

	Bahnanwendungen Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme Sicherheitsrelevante elektronische Systeme für Signaltechnik Deutsche Fassung EN 50129:2003	DIN EN 50129
VDE	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Vorstand beschlossenen Genehmigungsverfahrens unter nebenstehenden Nummern in das VDE-Vorschriftenwerk aufgenommen und in der etz Elektrotechnische Zeitschrift bekannt gegeben worden.	Klassifikation VDE 0831 Teil 129
ICS 93.100 Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling; German version EN 50129:2003 Applications ferroviaires – Systèmes de signalisation, de télécommunications et de traitement – Systèmes électroniques de sécurité pour la signalisation; Version allemande EN 50129:2003 Die Europäische Norm EN 50129:2003 hat den Status einer Deutschen Norm. Beginn der Gültigkeit Die EN 50129 wurde am 2002-12-01 angenommen. Daneben darf DIN V ENV 50129 (VDE V 0831 Teil 129):1999-07 noch bis 2005-12-01 angewendet werden. Nationales Vorwort Für die vorliegende Norm ist das nationale Arbeitsgremium UK 713.4 „Bahn-Signalanlagen“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE zuständig. Norm-Inhalt war veröffentlicht als E DIN EN 50129 (VDE 0831 Teil 129):2000-11. Ersatz für DIN V ENV 50129 (VDE V 0831 Teil 129):1999-07 Siehe Beginn der Gültigkeit Fortsetzung Seite 2 bis 4 und 98 Seiten EN DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Änderungen

Gegenüber **DIN V ENV 50129 (VDE V 0831 Teil 129):1999-07** wurden folgende Änderungen vorgenommen:

- a) Der normative Anhang A wurde aufgrund der vom CENELEC-Subkomitee SC9XA akzeptierten Ergebnisse der Arbeitsgruppe SC9XA/WGA10 (siehe CENELEC-Report R009-004) völlig neu erstellt.
- b) Dieser Anhang erläutert die Bedeutung, Ableitung und Verwendung der Sicherheitsanforderungsstufen (SIL). Die übrigen Teile dieser Norm mussten aufgrund dieser Überarbeitung geringfügig angepasst werden.
- c) Auch der Anwendungsbereich ist davon betroffen, so dass die Norm nun für alle elektronischen Signalanwendungen – unabhängig von deren Sicherheitsrelevanz – anwendbar ist.

Frühere Ausgaben

DIN V ENV 50129 (VDE V 0831 Teil 129):1999-07

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

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

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

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

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

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 50121-2:2000	–	DIN EN 50121-2 (VDE 0115 Teil 121-2):2001-05	VDE 0115 Teil 121-2
Normen der Reihe EN 50121-3	–	Normen der Reihe DIN EN 50121-3 (VDE 0115 Teil 121-3)	VDE 0115 Teil 121-3
EN 50121-4:2000	–	DIN EN 50121-4 (VDE 0115 Teil 121-4):2001-05	VDE 0115 Teil 121-4
EN 50124-1:2001	–	DIN EN 50124-1 (VDE 0115 Teil 107-1):2001-10	VDE 0115 Teil 107-1
EN 50124-2:2001	–	DIN EN 50124-2 (VDE 0115 Teil 107-2):2001-10	VDE 0115 Teil 107-2
EN 50125-1:1999	–	DIN EN 50125-1 (VDE 0115 Teil 108-1):2000-05	VDE 0115 Teil 108-1
EN 50125-3:2003	–	–	–

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 50126:1999	–	DIN EN 50126 (VDE 0115 Teil 103):2000-03	VDE 0115 Teil 103
EN 50128:2001	–	DIN EN 50128 (VDE 0831 Teil 128):2001-11	VDE 0831 Teil 128
EN 50155:2001	–	DIN EN 50155 (VDE 0115 Teil 200):2002-11	VDE 0115 Teil 200
EN 50159-1:2001	–	DIN EN 50159-1 (VDE 0831 Teil 159-1):2001-11	VDE 0831 Teil 159-1
EN 50159-2:2001	–	DIN EN 50159-2 (VDE 0831 Teil 159-2):2001-12	VDE 0831 Teil 159-2
EN 61508-1:2001	IEC 61508-1:1998 Corr. 1999	DIN EN 61508-1 (VDE 0803 Teil 1):2002-11	(VDE 0803 Teil 1)
Normen der Reihe EN 60664	Normen der Reihe IEC 60664	Normen der Reihe DIN IEC 60664	(VDE 0110-x)

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 50121-2 (VDE 0115 Teil 121-2):2001-05, *Bahnanwendungen – Elektromagnetische Verträglichkeit – Teil 2: Störaussendung des gesamten Bahnsystems in die Außenwelt; Deutsche Fassung EN 50121-2:2000.*

DIN EN 50121-3 (VDE 0115 Teil 121-3) Reihe, *Bahnanwendungen – Elektromagnetische Verträglichkeit.*

DIN EN 50121-4 (VDE 0115 Teil 121-4):2001-05, *Bahnanwendungen – Elektromagnetische Verträglichkeit – Teil 4: Störaussendung und Störfestigkeit von Signal- und Telekommunikationseinrichtungen; Deutsche Fassung EN 50121-4:2000.*

DIN EN 50124-1 (VDE 0115 Teil 107-1):2001-10, *Bahnanwendungen – Isolationskoordination – Teil 1: Grundlegende Anforderungen – Kriech- und Luftstrecken für alle elektrischen und elektronischen Betriebsmittel; Deutsche Fassung EN 50124-1:2001.*

DIN EN 50124-2 (VDE 0115 Teil 107-2):2001-10, *Bahnanwendungen – Isolationskoordination – Teil 2: Überspannungen und geeignete Schutzmaßnahmen; Deutsche Fassung EN 50124-2:2001.*

DIN EN 50125-1 (VDE 115 Teil 108-1):2000-05, *Bahnanwendungen – Umweltbedingungen für Betriebsmittel – Teil 1: Betriebsmittel auf Bahnfahrzeugen; Deutsche Fassung EN 50125-1:1999.*

DIN EN 50126 (VDE 0115 Teil 103):2000-03, *Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS); Deutsche Fassung EN 50126:1999.*

DIN EN 50128 (VDE 0831 Teil 128):2001-11, *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme; Deutsche Fassung EN 50128:2001.*

DIN EN 50155 (VDE 0115 Teil 200):2002-11, *Bahnanwendungen – Elektronische Einrichtungen auf Schienenfahrzeugen; Deutsche Fassung EN 50155:2001.*

DIN EN 50129 (VDE 0831 Teil 129):2003-12

DIN EN 50159-1 (VDE 0831 Teil 159-1):2001-11, *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Teil 1: Sicherheitsrelevante Kommunikation in geschlossenen Übertragungssystemen; Deutsche Fassung EN 50159-1:2001.*

DIN EN 50159-2 (VDE 0831 Teil 159-2):2001-12, *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Teil 2: Sicherheitsrelevante Kommunikation in offenen Übertragungssystemen; Deutsche Fassung EN 50159-2:2001.*

DIN EN 61508-1 (VDE 0803-1):2002-11, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:1998 + Corr. 1999); Deutsche Fassung EN 61508-1:2001.*

DIN IEC 60664 Reihe, *Isolationskoordination für elektrische Betriebsmittel in Niederspannungsanlagen (IEC 60664 (VDE 0110-x) Reihe); Deutsche Fassung EN 60664 Reihe.*

Deutsche Fassung

**Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und
Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für
Signaltechnik**

Railway applications – Communications,
signalling and processing systems – Safety
related electronic systems for signalling

Applications ferroviaires – Systèmes de
signalisation, de télécommunications et de
traitement – Systèmes électroniques de sécurité
pour la signalisation

Diese Europäische Norm wurde von CENELEC am 2002-12-01 angenommen. Die CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

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

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

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

CENELEC

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

Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel

© 2003 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Vorwort

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

Der Text des Schriftstücks wurde der formellen Abstimmung unterworfen und von CENELEC am 2002-12-01 als EN 50129 angenommen.

Diese Europäische Norm ersetzt ENV 50129:1998.

Diese Europäische Norm wurde unter einem an CENELEC von der Europäischen Kommission und der Europäischen Freihandelszone erteilten Mandat ausgearbeitet und unterstützt die grundsätzlichen Anforderungen der EU-Richtlinie 96/48/EG.

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): 2003-12-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2005-12-01

Anhänge, die als „normativ“ bezeichnet sind, gehören zum Norminhalt.

Anhänge, die als „informativ“ bezeichnet sind, enthalten nur Informationen.

In dieser Norm sind die Anhänge A, B und C normativ und die Anhänge D und E sind informativ.

Inhalt

Seite

Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	8
3 Begriffe und Abkürzungen	9
3.1 Begriffe	9
3.2 Abkürzungen.....	14
4 Gesamtrahmen dieser Europäischen Norm	15
5 Bedingungen für die Sicherheitsanerkennung und -zulassung.....	16
5.1 Der Sicherheitsnachweis	16
5.2 Nachweis des Qualitätsmanagements	18
5.3 Nachweis des Sicherheitsmanagements	21
5.4 Nachweis der funktionalen und technischen Sicherheit.....	26
5.5 Sicherheitsanerkennung und -zulassung	28
Anhang A (normativ) Sicherheitsanforderungsstufen.....	34
A.1 Einleitung	34
A.2 Sicherheitsanforderungen	34
A.3 Sicherheitsintegrität	35
A.4 Zuteilung der Sicherheitsintegritätsanforderungen.....	36
A.5 Sicherheitsanforderungsstufen.....	45
Anhang B (normativ) Detaillierte technische Anforderungen.....	48
B.1 Einleitung	48
B.2 Nachweis des korrekten funktionalen Verhaltens	48
B.3 Ausfallauswirkungen.....	51
B.4 Betrieb mit externen Einflüssen.....	58
B.5 Sicherheitsbezogene Anwendungsbedingungen	60
B.6 Sicherheitserprobung	63
Anhang C (normativ) Identifizierung der Ausfallarten von Hardware-Bauteilen.....	64
C.1 Einleitung	64
C.2 Allgemeines Verfahren	64
C.3 Das Verfahren für integrierte Schaltkreise (einschließlich Mikroprozessoren)	64
C.4 Das Verfahren für Bauteile mit unverlierbaren physikalischen Eigenschaften.....	65
C.5 Allgemeine Anmerkungen zu den Bauteil-Ausfallarten	65
C.6 Zusätzliche allgemeine Anmerkungen zu den Bauteilen mit unverlierbaren physikalischen Eigenschaften	66
C.7 Spezielle Anmerkungen zu den Bauteilen mit unverlierbaren physikalischen Eigenschaften	66
Anhang D (informativ) Ergänzende technische Informationen.....	81
D.1 Einleitung	81

D.2 Erlangung der physikalischen internen Unabhängigkeit.....	81
D.3 Erlangung der physikalischen externen Unabhängigkeit.....	82
D.4 Beispiel für eine Methode zur Einzelausfallanalyse	83
D.5 Beispiel für eine Methode zur Mehrfachausfallanalyse	84
Anhang E (informativ) Techniken und Maßnahmen für sicherheitsrelevante elektronische Systeme für Signaltechnik zur Vermeidung von systematischen Fehlern und zur Beherrschung von zufälligen und systematischen Ausfällen	89
Literaturhinweise	98

Bilder

Bild 1 – Anwendungsbereich der Haupt-CENELEC-Normen für Bahnanwendungen.....	8
Bild 2 – Struktur der EN 50129	16
Bild 3 – Struktur des Sicherheitsnachweises	18
Bild 4 – Beispiel eines Systemlebenszyklus (aus EN 50126).....	20
Bild 5 – Beispiel der Entwurfs- und Validationsteile eines Systemlebenszyklus	22
Bild 6 – Festlegung von Unabhängigkeiten	23
Bild 7 – Struktur des technischen Sicherheitsberichts.....	28
Bild 8 – Sicherheitsanerkennungs- und -zulassungsverfahren.....	31
Bild 9 – Beispiele von Abhängigkeiten zwischen Sicherheitsnachweisen und Zulassungen	33
Bild A.1 – Sicherheitsanforderungen und Sicherheitsintegrität.....	35
Bild A.2 – Übersicht über den Gesamtprozess	37
Bild A.3 – Beispiel eines Risikoanalyseprozesses.....	38
Bild A.4 – Definition von Gefährdungen in Bezug auf die Systemgrenzen.....	39
Bild A.5 – Beispiel eines Gefährdungsbeherrschungsprozesses	41
Bild A.6 – Interpretation von Ausfall- und Reparaturraten	42
Bild A.7 – Behandlung von funktionaler Unabhängigkeit durch FTA.....	44
Bild A.8 – Beziehungen zwischen SILs, Techniken und Zahlenwerten.....	46
Bild B.1 – Die Unabhängigkeit beeinträchtigende Einflussfaktoren.....	54
Bild B.2 – Einzelausfälle, Offenbarung und sicherheitsgerichtete Ausfallreaktion	57
Bild D.1 – Beispiel einer Ausfallanalysenmethode	86

Tabellen

Tabelle A.1 – SIL-Tabelle.....	47
Tabelle C.1 – Widerstände.....	70
Tabelle C.2 – Kondensatoren	71
Tabelle C.3 – Elektromagnetische Bauteile	71
Tabelle C.4 – Dioden	73
Tabelle C.5 – Transistoren.....	74

Tabelle C.6 – Gesteuerte Gleichrichter	75
Tabelle C.7 – Überspannungsschutz.....	76
Tabelle C.8 – Optoelektronische Bauelemente	77
Tabelle C.9 – Filter.....	77
Tabelle C.10 – Verbindungszubehör	78
Tabelle C.11 – Sicherungen	79
Tabelle C.12 – Schalter und Taster	79
Tabelle C.13 – Lampen.....	79
Tabelle C.14 – Batterien	79
Tabelle C.15 – Umwandler (Transducer)/Sensoren	79
Tabelle C.16 – Integrierte Schaltkreise.....	80
Tabelle D.1 – Maßnahmen zur Ausfalloffenbarung in hochintegrierten Schaltungen mittels periodischer Online-Tests mit Vergleich (Software oder Hardware) in einem 2-von-n-System.....	87
Tabelle E.1 – Sicherheitsplanung und Qualitätssicherungstätigkeiten.....	91
Tabelle E.2 – Systemanforderungsspezifikation	91
Tabelle E.3 – Sicherheitsorganisation	92
Tabelle E.4 – Architektur des/der Systems/Teilsystems/Einrichtung	92
Tabelle E.5 – Entwurfsmerkmale.....	93
Tabelle E.6 – Risikoreduktion auf Systemelementebene	94
Tabelle E.7 – Entwurf und Entwicklung des/der Systems/Teilsystems/Einrichtung	95
Tabelle E.8 – Entwurfsphasendokumentation	95
Tabelle E.9 – Verifikation und Validation des Systems und Produktentwurfs	96
Tabelle E.10 – Anwendung, Betrieb und Instandhaltung	97

Einleitung

Dieses Dokument ist die erste Europäische Norm, die Anforderungen für die Anerkennung und Zulassung von sicherheitsrelevanten elektronischen Systemen im Eisenbahnbereich definiert. Bis jetzt existierten auf diesem Gebiet nur einige sich unterscheidende nationale Empfehlungen und allgemeine Empfehlungen der UIC (Internationale Vereinigung der Eisenbahnen).

Sicherheitsrelevante elektronische Systeme für Signaltechnik umfassen Hardware- und Softwareaspekte. Für den Aufbau vollständiger sicherheitsrelevanter Systeme sind beide Teile innerhalb des gesamten Lebenszyklus des Systems zu betrachten. Die Anforderungen für sicherheitsrelevante Hardware und für das Gesamtsystem sind in dieser Norm definiert. Andere Anforderungen sind in verwandten CENELEC-Normen definiert.

Das Ziel der Europäischen Eisenbahnverwaltungen und der Europäischen Eisenbahnindustrie ist es, kompatible Eisenbahnsysteme auf der Grundlage gemeinsamer Normen zu entwickeln. Deshalb ist die gegenseitige Anerkennung von Sicherheitszulassungen für Teilsysteme und Einrichtungen durch unterschiedliche nationale Eisenbahnverwaltungen notwendig. Dieses Dokument ist die gemeinsame europäische Grundlage für die Sicherheitsanerkennung und -zulassung von elektronischen Systemen für Eisenbahnsignalanwendungen.

Die gegenseitige Anerkennung ist auf die generische Zulassung und nicht auf spezifische Anwendungen gerichtet. Öffentliche Ausschreibungen innerhalb der Europäischen Gemeinschaft betreffend sicherheitsrelevante elektronische Systeme für Eisenbahnsignalanwendungen werden in Zukunft auf diese Norm verweisen, wenn sie zur Europäischen Norm (EN) geworden ist.

Die Norm besteht aus einem Hauptteil ([Abschnitte 1 bis 5](#)) und den [Anhängen A, B, C, D](#) und [E](#). Die Anforderungen, definiert im Hauptteil dieser Norm und in den Anhängen [A, B](#) und [C](#), sind normativ, während die Anhänge [D](#) und [E](#) informativ sind.

Diese Europäische Norm ist im Einklang mit der [EN 50126](#) „Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS)“ und nutzt deren relevante Abschnitte. Diese Norm und [EN 50126](#) basieren auf dem Systemlebenszyklus und sind in Einklang mit [EN 61508-1](#), an deren Stelle die Normen [EN 50126/EN 50128/EN 50129](#) treten, wenn es sich um Telekommunikations-, Signal- und Datenverarbeitungssysteme der Eisenbahnen handelt. Wenn die Anforderungen dieser Normen erfüllt werden, ist eine weitere Bewertung der Übereinstimmung mit [EN 61508-1](#) nicht erforderlich.

Da sich diese Norm mit dem zu erbringenden Nachweis für die Anerkennung von sicherheitsrelevanten Systemen befasst, spezifiziert sie jene Lebenszyklusaktivitäten, die vor der Anerkennung erfüllt sein müssen, gefolgt von zusätzlich geplanten Aktivitäten, die danach auszuführen sind. Deswegen ist der Nachweis der Sicherheit über den gesamten Lebenszyklus erforderlich.

Diese Norm befasst sich mit der Art des Nachweises, der zu erbringen ist. Von wenigen Ausnahmen abgesehen, legt sie nicht fest, wer die notwendigen Arbeiten durchführen muss, denn dies kann von Fall zu Fall unterschiedlich sein.

Für sicherheitsrelevante Systeme, die programmierbare Elektronik enthalten, sind zusätzliche Bedingungen für die Software in [EN 50128](#) „Bahnanwendungen – Software für Eisenbahnsteuerungs- und Überwachungssysteme“ definiert.

Zusätzliche Anforderungen für sicherheitsrelevante Datenkommunikation sind in [EN 50159-1](#) und [EN 50159-2](#) definiert.

1 Anwendungsbereich

Diese Europäische Norm ist anwendbar auf sicherheitsrelevante elektronische Systeme (einschließlich Teilsysteme und Einrichtungen) für Eisenbahnsignalanwendungen.

Der Anwendungsbereich dieser Europäischen Norm und ihre Beziehung zu anderen CENELEC-Normen werden in [Bild 1](#) gezeigt.

Diese Europäische Norm ist für die Anwendung auf alle sicherheitsrelevanten Eisenbahnsignalsysteme, -Teilsysteme und -Einrichtungen gedacht. Für alle Eisenbahnsignalsysteme, -Teilsysteme und -Einrichtungen sind jedoch Gefährdungsanalyse und Risikobewertungsprozesse, wie in [EN 50126](#) und in dieser Norm definiert, notwendig, um die Sicherheitsanforderungen zu identifizieren. Zeigt die Analyse, dass es keine Sicherheitsanforderungen gibt (d. h., dass die Situation nicht sicherheitsrelevant ist), und muss diese Schlussfolgerung als Konsequenz späterer Änderungen nicht revidiert werden, braucht diese Sicherheitsnorm nicht mehr angewendet zu werden.

Diese Europäische Norm gilt für Spezifikation, Entwurf, Konstruktion, Installation, Abnahme, Betrieb, Instandhaltung und Änderung bzw. Erweiterung von kompletten Signalsystemen und auch für einzelne Teilsysteme und Einrichtungen innerhalb eines Gesamtsystems. Für elektronische Bauteile enthält [Anhang C](#) entsprechende Verfahren.

Diese Europäische Norm gilt für generische Teilsysteme und Einrichtungen (sowohl anwendungsunabhängig als auch für eine bestimmte Klasse von Anwendungen vorgesehen) sowie für anwendungsspezifische Systeme/Teilsysteme/Einrichtungen.

Diese Europäische Norm ist nicht anwendbar auf vorhandene Systeme/Teilsysteme/Einrichtungen (d. h. solche, die schon vor der Erstellung dieser Norm anerkannt wurden). Soweit vernünftigerweise machbar, sollte diese Norm jedoch auf Änderungen und Erweiterungen solcher Systeme, Teilsysteme und Einrichtungen angewendet werden.

Diese Europäische Norm ist vorwiegend anwendbar auf Systeme/Teilsysteme/Einrichtungen, die speziell für Eisenbahnsignalanwendungen entworfen und gefertigt wurden. Soweit vernünftigerweise machbar, sollte sie auch auf handelsübliche Einrichtungen (z. B. Stromversorgungen, Modems usw.) angewendet werden, die als Teil des sicherheitsrelevanten Signalsystems genutzt werden. In solchen Fällen muss mindestens der Nachweis erbracht werden

entweder dass die Einrichtungen nicht sicher sein müssen,

oder dass man sich bei den Einrichtungen im Hinblick auf die Funktionen, die sicherheitsrelevant sind, verlassen kann.

Diese Europäische Norm ist anwendbar auf die funktionale Sicherheit von Eisenbahnsignalsystemen. Sie befasst sich nicht mit der Arbeitssicherheit des Personals; dieses ist Gegenstand von anderen Normen.

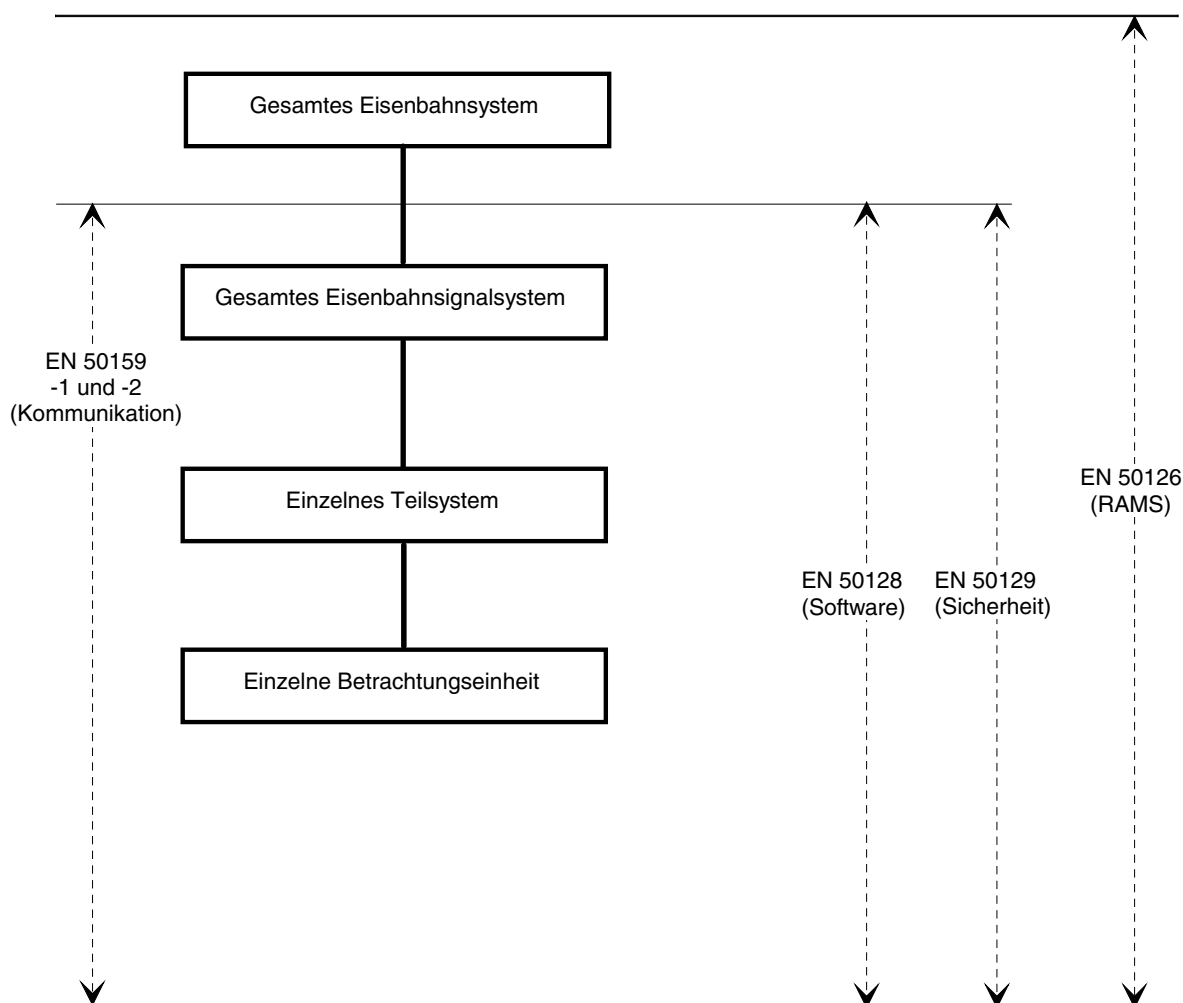


Bild 1 – Anwendungsbereich der Haupt-CENELEC-Normen für Bahnanwendungen

2 Normative Verweisungen

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

ANMERKUNG Zusätzliche informative Verweisungen sind in den Literaturhinweisen zu finden.

EN 50121 Reihe, *Railway applications: Electromagnetic compatibility (EMC) – Rolling stock*

EN 50124-1:2001, *Railway applications: Insulation co-ordination – Part 1: Overvoltages and creepage distances*

EN 50124-2:2001, *Railway applications: Insulation co-ordination – Part 2: Overvoltage and related protection*

EN 50125-1:1999, *Railway applications: Environmental conditions for equipment – Equipment on board rolling stock*

EN 50125-3:2003, *Railway applications: Environmental conditions for equipment – Signalling and communications*

EN 50126:1999, *Railway applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*

EN 50128:2001, *Railway applications: Software for railway control and protection systems*

EN 50155:2001, *Railway applications: Electronic equipment used on rail vehicles*

EN 50159-1:2001, *Railway applications: Signalling and communications – Safety-related communication in closed transmission systems*

EN 50159-2:2001, *Railway applications: Signalling and communications – Safety-related communication in open transmission systems*

EN 61508-1:2001, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 60664 Reihe, *Insulation coordination for equipment within low-voltage systems*

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieser Norm gelten die folgenden Begriffe.

3.1.1

Unfall

ein nicht beabsichtigtes Ereignis oder eine Reihe von Ereignissen mit der Folge von Toten, von Verletzten, des Verlustes eines Systems oder von Umweltschäden

3.1.2

Begutachtung

Analyseprozess zur Feststellung, ob die Entwurfsinstanz und der Validierer ein Produkt zustande gebracht haben, das die spezifizierten Anforderungen erfüllt, und um zu beurteilen, ob das Produkt für seinen gedachten Anwendungszweck geeignet ist

3.1.3

Bevollmächtigung

formale Erlaubnis, ein Produkt innerhalb der spezifizierten Anwendungsgrenzen zu verwenden

3.1.4

Verfügbarkeit

Fähigkeit eines Produktes, in einem Zustand zu sein, in dem es zu einem vorgegebenen Zeitpunkt oder während eines vorgegebenen Zeitintervalls eine geforderte Funktion unter vorgegebenen Bedingungen erfüllen kann, vorausgesetzt, dass die erforderlichen äußeren Mittel bereitgestellt sind

3.1.5

kann

ist möglich

3.1.6

Ursachenanalyse

Analyse der Gründe, wie und warum eine besondere Gefährdung zustande kommt

3.1.7

gleichartig wirkender Ausfall (common-cause failure)

gemeinsamer Ausfall in mehreren Betrachtungseinheiten, die unabhängig voneinander sein sollten

3.1.8

Konsequenzanalyse

Analyse von Ereignissen, die wahrscheinlich passieren werden, nachdem eine Gefährdung aufgetreten ist

3.1.9

Projektierung

Strukturieren und Verbinden der Hard- und Software eines Systems für seine beabsichtigte Anwendung

3.1.10

gegenseitige Anerkennung

Zustand eines Produktes, den es mit der Anerkennung durch eine Behörde nach den zuständigen Europäischen Normen erreicht und in dem es durch andere Behörden ohne weitere Begutachtungen ebenfalls anerkannt werden kann

3.1.11

Entwurf

durchgeführte Tätigkeit, um spezifizierte Anforderungen zu analysieren und in akzeptable Entwurfslösungen zu transformieren, die die geforderte Sicherheitsintegrität haben

3.1.12

Entwurfsabteilung

Stelle, die verantwortlich für die Formulierung eines Entwurfs zur Erfüllung der spezifizierten Anforderungen und für die Beaufsichtigung der folgenden Entwicklung und Inbetriebsetzung eines Systems in seiner vorgesehenen Umgebung ist

3.1.13

Diversität

Mittel, alle oder Teile der spezifizierten Anforderungen auf mehr als eine unabhängige und unterschiedliche Art und Weise zu erreichen

3.1.14

Einrichtung

funktionale, physische Betrachtungseinheit

3.1.15

Fehlzustand (error)

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

3.1.16

Fehlersicherheit (fail-safe)

Konzept, das in den Entwurf eines Produktes so einfließt, dass bei Eintreten einer Fehlfunktion ein sicherer Zustand eingenommen oder beibehalten wird

3.1.17

Fehlfunktion/Fehler (failure)

Abweichung vom spezifizierten Verhalten des Systems. Eine/ein Fehlfunktion/Ausfall ist die Folge einer Fehlerursache (fault) oder eines Fehlzustandes (error) im System.

3.1.18

Ausfall/Fehlerursache (fault)

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

3.1.19

Ausfalloffenbarungszeit

Zeitspanne, die zu dem Zeitpunkt beginnt, an dem ein Ausfall auftritt, und die endet, wenn das Vorhandensein dieses Ausfalls erkannt wird

3.1.20

Funktion

Art von Aktion oder Tätigkeit, durch die ein Produkt seinen beabsichtigten Zweck erfüllt

3.1.21**Gefährdung**

Bedingung, die zu einem Unfall führen kann

3.1.22**Gefährdungsanalyse**

Prozess der Identifikation von Gefährdungen und der Analyse ihrer Ursache sowie der Ableitung von Anforderungen, um die Wahrscheinlichkeit und die Folgen von Gefährdungen auf ein akzeptables Maß zu begrenzen

3.1.23**Gefährdungslogbuch**

Dokument, in dem alle Aktivitäten des Sicherheitsmanagements, erkannte Gefährdungen, getroffene Entscheidungen und verwendete Lösungen aufgezeichnet bzw. referenziert werden

3.1.24**menschliches Versagen**

menschliche Handlung, die zu einem ungewollten Verhalten des Systems oder zu einer Fehlfunktion führen kann

3.1.25**Implementierung**

durchgeführte Tätigkeit, um die spezifizierten Entwürfe in physikalische Realisierungen zu transformieren

3.1.26**Unabhängigkeit (funktional)**

Freisein von allen Mechanismen, die den korrekten Ablauf von mehr als einer Funktion auf Grund von systematischen oder zufälligen Fehlern beeinträchtigen können

3.1.27**Unabhängigkeit (personell)**

Freisein von Verwicklungen in dieselbe geistige, wirtschaftliche und/oder Managementeinheit

3.1.28**Unabhängigkeit (physikalisch)**

Freisein von allen Mechanismen, die das korrekte Arbeiten von mehr als einem/r System/Teilsystem/Einrichtung auf Grund von zufälligen Fehlern beeinträchtigen können

3.1.29**individuelles Risiko**

Risiko, dass nur auf ein einzelnes Individuum bezogen ist

3.1.30**Instandhaltbarkeitsmaß**

Wahrscheinlichkeit, dass unter festgelegten Bedingungen und bei Anwendung festgelegter Verfahren und Mittel eine geforderte aktive Instandhaltungsmaßnahme an einer unter vorgegebenen Anwendungsbedingungen genutzten Betrachtungseinheit innerhalb eines festgelegten Zeitintervalls ausgeführt wird

3.1.31**Instandhaltung**

Kombination aller technischen und administrativen Maßnahmen einschließlich Überwachungsmaßnahmen, mit denen eine Betrachtungseinheit im funktionsfähigen Zustand erhalten oder in ihn zurückversetzt werden soll

3.1.32**darf**

ist zulässig

3.1.33**sicherheitsgerichtete Ausfallreaktion (negation)**

Herbeiführen eines sicheren Zustandes, nachdem ein gefährlicher Ausfall entdeckt wurde

3.1.34

Reaktionszeit bis zum Erreichen des sicheren Zustandes (negation time)

Zeitspanne, die mit dem Entdecken eines Ausfalls beginnt und mit der Einnahme eines sicheren Zustandes endet

3.1.35

Produkt

Anzahl von Elementen, die so miteinander zu einem System, Teilsystem oder einer Betrachtungseinheit verbunden sind, dass die spezifizierten Anforderungen erfüllt werden

3.1.36

Qualität

Wahrnehmung der Eigenschaften und Merkmale eines Produktes durch den Nutzer

3.1.37

Eisenbahnverwaltung

Stelle, die gegenüber der Sicherheitsbehörde die Gesamtverantwortung für einen sicheren Eisenbahnbetrieb trägt

3.1.38

Sicherheit gegen zufällige Fehler

Grad, mit dem ein System frei von gefährlichen zufälligen Ausfällen ist

3.1.39

Ausfall, zufälliger

nicht vorhersehbares Eintreten eines Ausfalls

3.1.40

Redundanz

Bereitstellung von einer oder mehreren zusätzlichen, gewöhnlich identischen Maßnahmen, um die Fehlertoleranz zu erhalten

3.1.41

Zuverlässigkeit

Fähigkeit einer Betrachtungseinheit, eine geforderte Funktion unter gegebenen Bedingungen für eine gegebene Zeitdauer zu erbringen

3.1.42

Reparatur

Maßnahmen zur Wiederherstellung des geforderten Zustandes eines Systems, Teilsystems oder einer Einrichtung nach einem Ausfall/Fehler

3.1.43

Risiko

Kombination aus Häufigkeit oder Wahrscheinlichkeit und den Folgen eines spezifizierten gefährlichen Ereignisses

3.1.44

sicherer Zustand

Zustand, der die Sicherheit weiterhin bewahrt

3.1.45

Sicherheit

Freisein von nicht akzeptierbaren Risiken eines Schadens

3.1.46

Sicherheitsanerkennung

Sicherheitszustand, der einem Produkt durch den Endanwender zuerkannt wird

3.1.47**Sicherheitszulassung**

Sicherheitszustand, der einem Produkt durch die zuständige Behörde zuerkannt wird, wenn das Produkt einen Satz festgelegter Bedingungen erfüllt hat

3.1.48**Sicherheitsbehörde**

die Stelle, die verantwortlich für das Erteilen der Berechtigung zum Betrieb des sicherheitsrelevanten Systems ist

3.1.49**Sicherheitsnachweis**

dokumentierter Nachweis, dass ein Produkt die spezifizierten Sicherheitsanforderungen erfüllt

3.1.50**Sicherheitsintegrität**

die Fähigkeit eines sicherheitsrelevanten Systems, seine geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb einer festgelegten betrieblichen Umgebung und innerhalb eines festgelegten Zeitintervalls zu erbringen

3.1.51**Sicherheitsanforderungsstufe**

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

3.1.52**Sicherheitslebenszyklus**

für sicherheitsrelevante Systeme zusätzlich durchzuführende Tätigkeiten in Verbindung mit dem Systemlebenszyklus

3.1.53**Sicherheitsmanagement**

Managementstruktur, die sicherstellt, dass der Sicherheitsprozess richtig umgesetzt wird

3.1.54**Sicherheitsplan**

Plan mit den Ausführungseinzelheiten dafür, wie die Sicherheitsanforderungen des Projektes erreicht werden

3.1.55**Sicherheitsprozess**

Reihe von Verfahren, deren Abfolge sicherstellt, dass die Sicherheitsanforderungen eines Produktes identifiziert und erfüllt werden

3.1.56**sicherheitsrelevant**

trägt Sicherheitsverantwortung

3.1.57**muss**

ist notwendig

3.1.58**sollte**

ist empfohlen

3.1.59**Signalsystem**

spezielle Art eines bei der Eisenbahn benutzten Systems, um den Betrieb von Zügen zu steuern und zu sichern

3.1.60

Beanspruchungsprofil

Grad und Anzahl der externen Einflüsse, denen ein Produkt während der Erfüllung seiner geforderten Funktionalität widerstehen kann

3.1.61

Teilsystem

Teil eines Systems, der eine spezielle Funktion erfüllt

3.1.62

System

Menge von Teilsystemen, die entsprechend einem Entwurf zusammenwirken

3.1.63

Sicherheit gegen systematische Fehler

der Grad, in dem ein System frei von nicht identifizierten gefährlichen Fehlzuständen ist, und die Ursachen dafür

3.1.64

Fehler, systematischer

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

3.1.65

Systemlebenszyklus

Reihe von Tätigkeiten, die während eines Zeitraumes durchgeführt werden, der mit dem Konzept für ein System beginnt und mit der Stilllegung, nach der das System nicht mehr nutzbar ist, endet

3.1.66

technischer Sicherheitsbericht

dokumentierter technischer Nachweis für die Sicherheit des Entwurfs eines Systems, Teilsystems oder einer Betrachtungseinheit

3.1.67

Validation

auf Tests und Analysen beruhender Nachweis, dass das Produkt in allen Belangen seine spezifizierten Anforderungen erfüllt

3.1.68

Verifikation

die auf Analyse und Test beruhende Feststellung in jeder Phase des Lebenszyklus, dass die Anforderungen der betrachteten Phase das Ergebnis der vorausgehenden Phase erfüllen und dass das Ergebnis der betrachteten Phase die Anforderungen erfüllt.

3.2 Abkürzungen

Für diese Norm gelten die folgenden Abkürzungen:

3.2.1	AC	(alternating current)	Wechselstrom
3.2.2	ATP	(automatic train protection)	automatische Zugbeeinflussung
3.2.3	CENELEC	(Comité Européen de Normalisation Electrotechnique)	Europäisches Komitee für elektrotechnische Normung
3.3.4	CCF	(common cause failure)	Ausfall auf Grund einer gemeinsamen Ursache
3.2.5	DC	(direct current)	Gleichstrom
3.2.6	EMC	(electromagnetic compatibility)	Elektromagnetische Verträglichkeit
3.2.7	EMI	(electromagnetic interference)	Elektromagnetische Beeinflussung
3.2.8	EN		Europäische Norm

3.2.9	ESD	(electrostatic discharge)	elektrostatische Entladung
3.2.10	FET		Feldeffekttransistor
3.2.11	FMEA	(failure mode and effects analysis)	Ausfalleffektanalyse
3.2.12	FR	(failure rate)	Ausfallrate
3.2.13	FTA	(fault tree analysis)	Fehlerbaumanalyse
3.2.14	H	(hazard)	Gefährdung
3.2.15	HW	(hardware)	Hardware
3.2.16	IEC	(International Electrotechnical Commission)	Internationale Elektrotechnische Kommission
3.2.17	IRSE	(Institution of Railway Signal Engineers)	Verband der Eisenbahn-Signalingenieure
3.2.18	ISO	(International Organization for Standardization)	Internationale Organisation für Normung
3.2.19	RAMS	(reliability, availability, maintainability and safety)	Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit
3.2.20	SCR	(silicon controlled rectifier)	Thyristor
3.2.21	SDR	(safe down rate)	sichere Unklarrate
3.2.22	SDT	(safe down time)	sichere Unklardauer
3.2.23	SIL	(safety integrity level)	Sicherheitsanforderungsstufe
3.2.24	SW	(software)	Software
3.2.25	THR	(tolerable hazard rate)	tolerierbare Gefährdungsrate
3.2.26	UIC	(International Union of Railways)	Internationaler Eisenbahnverband
3.2.27	VDR	(voltage dependent resistor)	spannungsabhängiger Widerstand

4 Gesamtrahmen dieser Europäischen Norm

Abschnitt 5 dieser Europäischen Norm fordert ein systematisches, dokumentiertes Vorgehen für

- den Nachweis des Qualitätsmanagements;
- den Nachweis des Sicherheitsmanagements;
- den Nachweis der funktionalen und technischen Sicherheit;
- die Sicherheitsanerkennung und -zulassung.

Anhang A (normativ) definiert die Interpretation und die Verwendung der Sicherheitsanforderungsstufen (SIL).

Anhang B (normativ) enthält detaillierte technische Anforderungen für sicherheitsrelevante Systeme/Teilsysteme/Einrichtungen.

Anhang C (normativ) enthält Verfahren und Informationen über anzunehmende Ausfallarten für Bauteile.

Anhang D (informativ) enthält ergänzende technische Informationen.

Anhang E (informativ) enthält Tabellen von zu nutzenden Techniken und Maßnahmen bei den verschiedenen Sicherheitsanforderungsstufen.

Literaturhinweise (informativ) enthalten Referenzen auf Dokumente, die während der Erstellung dieser Norm in Betracht gezogen wurden.

Die Struktur dieser Europäischen Norm ist in Bild 2 zusammengefasst.

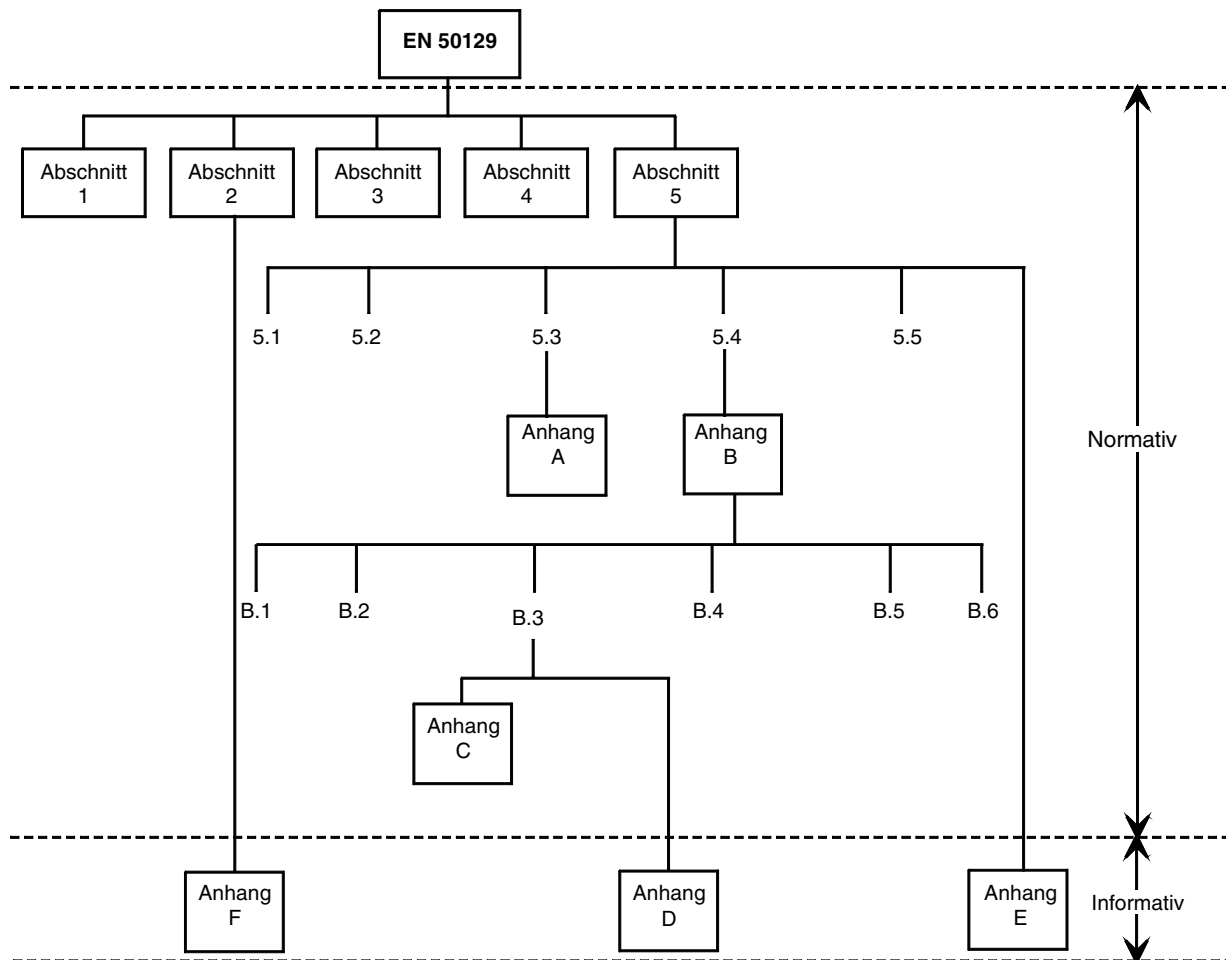


Bild 2 – Struktur der EN 50129

5 Bedingungen für die Sicherheitsanerkennung und -zulassung

5.1 Der Sicherheitsnachweis

Diese Europäische Norm definiert die Bedingungen, die ein sicherheitsrelevantes elektronisches System, Teilsystem oder eine Betrachtungseinheit der Eisenbahn erfüllen muss, um für die vorgesehene Anwendung als angemessen sicher anerkannt zu werden.

Die Bedingungen für die Sicherheitsabnahme werden in dieser Norm unter folgenden Überschriften zusammengefasst:

- 5.2 Nachweis des Qualitätsmanagements;
- 5.3 Nachweis des Sicherheitsmanagements;
- 5.4 Nachweis der funktionalen und technischen Sicherheit.

Alle diese Bedingungen müssen auf Einrichtungs-, Teilsystem- und System-Ebene erfüllt sein, bevor das sicherheitsrelevante System als angemessen sicher anerkannt werden kann.

Der dokumentierte Nachweis, dass diese Bedingungen erfüllt wurden, muss in einem strukturierten Dokument der Sicherheitsbegründung enthalten sein, das Sicherheitsnachweis genannt wird. Der Sicherheitsnachweis bildet einen Teil der gesamten Nachweisdokumentation, die der zuständigen Sicherheitsbehörde unterbreitet wird, um die Sicherheitszulassung für ein generisches Produkt, eine Klasse von Anwendungen oder für eine spezifische Anwendung zu erlangen. Zur Erklärung des Sicherheitszulassungsverfahrens siehe [5.5](#).

Der Sicherheitsnachweis enthält den dokumentierten Nachweis der Sicherheit für ein System, Teilsystem oder die Betrachtungseinheit einer Einrichtung und muss folgendermaßen strukturiert sein:

Teil 1 Definition des Systems (Teilsystem/Einrichtung)

Hier muss das System, Teilsystem oder die Einrichtung, auf das/die sich der Sicherheitsnachweis bezieht, genau definiert oder referenziert werden, einschließlich Versionsnummern und Änderungsstatus aller Anforderungs-, Entwurfs- und Anwendungsdokumentationen.

Teil 2 Qualitätsmanagementbericht

Dieser Teil muss den Nachweis des Qualitätsmanagements, wie in [5.2](#) spezifiziert, enthalten.

Teil 3 Sicherheitsmanagementbericht

Dieser Teil muss den Nachweis des Sicherheitsmanagements, wie in [5.3](#) spezifiziert, enthalten.

Teil 4 Technischer Sicherheitsbericht

Dieser Teil muss den Nachweis der funktionalen und technischen Sicherheit, wie in [5.4](#) spezifiziert, enthalten.

Teil 5 Beziehungen zu anderen Sicherheitsnachweisen

Dieser Teil muss die Bezüge zu Sicherheitsnachweisen von allen Teilsystemen oder Einrichtungen, von denen der Hauptsicherheitsnachweis abhängt, enthalten.

Dieser Teil muss ebenso aufzeigen, dass die sicherheitsbezogenen Anwendungsbedingungen, die in den zugehörigen Teilsystem- bzw. Einrichtungssicherheitsnachweisen spezifiziert sind,

entweder im Hauptsicherheitsnachweis erfüllt sind

oder in die sicherheitsbezogenen Anwendungsbedingungen des Hauptsicherheitsnachweises übernommen wurden.

Teil 6 Zusammenfassung

Dieser Teil muss den in den vorangegangenen Teilen erbrachten Nachweis zusammenfassen und bestätigen, dass das/die betreffende System/Teilsystem/Einrichtung bei Erfüllung der festgelegten Anwendungsbedingungen angemessen sicher ist.

Die Struktur des Sicherheitsnachweises ist in [Bild 3](#) dieser Norm gezeigt.

Der Sicherheitsnachweis braucht keine umfangreichen, detaillierten Nachweise und unterstützende Dokumentationen enthalten, wenn in ihm auf entsprechende Dokumente genau verwiesen wird und wenn die verwendeten Basiskonzepte und Verfahren eindeutig spezifiziert sind.

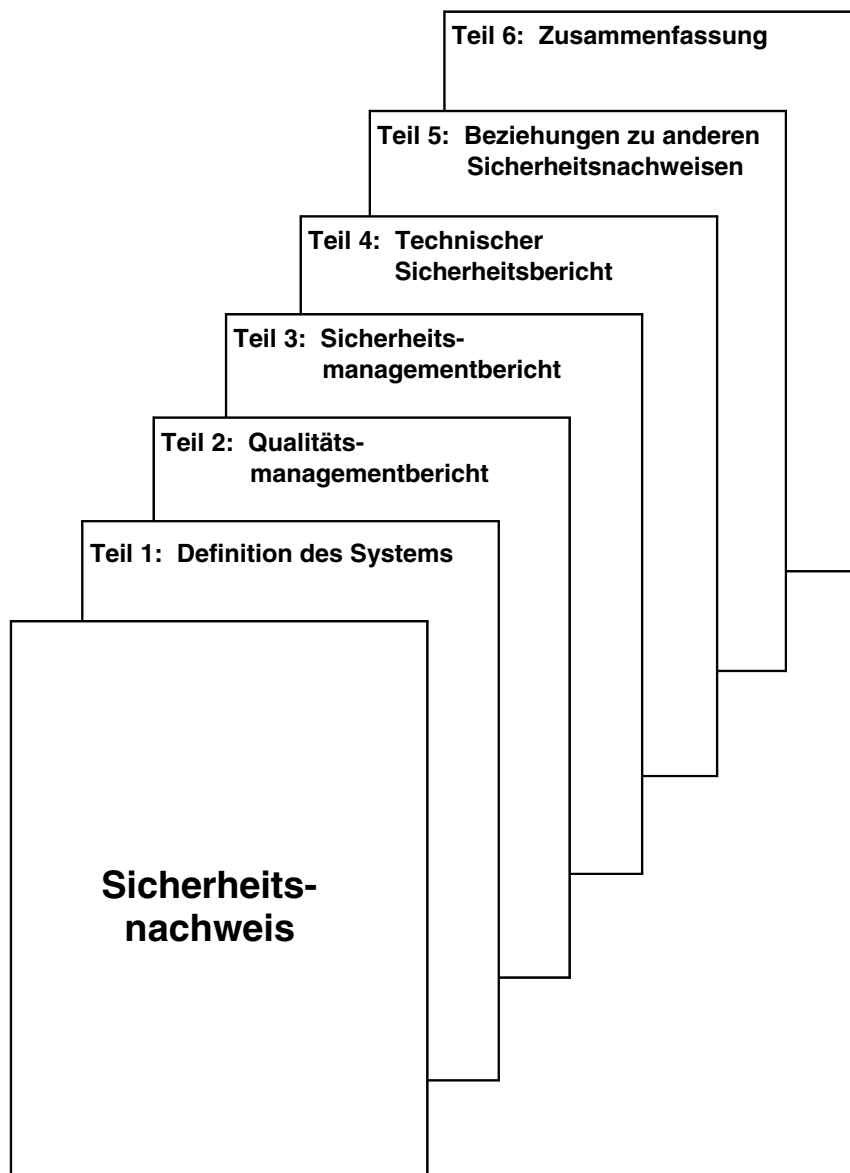


Bild 3 – Struktur des Sicherheitsnachweises

5.2 Nachweis des Qualitätsmanagements

Die erste Bedingung, die für die Sicherheitsanerkennung erfüllt sein muss, besteht darin, dass die Qualität des Systems, Teilsystems oder der Einrichtung durch ein entsprechendes Qualitätsmanagementsystem gewährleistet wurde und weiterhin über den gesamten Lebenszyklus gewährleistet wird. Der dokumentierte Nachweis muss im Qualitätsmanagementbericht erfolgen, der Teil 2 des Sicherheitsnachweises bildet.

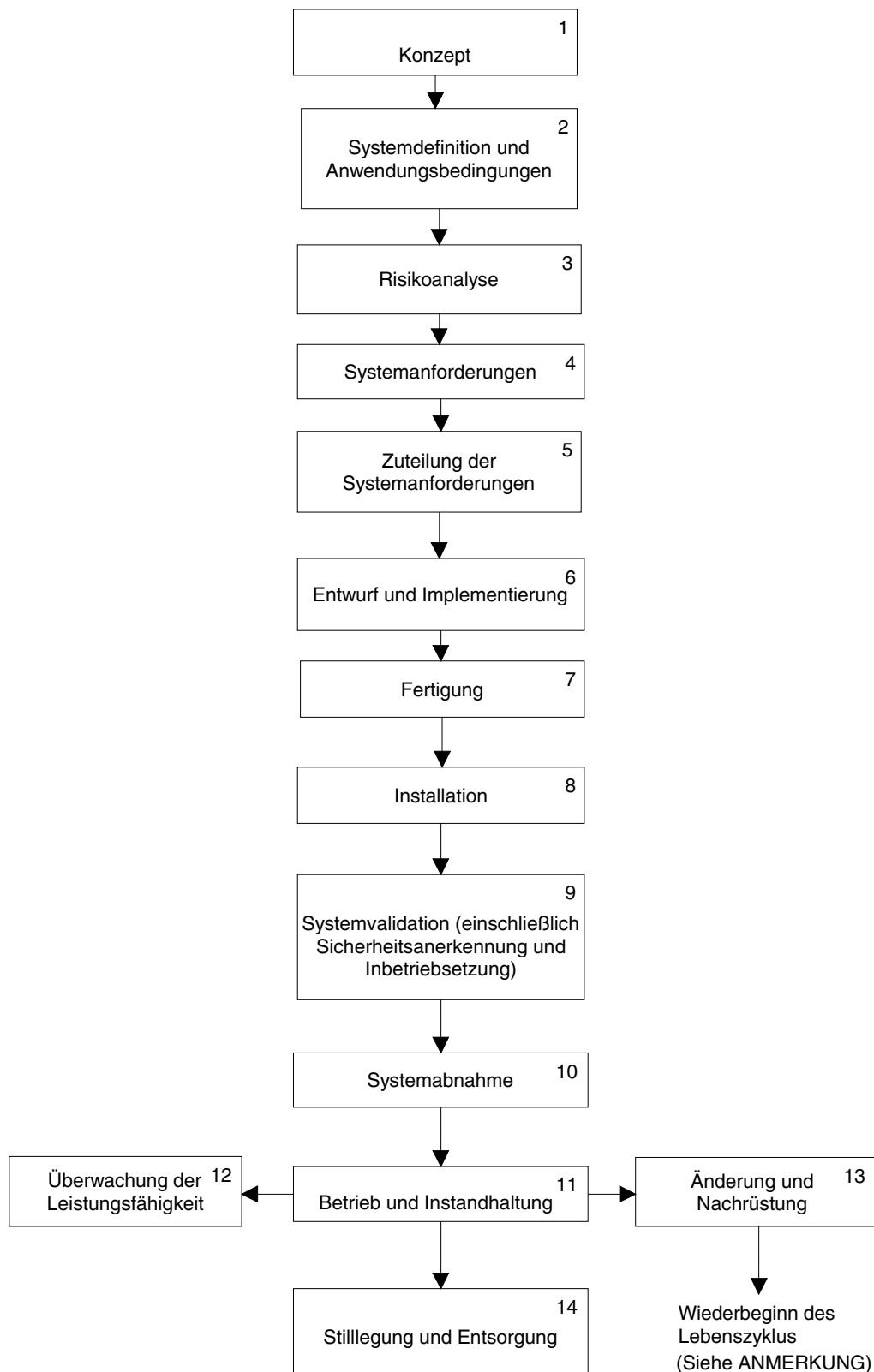
Der Zweck des Qualitätsmanagementsystems ist es, die Häufigkeit menschlichen Versagens in jeder Stufe des Lebenszyklus zu minimieren und damit das Risiko von systematischen Fehlern in dem System, Teilsystem oder der Einrichtung zu reduzieren.

Das Qualitätsmanagementsystem muss über den gesamten Lebenszyklus des/der Systems/Teilsystems/Einrichtung hinweg anwendbar sein, so wie in [EN 50126](#) definiert. Das Beispiel für einen Lebenszyklus eines Systems (aus [EN 50126](#)) wird in [Bild 4](#) dieser Norm wiedergegeben.

ANMERKUNG Aspekte, die durch das Qualitätsmanagementsystem gesteuert und in den Qualitätsmanagementbericht aufgenommen werden sollten, sind z. B.:

- Organisationsstruktur;
- Qualitätsplanung und -verfahren;
- Spezifikation von Anforderungen;
- Entwurfskontrolle;
- Entwurfsverifikation und Review;
- anwendungsorientiertes Engineering;
- Beschaffung und Fabrikation;
- Produktidentifikation und Verfolgbarkeit;
- Handhabung und Lagerung;
- Inspektion und Test;
- Nichtübereinstimmung und Korrekturmaßnahmen;
- Verpackung und Lieferung;
- Installation und Inbetriebnahme;
- Betrieb und Instandhaltung;
- Qualitätsüberwachung und Rückkopplung;
- Dokumentation und Protokolle;
- Konfigurationsmanagement/Änderungssteuerung;
- Mitarbeiterkompetenz und Ausbildung;
- Qualitäts-Audits und das Weiterverfolgen;
- Stilllegung und Entsorgung.

Die Übereinstimmung mit den Anforderungen eines Qualitätsmanagements ist verbindlich für die Sicherheitsanforderungsstufen 1 bis 4 (siehe [Anhang A](#) zur Erläuterung der Sicherheitsanforderungsstufen). Jedoch sollten die Tiefe der Darlegungen und der Umfang der begleitenden Dokumentation der Sicherheitsanforderungsstufe des/der betrachteten Systems/Teilsystems/Einrichtung angemessen sein (siehe [Tabellen E.1](#) und [E.8](#) als Richtlinien für die Nachweisführung entsprechend der Sicherheitsanforderungsstufe). Die Anforderungen für die Sicherheitsanforderungsstufe 0 (nicht sicherheitsrelevant) liegen außerhalb des Anwendungsbereiches dieser Sicherheitsnorm.



ANMERKUNG Die Phase, bei der eine Modifikation in den Lebenszyklus eingeführt wird, hängt sowohl von dem modifizierten System als auch von der spezifisch betrachteten Modifikation ab.

Bild 4 – Beispiel eines Systemlebenszyklus
(aus EN 50126)

5.3 Nachweis des Sicherheitsmanagements

5.3.1 Einführung

Die zweite Bedingung, die für die Sicherheitsanerkennung eines Systems, eines Teilsystems oder einer Einrichtung erfüllt sein muss, besteht darin, dass die Sicherheit durch einen wirkungsvollen Sicherheitsmanagementprozess, der mit dem Managementprozess für Verlässlichkeit für RAMS aus der [EN 50126](#) übereinstimmen sollte, gewährleistet wurde und weiterhin gewährleistet wird. Der Zweck dieses Prozesses ist es, das Eintreten sicherheitsrelevanten menschlichen Versagens innerhalb des Lebenszyklus weiter zu reduzieren und auf diese Weise das Restrisiko von sicherheitsrelevanten systematischen Fehlern zu minimieren. Die Elemente des Sicherheitsprozesses werden kurz zusammengefasst in 5.3.2 bis 5.3.13.

Der dokumentierte Nachweis der Übereinstimmung mit allen Elementen des Sicherheitsmanagementprozesses über den gesamten Lebenszyklus muss im Sicherheitsmanagementbericht erfolgen, der Teil 3 des Sicherheitsnachweises bildet. Der Sicherheitsmanagementbericht braucht keine umfangreichen, detaillierten Nachweise und unterstützenden Dokumentationen enthalten, wenn in ihm auf entsprechende Dokumente genau verwiesen wird.

Die Anwendung dieses Sicherheitsmanagementprozesses ist verbindlich für die Sicherheitsanforderungsstufen 1 bis 4 (siehe [Anhang A](#) zur Erläuterung der Sicherheitsanforderungsstufen). Jedoch sollten die Tiefe der Darlegungen und der Umfang der begleitenden Dokumentation der Sicherheitsanforderungsstufe des/der betrachteten Systems/Teilsystems/Einrichtung angemessen sein. Die Anforderungen für die Sicherheitsanforderungsstufe 0 (nicht sicherheitsrelevant) liegen außerhalb des Anwendungsbereiches dieser Sicherheitsnorm.

In allen Fällen sind Gefährdungsanalyse und Risikobewertungsprozesse, wie in [EN 50126](#) definiert, notwendig, um den benötigten Grad an Sicherheitsintegrität jeder einzelnen Situation zu identifizieren. Dies schließt jene Fälle mit ein, wo die Analyse und Bewertung offenbaren, dass die Sicherheitsanforderungsstufe 0 zugeordnet werden darf. Wenn man zu dieser Schlussfolgerung gelangt ist (d. h., die Situation ist nicht sicherheitsrelevant) und feststeht, dass die Stufe 0 bestehen bleibt, dann endet die Anwendbarkeit dieser Sicherheitsnorm.

5.3.2 Sicherheitslebenszyklus

Der Sicherheitsmanagementprozess muss aus einer Anzahl von Phasen und Tätigkeiten bestehen, welche zusammen den Sicherheitslebenszyklus bilden. Dieser sollte mit dem Systemlebenszyklus aus [EN 50126](#), wie er in [Bild 4](#) dieser Norm wiedergegeben ist, übereinstimmen. Die Entwurfs- und Validationsphase eines Systemlebenszyklus kann auch als „top-down“-Phase, gefolgt von einer „bottom-up“-Phase in Form eines „V“-Diagramms betrachtet werden, wie es als Beispiel in [Bild 5](#) gezeigt ist.

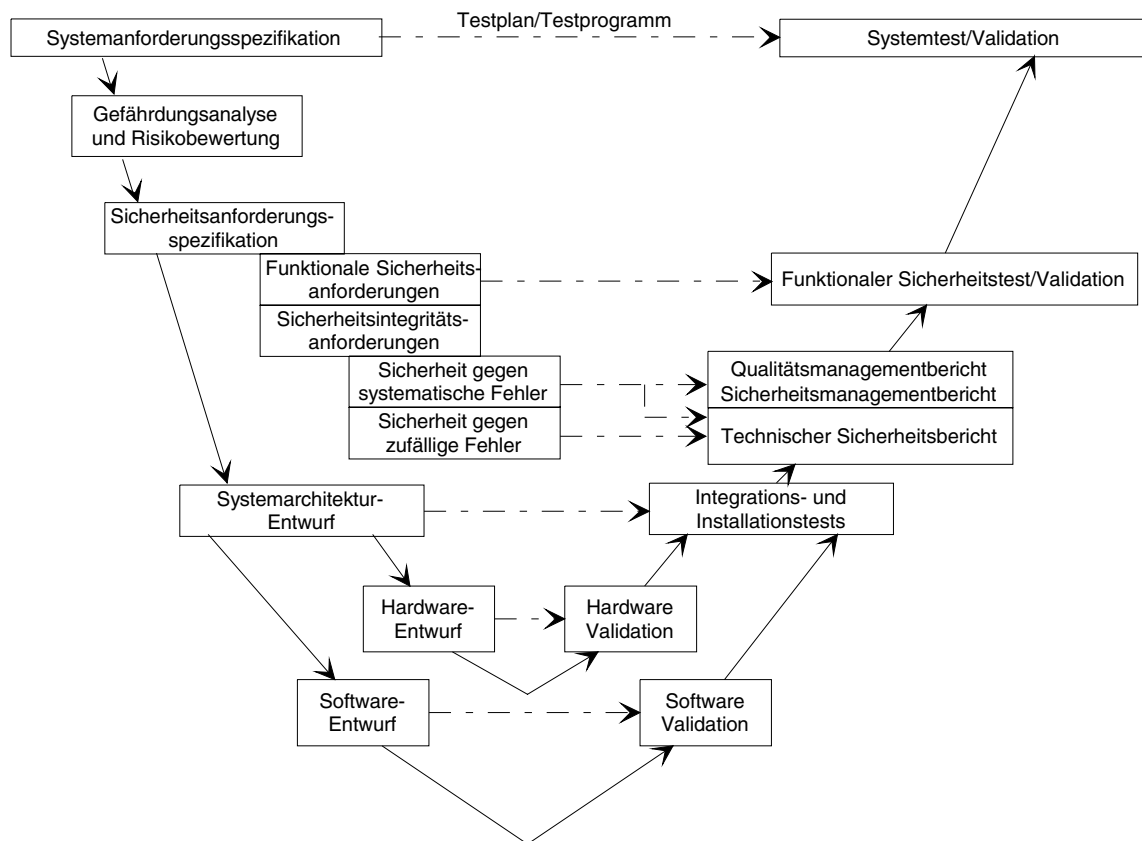
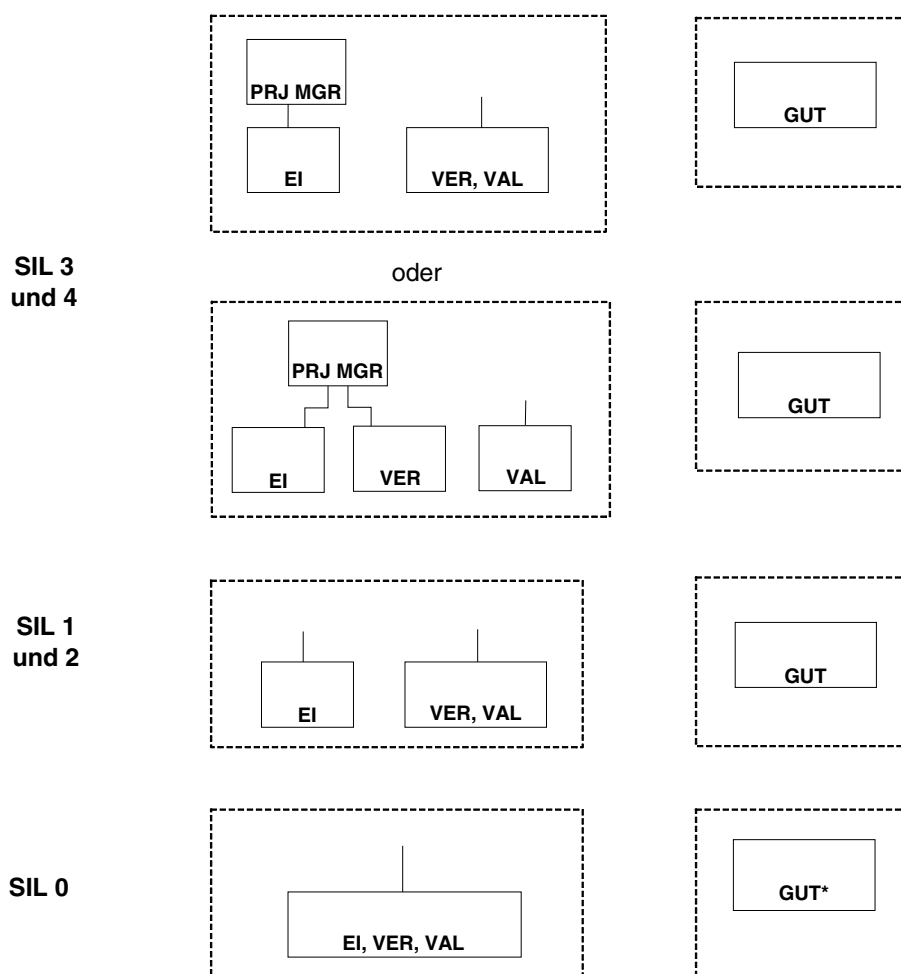


Bild 5 – Beispiel der Entwurfs- und Validationsteile eines Systemlebenszyklus

5.3.3 Sicherheitsorganisation

Der Sicherheitsmanagementprozess muss unter der Kontrolle einer geeigneten Sicherheitsorganisation, die aus fähigem Personal mit klarer Rollenverteilung besteht, ablaufen. Die Fähigkeiten des Personals, wie technisches Wissen, Qualifikation, Erfahrung auf dem Arbeitsgebiet, passende Ausbildung, müssen entsprechend den dafür zuständigen Normen eingeschätzt und dokumentiert werden. Ein entsprechender Grad an Unabhängigkeit zwischen den verschiedenen Rollen muss sichergestellt sein, wie in Bild 6 dargestellt (siehe auch Tabelle E.3 als Leitfaden für eine Sicherheitsorganisation, abhängig von der Sicherheitsanforderungsstufe).



Legende:

PRJ MGR = Projektmanager
 EI = Entwerfer
 VER = Verifizierer
 VAL = Validierer
 GUT = Gutachter



= Kann dieselbe Person sein



= Kann dieselbe Organisation sein

*

= Für SIL 0 ist ein Gutachter nur dann notwendig, wenn die Sicherheit des Gesamtsystems berührt sein könnte

Bild 6 – Festlegung von Unabhängigkeiten

5.3.4 Sicherheitsplan

Ein Sicherheitsplan muss zu Beginn des Lebenszyklus erstellt werden. Dieser Plan muss die Sicherheitsmanagementstruktur, sicherheitsrelevante Tätigkeiten und Zulassungs-Meilensteine während des Lebenszyklus sowie Anforderungen an die Überprüfung des Planes in geeigneten Zeitabständen enthalten. Der Sicherheitsplan muss nach Änderungen oder Ergänzungen des/der ursprünglichen Systems/Teilsystems/Einrichtung aktualisiert und überprüft werden. Wenn solche Änderungen durchgeführt werden, muss die Auswirkung auf die Sicherheit bewertet werden, angefangen an einer geeigneten Stelle des Lebenszyklus (siehe [Tabelle E.1](#) als Leitfaden für Sicherheitspläne entsprechend der Sicherheitsanforderungsstufe).

Der Sicherheitsplan muss alle Aspekte des/der Systems/Teilsystems/Einrichtung inklusive Hard- und Software behandeln. Er muss einen Software-Sicherheitsplan in Übereinstimmung mit [EN 50128](#) enthalten oder auf ihn verweisen.

Der Sicherheitsplan sollte einen Sicherheitsnachweisplan enthalten, in dem die vorgesehene Struktur und die hauptsächlichen Teile des endgültigen Sicherheitsnachweises angegeben sind.

5.3.5 Gefährdungslogbuch

Ein Gefährdungslogbuch muss erstellt und innerhalb des Sicherheitslebenszyklus geführt werden, wie in [EN 50126](#) angegeben. Es muss eine Liste aller erkannten Gefährdungen, zusammen mit der zugehörigen Risikoklassifizierung und Informationen über die Risikobeherrschung für jede Gefährdung enthalten. Das Gefährdungslogbuch muss nach Änderung oder Umbau des/der ursprünglichen Systems/Teilsystems/Einrichtung aktualisiert werden.

5.3.6 Sicherheitsanforderungsspezifikation

Die spezifischen Sicherheitsanforderungen für jedes/jeder System/Teilsystem/Einrichtung, einschließlich der Sicherheitsfunktionen und der Sicherheitsintegrität, müssen in der Spezifikation der Sicherheitsanforderungen genannt und dokumentiert werden.

Dies muss erreicht werden durch:

- Gefährdungserkennung und Analyse;
- Risikobewertung und -klassifizierung;
- Zuteilung der Sicherheitsanforderungsstufen,

wie in [EN 50126](#) erläutert. Einige Informationen zu den Sicherheitsanforderungsstufen von elektronischen Eisenbahnsystemen sind in [Anhang A](#) enthalten.

ANMERKUNG Die Sicherheitsanforderungsspezifikation kann Teil der Spezifikation der Funktionsanforderungen eines/einer Systems/Teilsystems/Einrichtung sein oder auch als eigenes Dokument geschrieben werden (siehe auch [Tabelle E.2](#) als Leitfaden für Systemanforderungsspezifikationen abhängig von der Sicherheitsanforderungsstufe).

5.3.7 System-/Teilsystem-/Einrichtungs-Entwurf

In dieser Phase des Lebenszyklus muss ein Entwurf erstellt werden, welcher die spezifizierten betrieblichen Anforderungen und Sicherheitsanforderungen erfüllt. Eine strukturierte „top-down“-Entwurfsmethode muss verwendet werden mit einer streng kontrollierten und überprüften Dokumentation. Insbesondere muss die Beziehung zwischen Hardware und Software, wie sie von der Software-Anforderungsspezifikation und der Software-/Hardware-Integration vorgegeben wird, exakt behandelt werden, und es muss die Norm [EN 50128](#) eingehalten werden. [Tabelle E.7](#) ist ein Leitfaden für Entwurf und Entwicklung von Systemen/Teilsystemen/Einrichtungen bezogen auf die Sicherheitsanforderungsstufen.

5.3.8 Sicherheitsreviews

Sicherheitsreviews müssen in entsprechenden Stadien des Lebenszyklus durchgeführt werden. Solche Reviews müssen im Sicherheitsplan spezifiziert und ihre Ergebnisse vollständig dokumentiert sein. Jede Änderung oder Erweiterung des ursprünglichen Systems, Teilsystems oder der Einrichtung muss ebenfalls einem Review unterzogen werden.

5.3.9 Sicherheitsverifikation und -validation

Der Sicherheitsplan muss Pläne mit Vorgaben zum Verifizieren enthalten oder sich darauf beziehen, d. h., dass in jeder Phase des Lebenszyklus die in der vorhergehenden Phase erkannten spezifischen Sicherheitsanforderungen erfüllt sind und zum Validieren, d. h., dass das/die gesamte System/Teilsystem/Einrichtung die ursprüngliche Sicherheitsanforderungsspezifikation erfüllt.

Diese Aktivitäten müssen ausgeführt und vollständig dokumentiert werden, einschließlich geeigneter Tests und Sicherheitsanalysen. Sie müssen bei jeder späteren Änderung oder Ergänzung des/der Systems/Teilsystems/Einrichtung entsprechend wiederholt werden.

Der für den Verifizierer und den Validierer notwendige Grad an Unabhängigkeit muss in Übereinstimmung mit der Sicherheitsanforderungsstufe des/der betrachteten Systems/Teilsystems/Einrichtung sein. Dieses ist in Bild 6 gezeigt. Tabelle E.9 ist ein Leitfaden für Verifikations- und Validationstechniken und -maßnahmen entsprechend der Sicherheitsanforderungsstufe.

Der Gutachter darf nach Ermessen der Sicherheitsbehörde Teil der Hersteller- oder Kundenorganisation sein. In solchen Fällen muss der Gutachter

- durch die Sicherheitsbehörde autorisiert sein,
- absolut unabhängig vom Projektteam sein,
- direkt der Sicherheitsbehörde berichten.

5.3.10 Sicherheitsbegründung

Der Nachweis, dass das/die System/Teilsystem/Einrichtung die festgelegten Bedingungen für die Sicherheitsanerkennung erfüllt, muss in einem strukturierten Dokument mit den Sicherheitsbegründungen, genannt Sicherheitsnachweis, wie in 5.1 erläutert, dargelegt werden.

5.3.11 System-/Teilsystem-/Einrichtungsübergabe

Vor der Übergabe des Systems, Teilsystems oder der Einrichtung an eine Eisenbahnverwaltung müssen die Bedingungen für die Sicherheitsanerkennung und die Sicherheitszulassung, definiert in [Abschnitt 5.5](#), erfüllt sein, was die Vorlage des Sicherheitsnachweises und des Sicherheitsgutachtens mit einschließt.

5.3.12 Betrieb und Instandhaltung

Nach der Übergabe müssen die im Sicherheitsplan und im Abschnitt 5 des technischen Sicherheitsberichtes (Teil des Sicherheitsnachweises) definierten Verfahren, unterstützenden Systeme und Sicherheitsüberwachungen berücksichtigt werden.

Während der Betriebslebenszeit eines Systems kann es aus verschiedensten Gründen Änderungswünsche geben. Nicht alle werden sicherheitsrelevant sein. Jeder Änderungswunsch muss hinsichtlich seines Einflusses auf die Sicherheit durch Heranziehen der relevanten Teile der Sicherheitsdokumentation bewertet werden. Hat ein Änderungswunsch eine Modifizierung zur Folge, welche die Sicherheit des Systems, damit verbundenen Systeme oder der Umgebung beeinflusst, dann müssen die entsprechenden Teile des Sicherheitslebenszyklus wiederholt werden, um sicherzustellen, dass die durchgeführte Modifikation den Grad der Sicherheit nicht unzulässig verringert. [Tabelle E.10](#) ist ein Leitfaden für Anwendung, Betrieb und Instandhaltung bezogen auf die Sicherheitsanforderungsstufen.

5.3.13 Stilllegung und Entsorgung

Am Ende der Betriebslebenszeit eines Systems muss dieses außer Betrieb genommen und entsorgt werden, und dieses muss in Übereinstimmung mit den im Sicherheitsplan und im Abschnitt 5 des technischen Sicherheitsberichtes (Teil des Sicherheitsnachweises) definierten Maßnahmen geschehen.

5.4 Nachweis der funktionalen und technischen Sicherheit

Zusätzlich zum Nachweis des Qualitäts- und Sicherheitsmanagements, wie in 5.2 und 5.3 dieser Norm beschrieben, muss eine dritte Bedingung erfüllt sein, bevor ein System, Teilsystem oder eine Einrichtung als angemessen sicher für eine vorgesehene Anwendung zugelassen werden kann. Diese Bedingung ist der technische Nachweis der Sicherheit des Entwurfs, der im technischen Sicherheitsbericht dokumentiert werden muss. Dieses Dokument bildet den Teil 4 des Sicherheitsnachweises für ein System/Teilsystem oder eine Einrichtung, wie in 5.1 erläutert.

Der technische Sicherheitsbericht ist für die Sicherheitsanforderungsstufen 1 bis 4 verbindlich (siehe Anhang A zur Erläuterung der Sicherheitsanforderungsstufen). Jedoch sollten die Informationstiefe und der Umfang der unterstützenden Dokumentation der Sicherheitsanforderungsstufe des/der betrachteten Systems/Teilsystems oder Einrichtung angemessen sein. Die Anforderungen für die Sicherheitsanforderungsstufe 0 (nicht sicherheitsrelevant) liegen außerhalb des Anwendungsbereiches dieser Sicherheitsnorm.

Der technische Sicherheitsbericht muss die technischen Prinzipien darlegen, die die Sicherheit des Entwurfs gewährleisten, einschließlich (oder Verweisung zu allen) aller unterstützenden Nachweise (z. B. Entwurfsprinzipien und Berechnungen, Testspezifikationen und -ergebnisse sowie Sicherheitsanalysen).

Der technische Sicherheitsbericht ist unter Verwendung der folgenden Kapitelüberschriften zu gliedern:

Abschnitt 1 Einleitung

In diesem Abschnitt ist der Entwurf im Überblick zu beschreiben und es sind die technischen Sicherheitsprinzipien zusammenzufassen, auf denen die Sicherheit beruht, sowie das Ausmaß anzugeben, in dem das/die System/Teilsystem/Einrichtung fail-safe im Sinne dieser Norm sein muss.

Dieser Abschnitt muss ebenso die Normen (mit deren Ausgabeständen) angeben, die Grundlage für die technische Sicherheit des Entwurfs waren. Im Falle von Änderungen oder Ergänzungen von bereits in Betrieb befindlichen Einrichtungen oder bei Neuerstellung von Normen oder bei abgeschlossener Entwicklung dürfen ausnahmsweise die Ausgabestände der Normen zugrunde gelegt werden, die für den ursprünglichen Entwurf Grundlage waren und bei der Zulassung der ursprünglichen Einrichtung akzeptiert wurden. Dies gilt nur, wenn bei Berücksichtigung der neuesten Ausgabestände der Normen weitere Modifikationen der existierenden Einrichtung nötig wären oder ungerechtfertigte Änderungskosten entstehen würden. Die Gründe, die dieses Vorgehen rechtfertigen, müssen angegeben werden.

Abschnitt 2 Nachweis des korrekten funktionalen Verhaltens

Dieser Abschnitt muss alle Nachweise dafür enthalten, dass das/die System/Teilsystem/Einrichtung im ausfallfreien, normalen Zustand die korrekte Funktion erfüllt, in Übereinstimmung mit den spezifizierten betrieblichen und Sicherheitsanforderungen.

Die nachfolgend genannten Aspekte sind zu berücksichtigen, für die in B.2 detailliertere Anforderungen enthalten sind:

- 2.1 Beschreibung der Systemarchitektur (siehe B.2.1 und Tabelle E.4);
- 2.2 Definition der Schnittstellen (siehe B.2.2);
- 2.3 Erfüllung der Systemanforderungsspezifikation (siehe B.2.3);
- 2.4 Erfüllung der Sicherheitsanforderungsspezifikation (siehe B.2.4);
- 2.5 Nachweis der korrekten Hardwarefunktionalität (siehe B.2.5);
- 2.6 Nachweis der korrekten Softwarefunktionalität (siehe B.2.6).

Abschnitt 3 Ausfallauswirkungen

Dieser Abschnitt muss zeigen, dass das/die System/Teilsystem/Einrichtung auch dann die spezifizierten Sicherheitsanforderungen einschließlich des quantifizierten Sicherheitszieles erfüllt, wenn zufällige Hardwareausfälle auftreten.

Daneben könnte, trotz der Qualitäts- und Sicherheitsmanagementprozesse, die in 5.2 und 5.3 festgelegt sind, immer noch ein systematischer Fehler vorhanden sein. Dieser Abschnitt muss zeigen, welche technischen Maßnahmen angewendet wurden, um das daraus folgende Risiko auf eine akzeptierbare Höhe zu reduzieren.

Dieser Abschnitt muss ebenfalls zeigen, dass Ausfälle in beliebigen Systemen/Teilsystemen oder Einrichtungen, deren Sicherheitsanforderungsstufen kleiner (einschließlich Stufe 0) als die des Gesamtsystems sind, nicht die Sicherheit des Gesamtsystems verringern können.

Die folgenden Überschriften sind in diesem Abschnitt zu verwenden. B.3 enthält dazu detailliertere Anforderungen. Einen Leitfaden hierzu geben Tabelle E.5 und Tabelle E.6.

- 3.1 Auswirkungen von Einzelausfällen (siehe B.3.1);
- 3.2 Unabhängigkeit von Betrachtungseinheiten (siehe B.3.2);
- 3.3 Offenbarung von Einzelausfällen (siehe B.3.3);
- 3.4 Aktion nach Ausfalloffenbarung (einschließlich des Beibehaltens des sicheren Zustandes) siehe B.3.4);
- 3.5 Auswirkungen von Mehrfachausfällen (siehe B.3.5);
- 3.6 Schutz gegen systematische Fehler (siehe B.3.6).

Abschnitt 4 Betrieb mit externen Einflüssen

Dieser Abschnitt muss zeigen, dass das/die System/Teilsystem/Einrichtung, wenn es den in der Systemanforderungsspezifikation festgelegten externen Einflüssen ausgesetzt wird,

- weiterhin die spezifizierten betrieblichen Anforderungen erfüllt;
- weiterhin die spezifizierten Sicherheitsanforderungen erfüllt (einschließlich Ausfallbedingungen).

Der Sicherheitsnachweis ist deswegen nur innerhalb des spezifizierten Bereiches von externen Einflüssen gültig, so wie in der Systemanforderungsspezifikation festgelegt. Die Sicherheit ist außerhalb dieser Grenzen nicht gewährleistet, sofern nicht zusätzliche spezielle Maßnahmen getroffen werden.

Die Methoden zum Schutz vor den spezifizierten externen Einflüssen müssen vollständig erläutert und begründet werden.

Detailliertere Anforderungen sind in B.4 enthalten.

Abschnitt 5 Sicherheitsbezogene Anwendungsbedingungen

Dieser Abschnitt muss die Regeln, Bedingungen und Einschränkungen spezifizieren (oder darauf verweisen), die bei der Anwendung des/der Systems/Teilsystems/Einrichtung eingehalten werden müssen. Dies muss auch die Anwendungsbedingungen aus den Sicherheitsnachweisen aller Teilsysteme oder Einrichtungen einschließen, auf die Bezug genommen wird.

Detailliertere Anforderungen sind in Anhang B.5 enthalten. Einen Leitfaden gibt auch Tabelle E.10.

Abschnitt 6 Sicherheitserprobung

Dieser Abschnitt muss den Nachweis erbringen, dass die Sicherheitserprobung unter Betriebsbedingungen erfolgreich abgeschlossen wurde. Dies ist in B.6 erläutert.

Die Struktur des technischen Sicherheitsberichts ist in Bild 7 dargestellt.