zu erzeugen. Zum Beispiel könnte für seltene Übertragung von kurzen Nachrichten die Wahrscheinlichkeit für absichtliche Versuche, Unfälle zu produzieren, relativ klein sein. Diese Faktoren können die Entscheidung beeinflussen, ob ein kryptographischer Sicherheitscode genommen wird, und falls ja, wie die Parameter (Schlüssellänge usw.) für diesen Code zu wählen sind.

D.2.4 Fall 2

D.2.4.1 Risikoreduktion

Falls in einer Notfallsituation (z. B. Hindernis auf dem Gleis) die Nothaltnachricht zum Zug verzögert ist, könnte eine Kollision entstehen. Angenommen wird, dass solche Notfallsituationen mit der Häufigkeit von 10^{-4} je Stunde zu rechtfertigen sind.

Weiter sei angenommen, dass durch die Verwendung eines öffentlichen Funksystems, das mit einer nicht kontrollierten Anzahl von anderen Nutzern zu teilen ist, keine größte Nachrichtenverzögerung sichergestellt ist. Deswegen muss eine Verzögerung angenommen werden (d. h., dass für eine Verzögerung die Wahrscheinlichkeit mit 1 anzusetzen ist).

Diese Norm schlägt als mögliche Schutzmaßnahme gegen Nachrichtenverzögerung vor, eine Zeitüberwachung in der Empfängereinrichtung zusammen mit einer zyklischen Nachrichtenübertragung anzuwenden.

Die Einführung dieser Schutzmaßnahme in den diesen Fall betreffenden Teil des Fehlerbaums liefert die Resultate im folgenden Bild D.3:

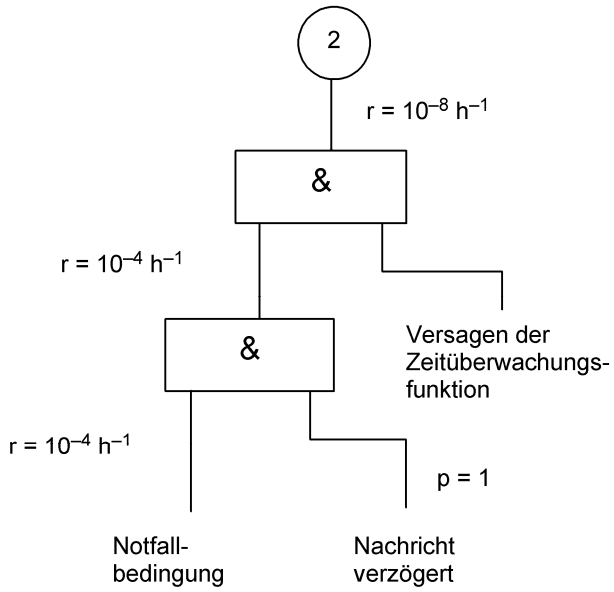


Bild D.3 – Fehlerbaum für Fall 2

Betrachtet man die quantitativen Sicherheitsziele, so ist deutlich, dass die Zeitüberwachung eine Restfehlerwahrscheinlichkeit von kleiner als 10^{-4} auf Anforderung haben muss.

D.2.4.2 SIL-Zuweisung und quantifizierter Zielwert

Ein Verweis auf EN 50129 zeigt an, wie die erforderliche SIL erreicht werden kann.

Die Implementierung dieser Funktion muss deshalb so vorgenommen werden, dass eine in EN 50129 vorgeschlagene Technik verwendet wird, die für die abgeleitete SIL geeignet ist, solange nicht andere Funktionen mit einer höheren SIL implementiert werden müssen (z. B. in einem Prozessorsystem).

Anhang E
(informativ)

Zuordnung zu vorhergehenden Normen

Diese Norm ist das Ergebnis der Überarbeitung und der Zusammenlegung der vorhergehenden Normen EN 50159-1:2001 and EN 50159-2:2001. Im wesentlichen wurden nur Korrekturen und Verbesserungen durchgeführt. Einige neue Teile waren aus Gründen der Konsistenz notwendig.

Die Tabellen E.1 und E.2 stellen die Zuordnung der (Unter)Abschnitte und Anhänge der vorhergehenden Normen zu den (Unter)Abschnitten und Anhängen der zukünftigen EN 50159:201X dar.

Das soll die Rückverfolgbarkeit im Fall von Wartung und/oder Erweiterung von Systemen erleichtern, die ehemals nach den vorhergehenden Normen zugelassen wurden und des Weiteren die Verständlichkeit der neuen Norm.

Die Referenz in der Tabelle bezieht sich nur von den vorhergehenden zur neuen Norm, aber nicht umgekehrt.

Tabelle E.1 – Zuordnung von EN 50159-1:2001 zu EN 50159:201X

(Unter)Abschnitt von EN 50159-1:2001		Informativ / Normativ	(Unter)Abschnitt der EN 50159:201X		Ungeändert / Modifiziert
Einleitung		Inf.	Einleitung		E
1	Anwendungsbereich	Nor.	1	Anwendungsbereich	E
2	Normative Verweisungen	Nor.	2	Normative Verweisungen	E
3	Begriffe	Nor.	3	Begriffe und Abkürzungen	E
4	Referenzarchitektur	Nor.	4	Referenzarchitektur	T
	Pr1	Nor.	6.3.1	Pr3	E
	Pr2	Nor.	6.3.1	Pr1	E
	Pr3	Nor.	6.3.1	Pr2	E
5	Beziehung zwischen den Eigenschaften des Übertragungssystems und den Sicherheitsprozeduren	Nor.	7.2.8		E
5.1	Funktionale Anforderung (Text bis P1)	Nor.	Nicht benutzt		
	P1 bis P5	Nor.	7.1	Einführung	T
	P6	Nor.	7.2.5		E
5.2	Sicherheitsanforderungen, R1 bis R6	Nor.	7.2	Allgemeine Anforderungen	T
6.1	Allgemeines	Nor.	Nicht benutzt		
6.2	Kommunikation zwischen signaltechnisch sicheren Einrichtungen	Nor.	7.1 und 7.2		T
6.3	Kommunikation zwischen signaltechnisch sicheren und nicht sicheren Einrichtungen	Nor.	7.2.2		E
			7.3.7.2.1		E
6.4	Kommunikation zwischen signaltechnisch nicht sicheren Einrichtungen	Nor.	Nicht benutzt		
7.1	Generelle Anforderungen	Nor.	7.3.7.2.3		E
7.2	Sicherheitsziel	Nor.	7.2.5		T
7.3	Länge des Sicherheitscodes	Nor.	7.3.7.2.4		E
Anhang A	Länge des Sicherheitscodes	Inf.	C.4	Länge des Sicherheitscodes	U

Legende

Inf. Informative

Nor. Normative

U (Ungeändert) enthalten:
Änderungen von Referenzen und Änderungen der Terminologie, um Konsistenz in der gesamten Norm zu erreichen.

E (Editorielle (redaktionelle) Änderungen) enthalten:
Keine Änderung des Inhaltes, nur Umgruppierungen und Verbesserungen.

T (Technische Änderungen) enthalten:
Inhalte entweder in andere (Unter)Abschnitte verschoben, oder geändert.

Tabelle E.2 – Zuordnung von EN 50159-2:2001 zu EN 50159:201X

(Unter)Abschnitt von EN 50159-2:2001		Informativ / Normativ	(Unter)Abschnitt der EN 50159:201X		Ungeändert / Modifiziert
Einleitung		Inf.	Einleitung		E
1	Anwendungsbereich	Nor.	1	Anwendungsbereich	E
2	Normative Verweisungen	Nor.	2	Normative Verweisungen	E
3	Begriffe	Nor.	3	Begriffe und Abkürzungen	E
4	Referenzarchitektur	Nor.	4	Referenzarchitektur	T
5	Bedrohungen auf das Übertragungssystem	Nor.	5	Bedrohungen auf das Übertragungssystem	U
6.1	Einleitung	Nor.	7.1	Einführung	U
6.2	Allgemeine Anforderungen	Nor.	7.2	Allgemeine Anforderungen	T
6.3	Spezifische Schutzmaßnahmen	Nor.	7.3	Spezifische Schutzmaßnahmen	U
6.3.1	Sequenznummer	Nor.	7.3.1	Sequenznummer	U
6.3.2	Zeitstempel	Nor.	7.3.2	Zeitstempel	U
6.3.3	Zeitüberwachung	Nor.	7.3.3	Zeitüberwachung	U
6.3.4	Quellen- und Zielbezeichner	Nor.	7.3.4	Quellen- und Zielbezeichner	U
6.3.5	Rücknachricht	Nor.	7.3.5	Rücknachricht	U
6.3.6	Identifikationsprozedur	Nor.	7.3.6	Identifikationsprozedur	U
6.3.7	Sicherheitscode	Nor.	7.3.7	Sicherheitscode	T
6.3.8	Kryptographische Techniken	Nor.	7.3.8	Kryptographische Techniken	T
7.1	Einleitung	Nor.	7.4.1	Einführung	U
7.2	Bedrohungs-/ Schutzmaßnahmenmatrix	Nor.	7.4.2	Bedrohungs-/ Schutzmaßnahmenmatrix	U
7.3	Auswahl und Gebrauch des Sicherheitscode und kryptographischen Techniken	Nor.	7.4.3	Wahl und Gebrauch von Sicherheitscodes und kryptographischen Techniken	U
A.1	Anwendung von Zeitstempeln	Inf.	C.1	Anwendung von Zeitstempeln	U
A.2	Auswahl und Gebrauch von Sicherheitscodes und kryptographischen Techniken	Inf.	C.2	Auswahl und Gebrauch von Sicherheitscodes und kryptographischen Techniken	T
Literaturhinweise		Inf.	Literaturhinweise		T
C.1	Anwendungsbereich/Zweck	Inf.	6.1	Allgemeines	T
C.2	Klassifikation von Übertragungssystemen	Inf.	6.2	Allgemeine Aspekte der Klassifikation	T
			Anhang B	Kategorien von Übertragungssystemen	T
C.3	Prozedur	Inf.	D.1	Prozedur	U
C.4	Beispiel	Inf.	D.2	Beispiel	U
Anhang D	Bedrohungen auf offenen Übertragungssysteme	Inf.	Anhang A	Bedrohungen auf offenen Übertragungssysteme	E

Legende

Inf. Informative

Nor. Normative

U (Ungeändert) enthalten:
Änderungen von Referenzen und Änderungen der Terminologie, um Konsistenz in der gesamten Norm zu erreichen.

E (Editorielle (redaktionelle) Änderungen) enthalten:
Keine Änderung des Inhaltes, nur Umgruppierungen und Verbesserungen.

T (Technische Änderungen) enthalten:
Inhalte entweder in andere (Unter)Abschnitte verschoben, oder geändert.

Anhang ZZ
(informativ)

Zusammenhang mit Grundlegenden Anforderungen von EG-Richtlinien

Diese Europäische Norm wurde unter einem Mandat erstellt, das von der Europäischen Kommission und der Europäischen Freihandelszone an CENELEC gegeben wurde. Diese Europäische Norm deckt innerhalb ihres Anwendungsbereiches alle relevanten grundlegenden Anforderungen ab, die in Anhang III der EG-Richtlinie 2008/57/EG (RAIL) enthalten sind.

Die Übereinstimmung mit dieser Norm ist eine Möglichkeit, die Konformität mit den festgelegten grundlegenden Anforderungen der betreffenden EG-Richtlinie zu erklären.

WARNHINWEIS: Für Produkte, die in den Anwendungsbereich dieser Norm fallen, können weitere Anforderungen und weitere EG-Richtlinien anwendbar sein.

Literaturhinweise

EN 61025, *Fehlzustandsbaumanalyse (IEC 61025)*

ISO/IEC 9796-2:2002, *Information technology – Security techniques – Digital signatures scheme giving message recovery – Part 2: Integer factorization based mechanisms*

ISO/IEC 9796-3:2006, *Information technology – Security techniques – Digital signatures scheme giving message recovery – Part 3: Discrete logarithm based mechanisms*

ISO/IEC 9797-1:1999, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*

ISO/IEC 9797-2:2002, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*

ISO/IEC 9979:1999 [8)], *Information technology – Security techniques – Procedures for the registration of cryptographic algorithms*

ISO/IEC 10116:2006, *Information technology – Security techniques – Modes of operation for an n-bit block cipher*

ISO/IEC 10118-1:2000, *Information technology – Security techniques – Hash-functions – Part 1: General*

ISO/IEC 10118-2:2000, *Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher*

ISO/IEC 10118-3:2004, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated Hash-functions*

ISO/IEC 10118-4:1998, *Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic*

ISO/IEC 11770-1:1996, *Information technology – Security techniques – Key management – Part 1: Framework*

ISO/IEC 11770-2:2008, *Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques*

ISO/IEC 11770-3:2008, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*

UIC 738, *Wichtigste Sicherheitsbedingungen bei Verwendung von elektronischen Bauelementen in der Eisenbahntechnik*

[A155] UIC/ORE A155.1 Report RP 4, September 1984: *Survey of available measures for protection of safety information during transmission* (auch in Deutsch und Französisch verfügbar)

[AES] FIPS PUB 197, 26.11.2001: *Advanced Encryption Standard*

[Davies] D.W. Davies and W.L. Price: *Security for Computer Networks*, 2. Ausgabe, J. Wiley & Sons, Chichester

[Peterson] W. Wesley Peterson: *Error correction Codes*, M.I.T. Press, 1967

8) Zurückgezogen.

[Rivest] R. Rivest: *The MD4 Message-Digest Algorithm*, 4/92, auf Internet veröffentlicht

[Schneier] Bruce Schneier: *Applied Cryptography*, J. Wiley & Sons, Inc, 2. Ausgabe, 1995

[TBaum] A. Tanenbaum: *Distributed Systems*, Prentice Hall 1995

Wolf, J. K., Michelson, A. M. und Levesque, A. H.: „*On the probability of undetected error for linear block codes*“

IEEE COM-30, Dodunekova R., Dodunekov S. M.: „*Sufficient conditions for good and proper detecting codes*“ 1982, 317-324

IEEE Trans. Inform. Theory, vol. 43. pp. 2023-2026, Nov. 1997