

	DIN EN 50126-2 (VDE 0115-103-2)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
ICS 29.280; 45.020 Bahnanwendungen – Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Teil 2: Systembezogene Sicherheitsmethodik; Deutsche Fassung EN 50126-2:2017 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety; German version EN 50126-2:2017 Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) – Partie 2: Approche systématique pour la sécurité; Version allemande EN 50126-2:2017 Gesamtumfang 99 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2017-07-03 angenommene Europäische Norm als DIN-Norm ist 2018-10-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 50126-2 (VDE 0115-103-2):2016-02.

Für dieses Dokument ist das nationale Arbeitsgremium K 351 „Elektrische Ausrüstungen für Bahnen“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Hinweise zur Anwendung der Norm

Dem deutschen nationalen Komitee ist bekannt, dass beim Anwenden der EN 50126 der in der Norm festgelegte Anwendungsrahmen nicht immer beachtet wird. So werden in der Praxis z. B. das projektspezifische Zuschneiden der Prozesse des Lebenszyklus als Grundlage zur Planung, Herstellung, Betrieb, Prüfung und Genehmigung nicht zugelassen. Gerade dies wird aber von der vorliegenden Norm explizit ermöglicht. Aus diesem Grund weist das nationale Komitee an dieser Stelle auf dieses Prüfen der anwendungsspezifischen Gegebenheiten explizit hin.

Die seit 1999 existierende Norm wurde schon vielfach auch im Sektor der städtischen Schienenbahnen angewendet, jedoch nicht immer im Sinne der Normersteller. Eine erfolgreiche und einvernehmliche Anwendung dieser Norm als Ganzes oder in Teilen ist nur dann möglich, wenn sie richtig angewendet wird.

Hinweis zur deutschen Übersetzung – Änderungen zwischen FprEN und EN

Das deutsche Komitee weist auf die folgenden Begriffe hin, die nach der finalen Verabschiedung der FprEN noch von CENELEC geändert wurden. Dadurch bekommen die geänderten Begriffe in der Version EN eine andere bahnspezifische Bedeutung und bei der Verwendung in der Norm führt dies zu Inkonsistenzen. In den meisten Fällen wurde die IEV-Definition eingeführt, um den gewählten Begriff zu ersetzen, ohne dass die Konsequenzen für den Inhalt beider Teile der Norm bekannt sind.

Folgende Begriffe wurden bei der Erstellung der EN:2017 gegenüber dem Entwurf (FprEN) verändert:

Begriff im Entwurf (FprEN)	Begriff neu (EN)	Weiteres
3.2 Unfall (en: accident) ein nicht beabsichtigtes Ereignis oder eine Reihe von Ereignissen mit der Folge des Verlustes der Gesundheit oder Lebens von Menschen, der Beschädigung von Eigentum oder von Umweltschäden Anmerkung 1 zum Begriff Der Begriff schließt Verluste aus Unfällen ein, die innerhalb sehr kurzer Zeit entstehen (z. B. Kollision, Explosion) und sich auch über eine längere Zeit entwickeln können (z. B. Freisetzen eines giftigen Stoffes).	3.2 Unfall (en: accident) nicht beabsichtigtes Ereignis oder Reihe von Ereignissen mit der Folge von Toten, von Verletzten, von Verlust eines Systems oder eines Dienstes, oder von Umweltschäden [QUELLE: IEC 60050-821: FDIS 2016, 821-12-02]	Die IEV-Definition wurde eingeführt.

Begriff im Entwurf (FprEN)	Begriff neu (EN)	Weiteres
3.6 Audit (en: audit) eine dokumentierte, systematische und unabhängige Prüfung, um zu ermitteln, ob die gestellten Anforderungen an die angewandten Verfahren – mit den geplanten Maßnahmen übereinstimmen, – wirkungsvoll eingesetzt werden und – geeignet sind, die festgelegten Ziele zu erreichen	3.5 Audit (en: audit) systematischer, unabhängiger, dokumentierter Prozess zur Erlangung von Aufzeichnungen, Darlegungen von Fakten oder anderen relevanten Informationen und deren objektiver Begutachtung, um zu ermitteln, inwieweit festgelegte Anforderungen erfüllt sind Anmerkung 1 zum Begriff: Während „Audit“ für Managementsysteme gilt, wird „Begutachtung“ für Konformitätsbewertungsstellen und darüber hinaus als allgemeiner Begriff verwendet. [QUELLE: ISO/IEC 17000:2004, 4.4, modifiziert – Die Verweisungen auf andere Begriffe in ISO/IEC 17000 wurden (in Electropedia) durch Hyperlinks auf Einträge im IEV ersetzt.] QUELLE: IEC 60050-902:2013, 902-03-04]	Die IEV-Definition wurde eingeführt.
3.7 Verfügbarkeit (en: availability) Fähigkeit einer Einheit, zu einem gegebenen Zeitpunkt oder während eines gegebenen Zeitintervalls eine geforderte Funktion unter gegebenen Bedingungen erfüllen zu können [QUELLE: IEC 60050-821: CDV2015, 821-05-82, modifiziert]	3.6 Verfügbarkeit <eines Produktes> (en: availability, <of a product>) Fähigkeit eines Betriebsmittels, zu einem gegebenen Zeitpunkt oder während eines gegebenen Zeitintervalls eine geforderte Funktion unter gegebenen Bedingungen erfüllen zu können, vorausgesetzt, dass die erforderlichen äußeren Hilfsmittel bereitgestellt sind [QUELLE: IEC 60050-821: FDIS 2016, 821-05-82, modifiziert]	
3.11 Ausfall aufgrund gemeinsamer Ursache (en: common cause failure) Ausfälle verschiedener Einheiten aufgrund derselben Ursache und diese Fehler nicht Folge von voneinander sind [QUELLE: IEC 60050-821: CDV2015, 821-12-10]	3.10 Ausfälle aufgrund gemeinsamer Ursache (en: common cause failure) Ausfälle mehrerer Einheiten, die ansonsten als voneinander unabhängig angesehen werden würden, aufgrund einer einzigen Ursache [QUELLE: IEC 60050-192:2015, 192-03-18]	Die IEV-Definition wurde eingeführt. Anmerkung des nationalen Komitees: Gemeint sind gleichartig wirkende Fehler infolge gemeinsame Ursache für Ausfälle.

Begriff im Entwurf (FprEN)	Begriff neu (EN)	Weiteres
3.23 Ausfall (en: failure) (einer Einheit) Verlust der Fähigkeit, wie gefordert zu funktionieren Anmerkung 1 zum Begriff: Der Fehler ist ein Ereignis im Unterschied zum Ausfall welcher ein Zustand ist. [QUELLE: IEC 60050-192:2015, 192-03-01]	3.21 Ausfall<einer Einheit> (en Failure (, <of an item) >) Verlust der Fähigkeit, wie gefordert zu funktionieren Anmerkung 1 zum Begriff: Qualifizierende Bezeichnungen wie katastrophal, kritisch, Haupt-, Neben-, Marginal- und nicht signifikant dürfen verwendet werden, um die Ausfälle hinsichtlich der Schwere ihrer Auswirkungen einzuteilen, wobei die Wahl und die Festlegungen der Schweregrade von dem Anwendungsfall abhängen. Anmerkung 2 zum Begriff: Qualifizierende Bezeichnungen wie Missbrauch, Fehlbedienung und Schwachstelle dürfen verwendet werden, um Ausfälle hinsichtlich ihrer Ursache einzuteilen. [QUELLE: IEC 60050-192:2015, 192-03-01, modifizierte Anmerkung 1 zum Begriff wurde entfernt. Anmerkung 3 zum Begriff: Der Fehler ist ein Ereignis im Unterschied zum Ausfall welcher ein Zustand ist.	Die IEV-Definition wurde eingeführt. Anmerkung des nationalen Komitees: In dieser Norm ist in den meisten Fällen mit „Failure“ der „Fehler“ gemeint und wird an diesen Stellen so umgesetzt.
3.25 Ausfallrate (en: failure rate) Grenzwert, falls ein solcher existiert, der Verhältniszahl der herstellungsbedingten Wahrscheinlichkeit, dass der Zeitpunkt T der Fehlfunktion von einem Produkt in ein gegebenes Zeitintervall $(t, t + \Delta t)$ fällt und der Länge dieses Intervalls Δt mit Δt gegen Null, vorausgesetzt das Objekt ist zu Beginn des Zeitintervalls in einem einwandfreien Zustand Anmerkung 1 zum Begriff: Ausfallraten werden oftmals als konstant angenommen. Dies ist nicht immer gültig, z. B. bei Komponenten, die (mechanischem, pneumatischem, elektromechanischem usw.) Verschleiß unterliegen. Anmerkung 2 zum Begriff: Die Benennung „Ausfallrate“ wird häufig im Sinne der „mittleren Ausfallrate“ verwendet, deren Definition in IEC 60050-192:2015, 192-05-07 angegeben ist.	3.23 Ausfallrate (en: failure rate) Grenzwert des Quotienten der bedingten Wahrscheinlichkeit, dass der Zeitpunkt T des Ausfalls in ein gegebenes Zeitintervall $(t, t + \Delta t)$ fällt, und der Länge dieses Intervalls Δt, wenn Δt gegen 0 geht, vorausgesetzt, das Produkt ist zu Beginn des Zeitintervalls in betriebsfähigem Zustand Anmerkung 1 zum Begriff: Für Anwendungen, bei denen die Reiseentfernung oder die Anzahl der Betriebszyklen relevanter als die Zeit ist, kann die Zeiteinheit durch die Einheiten Entfernung oder Zyklen sachgerecht ersetzt werden. Anmerkung 2 zum Begriff: Der Begriff „Ausfallrate“ wird oft im Sinne der „mittleren Ausfallrate“, wie in 192-05-07 definiert, verwendet. [QUELLE: IEC 60050--21:FDIS2016]	Die IEV-Definition wurde eingeführt. Anmerkung 1 zum Begriff wurde ersetzt.

Begriff im Entwurf (FprEN)	Begriff neu (EN)	Weiteres
3.26 Fehler (en: fault) Zustand einer Einheit, in dem sie unfähig ist, eine geforderte Funktion zu erfüllen, wobei die durch Wartung oder andere geplante Handlungen verursachte Leistungsunfähigkeit ausgeschlossen ist Anmerkung 1 zum Begriff Ein Fehler ist oft das Ergebnis einer Fehlfunktion der Einheit selber, kann aber auch ohne frühere Fehlfunktion vorhanden sein (z. B. im Fall eines Entwicklungsfehlers).	3.24 Fehlzustand <in einem System> (en: fault <in a system>) abnormaler Zustand, der zu einem Fehler oder Ausfall in einem System führen könnte Anmerkung 1 zum Begriff: Ein Fehlzustand kann zufällig oder systematisch sein. [QUELLE: IEC 60050-821:FDIS2016, 821-11-20]	Die IEV-Definition wurde eingeführt. In dieser Norm ist mit „fault <in a system>“ der „Ausfall“ gemeint und wird im weiteren Text so umgesetzt.
3.27 Funktion (en: funktion) eine festgelegte Aktion oder Tätigkeit, die mit technischen Mitteln und/oder von Menschen ausgeführt werden kann und die auf eine definierte Eingangsgröße eine definierte Ausgangsgröße hat Anmerkung 1 zum Begriff Eine Funktion kann festgelegt oder beschrieben sein, ohne dass es einen Hinweis auf die physikalischen Mittel gibt, mit denen sie erreicht wird.	3.25 Funktion < einer Einheit> (en: function, < of an item>) festgelegte Aktion oder Tätigkeit, die mit technischen Mitteln und/oder von Menschen ausgeführt werden kann und die auf eine definierte Eingangsgröße eine definierte Ausgangsgröße liefert Anmerkung 1 zum Begriff: Eine Funktion kann ohne Verweis auf die physikalischen Mittel zu ihrer Umsetzung festgelegt oder beschrieben werden. [QUELLE: IEC 60050-821: FDIS2016, 821-12-25, modifiziert]	Die IEV-Definition wurde eingeführt. Die Beschreibung des Begriffs ist die gleiche geblieben. Die ursprüngliche Anmerkung wurde geändert.
3.29 generisches Produkt (en: generic product) Produkt (Hardware und/oder Software), das für eine Vielzahl von Anlagen benutzt werden kann, wobei entweder keine Veränderungen vorgenommen werden oder bloß durch Konfiguration der Hardware oder Software (z. B. durch Bereitstellung von anwendungsspezifischen Daten und/oder Algorithmen) [QUELLE: IEC 62290-1:2014, 3.1.11, modifiziert]	3.27 generisches Produkt (en: generic product) Produkt, das unabhängig von Anwendungen definierten Randbedingungen, Schnittstellen und Funktionalitäten (black box) erfüllt Beispiel: Beispiele für generische Produkte sind Weichenantriebe, Achszähler, Echtzeit-Betriebssysteme und sichere Rechnerplattform ohne Anwendungssoftware [QUELLE: IEC 60050-821: FDIS2016, 821-01-57]	Die IEV-Definition wurde eingeführt.

Begriff im Entwurf (FprEN)	Begriff neu (EN)	Weiteres
3.32 Gefährdungslogbuch (en: hazard log) Dokument, in dem erkannte Gefährdungen, getroffene Entscheidungen und verwendete Lösungen und der Stand von deren Implementierung aufgezeichnet bzw. referenziert werden Anmerkung 1 zum Begriff: Im Gefährdungslogbuch werden die Belege für die Implementierung der Sicherheitsanforderungen hinsichtlich aller identifizierten Gefährdungen zusammengefasst und auf diese Weise der Nachweis der Vollständigkeit zur Sicherstellung der Sicherheit erforderlichen Aktivitäten unterstützt. Anmerkung 2 zum Begriff: Ein „Gefährdungseintrag“ ist ein Auszug aus dem Gefährdungslogbuch, der zur Übermittlung zwischen den Projektbeteiligten geeignet ist	3.30 Gefährdungslogbuch (en: hazard log) Dokument, in dem erkannte Gefährdungen, getroffene Entscheidungen, verwendete Lösungen und ihr Implementierungszustand aufgezeichnet bzw. referenziert werden [QUELLE: IEC 60050-821: FDIS2016, 821-12-27]	Die IEV-Definition wurde eingeführt. Die beiden ursprünglichen Anmerkungen wurden gelöscht.
3.39 Instandhaltbarkeit (en: maintainability) Fähigkeit, unter gegebenen Anwendungs- und Instandhaltungsbedingungen in einem wie geforderten funktionsfähigen Zustand erhalten bzw. in ihn zurückversetzt werden zu können Anmerkung 1 zum Begriff: Zu den gegebenen Bedingungen gehören Gesichtspunkte mit Auswirkung auf die Instandhaltbarkeit, wie etwa: Ort der Instandhaltung, Zugänglichkeit, Instandhaltungsverfahren und Instandhaltungsmittel. [QUELLE: IEC 60050-192:2015, 192-01-27]	3.37 Instandhaltbarkeit, <einer Einheit> (en: maintainability, < of an item>) Fähigkeit, unter gegebenen Anwendungs- und Instandhaltungsbedingungen in einem wie geforderten funktionsfähigen Zustand erhalten bzw. in ihn zurückversetzt werden zu können Anmerkung 1 zum Begriff: Zu den gegebenen Bedingungen gehören Gesichtspunkte mit Auswirkung auf die Instandhaltbarkeit, wie etwa: Ort der Instandhaltung, Zugänglichkeit, Instandhaltungsverfahren und Instandhaltungsmittel. [QUELLE: IEC 60050-192:2015, 192-01-27]	Die Beschreibung des Begriffs ist die gleiche geblieben.
	3.51 wurde neu hinzugefügt: zufälliger Fehler (en: random failure)	

Begriff im Entwurf (FprEN)	Begriff neu (EN)	Weiteres
3.59 Risiko (en: risk>) Kombination aus erwarteter Häufigkeit eines Schadens und erwartetem Schweregrad dieses Schadens	3.57 Risiko < für Eisenbahn RAMS> (en: risk , <for railway RAMS>) Kombination aus erwarteter Häufigkeit eines Schadens und erwartetem Schweregrad dieses Schadens	Die Begriff Beschreibung ist die gleiche geblieben
3.67 Sicherheitsbehörde (en: safety authority) Instanz, die mit Genehmigungsaufgaben hinsichtlich der Bahnsicherheit in Übereinstimmung mit dem betreffenden gesetzlichen Rahmen betraut ist	3.65 Sicherheitsbehörde (en: safety authority) Stelle, die verantwortlich für das Erteilen der Zulassung zum Betrieb eines sicherheitsrelevanten Systems ist [QUELLE: IEC 60050-821: FDIS 2016, 821-12-52]	Die IEV-Definition wurde eingeführt.
3.71 Sicherheitsintegrität (en: safety integrity) Fähigkeit einer sicherheitsrelevanten Funktion unter allen angegebenen Bedingungen, innerhalb einer angegebenen Betriebsumgebung und innerhalb eines festgelegten Zeitraumes anforderungsgemäß zu funktionieren Anmerkung 1 zum Begriff Die Sicherheitsintegrität kann eine Eigenschaft sein, die mit technischen oder nicht-technischen Funktionen als auch mit weiteren Aspekten in Verbindung steht (z. B. betriebliche und strukturelle Aspekte). Anmerkung 2 zum Begriff: Die Basisintegrität ist die für sicherheitsrelevante Funktionen mindestens erforderliche Integrität. Dieses Attribut kann auch mit nicht sicherheitsbezogenen Funktionen verbunden sein.	3.69 Sicherheitsintegrität (en: safety integrity) Fähigkeit eines sicherheitsrelevanten Systems, seine geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb einer festgelegten betrieblichen Umgebung und innerhalb einer festgelegten Dauer zu erbringen [QUELLE: IEC 60050-821: FDIS2016, 821-12-54]	Die IEV-Definition wurde eingeführt. Die ursprünglichen Anmerkungen wurden gelöscht.
	3.75 wurde neu hinzugefügt sicherheitsbezogene Anwendungsbedingungen (en: safety-related application conditions)	

Nationaler Anhang NA (informativ)

Zusammenhang mit europäischen und internationalen Dokumenten

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

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

Eine Information über den Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ist nachstehend wiedergegeben.

Tabelle NA.1

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 50126-1:2017	–	DIN EN 50126-1 (VDE 0115-103-1):2018-10	VDE 0115-103-1
EN ISO 9001	ISO 9001	DIN EN ISO 9001	–
–	ISO/IEC 90003	–	–
–	ISO/IEC Guide 51	DIN 820-12	–
–	IEC 61882:2001 <i>zurückgezogen</i>	–	–
EN 61882:2016	ersetzt durch: IEC 61882:2016	DIN EN 61882 (VDE 0050-8):2017-02	VDE 0050-8
EN 60812:2006	IEC 60812:2006	DIN EN 60812:2006-11	–
EN 62502:2010	IEC 62502:2010	DIN EN 62502 (VDE 0050-3):2011-06	VDE 0050-3
EN 61025:2007	IEC 61025:2010	DIN EN 61025:2007-08	–
EN 61165:2006	IEC 61165:2006	DIN EN 61165:2007-02	–
EN 61078:2006	IEC 61078:2006	DIN EN 61078:2006-10	–
EN 61508-5:2010	IEC 61508-5	DIN EN 61508-5 (VDE 0803-5)	VDE 0803-5

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN 820-12, *Normungsarbeit – Teil 12: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen*

DIN EN 50126-1 (VDE 0115-103-1):2018-10 (in Vorbereitung), *Bahnanwendungen – Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Teil 1: Generischer RAMS Prozess*

DIN EN 60812:2006-11, *Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA) (IEC 60812:2006); Deutsche Fassung EN 60812:2006*

DIN EN 61025:2007-08, *Fehlzustandsbaumanalyse (IEC 61025:2006); Deutsche Fassung EN 61025:2007*

DIN EN 61078:2006-10, *Techniken für die Analyse der Zuverlässigkeit – Zuverlässigkeitsblockdiagramm und Boole'sche Verfahren (IEC 61078:2006); Deutsche Fassung EN 61078:2006*

DIN EN 61165:2007-02, *Anwendung des Markoff-Verfahrens (IEC 61165:2006); Deutsche Fassung EN 61165:2006*

DIN EN 61508-5 (VDE 0803-5), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level)*

DIN EN 61882 (VDE 0050-8):2017-02, *HAZOP-Verfahren (HAZOP-Studien) – Anwendungsleitfaden (IEC 61882:2016); Deutsche Fassung EN 61882:2016*

DIN EN 62502 (VDE 0050-3):2011-06, *Verfahren zur Analyse der Zuverlässigkeit – Ereignisbaumanalyse (ETA) (IEC 62502:2010); Deutsche Fassung EN 62502:2010*

DIN EN ISO 9001, *Qualitätsmanagementsysteme – Anforderungen*

**Bahnanwendungen –
Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit,
Instandhaltbarkeit und Sicherheit (RAMS) –
Teil 2: Systembezogene Sicherheitsmethodik**

Railway Applications –
The Specification and Demonstration of
Reliability, Availability, Maintainability and Safety
(RAMS) –
Part 2: Systems Approach to Safety

Applications ferroviaires –
Spécification et démonstration de la fiabilité, de
la disponibilité, de la maintenabilité et de la
sécurité (FDMS) –
Partie 2: Approche systématique pour la
sécurité

Diese Europäische Norm wurde von CENELEC am 2017-07-03 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 CEN-CENELEC Management Centre 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 CEN-CENELEC Management Centre mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brüssel

© 2017 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 50126-2:2017 D

Inhalt

Seite

Europäisches Vorwort.....	7
Einleitung	8
1 Anwendungsbereich	10
2 Normative Verweisungen	11
3 Begriffe	11
4 Abkürzungen	11
5 Sicherheitsprozess	12
5.1 Risikobewertung und Gefährdungsbeherrschung	12
5.2 A. Risikobewertung.....	13
5.2.1 Allgemeines	13
5.2.2 Durchführen der Risikobewertung.....	14
5.3 B. Ergebnis der Risikobewertung	14
5.4 C. Gefährdungsbeherrschung	14
5.5 D. Überprüfung der Risikobewertung	16
5.6 Verantwortlichkeiten	16
6 Nachweis der Sicherheit und der Sicherheitsabnahme	16
6.1 Einleitung.....	16
6.2 Prozess zum Nachweis der Sicherheit und zur Sicherheitsabnahme.....	17
6.3 Verantwortung für das Management des Sicherheitsnachweises	20
6.4 Modifikationen nach einer Sicherheitsabnahme	20
6.5 Abhängigkeiten zwischen Sicherheitsnachweisen.....	20
6.6 Beziehung zwischen Sicherheitsnachweisen und Systemarchitektur.....	21
7 Organisation und Unabhängigkeit Rollen.....	22
7.1 Allgemeines	22
7.2 Frühe Phasen des Lebenszyklus (Phasen 1 bis 4).....	23
7.3 Spätere Phasen des Lebenszyklus (ab Phase 5)	24
7.4 Kompetenz der Mitarbeiter	26
8 Risikobewertung	27
8.1 Einleitung.....	27
8.2 Risikoanalyse	27
8.2.1 Allgemeines	27
8.2.2 Das Risikomodell.....	27
8.2.3 Methoden der Auswirkungsanalyse	30
8.2.4 Expertenurteil	30
8.3 Risikoakzeptanzprinzipien und Risikobeurteilung	31
8.3.1 Anwenden der Regelwerke	31
8.3.2 Anwenden eines Referenzsystems.....	31
8.3.3 Anwenden der expliziten Risikoeinschätzung	32

8.4	Anwenden der expliziten Risikoeinschätzung.....	33
8.4.1	Quantitativer Ansatz.....	33
8.4.1.1	Allgemeines.....	33
8.4.1.2	Für Unfälle geltende Sicherheitsziele	35
8.4.1.3	Tolerierbare Gefährdungsrate (THR).....	35
8.4.1.4	Verantwortlichkeiten.....	36
8.4.2	Variabilität bei der Anwendung von quantitativen Risikoeinschätzungen.....	36
8.4.2.1	Allgemeines.....	36
8.4.2.2	„Ungünstigstes Szenario“.....	37
8.4.2.3	„Angemessene Einschätzungen“	37
8.4.2.4	„Angemessene ungünstigster Fall“	37
8.4.3	Qualitative und semi-quantitative Ansätze.....	38
9	Festlegung von Systemsicherheitsanforderungen.....	38
9.1	Allgemeines.....	38
9.2	Sicherheitsanforderungen	38
9.3	Kategorisierung von Sicherheitsanforderungen.....	39
9.3.1	Allgemeines.....	39
9.3.2	Funktionale Sicherheitsanforderungen	39
9.3.3	Technische Sicherheitsanforderungen	40
9.3.4	Kontextuelle Sicherheitsanforderungen	40
10	Aufteilung der funktionalen Sicherheitsintegritätsanforderungen	41
10.1	Ableitung und Aufteilung von Systemsicherheitsanforderungen	41
10.2	Funktionale Sicherheitsintegrität bei elektronischen Systemen.....	41
10.2.1	Ableitung von funktionalen Sicherheitsanforderungen für elektronische Systeme.....	41
10.2.2	Aufteilung von Sicherheitsanforderungen	41
10.2.3	Sicherheitsintegritätsfaktoren.....	44
10.2.4	Funktionale Sicherheitsintegrität und zufällige Fehler	44
10.2.5	Systematischer Aspekt der funktionalen Sicherheitsintegrität	45
10.2.6	Ausgewogene Anforderungen zur Beherrschung zufälliger und systematischer Fehler.....	45
10.2.7	SIL-Tabelle	46
10.2.8	SIL-Zuordnung	47
10.2.9	Aufteilung von TFFR nach der SIL-Zuordnung.....	47
10.2.10	Nachweis von quantifizierten Zielen	47
10.2.11	Anforderungen an die Basisintegrität.....	47
10.2.12	Verhinderung der falschen Verwendung von SIL	49
10.3	Sicherheitsintegrität bei nicht-elektronischen Systemen – Anwenden der Regelwerke	49
11	Entwurf und Implementierung	50
11.1	Einleitung.....	50
11.2	Ursachenanalyse.....	50

11.3	Gefährdungsermittlung (detailliert)	51
11.4	Analyse gemeinsamer Ursachen	51
Anhang A (informativ) ALARP, GAME, MEM		53
A.1	ALARP, GAME und MEM als Verfahren für die Festlegung von Risikoakzeptanzkriterien	53
A.2	ALARP (so niedrig wie vernünftigerweise in der Praxis praktikabel)	54
A.2.1	Allgemeines	54
A.2.2	Vertretbarkeit und ALARP	55
A.3	Globalement au Moins Equivalent (GAME)-Grundsatz	55
A.3.1	Kurzbeschreibung	55
A.3.2	Anwendung von GAME	56
A.3.2.1	Allgemeines	56
A.3.2.2	Grundlagen	56
A.3.2.3	Anwendung von GAME zur Entwicklung eines qualitativen Sicherheitsarguments	57
A.3.2.4	GAME mit Nutzung von quantitativen Risikozielen	57
A.4	Minimale endogene Mortalität (MEM)	57
Anhang B (informativ) Anwendung von Ausfall- und Unfallstatistiken für die Ableitung einer THR		59
Anhang C (informativ) Anleitung für die SIL-Zuordnung		61
Anhang D (informativ) Verfahren für die Aufteilung von Sicherheitszielen		63
D.1	Analyse des Systems und der Verfahren	63
D.2	Beispiel für ein qualitatives Aufteilungsverfahren	63
D.2.1	Allgemeines	63
D.2.2	Beispiel für ein qualitatives Verfahren für die Effizienz der Barriere	64
D.3	Beispiel für ein quantitatives Zuteilungsverfahren	66
D.3.1	Einleitung	66
D.3.2	Funktionen mit unabhängigen Mechanismen für die Fehlererkennung und sicherheitsgerichtete Ausfallreaktion	68
D.3.3	Funktion und unabhängige Barriere, die zusammen als Mechanismus der Fehlererkennung und sicherheitsgerichteten Ausfallreaktion wirken	70
D.3.4	Aufteilen eines als Wahrscheinlichkeit gegebenen Sicherheitszieles	71
D.3.5	Aufteilen eines „zeitbezogenen“ Sicherheitsziels	71
Anhang E (informativ) Häufige Fehler bei der Quantifizierung		73
E.1	Häufige Fehlanwendungen	73
E.2	Vermischen von Ausfallraten mit Wahrscheinlichkeiten	73
E.3	Verwendung von Formeln außerhalb ihres Anwendbarkeitsbereichs	74
Anhang F (informativ) Techniken/Methoden der Sicherheitsanalyse		75
Anhang G (informativ) Für die Systemsicherheit entscheidende Funktionen und Verantwortlichkeiten		78
Anhang ZZ (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2008/57/EG		83
Literaturhinweise		89

Bilder

Bild 1 – Das Sanduhrmodell	13
Bild 2 – Darstellung der Gefährdungen in Bezug auf die Systemgrenzen	15
Bild 3 – Beispiel für Sicherheitsabnahmeprozesse	19
Bild 4 – Beispiele für Abhängigkeiten zwischen Sicherheitsnachweisen	21
Bild 5 – Unabhängigkeit von Rollen in den frühen Phasen (Phasen 1 bis 4) des Lebenszyklus	24
Bild 6 – Unabhängigkeit der Rollen in den späteren Phasen des Lebenszyklus (ab Phase 5)	26
Bild 7 – Ein Beispiel eines Risikomodells	28
Bild 8 – Tolerierbare Raten in einem Risikomodellbeispiel	34
Bild 9 – Klassifikation von Anforderungen	39
Bild 10 – Zuteilung von funktionalen Sicherheitsanforderungen	42
Bild 11 – Kategorisierung von Sicherheitsintegritätsmaßnahmen	46
Bild 12 – Auswirkungen funktionaler Abhängigkeiten in einer Fehlerbaumanalyse	52
Bild A.1 – Differentielle Risikoaversion	58
Bild D.1 – Beispiel für ein qualitatives Aufteilungsverfahren	64
Bild D.2 – Interpretation von Ausfall- und Reparaturzeiten	67
Bild D.3 – Kombination von zwei Funktionen mit unabhängigen Mechanismen für die Fehlererkennung und sicherheitsgerichtete Ausfallreaktion	68
Bild D.4 – Zuordnung von Sicherheitsintegritätsanforderungen	69
Bild D.5 – Kombination von Funktion und unabhängiger Barriere, die zusammen als Mechanismus der Fehlererkennung und sicherheitsgerichteten Ausfallreaktion wirken	70
Bild D.6 – Beispiel für eine quantifizierte Aufteilung	72
Bild E.1	73

Tabellen

Tabelle 1 – Beispiele für Gefährdungen	29
Tabelle 2 – SIL-bezogene quantitative und qualitative Maßnahmen	46
Tabelle A.1 – Übersicht über ALARP, GAME, MEM	53
Tabelle D.1 – Effizienz basierend auf den Ausfällen der Komponente	65
Tabelle D.2 – Effizienz basierend auf dem Wissen der Komponente	65
Tabelle D.3 – Effizienz basierend auf der Verwendung der Komponente	65
Tabelle D.4 – Effizienz basierend auf der Instandhaltung der Komponente	66
Tabelle F.1 – Techniken/Methoden der Sicherheitsanalyse	75
Tabelle F.2 – Verfahren/Methoden für BI und SIL	76
Tabelle G.1 – Funktionsspezifikation für Entwerfer	78
Tabelle G.2 – Funktionsspezifikation für Verifizierer	79
Tabelle G.3 – Funktionsspezifikation für Validierer	80
Tabelle G.4 – Funktionsspezifikation für den unabhängigen Sicherheitsbewerter	81
Tabelle G.5 – Funktionsspezifikation für Projektmanager	82

Tabelle ZZ.1 – Zusammenhang zwischen dieser Europäischen Norm, der TSI „Zugsteuerung, Zugsicherung und Signalgebung“ (KOMMISSION VERORDNUNG (EU) 2016/919 vom 24. Mai 2016) und der Richtlinie 2008/57/EG	83
Tabelle ZZ.2 – Zusammenhang zwischen dieser Europäischen Norm, der TSI „Lokomotiven und Personenwagen“ (VERORDNUNG (EU) Nr. 1302/2014 vom 18. November 2014) und der Richtlinie 2008/57/EG	86
Tabelle ZZ.3 – Zusammenhang zwischen dieser Europäischen Norm, der TSI „Energie“ (VERORDNUNG (EU) Nr. 1301/2014 vom 18. November 2014) und der Richtlinie 2008/57/EG	87
Tabelle ZZ.4 – Zusammenhang zwischen dieser Europäischen Norm, der TSI „Infrastruktur“ (VERORDNUNG (EU) Nr. 1299/2014 vom 18. November 2014) und der Richtlinie 2008/57/EG	88

Europäisches Vorwort

Dieses Dokument (EN 50126-2:2017) wurde vom Technischen Komitee CLC/TC 9X „Elektrische und elektronische Anwendungen für Bahnen“ erstellt.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2018-07-03
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2020-07-03

Dieses Dokument ersetzt CLC/TR 50126-2:2007.

Die frühere Ausgabe von CLC/TR 50126-2:2007 wird durch die neuen Editionen **EN 50126-1:2017** und EN 50126-2:2017 überholt; Der Grund dafür ist, dass der Anwendungsbereich des vorliegenden Teils im Vergleich zur ersetzten Ausgabe geändert wurde

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

EN 50126, *Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS)*, beinhaltet die folgenden Teile:

- **Teil 1:** Generischer RAMS-Prozess;
- **Teil 2:** Systembezogene Sicherheitsmethodik.

Dieses Dokument wurde unter einem Mandat erstellt, das von der Europäischen Kommission und der Europäischen Freihandelszone an CENELEC gegeben wurde, und unterstützt grundlegende Anforderungen von EU-Richtlinie(n).

Zum Zusammenhang mit EU-Richtlinien siehe informativen [Anhang ZZ](#), der Bestandteil dieses Dokuments ist.

Einleitung

EN 50126-1:1999 hatte das Ziel, die Anwendung eines systematischen RAMS-Managementprozesses im Bahnsektor einzuführen. Aufgrund der Anwendung dieser Norm und der gewonnenen Erfahrungen der letzten Jahre war es erforderlich, diese zu überarbeiten, neu zu gestalten und einen systematischen und kohärenten Ansatz für RAMS für alle Bahnanwendungsbereiche, d. h. Zugsteuerung, Zugsicherung und Signalgebung (Signaltechnik), Bahnfahrzeuge und ortsfeste Anlagen, zur Verfügung zu stellen.

Die überarbeitete Fassung hat die Kohärenz und Konsistenz der Normen, das Konzept des Sicherheitsmanagements und die praktische Anwendung von EN 50126 verbessert und auch die bestehenden und verwandten Technischen Berichte einbezogen.

Mit dieser Europäischen Norm wird den Bahnunternehmen und deren Lieferanten in der gesamten Europäischen Union ein Prozess zur Verfügung gestellt, der die Implementierung eines in sich konsistenten Ansatzes für das Management von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (en: reliability, availability, maintainability and safety), abgekürzt „RAMS“, ermöglicht.

Die Prozesse für die Spezifikation und den Nachweis der Erfüllung der RAMS-Anforderungen sind die Ecksteine dieser Norm. Diese Europäische Norm fördert ein gemeinsames Verständnis und eine gemeinsame Vorgehensweise für das RAMS-Management.

EN 50126 ist ein Teil der für den Bahnsektor spezifischen Anwendung von IEC 61508. Die Einhaltung der Anforderungen dieser Europäischen Norm in Verbindung mit den Anforderungen anderer geeigneter Normen ist ausreichend, um sicherzustellen, dass ein zusätzlicher Nachweis der Übereinstimmung mit IEC 61508 nicht erforderlich ist.

Hinsichtlich der Sicherheit liefert **EN 50126-1** einen Sicherheitsmanagementprozess, der durch die in EN 50126-2 gegebene Anleitung und beschriebenen Verfahren unterstützt wird.

EN 50126-1 und EN 50126-2 sind unabhängig von der angewendeten Technologie. Soweit Sicherheit betroffen ist, basiert EN 50126 auf einem funktionalen Ansatz.

Die Anwendung dieser Norm sollte an die spezifischen Anforderungen des betrachteten Systems adaptiert werden.

Diese Europäische Norm kann von den Bahnunternehmen und Lieferanten systematisch während aller Phasen des Lebenszyklus angewendet werden, um bahnspezifische RAMS-Anforderungen zu entwickeln und um Übereinstimmung mit diesen Anforderungen zu erzielen. Der in dieser Europäischen Norm entwickelte Ansatz über verschiedene Systemebenen ermöglicht die Bewertung von RAMS-Wechselbeziehungen zwischen den Elementen von Bahnanwendungen – selbst dann, wenn diese von komplexer Art sind.

Diese Europäische Norm fördert die Zusammenarbeit zwischen den Akteuren des Eisenbahnwesens um für Bahnanwendungen eine optimale Kombination von RAMS und Kosten zu erreichen. Die Übernahme dieser Europäischen Norm unterstützt die Grundsätze des europäischen Binnenmarkts und erleichtert die Interoperabilität der europäischen Bahnen.

Entsprechend den CENELEC-Regeln¹ werden die verbindlich vorgeschriebenen Anforderungen in dieser Norm durch das Modalverb „muss/müssen“ angezeigt. Wo dies berechtigt ist, erlaubt die Norm die Anpassung der Prozesse.

In EN 50126-2 wird eine spezifische Anleitung zur Anwendung dieser Norm bei Sicherheitsaspekten gegeben. EN 50126-2 stellt verschiedene Verfahren für die Anwendung im Sicherheitsmanagementprozess zur Verfügung. Wurde ein bestimmtes Verfahren für das betrachtete System ausgewählt, so sind die

¹ CEN/CENELEC *Internal Regulations Part 3: Rules for the structure and drafting of CEN/CENELEC Publications* (2017-02), Annex H.

verbindlich vorgeschriebenen Anforderungen dieses Verfahrens notwendigerweise auch für das Sicherheitsmanagement des betrachteten Systems verbindlich vorgeschrieben.

Diese Europäische Norm besteht aus dem Hauptteil ([Abschnitt 1](#) bis [Abschnitt 11](#)) und den [Anhängen A, B, C, D, E, F, G](#) und [ZZ](#). Die im Hauptteil dieser Norm definierten Anforderungen sind normativ, während die Anhänge informativ sind.

1 Anwendungsbereich

Dieser Teil 2 von EN 50126:

- behandelt die sicherheitsbezogenen generischen Aspekte des RAMS-Lebenszyklus;
- legt Verfahren und Werkzeuge fest, die von der tatsächlichen Technik der Systeme und Subsysteme unabhängig sind;
- vermittelt:
 - dem Anwender der Norm ein Verständnis des Systemansatzes zur Sicherheit, bei dem es sich um ein Schlüsselkonzept von EN 50126 handelt;
 - Verfahren für die Ableitung der Sicherheitsanforderungen und der dazugehörigen Sicherheitsintegritätsanforderungen an das System sowie zu deren Aufteilung auf die Subsysteme;
 - Verfahren zur Ableitung der Sicherheits-Integritätslevels (SIL) für die sicherheitsbezogenen elektronischen Funktionen.

ANMERKUNG Diese Norm gestattet nicht die Zuordnung von Sicherheits-Integritätslevels zu nicht-elektronischen Funktionen. .

- enthält Anleitungen und Verfahren für die folgenden Bereiche:
 - Sicherheitsprozess;
 - Nachweis der Sicherheit und -abnahme,
 - Organisation und Unabhängigkeit von Funktionen,
 - Risikobewertung,
 - Festlegung von Sicherheitsanforderungen,
 - Aufteilung von funktionsbezogenen Sicherheitsanforderungen,
 - Entwurf und Implementierung;
- stellt dem Anwender dieser Norm die Verfahren für die Sicherstellung der Sicherheit in Bezug auf das betrachtete System und dessen Wechselwirkungen zur Verfügung;
- enthält Anleitungen für das Definieren des betrachteten Systems, einschließlich der Ermittlung der Schnittstellen und der Wechselwirkungen dieses Systems mit seinen Subsystemen oder anderen Systemen, mit dem Ziel der Durchführung der Risikoanalyse;
- definiert keine(n):
 - RAMS-bezogene Ziele, Quantitäten, Anforderungen an oder Lösungen für spezifische Bahnanwendungen,
 - Regeln oder Prozesse in Bezug auf die Zertifizierung von Bahnprodukten entsprechend den Anforderungen dieser Norm,
 - Prozess für die Zulassung durch Sicherheitsbehörden.

Dieser Teil 2 von EN 50126 ist auf alle Bahnanwendungsbereiche anwendbar, namentlich auf die Zugsteuerung, Zugsicherung und Signalgebung (Signaltechnik), auf Bahnfahrzeuge und ortsfeste Anlagen, und speziell:

- auf die Festlegung und den Nachweis der Sicherheit für alle Bahnanwendungen und auf alle Ebenen einer solchen Anwendung, soweit zutreffend, von kompletten Bahnsystemen bis zu Hauptsystemen und individuellen und kombinierten Subsystemen und Komponenten innerhalb dieser Hauptsysteme einschließlich jener, die Software enthalten; insbesondere:
 - auf neue Systeme;
 - auf neue Systeme, die in bestehende und bereits abgenommene Systeme integriert sind, jedoch nur sofern und soweit das neue System mit der neuen Funktionalität integriert ist; er ist ansonsten nicht anwendbar auf jegliche unveränderten Aspekte des bestehenden Systems;

- soweit vernünftigerweise machbar, auf Modifikationen und Erweiterungen von bestehenden und bereits vor Erstellung dieser Norm anerkannten Systemen, jedoch nur sofern und soweit bestehende Systeme modifiziert werden; er ist ansonsten nicht anwendbar auf jegliche unveränderten Aspekte des bestehenden Systems;
- in allen maßgeblichen Lebenszyklusphasen einer Anwendung;
- für die Anwendung durch Bahnunternehmen und Bahnzulieferer.

Es ist nicht erforderlich, diese Norm auf bestehende Systeme anzuwenden, die unverändert bleiben, einschließlich jener Systeme, die bereits mit einer älteren Version von EN 50126 übereinstimmen.

Der in dieser Europäischen Norm definierte Prozess setzt voraus, dass die betreffenden Bahnunternehmen und deren Lieferanten Unternehmensstrategien bezüglich Qualität, Leistung und Sicherheit besitzen. Der in dieser Norm definierte Ansatz entspricht der Anwendung von Anforderungen aus EN ISO 9001 an das Qualitätsmanagement.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, 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).

EN 50126-1:2017, *Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach **EN 50126-1:2017**.

4 Abkürzungen

ALARP	so niedrig wie vernünftigerweise in der Praxis akzeptabel (en: As Low As Reasonably Practicable)
CBA	Kosten-Nutzen-Analyse (en: Cost Benefit Analysis)
CCF	Ausfall infolge gemeinsamer Ursache (Analyse) (en: Common Cause Failure (Analysis))
CoP	Regelwerke (en: Code of Practice)
COTS	kommerzielles Standardprodukt (en: Commercial Off-The-Shelf)
DRA	differentielle Risikoaversion (en: Differential Risk Aversion)
ERE	explizite Risikoeinschätzung (en: Explicit Risk Estimation)
EMV	elektromagnetische Verträglichkeit (en: ElectroMagnetic Compatibility)
ETA	Ereignisbaumanalyse (en: Event Tree Analysis)
FMECA	Fehlermöglichkeits-, Einfluss- und Kritikalitäts-Analyse (en: Failure Mode, Effects and Criticality Analysis)
FTA	Fehlerbaumanalyse (en: Fault Tree Analysis)
GA	generische Anwendung (en: Generic Application)
GASC	Sicherheitsnachweis der generischen Anwendung (en: Generic Application Safety Case)
GP	generisches Produkt (en: Generic Product)
GPSC	Sicherheitsnachweis des generischen Produkts (en: Generic Product Safety Case)
GAME	Insgesamt mindestens gleichwertig Globalement Au Moins Equivalent
HAZOP	Gefahren- und Operabilitätsstudie(en: Hazard and Operability study)

IM	Infrastrukturbetreiber (en: Infrastructure Manager)
LRU	vor Ort auswechselbare Einheit (en: Line Replaceable Unit)
MEM	minimale endogene Mortalität (en: Minimum Endogenous Mortality)
RAC	Risikoakzeptanzkriterium (en: Risk Acceptance Criterion)
RAMS	Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (en: Reliability, Availability, Maintainability and Safety)
RAP	Risikoakzeptanzprinzip (en: Risk Acceptance Principle)
RBD	Zuverlässigkeitsblockdiagramm (en: Reliability Block Diagram)
RRA	Rapid-Ranking-Analyse (en: Rapid Ranking Analysis)
RU	Bahnunternehmen (en: Railway Undertaking)
SA	spezifische Anwendung (en: Specific Application)
SASC	Sicherheitsnachweis der spezifischen Anwendung (en: Specific Application Safety Case)
SDR	sichere Ausfallrate (en: Safe Down Rate)
SDT	sichere Unklardauer (en: Safe Down Time)
SIL	Sicherheits-Integritätslevel (en: Safety Integrity Level)
SRAC	sicherheitsbezogene Anwendungsbedingungen (en: Safety-Related Application Conditions)
TFFR	tolerierbare funktionale Ausfallrate (en: Tolerable Functional Failure Rate)
THR	tolerierbare Gefährdungsrate (en: Tolerable Hazard Rate)

5 Sicherheitsprozess

5.1 Risikobewertung und Gefährdungsbeherrschung

In diesem Abschnitt wird das „Sanduhrmodell“ eingeführt: Es bietet einen vereinfachten Ansatz, der hilft, einige Fragen zu klären, obwohl er nicht alle vom Lebenszyklusmodell implizierten Aspekte enthält.

Das Sanduhrmodell liefert einen Überblick über die wesentlichen sicherheitsbezogenen Aktivitäten, die erforderlich sind, um einen akzeptablen Sicherheitsniveau eines technischen Systems, einschließlich der entsprechenden Verantwortungsbereiche, sicherzustellen.

Technisches System bedeutet ein Produkt oder der Verbund von Produkten, einschließlich des Entwurfs, der Implementierung und der für den Support erforderlichen Dokumentation. Die Entwicklung eines technischen Systems beginnt mit der Spezifikation seiner Anforderungen und endet mit seiner Abnahme. Der Entwurf von relevanten Schnittstellen wird unter Berücksichtigung der Wechselwirkungen mit Bedienungspersonen und ihrem Verhalten betrachtet, obgleich diese Bedienungspersonen selbst und ihre Aktionen nicht Bestandteil des technischen Systems sind. Sowohl der Instandhaltungsprozess (beschrieben in den Instandhaltungshandbüchern) als auch der Betrieb werden festgelegt bzw. spezifiziert, aber nicht als Teil des technischen Systems selbst betrachtet. Sie können durch die „Anwendungsbedingungen“ beschränkt werden.

Der Zweck dieses Modells ist es, die Trennung der Risikoanalyse als Teil der Risikobewertung (auf der Ebene des Bahnsystems) von der Gefährdungsanalyse als Teil der Gefährdungsbeherrschung (auf der Ebene des betrachteten Systems) hervorzuheben.

Dieses fördert die Zusammenarbeit zwischen den relevanten Akteuren, indem die Verantwortlichkeiten und Schnittstellen geklärt werden, und hat den Vorteil, die Komplexität zu verringern und die Modularisierung zu erleichtern.

Das Sanduhrmodell beschreibt zwei Hauptaspekte:

- die Risikobewertung, in der Sicherheitsanforderungen an betriebliche und technische Aspekte (einschließlich Instandhaltung) abgeleitet werden, und
- die Gefährdungsbeherrschung, die mittels Ursachenermittlung und -analyse und mit Hilfe des Entwurfs und der Implementierung von Steuerungsmaßnahmen gegebene, von höheren Ebenen gestellte Anforderungen an die Funktionssicherheit erfüllt.

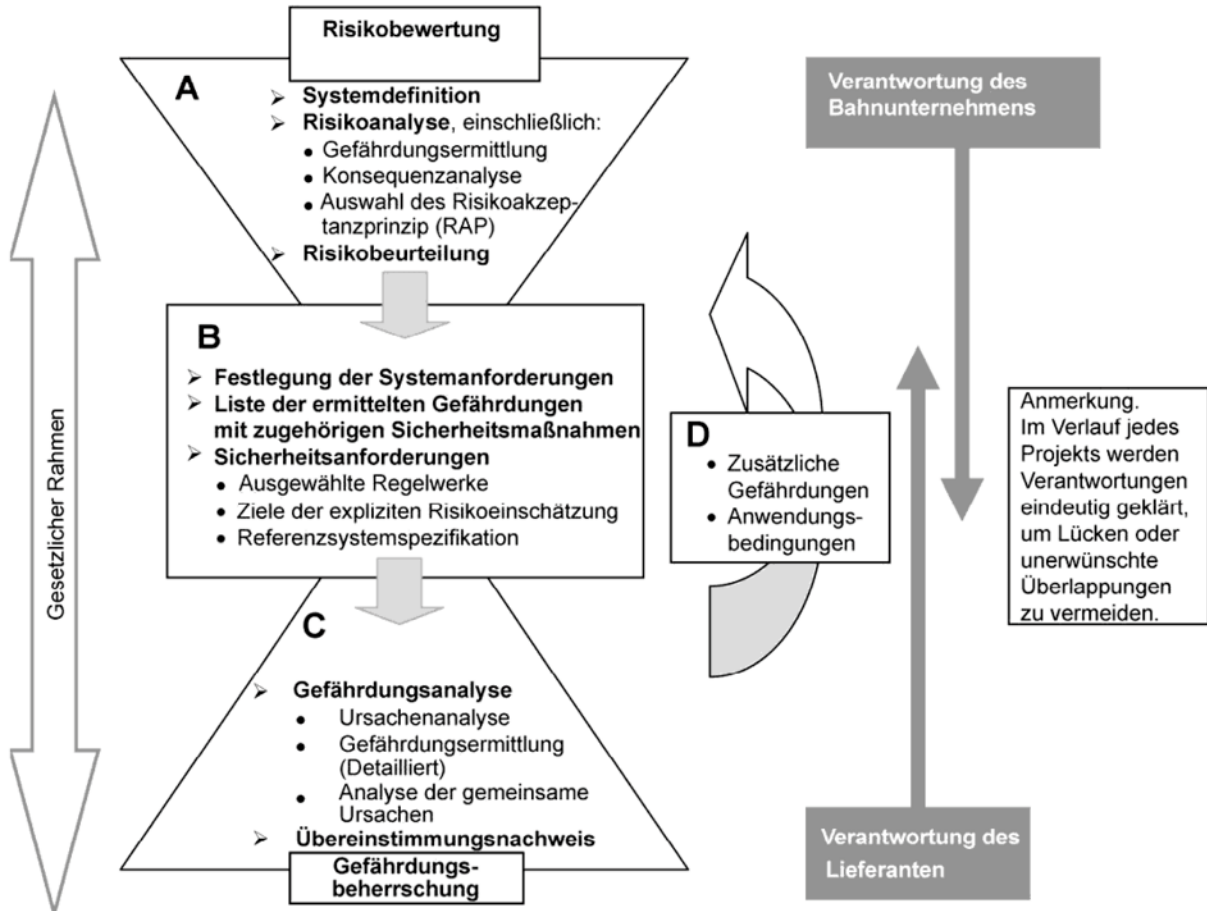


Bild 1 – Das Sanduhrmodell

ANMERKUNG Teil A (Risikobewertung) ist mit den Phasen 1 bis 3 des Lebenszyklus verbunden, wie in EN 50126-1:2017, Bild 4 dargestellt. Teil B entspricht Phase 4 und Teil C den Phasen 5 bis 9. Teil D zeigt die „Rückkopplung von später ermittelten Gefährdungen an die Risikoanalyse“ (siehe EN 50126-1:2017, Bild 4).

5.2 A. Risikobewertung

5.2.1 Allgemeines

Die Risikobewertung erfolgt auf der Bahnsystemebene.

Sie beruht auf einer Systemdefinition und umfasst die Risikoanalyse und die Risikobeurteilung.

Sie legt auf hoher Ebene die Sicherheitsanforderungen an das System und besonders Sicherheitsanforderungen an das betrachtete System aus der Perspektive des Bahnunternehmens und des Betreibers fest. Sie berücksichtigt sicherheitsbezogene betriebliche Aspekte, frühere Erfahrungen und gesetzliche Anforderungen an die Bahnanwendung.

Die Hauptaufgabe für diese Tätigkeit ist die Risikoanalyse, die aus der Systemdefinition abgeleitet wird. Die Risikoanalyse umfasst die Gefährdungsermittlung, die Auswirkungsanalyse und die Auswahl des Risikoakzeptanzprinzips (RAP).

Die Festlegung von Sicherheitsanforderungen ist das Endergebnis der Risikobewertung^{N1}; in [Bild 1](#) ist dies dem Kästchen B zugeordnet, weil sie (zusammen mit den Systemanforderungsspezifikationen und der Liste der ermittelten Gefährdungen) eine Schnittstelle zwischen unterschiedlichen Verantwortungen bildet.

5.2.2 Durchführen der Risikobewertung

Der Detaillierungsgrad einer Risikobewertung sollte geeignet sein, eine sachgemäße Betrachtung des Risikos zu ermöglichen. Es ist weder das Ziel, jede banale Gefährdung zu katalogisieren, noch wird erwartet, dass immer alle Gefährdungen jenseits der Grenzen des aktuellen Kenntnisstands identifiziert werden. Eine Risikobewertung sollte eine vernünftige Analyse der Gefährdungen und der damit verbundenen Risiken innerhalb des Bahnbetriebs und innerhalb der angewendeten Technik selbst wiedergeben. Falls dies als lohnend erachtet wird, sollten Risikobewertungen mit historischen Datensätzen zu Unfällen und deren Ursachen korreliert werden.

Wenn möglich, sollte die Betrachtung der technischen Implementierung/Architektur in dieser ersten Phase vermieden werden, d. h. das zu entwickelnde System sollte als „Black Box“ angesehen werden, deren Funktionen und Gefährdungen nur an den Grenzen bewertet werden. Diese Grenzen sind eindeutig definierte Schnittstellen zwischen der Betriebsumgebung und dem betrachteten System.

Eine „unbeabsichtigte Zugbewegung“ z. B. ist eine Gefährdung für einen Zug. Abstrahiert kann sie an der Grenze des „Systems Zug“ beobachtet werden, und sie könnte, abhängig vom betrieblichen Kontext, zu unterschiedlichen Unfällen führen (z. B. zu einer Kollision im Zusammenhang mit Geschwindigkeitsüberschreitung während der Fahrt oder zum Sturz von Personen in Verbindung mit einer Zugbewegung im Bahnhof, wo ein Stillstand erwartet wird, usw.).

Die im Rahmen der Risikobewertung definierten Annahmen müssen im gesamten Verlauf der Phasen des Lebenszyklus überprüft und aktualisiert werden.

5.3 B. Ergebnis der Risikobewertung

Die Ergebnisse der Risikobewertung sind ein Satz von Sicherheitsanforderungen, die mit eindeutig ermittelten Funktionen, Systemen oder Betriebsregeln verbunden sind. Sie sind Teil der Systemanforderungsspezifikation, die die technische Schnittstelle zwischen den Akteuren festschreibt.

ANMERKUNG Die Projekt-Organisationsstruktur und Verantwortlichkeiten sind weitere Faktoren, die für das Verständnis und die Beherrschung des Risikos zu berücksichtigen sind. Zu den organisatorischen Aspekten und Anforderungen wird empfohlen, auf [Abschnitt 7](#) Bezug zu nehmen.

Auf Basis der gewählten Risikoakzeptanzprinzipien können sich Sicherheitsanforderungen auf das Anwenden der Regelwerke oder auf Referenzsysteme beziehen oder aus der expliziten Risikoeinschätzung (ERE) abgeleitete explizite Ziele angeben.

Die Sicherheitsanforderungen umfassen notwendige Sicherheitsfunktionen, die quantitativ (z. B. maximale Gefährdungsraten), semiquantitativ oder qualitativ (z. B. der Verwendung von geschulten Triebfahrzeugführern, um menschliche Fehler zu beherrschen) bewertet werden können.

Sicherheitsanforderungen sollten unter Anwendung eines ganzheitlichen Ansatzes auf das betrachtete System bewertet werden, d. h. das Restrisiko des Gesamtsystems nach Einführung der Sicherheitsanforderungen sollte unter Berücksichtigung aller ermittelten Gefährdungen bewertet werden.

5.4 C. Gefährdungsbeherrschung

Die Phase der Gefährdungsbeherrschung im Sanduhrmodell stellt sicher, dass das betrachtete System den Sicherheitsanforderungen genügt. Die Gefährdungsbeherrschung wird für eine bestimmte Systemarchitektur durchgeführt.

^{N1} Nationale Fußnote: Das nationale Komitee weist darauf hin, dass hier die Risikobeurteilung gemeint ist.

Die wesentlichen Auswirkungen von menschlichen Faktoren, betrieblichen und allgemeinen Instandhaltungsregeln und -verfahren sind Teil der vorausgegangenen Risikoanalyse und sollten in den Sicherheitsanforderungen bereits berücksichtigt sein. Daher kann der Entwerfer des betrachteten Systems seinen Schwerpunkt während der Gefährdungsbeherrschung auf die internen Ursachen der ermittelten Gefährdungen legen.

Die Hauptaufgabe ist die „Gefährdungsanalyse“, die Folgendes umfasst:

- eine zweckbestimmte Gefährdungsermittlung, die sich schwerpunktmäßig auf das betrachtete System konzentriert (detailliert);
- eine Ursachenanalyse;
- eine Analyse von gemeinsamen Ursachen (zu Einzelheiten siehe 11.4).

Die Gefährdungsermittlung ist eine wiederkehrende Aufgabe, die auf mehreren Ebenen während der Entwicklung des betrachteten Systems iteriert. Um diese verschiedenen Aufgaben (und die zugehörigen Dokumente) zu unterscheiden, ist die Gefährdungsermittlung in Bild 1 zweimal aufgeführt:

1. Während der Risikobewertung liegt der Schwerpunkt der Gefährdungsermittlung auf den aus den Systemfunktionen (Black Box) und dem damit verbundenen Betrieb des Systems sowie seiner Umgebung abgeleiteten Gefährdungen auf hoher Systemebene;
2. Im Rahmen der Gefährdungsbeherrschung wird der Schwerpunkt einer verfeinerten/iterativen Gefährdungsermittlung auf Gefährdungen und ihre sich aus technischen Lösungen, d. h. aus der definierten Architektur und internen Schnittstellen des betrachteten Systems, ableitenden Ursachen sowie auf potenzielle neue Gefährdungen gelegt, die vom System selbst eingeführt werden.

Beide Arten der ermittelten Gefährdungen müssen im Rahmen der Gefährdungsbeherrschung behandelt werden. Bild 2 zeigt den allgemeinen Fall, bei dem die Ursache einer Gefährdung auf der Ebene des Bahnsystems in einer Gefährdung auf der Ebene des betrachteten Systems in Bezug auf dessen Grenzen besteht. Die Grenze für eine Gefährdungsermittlung ist immer durch die Systemdefinition, die den Anwendungsbereich der Aufgabe begrenzt, gegeben. Das bedeutet, dass die Gefährdungen hierarchisch strukturiert sind. Daher sollte ein hierarchischer Ansatz der Gefährdungsanalyse und Gefährdungsprotokollierung angewendet werden.

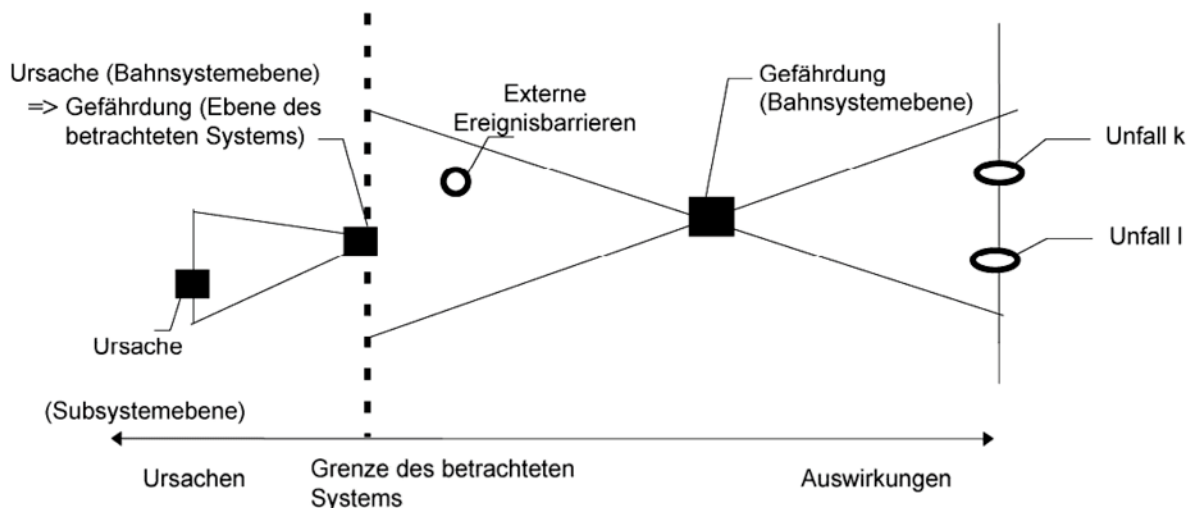


Bild 2 – Darstellung der Gefährdungen in Bezug auf die Systemgrenzen

Das Bild ist gefährdungsorientiert und hat die Form eines Querbinders (Krawattenschleife, „Fliege“) und zeigt damit auf, dass verschiedene Ursachen zur selben Gefährdung führen können und dass eine Gefährdung zu verschiedenen Unfällen führen kann.

BEISPIEL Die Gefährdung auf der Bahnsystemebene ist ein Zug, der ein Signal unter Gefahr überfährt und damit in die Strecke eines anderen Zuges einfährt, was potenziell zu einer Kollision (dem Unfall) führt. Die Ursache auf der Bahnsystemebene (die Gefährdung auf der Ebene des betrachteten Systems) ist ein zu langer Bremsweg. Die Ursache

auf der Subsystemebene ist, dass der Triebfahrzeugführer die Bremsen nicht (oder zu spät) betätigte. Die externe Ereignisbarriere wird durch eine Schutzeinrichtung gebildet, die eine Notbremsung befiehlt.

Der Nachweis der Übereinstimmung des betrachteten Systems mit den Sicherheitsanforderungen kann mittels verschiedener Formen der Verifizierung geführt werden. Diese Formen hängen von der Beschaffenheit des zu Beginn der Gefährdungsbeherrschung zugrundeliegenden Anforderungssatzes ab.

5.5 D. Überprüfung der Risikobewertung

Während der Phase der Gefährdungsbeherrschung kann die Erfüllung von Sicherheitsanforderungen unter Umständen nicht mit der ersten Iteration erreicht werden. Drei mögliche Ursachen sind, dass:

- auf der Ebene des betrachteten Systems zusätzliche Gefährdungen ermittelt werden;
- sich ein Bedarf nach neuen Betriebsregeln ergibt;
- zusätzliche externe Sicherheitsmaßnahmen erforderlich sein können, um die Sicherheitsziele zu erfüllen.

In all diesen Fällen ist eine Überprüfung und gegebenenfalls Überarbeitung der Risikobewertung notwendig.

In diese Überprüfung sollten auch die Anwendungsbedingungen einbezogen werden, die auf der Ebene des betrachteten Systems entstehen können.

5.6 Verantwortlichkeiten

Die Risikobewertung liegt hauptsächlich in der Verantwortung der Bahnunternehmen und Betreiber. Falls vom Bahnunternehmen oder Betreiber keine Risikobewertung zur Verfügung gestellt wird, dürfen die Funktionen und Verantwortlichkeiten im Unterauftrag an andere Parteien (Hersteller und Lieferanten) delegiert werden, vorausgesetzt, diese besitzen dokumentierte und ausreichende Kompetenzen, um den gesamten betrieblichen Kontext im Detail betrachten zu können. Sie müssen unter Berücksichtigung von sicherheitsbezogenen betrieblichen Aspekten, früheren Erfahrungen und gesetzlichen Anforderungen das Risiko bewerten, das sich aus der Einführung von Änderungen am betrieblichen Kontext ergibt. In jedem Fall sollten die Bahnunternehmen die Ergebnisse der Risikobewertung akzeptieren.

Der Lieferant des technischen Systems trägt die Verantwortung für die Gefährdungsbeherrschung. Falls mehrere Lieferanten für verschiedene betrachtete Systeme verantwortlich sind, muss das Bahnunternehmen die Verantwortung für die Organisation der übergreifenden Gefährdungsbeherrschung tragen.

Bahnunternehmen und Lieferanten müssen die geltenden gesetzlichen Anforderungen erfüllen.

6 Nachweis der Sicherheit und der Sicherheitsabnahme

6.1 Einleitung

Dieser Abschnitt enthält zusätzliche Einzelheiten zu den Prozessen zum Nachweis der Sicherheit (en: safety demonstration) und der Sicherheitsabnahme für das betrachtete System. Mit Ausnahme der Stellen, an denen dies als angemessen angesehen wird, legt er nicht fest, wer die Arbeit in jeder Phase durchführen sollte, weil dies aufgrund verschiedener Umstände variieren kann.

Die Belege für den Nachweis der Sicherheit basieren auf dem Sicherheitsnachweis (en: safety case). Zweck und Inhalt des Sicherheitsnachweises sind in **EN 50126-1:2017, Abschnitt 8** definiert.

In Bezug auf Sicherheitsprozesse kann die Entwicklung eines Systems in drei Typen kategorisiert werden:

- Generisches Produkt: Das System wird von einem generischen Standpunkt aus betrachtet, der für verschiedene Anwendungsklassen geeignet ist;
Analysen werden innerhalb eines betrieblichen Kontextes durchgeführt, der anwendungsunabhängig ist.
- Generische Anwendung: Das System wird als für mehrfache Anwendungen derselben Klasse geeignet angesehen.

Analysen werden innerhalb eines betrieblichen Kontextes durchgeführt, der anwendungsabhängig ist. Der Sicherheitsprozess schließt die Festlegung des Anwendungsentwurfsprozesses ein.

- Spezifische Anwendung: Das System wird für eine spezifische Anwendung (einschließlich deren physischer Implementierung) betrachtet.

6.2 Prozess zum Nachweis der Sicherheit und zur Sicherheitsabnahme

Drei verschiedenen Kategorien von Sicherheitsnachweisen - wie zuvor definiert - können entsprechend des betroffenen Entwicklungstyps festgelegt werden.

- generisches Produkt;
- generische Anwendung;
- spezifische Anwendung.

In allen drei Kategorien ist die Gliederung des Sicherheitsnachweises im Wesentlichen gleich.

Der Sicherheitsnachweis für die spezifische Anwendung muss die beiden folgenden Aspekte behandeln:

- den Anwendungsentwurf;
- die physische Implementierung, einschließlich Herstellung, Installation und der Einrichtungen für Betrieb und Instandhaltung.

Falls für den Anwendungsentwurf und die physische Implementierung der Anwendung getrennte Sicherheitsnachweise benötigt werden, kann die Möglichkeit bestehen, den Sicherheitsnachweis für spezifische Anwendungen in zwei Teile aufzuteilen:

- den Sicherheitsnachweis für den Anwendungsentwurf;
- den Sicherheitsnachweis für die physische Implementierung.

Der Sicherheitsnachweis, wie in **EN 50126-1:2017, Abschnitt 8** festgelegt, umfasst Folgendes:

- **Teil 1:** Definieren des Systems (Systemdefinition);
- Teil 2: Qualitätsmanagementbericht;
- Teil 3: Sicherheitsmanagementbericht;
- Teil 4: technischer Sicherheitsbericht;
- Teil 5: Beziehung zu anderen Sicherheitsnachweisen (sofern anwendbar);
- Teil 6: Schlussfolgerung.

Immer wenn eine unabhängige Sicherheitsbewertung für das betrachtete System gefordert ist, wird diese vor der Systemabnahme durchgeführt, um zusätzlich zu belegen, dass das notwendige Sicherheitsniveau erreicht wurde.

In diesem Fall muss die unabhängige Sicherheitsbewertung den zum betrachteten System gehörenden Sicherheitsnachweis einbeziehen und unter Einhaltung der in **EN 50126-1:2017, 6.8** festgelegten Anforderungen durchgeführt werden, wobei die Unabhängigkeit der Funktionen, wie in EN 50126-2:2017, **7.3** definiert, zu wahren ist.

Die Abnahme des betrachteten Systems als für seine vorgesehene Anwendung angemessen sicher muss auf den folgenden Bedingungen basieren:

- Es wurde entsprechend der Normenreihe EN 50126 entwickelt, verifiziert und validiert;
- die festgelegten Sicherheitsanforderungen wurden entsprechend der Normenreihe EN 50126 erfüllt.

Die dokumentierten Nachweise für die Systemabnahme insgesamt sollten Folgendes umfassen:

- die Systemdefinition und den betrieblichen Kontext;
- die Systemanforderungen und -kennwerte, einschließlich der Sicherheitsanforderungen (und der damit verbundenen Risikoanalyse, sofern anwendbar);

- den Sicherheitsnachweis;
- den Bericht zur unabhängigen Sicherheitsbewertung, falls gefordert. Dieser Bericht erläutert die Aktivitäten, die durchgeführt werden, um festzustellen, ob das betrachtete System so ausgelegt ist, dass es die dafür festgelegten Sicherheitsanforderungen erfüllt, und um bei Bedarf einige zusätzliche Bedingungen für seinen Betrieb festzulegen.

Die Sicherheitsabnahme kann von denjenigen, die für die Integration in ein anderes System oder den letztendlichen Gebrauch des betrachteten Systems verantwortlich sind, erteilt werden, sofern alle Bedingungen für die Sicherheitsabnahme, wie durch den Sicherheitsnachweis belegt, erfüllt sind und die Ergebnisse der unabhängigen Sicherheitsbewertung, sofern diese gefordert ist, vorliegen.

Wird im Zusammenhang mit einer spezifischen Anwendung ein generisches (d. h. von der Anwendung unabhängiges) Produkt oder eine generische Anwendung (d. h. die Anwendungsklasse) verwendet, so sollte es möglich sein, die Sicherheitsabnahme auf einer vorhandenen, diesbezüglich unabhängige Sicherheitsbewertung^{N2} basieren zu lassen. Diese Vorgehensweise gilt als nicht übertragbar auf spezifische Anwendungen.

Wird ein Sicherheitsnachweis für ein generisches (d. h. von der Anwendung unabhängiges) Produkt oder für eine generische Anwendung (d. h. die Anwendungsklasse) entwickelt, so muss eine Validierungsaktivität für das betrachtete System, die üblicherweise in der als „Systemvalidierung“ bezeichneten Lebenszyklusphase 9 des Systems durchgeführt wird, auch am Ende der Lebenszyklusphase 6 „Entwurf und Implementierung“ durchgeführt werden, wobei auch die Herstellung der ersten Baueinheit^{N3} zu berücksichtigen ist.

Bild 3 zeigt ein Beispiel für einen Sicherheitsabnahmeprozess für alle drei Kategorien von Sicherheitsnachweisen, bei dem der Sicherheitsprozess für eine spezifische Anwendung sowohl allein als auch als Herleitung aus einem Sicherheitsprozess für ein generisches Produkt oder eine generische Anwendung betrachtet wird.^{N4}

Entsprechend den in **EN 50126-1** definierten Anforderungen zur Anpassung muss der für einen gegebenen Sicherheitsprozess verantwortliche Akteur Nachweise und Begründungen für die Abdeckung und die Grenzen der betreffenden Lebenszyklusphasen bringen.

^{N2} Nationale Fußnote: Das nationale Komitee weist darauf hin, dass die Sicherheitsbewertung hier die des generischen Produktes oder der generischen Anwendung ist.

^{N3} Nationale Fußnote: Das nationale Komitee weist darauf hin, dass hier die erste Baueinheit des generischen Produktes oder der generischen Anwendung gemeint ist.

^{N4} Nationale Fußnote: Das nationale Komitee weist darauf hin, dass hier „nicht auf Basis der generischen Anwendung oder des generischen Produktes“ gemeint ist.

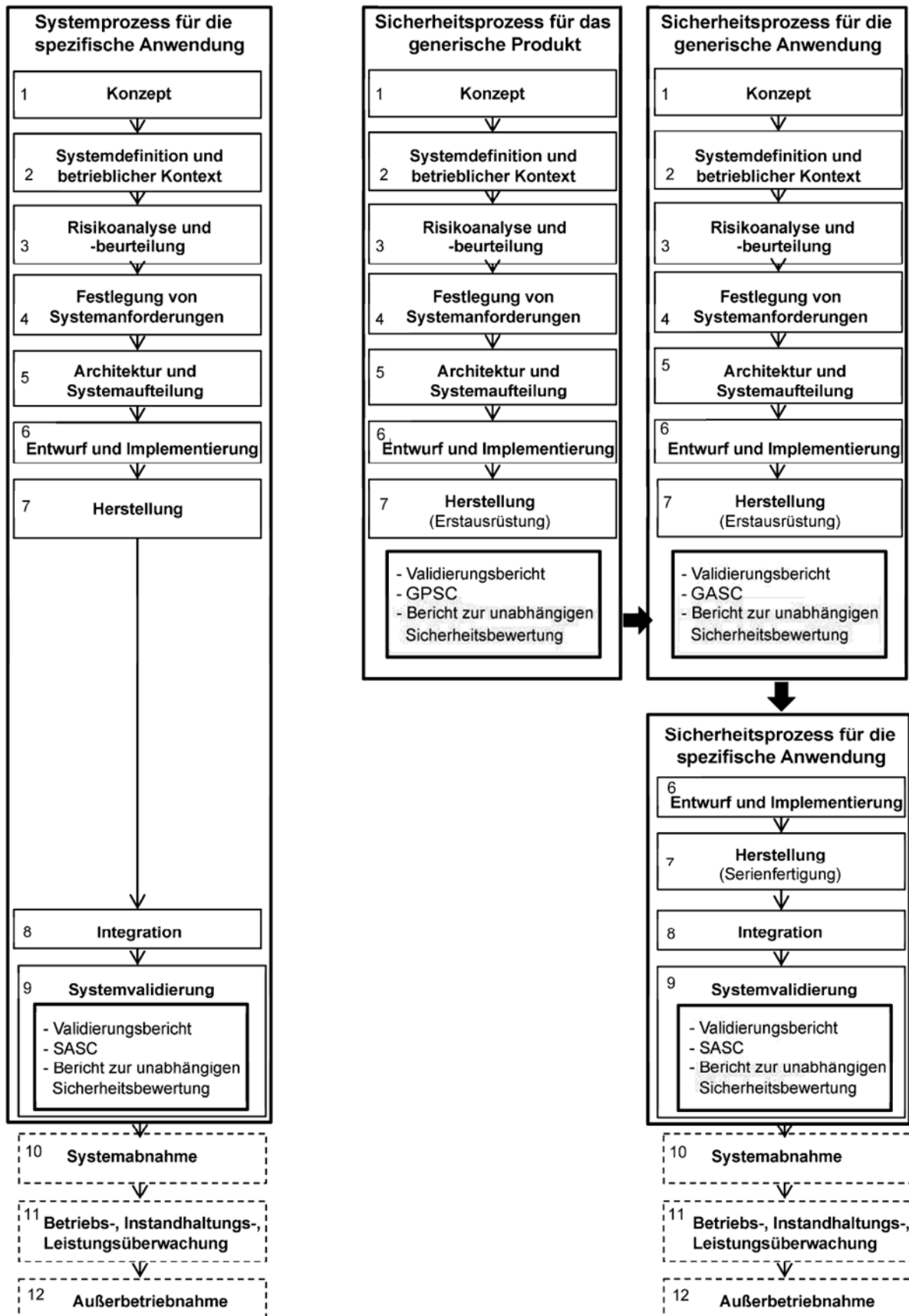


Bild 3 – Beispiel für Sicherheitsabnahmeprozesse

6.3 Verantwortung für das Management des Sicherheitsnachweises

Die Verantwortung für das Management des Sicherheitsnachweises hängt von der festgelegten Beziehung zwischen den Akteuren ab und unterliegt vertraglichen Vereinbarungen. Üblicherweise:

- ist der Sicherheitsnachweis für das generische Produkt der Beleg, der vom Lieferant für die Partei ausgestellt wird, die die Verantwortung für die Konfiguration des Produkts für die Nutzung trägt (z. B. ein Lieferant oder eine Vertragspartei);
- ist der Sicherheitsnachweis für die generische Anwendung der Beleg, der von der Partei, die die Verantwortung für die generische Konfiguration des Produktes trägt (z. B. ein Produktlieferant), der Partei ausgestellt wird, die die Verantwortung für die spezifische Konfiguration trägt (z. B. der Lieferant, eine Vertragspartei oder die Lieferorganisation im Falle eines RU/IM-Projekts);
- ist der Sicherheitsnachweis für die spezifische Anwendung der Beleg, der von der Partei, die das System für die Nutzung konfiguriert (z. B. der Lieferant oder eine Vertragspartei oder die Lieferorganisation im Falle eines RU/IM-Projektes), für die Partei ausgestellt wird, die die Verantwortung für die in Betrieb befindliche Bahn trägt (z. B. das Bahnunternehmen [en: Railway Undertaking, RU] oder der Infrastruktur Manager [IM]).

Mit dem Voranschreiten des Arbeitsprozesses von generischen zu spezifischen Anforderungen entwickelt sich das Sicherheitsargument und baut auf jedem vorangegangenen Sicherheitsnachweis auf, weswegen der endgültige Sicherheitsnachweis für die spezifische Anwendung Belege aus allen in Beziehung stehenden Sicherheitsnachweisen umfasst. In jeder Phase werden sicherheitsbezogene Anwendungsbedingungen entwickelt und vom jeweils nächsten Akteur weitergeführt. Der Sicherheitsnachweis für eine spezifische Anwendung und die darin festgelegten sicherheitsbezogenen Anwendungsbedingungen werden, sobald sie vom RU oder IM akzeptiert sind, definitionsgemäß zu einer Erweiterung des Sicherheitsmanagementsystems des RU oder IM. Auf dieser Ebene werden alle SRAC als erfüllt gewertet.

6.4 Modifikationen nach einer Sicherheitsabnahme

Nachdem ein System, ein Subsystem oder eine Komponente die Sicherheitsabnahme erhalten hat, muss jede nachträgliche Modifikation mit demselben Qualitäts- und Sicherheitsmanagement und anhand derselben funktionalen/technischen Sicherheitskriterien überwacht werden, wie für einen neuen Entwurf üblich. Die gesamte relevante Dokumentation, einschließlich des Sicherheitsnachweises, muss aktualisiert oder um zusätzliche Unterlagen ergänzt werden, und der modifizierte Entwurf sollte den Abnahmeprozessen des Sicherheitsmanagementsystems des Bahnunternehmens wie auch den im geltenden gesetzlichen Rahmen geforderten Zulassungsprozessen unterzogen werden.

Sobald ein installiertes System bzw. Subsystem oder eine installierte Komponente validiert und abgenommen ist, werden angemessene Verfahren, unterstützende Systeme und Sicherheitsüberwachungen, wie sie im Sicherheitsplan definiert wurden, angewendet, um den über den gesamten Lebenszyklus dauerhaft sicheren Betrieb, einschließlich Betrieb, Instandhaltung, Änderungen, Erweiterungen und eventuelle Außerbetriebnahme, sicherzustellen. Diese Aktivitäten werden mit Hilfe eines Qualitätsmanagements, Sicherheitsmanagements und von technischen Sicherheitskriterien überwacht, die mindestens so sicher sind wie die auf den ursprünglichen Entwurf angewendeten. Die kontinuierliche Sicherheit des Systems wird vom Bahnunternehmen gesteuert, und dies sollte erfordern, dass die maßgebliche Dokumentation, einschließlich des Sicherheitsnachweises, aktuell gehalten wird.

6.5 Abhängigkeiten zwischen Sicherheitsnachweisen

Der Sicherheitsnachweis für ein System könnte von den Sicherheitsnachweisen anderer Subsysteme oder Ausrüstung abhängen. In solchen Fällen ist die Sicherheitsabnahme des Hauptsystems nicht ohne eine vorherige Sicherheitsabnahme der in Beziehung stehenden Subsysteme/Betriebsmittel möglich.

Die Beziehung zwischen Sicherheitsnachweisen muss mit einer entsprechenden Dekomposition des Systems, die während der Lebenszyklusphase 2 „Systemdefinition und betrieblicher Kontext“ festgeschrieben wurde, in Zusammenhang stehen

Die verschiedenen Arten von Sicherheitsnachweisen dürfen dem Wiederverwendungsbedarf entsprechend festgelegt werden.

Wenn ein Bericht zur unabhängigen Sicherheitsbewertung für ein generische Produkt oder eine generische Anwendung erhalten wurde, darf für die Sicherheitsabnahme einer spezifischen Anwendung darauf verwiesen werden; es ist nicht notwendig, den generischen Prozess der unabhängigen Sicherheitsbewertung für jede spezifische Anwendung zu wiederholen. Diese Abhängigkeit zwischen Sicherheitsnachweisen wird anhand von Beispielen in Bild 4 veranschaulicht.

Ein Sicherheitsnachweis darf sich auf den Nachweis stützen, dass die vorgeschlagene spezifische Anwendung technisch gleichwertig zu einer vorhandenen Anwendung mit einer spezifischen Sicherheitsabnahme ist. Eine neue Sicherheitsabnahme für diese spezifische Anwendung ist notwendig.

Es ist von entscheidender Bedeutung, sicherzustellen, dass die sicherheitsbezogenen Anwendungsbedingungen (SRAC), die im technischen Sicherheitsbericht zu jedem Sicherheitsnachweis angegeben sind, im Sicherheitsnachweis der höheren Ebene erfüllt oder anderenfalls in die SRAC des Sicherheitsnachweises der höheren Ebene übernommen werden.

BEISPIEL 1 Bild 4 zeigt auf der linken Seite ein Beispiel, bei dem ein vollständiges ERTMS-System für die Strecke Nr 1 in einem Sicherheitsnachweis der spezifischen Anwendung behandelt wird, der auch ein Bahn-Stellwerk-System (IXL-System Nr 3) und ein Zugbeeinflussungssystem (ATC-System Nr 2) umfasst. Es werden keine anderen Sicherheitsnachweise wiederverwendet oder in Bezug genommen. Das bedeutet, dass die beiden Subsysteme (Stellwerk und Zugbeeinflussungssystem) innerhalb dieser Anwendung entwickelt werden und nicht von einer früher erfolgten Abnahme abhängen.

BEISPIEL 2 Bild 4 zeigt auf der rechten Seite ein Beispiel, bei dem ein Stellwerk-System für den Bahnhof Nr 4 auf einer generischen Anwendung basiert, die den Einsatz einer Klasse von ähnlichen Bahnhöfen unterstützt. Umgekehrt verwendet das generische Stellwerk-System seinerseits eine generische Signalstelleinrichtung. Daher basiert der Sicherheitsnachweis für die spezifische Anwendung auf zwei generischen Sicherheitsnachweisen.

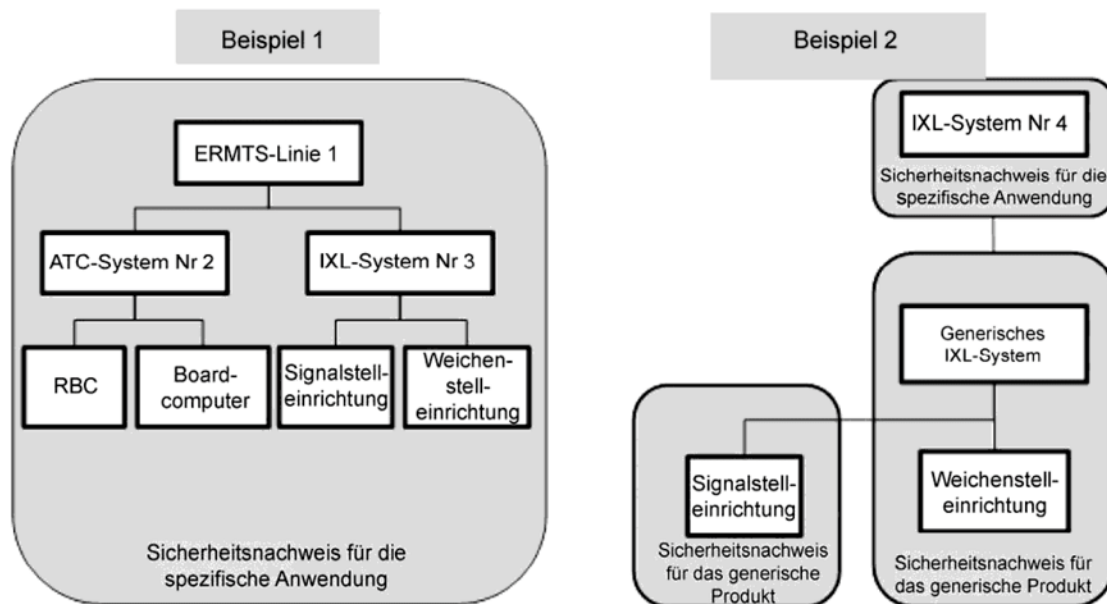


Bild 4 – Beispiele für Abhängigkeiten zwischen Sicherheitsnachweisen

6.6 Beziehung zwischen Sicherheitsnachweisen und Systemarchitektur

Es ist nicht notwendig, dass die Anzahl, der Anwendungsbereich und die Hierarchie der verschiedenen Sicherheitsnachweise (GPSC, GASC, SASC) die Architektursicht des in der Entwicklung befindlichen Systems widerspiegeln, d. h. „generisches Produkt“ (GP), „generische Anwendung“ (GA) und „spezifische Anwendung“ (SA). Die Sicherheitsnachweisarchitektur sollte nicht mit „System“, „Subsystem“ und „Komponente“ Architektursicht verwechselt werden.