NeGSt

Neue Generation Signaltechnik

Sektorweite Initiative zur Sicherung der Zukunftsfähigkeit der Leit- und Sicherungstechnik

Teilbericht

AP 2300

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

06.08.2013

Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

Laufzeit: 01.09.2011 – 31.08.2013

Projektträger: TÜV Rheinland Consulting GmbH

Änderungsverfolgung

Datum	Bearbeiter	Version	Inhalt
07.05.2013	Schaefer (Funkwerk AG)	0.1	Dokumentenstruktur
05.06.2013	Schaefer (Funkwerk AG)	0.2	Beurteilung der vorliegenden Argumentation; Ansatz für Normenvergleich; Reviewergebnisse
27.06.2013	Schaefer (Funkwerk AG)	0.3	Allgemeine Anforderungen
01.07.2013	Schaefer (Funkwerk AG)	0.4	System und Hardware
03.07.2013	Schaefer (Funkwerk AG)	0.5	Erstellung
06.08.2013	Schaefer (Funkwerk AG)	0.6	Vergleich des Sicherheitsnachweises; Ausblick und Zusammenfassung umformuliert
15.07.2013	Möller-Neustock	0.7	Übernahmen Sicht aus Ergebnisbericht
06.08.2013	Holger Neustock Klaus-Dieter Winkler	1.0	Finalisierung

Inhaltsverzeichnis

Tabellenverzeichnis

1 Einleitung

Elektronische Stellwerke sind weltweit ab etwa Mitte der 80er Jahre im Einsatz. In Deutschland wurden sie ab 1990 in großem Umfang installiert, um die bis dahin eingesetzte Relaistechnik zu ersetzen.

Nahezu alle Stellwerkstypen aus der Anfangszeit wurden vollständig von Grund auf in den Firmen entwickelt und gefertigt. Dabei waren die Zukaufteile, also im Grunde Industriestandard, auf elektrische und elektronische Komponenten wie CPU, Speicher, Widerstände und einfache integrierte Schaltkreise begrenzt. Auch selbst entwickelte CPU kamen zum Einsatz. So sollte sichergestellt sein, dass der gesamte Herstellungsprozess in eigener Hand und eigener Kontrolle liegt. Die Erwartungshaltung war, dass durch den Einsatz von Elektronik die Stellwerke baulich kleiner und vor allem kostengünstiger werden.

Schon in den 90er Jahren wurde die Normenserie CENELEC 50126/28/29 (im Weiteren als CENELEC bezeichnet) zur Entwicklung von Stellwerken entworfen, um den Zulassungsprozess zu standardisieren. Sie sind Fachnormen zur übergeordneten IEC 61508 (im Weiteren als IEC bezeichnet), „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“

Parallel zur Entwicklung der Stellwerkstechnik waren Industriesteuerungen bereits in den 80 Jahren weit verbreitet und haben die Steuerungen von industriellen Systemen gewandelt. Die Herstellung der Steuerungen wurde von den Betreibern von Kraftwerken, der Automobilindustrie oder der Chemieindustrie auf Hersteller von SPS verlagert. Dabei sieht Siemens sich als Marktführer, andere namhafte Hersteller sind Schneider, Mitsubishi, Pilz und viele andere. Da die Sicherheit in vielen Prozessbereichen von herausragender Bedeutung ist, wurde zur Standardisierung der Bewertung und Zulassung die IEC 61508 entworfen. Alle sicherheitsgerichteten Systeme in Industriebereichen wurden nach dieser Norm entwickelt und dokumentiert.

Die Signaltechnik hat mit den CENELEC Normen EN 50126/28/29 Fachnormen mit Abweichungen entworfen.

So hat sich heute gezeigt, dass die erhofften Einsparungen beim Einsatz von in weiten Teilen selbst entwickelter Elektronik und Software bei den geringen Stückzahlen nicht kosteneffizient wird. So wird vermehrt auf bereits zugelassene Hard- und Software zurückgegriffen. Daraus ergibt sich zwangsweise die Fragestellung bzgl. einer Überleitung der Zulassung nach IEC-Norm in die CENELEC-Norm, d. h. unter welchen Voraussetzungen eine Begutachtung nach IEC im Anwendungsbereich Signaltechnik/Bahnsysteme anerkannt werden kann.

Die Zielstellung dieses Ergebnisberichts ist, auf Basis eines Normenvergleichs geeignete Ansätze für Maßnahmen aufzuzeigen, wie nach IEC zugelassene Standardindustriekomponenten, zulassungsfähig für einen Einsatz in der LST werden können.

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

2 Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

Zulassungen nach IEC 61508 werden bisher nicht ohne weiteres vom EBA anerkannt. Auch wenn die CENELEC Normenreihe als Fachnorm auf der IEC basiert, gilt die Fachnorm als verbindlich. Die folgenden Kapitel beleuchten einige der Zulassungsbedingungen in diesem Umfeld.

Zusätzlich ist zu berücksichtigen, dass für die größte Anzahl der Zulassungen beim EBA eher Mü8004 als Standard galt und erst jetzt in zunehmendem Maße CENELEC eingesetzt wird. Daher lässt sich mutmaßen, dass in der Umsetzung der CENELEC Normen noch nicht an allen Stellen ein klares Bild besteht.

Dabei kann man den grundsätzlichen Unterschied in der Verfahrensweise der Zulassung nach Mü8004 und CENELEC so beschreiben:

Mü 8004: Das Prinzip der absoluten Sicherheit. Das Produkt wird vom Hersteller nach vorgegebenen Merkmalen entwickelt und in einem Sicherheitsnachweis dokumentiert. Dieser fokussiert sich auf Fehler- und Ausfallbetrachtungen. Alle denkbaren Fehler müssen abgefangen werden. Es gibt keine Wahrscheinlichkeitsbetrachtungen. Der Entwicklungsprozess wird nur sehr begrenzt betrachtet. Die Mü 8004 gibt nur bedingt Prozesse vor, eher technische Ansätze zur Lösung. Man kann dies auch als regelbasierten Ansatz beschreiben. Die Zulassung erfolgt, wenn den Regeln gefolgt wurde.

CENELEC (und auch IEC 61508): Das Prinzip des risikobasierten Ansatzes. Nach der Risikoanalyse wird per Funktion ein Sicherheitsniveau festgelegt. Innerhalb der Grenzen des jeweiligen Sicherheitsniveaus wird das Auftreten von Fehlern und Gefährdungen toleriert. Die Dokumentation umfasst den vollständigen Lebenszyklus des Produktes. Die Norm selbst gibt nahezu ausschließlich Prozesse vor, keine technischen Lösungen. Diesen Ansatz kann man als prozessorientiert beschreiben. Die Zulassung wird erteilt, wenn über den gesamten Lebenszyklus der Prozess gemäß Norm eingehalten und dokumentiert wurde. Es obliegt dem Hersteller den Prozess mit Inhalten zu füllen und für die Sicherheit zu argumentieren.

Inhalt dieses Dokuments ist eine Gegenüberstellung der Zulassungsbedingungen für die Normen

- IEC 61508 [IN] (im Folgenden kurz: „Industrienorm“)

und

- IEC 50126 [BN6], 50128 [BN8] und 50129 [BN9] (im Folgenden kurz: „Bahnnorm“).

Das Motiv für diese Betrachtung ist die Frage, wie bahnspezifische Nachweise bei der Bewertung nach der Industrienorm zulassungsfähig für den Einsatz in der Leit- und Sicherungstechnik genutzt werden können.

2.1 Beurteilung der vorliegenden Argumentation

Dieses Kapitel stellt die Argumentation der TÜV-Präsentation [SSE] dar und diskutiert verschiedene Aspekte des Vortrags.

2.1.1 These

Die Kernthese des Vortrags ist, dass elektronische Systeme, die nach der Industrienorm zertifiziert sind, mit zusätzlichen Maßnahmen auch nach der Bahnnorm zertifiziert werden können.

2.1.2 Argumentationskette

1. In einem Schaubild werden die Bahnnormen EN 50126, 50128, 50129 als Spezialisierung der Fachgrundnorm IEC 61508 dargestellt.
2. Eine Betrachtung der Produktkategorien stellt heraus, dass das Generische Produkt aus den Bahnnormen mit der Industrienorm korreliert.
3. Ein Vergleich der Einteilung von qualitativen Anforderungen stellt für die Industrienorm vier Sicherheitsstufen und für die Bahnnorm zwei „Sicherheitsklassen“ dar. Ferner wird eine Abbildung der Sicherheitsstufen der Industrienorm auf die Sicherheitsstufen der Bahnnorm angegeben.

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

4. Es werden Kategorien aufgelistet, für die Unterschiede zwischen den Normen betrachtet werden können: Software, Hardware, Dokumentation, Sicherheitsprozess.
5. Eine Folie stellt den Aufbau der Normen aus den jeweiligen Teilnormen dar.
    a. Die ersten drei Teile der Industrienorm entsprechen den drei Bahnnormen.
    b. Die übrigen Teile der Industrienorm sind Definitionen, Beispiele, Richtlinien und Techniken.
6. Die Anforderungen zur Kommunikation scheinen ähnlich zu sein. Eine genaue Aussage ist aus der Tabelle mit einem Farbcode aber nicht zu entnehmen.
7. Das Sicherheitsmanagement unterscheidet sich bzgl. notwendiger Dokumentation und Unabhängigkeit der Rollen.
8. Bzgl. komplexer Komponenten ist die Industrienorm spezifischer als die Bahnnorm.
9. Die Anforderungen zur Fehlerbetrachtung sind zu großen Teilen gleichwertig. Lediglich eine Architekturkategorie (Fehlertoleranz 0 + Anteil ungefährlicher Ausfälle ≥ 99% könnte im Sinne der Bahnnorm eine Problematik darstellen).
10. Bzgl. der Architekturvorschriften ist die Industrienorm spezifischer als die Bahnnorm.
11. Die Betrachtung von Common Cause Analysen wird in der Industrienorm ausführlicher behandelt.
12. Zum Diagnoseabdeckungsgrad (Fehleroffenbarungswahrscheinlichkeit durch Diagnosetests) finden sich nur in der Industrienorm ausreichende Informationen. Dies wird als größter Unterschied zwischen den Normen EN 50129 und IEC 61508 bezeichnet.
13. Zur probabilistischen Berechnung von Gefährdungen sagt die Bahnnorm nur wenig aus. Die Industrienorm enthält umfangreiche Beispiele zur Berechnung und berücksichtigt Diagnosemaßnahmen und weitere Faktoren.
14. Ein Berechnungsbeispiel illustriert den Lösungsvorschlag, dass die Bahnnorm das Vorgehen der Industrienorm akzeptiert.
15. Eine Folie von Pilz zeigt: Das reale Ausfallverhalten ist um den Faktor 4-5 geringer als die theoretische Prognose. Damit würden schon heute viele SIL3-Baugruppen die THR für bahntechnische Anwendungen nach SIL4 erfüllen.
16. Der Zusammenhang spezieller, statistischer Werte wird in einer weiteren Folie dargestellt. Die Umrechnung von HR (Hazard Rate) der Bahnnorm in PFH (Probability of a dangerous Failure per Hour) erfolgt mittels der Identität, d.h. HR = PFH.
17. Als Ergebnis des Vergleichs werden einige Bedingungen genannt, bei deren Beachtung eine Anerkennung nach der Bahnnorm möglich sein soll:
    a. Zertifizierung nach IEC 61508
    b. Zertifizierung nach IEC 62061 oder einer vergleichbaren Norm
    c. Beachtung der Wahrscheinlichkeitsberechnung
    d. Unabhängige Validierung
    e. Zusätzliche Dokumentation
18. Es folgen noch einige Folien mit Anregungen und Vorschlägen, die keine neuen Argumente zur These beitragen.

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

2.1.3 Beurteilung der Argumente

2.1.3.1 Spezialisierungshierarchie

Die Abbildung für Argument 1 vermittelt einen anschaulichen Überblick, über die Entwicklungsgeschichte der Normen. Zur Darstellung inhaltlicher Zusammenhänge ist sie aber weniger geeignet. Sie legt nahe, die dargestellten Beziehungen als „Spezialisierung“ zu interpretieren. D.h. anzunehmen, die Grundnorm wäre eine abstraktere Formulierung und die abgeleiteten Normen eine Spezialisierung der Grundnorm für bestimmte Bereiche. In diesem Fall sollten die Bedingungen der abstrakten Grundnorm auch für alle Spezialisierungen gelten. Anders herum gelten die Bedingungen einer speziellen Norm nicht unbedingt in einer abstrakteren Weise (und damit auch für alle anderen Ableitungen).

Für eine Argumentation im Sinne der Kernthese hilft so eine Spezialisierung aber nicht weiter, da die Anforderungen aus der Industrienorm nicht hinreichend für die Anforderungen der Bahnnormen sind. Es ist sogar so, dass einige Argumente (z.B. 8, 10 und 11) eine Spezialisierung in der anderen Richtung nahelegen.

Hilfreicher wäre eine Betrachtung der gemeinsamen Anteile (bzw. eine Abbildung zwischen diesen), sowie eine Darstellung jeweils ergänzender Anforderungen bei einer Überleitung von einer Norm auf die andere.

2.1.3.2 Produktkategorien

Die Korrelation des Generischen Produkts aus den Bahnnormen mit der Industrienorm wird in der Präsentation nicht konkret beschrieben, ergibt sich zum Teil (auch für GA/SA) aber aus Kapitel 2.2. Mit so einer Korrelation können Aussagen aus der Industrienorm auf die Bahnnormen übertragen werden.

2.1.3.3 Einteilung für qualitative Anforderungen

Da beide Normen die SIL-Einteilung für qualitative Anforderungen verwenden, ist die dargestellte Zuordnung nachvollziehbar.

Die Strukturkategorien Software, Hardware, Dokumentation und Sicherheitsprozess scheinen für einen Vergleich der Normen geeignet zu sein und motivierten auch die Struktur des Vergleichs in Kapitel 2.2. Softwareaspekte und Risikoanalyse werden in der Präsentation nicht betrachtet.

2.1.3.4 Aufbau der Normen

Die Zuordnung der Normenteile erleichtert den Vergleich und zeigt eine strukturelle Ähnlichkeit der Normen auf. Damit wird eine Argumentation im Sinne der Kernthese vereinfacht. Diese Grundstruktur wurde auch für den Vergleich in Kapitel 2.2 genutzt.

2.1.3.5 Kommunikationsanforderungen

Der verwendete Farbcode legt nahe, dass sich die Kommunikationsanforderungen der Normen entsprechen sollen. Inhaltlich wird aber kein Argument angegeben. Eine erfolgreiche Argumentation würde aber die Kernthese stützen.

2.1.3.6 Sicherheitsmanagement

Beim Sicherheitsmanagement werden zwei Unterschiede identifiziert:

1. Die Bahnnorm fordert einen expliziten Sicherheitsnachweis, der bei der Industrienorm lediglich „implizit“, in Form eines dokumentierten Lebenszyklus gefordert wird.
2. Die Bahnnorm fordert die Unabhängigkeit aller Sicherheitsrollen (gestaffelt nach SIL). Bei der Industrienorm ist die Unabhängigkeit aller Sicherheitsrollen nicht gefordert, aber „geübte Praxis“.

Obwohl die Unterschiede durch den „impliziten“ Sicherheitsnachweis und die „geübte Praxis“ eingeschränkt werden, sind diese Unterschiede doch wesentlich. Die Gleichwertigkeit des dokumentierten Lebenszyklus wird nicht argumentiert, und lediglich praktizierte (aber nicht geforderte) Maßnahmen bei der Vergabe der Rollen werden weder überprüft noch zertifiziert.

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

2.1.3.7 Umfang der Vorgaben

Die Argumente 8 und 10 bis 13 vermitteln den Eindruck, dass die Industrienorm konkretere Vorgaben als die Bahnnorm macht, und in diesem Sinne „spezieller“ ist. Dies steht im Widerspruch zur dargestellten Spezialisierungshierarchie (vgl. 2.1.3.1).

2.1.3.8 Ausfallratenprognose

Die Argumentation in 15 ist zwar verständlich, aber nicht unbedingt hilfreich. Wenn es so ist, dass die Bahnnorm eine große Freiheit bei der Wahl der Berechnungsmethode lässt (Argument 13), dann kann man die Untersuchungen zum realen Ausfallverhalten zur formalen Argumentation heranziehen.

Falls andererseits eine konkrete Berechnungsvorschrift einzuhalten ist, so nützt es auch nichts, dass Untersuchungen zum realen Ausfallverhalten zu einem niedrigeren Wert kommen. Eine Differenz zwischen dem realen und dem berechneten Ausfallverhalten kann ja, z.B. als rechnerischer „Sicherheitsabstand“, durchaus erwünscht sein.

Bei der Zulassung neuer Komponenten kann diese Argumentation ferner nicht verwendet werden, da keine ausreichende Datenbasis über das reale Ausfallverhalten vorhanden sein muss.

2.1.3.9 Umrechnung von Gefährdungsraten

Für die untersuchten Begriffe „Hazard Rate“ (HR) und „Probability of a dangerous failure per hour“ (PFH) liegen keine normativen Definitionen vor. Dies erschwert eine Beurteilung der Aussage „HR = PFH“.

Trotz des Namens, wird für die Betrachtung in diesem Dokument für PFH kein dimensionsloser Wahrscheinlichkeitswert angenommen, sondern eine Rate, die in 1/h gemessen wird (vgl. z.B. [ESS]).

Für HR wird die folgende Bedeutung angenommen: Die HR gibt an, wie viele Objekte (z.B. Systeme, Teilsysteme oder Funktionen) in einer Zeiteinheit durchschnittlich (d.h. relativ zur Gesamtzahl) mit einem gefährlichen Fehler ausfallen.

Bei dieser Betrachtung, macht die Aussage „HR = PFH“ Sinn.

2.1.3.10 Abstufung der Sicherheitsniveaus im Vergleich

Dieses Kapitel beschreibt vergleichend die Einstufungen der Sicherheitsniveaus beider Normen.

Table A.1 – SIL-table

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

Tabelle 1: SIL-Klassen in EN 50129

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

Sicherheits-Integritätslevel	Rate gefahrbringender Ausfälle der Sicherheitsfunktion (h^{-1})
4	$\geq 10^{-9}$ bis $< 10^{-8}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$
ANMERKUNG Siehe nachfolgende Anmerkungen 2 bis 6 für Einzelheiten zur Interpretation dieser Tabelle.	

Tabelle 2: SIL-Klassen in IEC 61508

Allein von den gefährlichen Ausfällen scheinen die Sicherheitsniveaus identisch eingeteilt. Es ist zu beachten, dass die Berechnungsmethoden abweichen, so dass keine direkte 1:1-Beziehung hergestellt werden kann. Als größte Unterschiede wird angegeben, dass Diagnoseabdeckungsgrade in der IEC dezidiert zu berücksichtigen sind, während die CENELEC diese nicht erwähnt.

Common Cause failure werden in IEC explizit in die Rechnung aufgenommen, bei CENELEC wird nur eine pauschale Betrachtung gefordert. Berechnungen bei Funkwerk am Beispiel des ESTW-R Alister haben ergeben, dass die Berechnung nach IEC konservativere Werte ergibt als die Berechnung nach CENELEC. Dies ist vor allem auf die Berücksichtigung von Common Cause Failure zurückzuführen.

2.1.4 Ergebnis

Das Ergebnis fasst die Argumente noch einmal zusammen und ist zur bisherigen Argumentation konsistent. Unklar ist, inwiefern eine abgeschlossene Zertifizierung nach der Industrienorm nachträglich zu einer Zertifizierung nach der Bahnnorm überführt werden kann, da der Entwicklungsprozess an dieser Stelle ja bereits abgeschlossen ist.

Im Einzelfall kann ein Hersteller durch zusätzliche Prozess-Dokumentation ein normgerechtes Vorgehen nachweisen.

Bei einer Neuentwicklung kann das nachfolgende Kapitel nützliche Hinweise geben, welche Anforderungen entwicklungsbegleitend beachtet werden sollten, um eine Zulassung nach beiden Normwerken zu ermöglichen.

2.2 Normenvergleich

In diesem Kapitel sollen die Anforderungen der Industrienorm mit denen der Bahnnormen verglichen werden. Strukturell wird dabei die Organisation aus Argument 5 (vgl. 2.1.2) ausgenutzt.

2.2.1 Allgemeine Anforderungen

Hier werden im Wesentlichen die Bedingungen der Industrienorm IEC 61508-1 mit den Bedingungen der Bahnnorm EN 50126 verglichen. An den Stellen, an denen die Bereiche von IEC 61508-1 bzw. EN 50126 verlassen werden, wird dies ausdrücklich angegeben.

2.2.1.1 Anwendungsbereich

Die folgende Tabelle beschreibt ausgewählte Themen aus dem Teil der Normen, die den Anwendungsbereich beschreiben.

Thema	Industrienorm	Bahnnorm
Domäne	Sicherheit	Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS)
Spezialisierungsbeziehung	Ein wichtiges Ziel ist es, die Erstellung sektorspezifischer Normen zu ermöglichen.	Erklärt keine Spezialisierungsbeziehung
Technik	Elektrische / elektronische / programmierbare, elektronische Systeme	Keine explizite Einschränkung

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

Thema	Industrienorm	Bahnnorm
Systematik	Allgemeines Sicherheits-Lebenszyklus-Modell	Prozess auf Grundlage des System-Lebenszyklusses zwecks RAMS-Management
Abgrenzung der Angriffssicherheit zur Betriebssicherheit	Deckt keine vorbeugenden Maßnahmen ab, um Schaden oder sonstigen nachteiligen Einfluss auf die funktionale Sicherheit durch unbefugte Personen zu verhindern.	Spezifiziert keine Anforderungen für die Sicherheit im Sinne des Wachschutzes (Security).

Tabelle 3: Themenauswahl für den Anwendungsbereich

2.2.1.1.1 Domäne

Obwohl sich beide Normenwerke auf die Betriebssicherheit konzentrieren, gibt es bzgl. der betrachteten Fachgebiete noch Unterschiede. So konzentriert sich die Industrienorm im Anwendungsbereich auf die Domäne „Sicherheit“, wohingegen die Bahnnorm alle RAMS-Domänen für sich beansprucht. Allein daran ist zu erkennen, dass die Anforderungen der Industrienorm nicht hinreichend für die Bahnnorm sein können.

2.2.1.1.2 Spezialisierung

Während die Industrienorm die Gestaltung sektorspezifischer Normen geradezu erwartet, stellt sich die Bahnnorm nicht ausdrücklich als eine solche Spezialisierung dar. Diese Abgrenzung und Eigenständigkeit der Bahnnorm fördert keine Argumentation im Sinne der These (2.1.1). Sowohl im Sinne der betrachteten Fachgebiete (Domänen) als auch im Sinne der betrachteten Technik, stellt sich die Bahnnorm als allgemeiner und eben nicht spezifischer als die Industrienorm dar.

2.2.1.1.3 Systematik

Da beide Normenwerke eine ähnliche Systematik verwenden (Lebenszyklus-Modell) findet man hier einen Ansatz für einen weiteren Vergleich, der auch in Abschnitt 2.2.1.3 verfolgt wird.

2.2.1.2 Begriffe

Tabelle 4 stellt die Definitionen der Normenwerke für ausgewählte Fachbegriffe nebeneinander dar.

Die Begriffe der Industrienorm sind in Teil 4 der Norm definiert. Insofern verlässt der Vergleich damit den Bereich von IEC 61508-1. Auch sind bestimmte Definitionen der EN 50126 problematisch, so dass an den ausgezeichneten Stellen die Definitionen eines anderen Teils der Bahnnorm verwendet werden. Bemerkenswert ist die Tatsache, dass die Bahnnorm überhaupt unterschiedliche Begriffsdefinitionen in verschiedenen Teilen der Norm verwendet.

Begriff	Industrienorm	Bahnnorm
Gefahr	Potentielle Quelle für eine direkte oder indirekte (als Folge eines Umweltschadens) physische Verletzung oder einen Gesundheitsschaden an einer Person.	Eine physikalische Situation, die potentiell einen Schaden für den Menschen beinhaltet.
Risiko	Kombination der Wahrscheinlichkeit eines Schadens und der Schwere dieses Schadens	Die Wahrscheinlichkeit des Auftretens einer Gefahr, die einen Schaden verursacht, sowie der Schweregrad des Schadens
Safety Integrity	Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb einer bestimmten Zeitspanne erfüllt.	Die Wahrscheinlichkeit dafür, dass ein System die festgelegten Sicherheitsanforderungen unter allen festgelegten Bedingungen innerhalb einer bestimmten Zeitspanne erfüllt.
Sicherheit	Freiheit von unvertretbaren Risiken	Das Nichtvorhandensein eines unzulässigen Schadensrisikos

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

Begriff	Industrienorm	Bahnnorm
Sicherheits-Lebenszyklus (Systemlebens-zyklus)	Notwendige Aktivitäten bei der Implementation sicherheitsbezogener Systeme während einer Zeitspanne, die mit der Konzeptphase eines Projekts beginnt und endet, wenn alle E/E/PE sicherheitsbezogenen Systeme, sonstige sicherheitsbezogener Systeme anderer Technologie und externe Einrichtungen zur Risikominderung nicht mehr für den Gebrauch zur Verfügung stehen.	Die Aktivitäten während einer Zeitspanne, die mit der Konzipierung des Systems beginnt und mit seiner Stilllegung, wenn das System nicht länger für den Gebrauch verfügbar ist, endet.
System (Produkt)	Menge von Elementen, welche gemäß einem Entwurf interagieren. Elemente können hierbei wiederum Systeme (Subsysteme) sein. Sie können kontrollierende oder kontrollierte Systeme sein und können Hardware, Software und menschliche Interaktionen beinhalten.	Menge von Elementen, die in einer zur Erfüllung der spezifischen Anforderung geeigneten Art und Weise zu einem System, Subsystem oder Bestandteil einer Einrichtung zusammengeschaltet sind. In dieser Europäischen Norm (EN 50128) kann ein Produkt als ausschließlich aus Software oder Dokumenten aufgebaut angesehen werden[1].
Validierung	Nachweis, dass das sicherheitsgerichtete System alle spezifizierten Sicherheitsanforderungen erfüllt[2].	Analyse und Testen zur Demonstration, dass das Produkt in allen Belangen seine spezifizierten Anforderungen erfüllt[3].
Verifikation	Nachweis, dass für jede Phase des bestimmten Sicherheits-Lebenszyklus, die aus bestimmten Eingaben abgeleiteten Lieferungen, alle Vorgaben und Anforderungen dieser spezielle Phase erfüllen[2].	Analyse und Testen, um festzustellen, ob das Ausgangsprodukt jeder Phase des Lebenszyklus die Anforderungen aus der vorherigen Phase erfüllt[3].
Vertretbares Risiko	Das in einem bestimmten Kontext akzeptierte Risiko auf der Grundlage der Werte einer Gesellschaft	Der maximale Grad an Risiko durch ein Produkt, der für ein Bahnunternehmen toleriert werden kann

Tabelle 4: Auswahl von Fachbegriffen

Auch wenn Tabelle 4 nur eine kleine Auswahl der Fachbegriffe darstellt, reicht das für den Eindruck aus, dass die beiden Normwerke die gleiche Fachsprache verwenden. Jedenfalls unterscheiden sich die Definitionen oft weniger als unterschiedliche Definitionen eines Begriffs in der gleichen Norm.

2.2.1.3 Lebenszyklus

Industrienorm	Bahnnorm
1: Konzept	1: Konzept
2: Definition des gesamten Geltungsbereiches	2: Systemdefinition Anwendungsvoraussetzungen und Anwendungsbedingungen
3: Gefahren- und Risikoanalyse	3: Risikoanalyse
4: Anforderungen an die gesamte Sicherheit	4: Systemanforderungen
5: Zuordnung der Sicherheitsanforderungen	5: Zuteilung der Systemanforderungen
6: Planung von Betrieb und Instandhaltung insgesamt	6: Entwicklung/Konstruktion und Implementierung 7: Fertigung
7: Planung der Validierung der gesamten Sicherheit	
8: Planung der gesamten Installation und Inbetriebsetzung	
9: Sicherheitsbezogene Systeme: E/E/PES – Realisierung	
10: Sicherheitsbezogene Systeme: andere Technologien – Realisierung	
11: Externe Einrichtungen zur Risikominderung –	

[1]) Mangels Definition in EN 50126 wurde der Begriff anhand der Definition „Produkt“ in EN 50128 hergeleitet.

[2]) Berücksichtigt auch die Anmerkungen zur Definition, welche die Begriffsbestimmung verbessern und präzisieren.

[3]) Da die Definitionen aus EN 50126 unbrauchbar sind, werden hier die Definitionen aus EN 50128 verwendet.

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

Industrienorm	**Bahnnorm**
Realisierung	
12: Installation und Inbetriebsetzung insgesamt	8: Installation/Montage
13: Validierung der gesamten Sicherheit	9: System-Validierung
	10: Systemabnahme
14: Betrieb, Instandhaltung und Wartung insgesamt	11: Betrieb und Instandhaltung
	12: Erfassung der Leistungsfähigkeit
15: Abänderung und Nachrüstung insgesamt	13: Änderungen und Nachrüstung
16: Außerbetriebsetzung oder Entsorgung	14: Stilllegung und Entsorgung

Tabelle 5: Vergleich der Lebenszyklus-Phasen

Wie in Tabelle 5 zu sehen ist, lassen sich die verwendeten Lebenszyklen der beiden Normwerke vergleichen. Es gibt eine Beziehung zwischen den Phasen und auch die Reihenfolge der Phasen passt zueinander.

In den folgenden Abschnitten werden die einzelnen Phasen miteinander verglichen.

2.2.1.3.1 Konzept

Industrienorm	**Bahnnorm**
7.2.2.1 Eingehende Vertrautheit mit den kontrollierten Geräten und ihrer physikalischen Umgebung	6.1.3.1 Vorstellung vom Zweck des Systems, seiner Umgebung und seinen allgemeinen RAMS-Auswirkungen
7.2.2.2 Mutmaßliche Gefahrenquellen	
7.2.2.3 Informationen über identifizierte Gefahren	
7.2.2.4 Informationen über aktuelle Sicherheitsbestimmungen	6.1.3.2 RAMS-Auswirkungen
	6.1.3.4 RAMS-Anforderungen ähnlicher Systeme, Sicherheitsgesetzgebung und -politik
7.2.2.5 Gefahren aufgrund von Wechselwirkungen mit anderen kontrollierten Geräten	6.1.3.3 Gefahrenquellen für RAMS-Performance
7.2.2.6 Dokumentation	6.1.4.1 Ergebnisse

Tabelle 6: Vergleich der Konzept-Anforderungen

Aus Tabelle 6 ist ersichtlich, dass sich die Anforderungen der Konzeptphase durchaus einander zuordnen lassen. Grundsätzlich stellt die Industrienorm aber primär auf die Sicherheit ab, während die Bahnnorm hier den allgemeineren RAMS Begriff verwendet. Wie schon in 2.2.1.1.1 angemerkt sind die Anforderungen der Industrienorm daher nicht hinreichend für die Bahnnorm.

2.2.1.3.2 Definition des gesamten Geltungsbereiches

Industrienorm	**Bahnnorm**
7.3.1.1 Spezifikation der materiellen Ausrüstung	6.2.3.1.a Festlegung des Betriebsaufgaben-Profils
	6.2.3.1.c Festlegung des Umfangs der Anwendungsbedingungen
7.3.2.2 Spezifikation externer Ereignisse	6.2.3.1.b Festlegung der Systemgrenzen
7.3.2.3 Spezifikation gefährdeter Subsysteme 7.3.2.4 Spezifikation von Störfalltypen	6.2.3.1.d Festlegung des Umfangs der Gefahrenanalyse 6.2.3.2.b Vorläufige Gefahrenanalyse
	6.2.3.2.a Vorläufige RAM-Analyse
	6.2.3.3 RAMS-Politik
	6.2.3.4 Erstellung des Sicherheitsplans
7.3.2.5 Dokumentation	6.2.4.1 Ergebnisse
	(6.2.4.2 – 6.2.4.4 Wiederholung von Anforderungen)

Tabelle 7: Vergleich der Anforderungen zur Definition des gesamten Geltungsbereiches

Die Zuordnung der Anforderungen in dieser Phase ist nun nicht mehr so vollständig. Die Industrienorm zählt weder eine RAM-Analyse noch eine RAMS-Politik zum Inhalt dieser Phase. Auch die Erstellung eines Sicherheitsplans gehört nicht dazu. Für die übrigen Anforderungen lassen sich Zuordnungen finden.

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

2.2.1.3.3 Gefahren- und Risikoanalyse

In der folgenden Tabelle werden auch Anforderungen aus Softwareteil der Bahnnorm (EN 50128) abgebildet. Die Bezüge zur Bahnnorm werden daher um ein Präfix (N6 = EN 50126, N8 = EN 50128) ergänzt.

Industrienorm	**Bahnnorm**
7.4.2.1 Gefahren- und Risikoanalyse durchführen	N6.6.3.3.1.a Erkennen von vorhersehbaren Gefahren N8.5.2.4 Zu berücksichtigende Risiken
7.4.2.3 Bestimmung von vorhersehbaren Gefahren und gefährlichen Ereignissen	
7.4.2.2 Beseitigung von Gefahren erwägen	
7.4.2.4 Bestimmung von Ereignisketten für gefährlichen Ereignisse	N6.6.3.3.1.b Identifikation von Abläufen, die Gefährdungen bergen
7.4.2.5 Spezifikation der Wahrscheinlichkeit gefährlicher Ereignisse	N6.6.3.3.1.c Ermittlung der Häufigkeit des Eintretens von Gefahren
7.4.2.6 Bestimmung möglicher Auswirkungen gefährlicher Ereignisse	N6.6.3.3.1.d Ermittlung des Ausmaßes der Auswirkungen von Gefahren
7.4.2.7 Risikoberechnung oder -abschätzung für jedes gefährliche Ereignis	N6.6.3.3.1.e Ermittlung des Systemrisikos für jede Gefahr
	N6.6.3.3.2 Festlegung und Klassifizierung von Risiken
(7.4.2.8 Durchführungshinweis)	
7.4.2.9 Angemessenheit der Techniken	N6.6.3.3.3 Erstellung des Gefahrenprotokolls
7.4.2.10 Inhalt der Gefahren- und Risikoanalyse	
7.4.2.12 Pflege der Gefahren- und Risikoanalyse	
7.4.2.11 Dokumentation	N6.6.3.4 Ergebnisse

Tabelle 8: Vergleich der Gefahren- und Risikoanalyse

Die Anforderungen dieser Phase lassen sich, wie in Tabelle 8 beschrieben, einander zuordnen und sind vergleichbar.

2.2.1.3.4 Anforderungen an die gesamte Sicherheit

Industrienorm	**Bahnnorm**
7.5.2.1 Spezifikation der Sicherheitsfunktionen	6.4.3.1 Festlegung der RAMS-Anforderungen
	6.4.3.2 Übergreifende Anforderungen für Erfüllung
	6.4.3.3 RAM-Programm
	6.4.3.4 Ergänzung Sicherheitsplan
7.5.2.2. Bestimmung der Risikominderung	
7.5.2.3 Verwendung Internationaler Standards zur Risikominderung	
7.5.2.4 Nicht sicherheitsbezogene Kontrollsysteme	
(7.5.2.5 Wiederholung)	
7.5.2.6 Spezifikation der Anforderungen zur Sicherheitsintegrität	6.4.3.1 Festlegung der RAMS-Anforderungen
(7.5.2.7 Bezeichnung)	

Tabelle 9: Vergleich der Anforderungen an die gesamte Sicherheit

Bei den Anforderungen an diese Phase setzen die beiden Normenwerke recht unterschiedliche Schwerpunkte. Auf eine Bestimmung der Risikominderung wird in der Bahnnorm in dieser Phase nicht ausdrücklich Wert gelegt. Dafür finden sich in der Industrienorm für diese Phase keine Übergreifenden Anforderungen oder Anforderungen an einen Sicherheitsplan. Erwartungsgemäß, finden sich in der Industrienorm auch keine Angaben zu einem RAM-Programm.

2.2.1.3.5 Zuordnung der Sicherheitsanforderungen

In der folgenden Tabelle werden auch Anforderungen aus Softwareteil der Bahnnorm (EN 50128) abgebildet. Die Bezüge zur Bahnnorm werden daher um ein Präfix (N6 = EN 50126, N8 = EN 50128) ergänzt.

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

Industrienorm	Bahnnorm
7.6.2.1 Spezifikation der sicherheitsbezogenen Systeme	N6.6.5.3.1.a Zuordnung der funktionalen Anforderungen
	N6.6.5.3.1.c Spezifizierung der Subsysteme, Komponenten und externen Einrichtungen
7.6.2.2 Prüfung von Fähigkeiten und Ressourcen	
7.6.2.3 Verteilung von Sicherheitsfunktionen auf sicherheitsbezogene Systeme	N6.6.5.3.1.b Zuordnung der Sicherheitsanforderungen
	N6.6.5.3.1.d Aktualisierung des RAM-Programms
7.6.2.4 Vollständigkeit der Verteilung und Konsistenz mit den Anforderungen zur Sicherheitsintegrität	N6.6.5.3.3 Überprüfung und Aktualisierung des Sicherheits- und Validierungsplans
	N6.6.5.3.2 Bedingungen für Übereinstimmung der Anforderungen
7.6.2.5 Betriebsweise für die Anforderungen zur Sicherheitsintegrität festlegen	
7.6.2.6 Verteilung unter Benutzung geeigneter Techniken zur Kombination von Wahrscheinlichkeiten	
7.6.2.7 Verteilung berücksichtigt mögliche Fehler mit gemeinsamer Ursache	
7.6.2.8 Unabhängigkeit E/E/PE, andere Sicherheitstechnologien, externe Einrichtungen zur Risikominderung	
7.6.2.9 Zuweisung von Sicherheitsanforderungsstufen (SIL) an Sicherheitsfunktionen	N8.5.2.2 Festlegung der Software-Sicherheitsanforderungsstufe
	N8.5.2.3 Mindest-Software-Sicherheitsanforderungsstufe
	N8.5.2.5 Software-Sicherheitsanforderungsstufen
	N8.5.2.6 Dokumentation der Software-Sicherheitsanforderungsstufe
7.6.2.10 Systeme mit Sicherheitsfunktionen verschiedener Sicherheitsanforderungsstufen	
7.6.2.11 Architekturen einzelner, sicherheitsbezogener E/E/PES Systeme	
7.6.2.12 Maximale Sicherheitsanforderungsstufe für einzelne, sicherheitsbezogene E/E/PE Systeme	
7.6.2.13 Dokumentation	N6.6.5.4 Ergebnisse

Tabelle 10: Vergleich der Zuordnung der Sicherheitsbedingungen

Im Gegensatz zur Industrienorm beschreibt die Bahnnorm in dieser Phase keine Zuordnung von Sicherheitsanforderungsstufen. Safety Integrity wird hier als RAMS-Konzept beschrieben welches keiner bestimmten Lebenszyklusphase zugeordnet ist.

2.2.1.3.6 Entwicklung, Konstruktion, Implementierung und Fertigung

Industrienorm	Bahnnorm
7.7.2.1 Erstellung des Wartungsplans	6.6.3.3 Planung nachfolgender Lebenszyklusaufgaben 6.7.3.2 Unterstützende Maßnahmen für Subsysteme und Komponenten 6.7.3.3.a Planung einer Fertigung 6.7.3.3.c Einführung einer RAMS-Prozess-Sicherung
7.7.2.2 Wartungsaktivitäten zur Offenbarung unentdeckter Fehler	
7.7.2.3 Bestätigung des Wartungsplans durch das Wartungspersonal	
7.8.2.1 Erstellung eines Validierungsplans	
7.9.2.1 Erstellung eines Installationsplans	
7.9.2.2 Erstellung eines Inbetriebsetzungsplans	
7.8.2.2 Dokumentation	6.6.4 Ergebnisse
7.9.2.3 Dokumentation	
7.10.2 Realisierung E/E/PES: siehe 2.2.2 und 2.2.3	6.6.3.1 Entwicklung/Konstruktion der Subsysteme und Komponenten
	6.6.3.2 Realisierung der Subsysteme und Komponenten

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

Industrienorm	Bahnnorm
	6.6.3.4 Definition, Verifikation und Erstellung eines Produktionsverfahrens
	6.7.3.1 Verifikation und Implementierung des Fertigungsprozesses
	6.7.3.3.b Einführung einer Fertigung
7.11.2 Realisierung anderer Technologien: nicht im Anwendungsbereich der Industrienorm	
7.12.2 Realisierung externer Einrichtungen zur Risikominderung: nicht im Anwendungsbereich der Industrienorm	
	6.6.3.5.a Erstellung System-Sicherheitsnachweis
	6.6.3.5.b Vorbereitung eines Anwendungssicherheitsnachweises (vgl. auch 6.9.3.3)

Tabelle 11: Vergleich der Entwicklung, Konstruktion, Implementierung und Fertigung

Nicht abgedeckte Anforderungen der Bahnnorm beziehen sich hier auf die Sicherheitsnachweise. Für die übrigen Anforderungen lassen sich Zuordnungen finden. Die Bahnnorm differenziert hier stärker bzgl. der einzelnen Realisierungsschritte.

Zu Punkt 7.10.2 gibt es innerhalb der Industrienorm Verweise auf die Teile 2 und 3 der Norm. Anders die Bahnnorm, die hier auf Verweise zu den Normen EN 50128 und EN 50129 verzichtet. Die Teile der Bahnnorm grenzen sich damit stärker, auch gegeneinander ab.

2.2.1.3.7 Installation und Inbetriebsetzung insgesamt

Industrienorm	Bahnnorm
7.13.2.1 Verwendung des Installationsplans	6.8.3.1 Zusammenbau und Montage
7.13.2.3 Verwendung des Inbetriebsetzungsplans	
7.13.2.2 Umfang der Installationsdokumentation	6.8.3.2 Dokumentation des Montageprozesses
7.13.2.4 Umfang der Inbetriebsetzungsdokumentation	
	6.8.3.3 Überprüfung und Anpassung des Sicherheitsplans
	6.8.3.4 Schulung, Arbeitsanweisungen, Lagerhaltung

Tabelle 12: Vergleich der Installation und Inbetriebsetzung insgesamt

In dieser Phase finden sich für die Überprüfung des Sicherheitsplans, sowie für Schulung, Arbeitsanweisungen und Lagerhaltung keine Entsprechungen in der Industrienorm.

2.2.1.3.8 Validierung der gesamten Sicherheit

Industrienorm	Bahnnorm
7.14.2.1 Verwendung des Validierungsplans	6.9.3.1 Validierung gemäß Validierungsplan
	6.9.3.2 Inbetriebsetzung/Betriebserprobung
	6.9.3.3 Vorbereitung eines Anwendungssicherheitsnachweises (vgl. auch 6.6.3.5.b)
	6.9.3.4 Verfahren zur Ermittlung von Felddaten
7.14.2.2 Kalibrierung von Werkzeugen für Messungen	
7.14.2.3 Dokumentation der Validierung	6.9.4 Ergebnisse
7.14.2.4 Dokumentation der Maßnahmen bei Abweichungen	

Tabelle 13: Vergleich der Validierung der gesamten Sicherheit

In dieser Phase finden sich für die Vorbereitung eines Anwendungssicherheitsnachweises, sowie für die Verfahren zur Ermittlung von Felddaten keine Entsprechungen in der Industrienorm.

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

2.2.1.3.9 Betrieb und Instandhaltung

Industrienorm	**Bahnnorm**
7.15.2.1 Umsetzung des Wartungsplans und von Wartungsroutinen für Systeme und Software 7.15.2.2 Umsetzung eines Wartungsaktivitätsmodells	6.11.3.1 Überwachung von Systemausführung, sowie von Betriebs- und Instandhaltungsverfahren 6.11.3.2.a Regelmäßige Überprüfung und Anpassung der Betriebs- und Instandhaltungsverfahren
7.15.2.3 Chronologische Dokumentation von Betrieb, Wartung und Reparatur	6.11.3.2.b Regelmäßige Überprüfung der Schulungsdokumentation 6.11.3.2.e Einsatz des FRACAS-Systems für die Ausfallerfassung und Korrekturmaßnahmen
	6.11.3.2.c Regelmäßige Überprüfung und Anpassung des Gefahrenprotokolls und des Sicherheitsnachweises
	6.11.3.2.d Wirksame logistische Unterstützung
7.15.2.4 (Verweis auf sektorspezifische Normen)	
	6.12.3.1 Leistungserfüllung, RAMS-Statistik und Überprüfung des Sicherheitsnachweises
	6.12.3.2 Analyse von Leistungserfüllung und RAMS-Daten

Tabelle 14: Vergleich des Betriebs und der Instandhaltung

Die Formulierungen in der Industrienorm sind für diese Phase etwas abstrakter als in der Bahnnorm. Daher kann hier auch nur eine teilweise und nur wenig präzise Zuordnung der Anforderungen vorgenommen werden.

2.2.1.3.10 Abänderung und Nachrüstung

Industrienorm	**Bahnnorm**
7.16.2.1 Planung von Änderungen und Nachrüstungen	6.13.3.1 Erstellung eines Sicherheitsplans
7.16.2.2 Auslösung durch formale Problemmeldungen	6.13.3.2 Prozess für die Lenkung von Änderungen
7.16.2.3 Durchführung einer Auswirkungsanalyse	
7.16.2.4 Dokumentation der Auswirkungsanalyse	
7.16.2.5 Berücksichtigung der Auswirkungsanalyse	
7.16.2.6 Wiederholung geeigneter Lebenszyklusphasen	
7.16.2.7 Chronologische Dokumentation	6.13.4 Ergebnisse

Tabelle 15: Vergleich von Lebenszyklus

Die Anforderungen in der Industrienorm sind hier etwas detaillierter, passen aber zu den Anforderungen aus der Bahnnorm.

2.2.1.3.11 Stilllegung und Entsorgung

Industrienorm	**Bahnnorm**
7.17.2.1 Durchführung einer Auswirkungsanalyse	6.14.3.1.a Feststellen der Auswirkungen der Stilllegung und Entsorgung
7.17.2.2 Dokumentation der Auswirkungsanalyse	
7.17.2.4 Berücksichtigung der Auswirkungsanalyse	
7.17.2.3 Auslösung durch Prozedur zum Management der funktionalen Sicherheit	
7.17.2.5 Vorbereitung eines Stilllegung- und Zerlegungsplans	6.14.3.1.b Planung der Stilllegung
7.17.2.6 Wiederholung geeigneter Lebenszyklusphasen	
	6.14.3.2 Erstellung der Analyse der RAMS-Lebenszyklus-Leistungsfähigkeit
7.16.2.7 Chronologische Dokumentation	6.14.4 Ergebnisse

Tabelle 16: Vergleich von Lebenszyklus

Bis auf die RAM-Analyse können hier wieder Anforderungszuordnungen gefunden werden.

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

2.2.1.4 Dokumentation und Management

Anforderungen zur Dokumentation und zum Management befinden sich in der Bahnnorm EN 50128. In der Industrienorm sind die Anforderungen zu dem Thema auf die Teile 1 und 3 der Norm aufgeteilt. Eine Diskussion der Anforderungen findet daher in 2.2.3.1 statt.

2.2.1.5 RAMS für Bahnanlagen und RAMS-Management für Bahnen

Diese Abschnitte der Bahnnorm können aus verschiedenen Gründen nur schwer den Abschnitten der Industrienorm zugeordnet werden:

- Starker Bezug zur Bahndomäne
- Keine ausdrückliche Kennzeichnung von Anforderungen
- Allgemeiner, beschreibender Charakter
- Einleitende Funktion für RAMS-Lebenszyklus
- Fokus der Industrienorm auf Sicherheitsaspekte

Am ehesten könnte man noch versuchen, einzelne Teile den Dokumentationsabschnitten der Industrienorm zuzuordnen. Die eher beschreibende Form und das Fehlen expliziter Anforderungen erschweren jedoch einen systematischen Zugang, so dass ein Zuordnungsversuch hier nicht vorgenommen wird.

2.2.2 System und Hardware

Hier werden im Wesentlichen die Bedingungen der Industrienorm IEC 61508-2 mit den Bedingungen der Bahnnorm EN 50129 verglichen. Das Fehlen von expliziten Anforderungen oder ähnlich detaillierter Strukturmerkmalen in der Bahnnorm erschwert hier (wie bereits in 2.2.1.5) eine systematische Aufbereitung über Vergleichstabellen.

Die Struktur der nachstehenden Abschnitte folgt daher dem Aufbau der Bahnnorm und zählt relevante Anforderungen aus der Industrienorm auf.

2.2.2.1 Nachweis des Qualitätsmanagements

- 7.4.4.1 Einsatz von Techniken und Maßnahmen zur Vermeidung von Fehlern beim Design und bei der Entwicklung von Hardware
- 7.4.4.2 Eigenschaften der Design-Methode
- 7.4.4.3 Formalisierung von Wartungsanforderungen
- 7.4.4.4 Verwendung automatischer Testwerkzeuge und integrierter Entwicklungsumgebungen
- 7.4.4.5 Planung von E/E/PES Integrationstests
- 7.4.4.6 Unterscheidung von Aktivitäten, die im Werk oder beim Kunden durchgeführt werden
- 7.4.5.1 Entwurfseigenschaften zur Kontrolle systematischer Fehler
- 7.4.5.2 Berücksichtigung von Wartbarkeit und Testbarkeit beim Entwurf und bei der Entwicklung
- 7.4.5.3 Benutzerfreundliche Schnittstellengestaltung

2.2.2.2 Nachweis des Sicherheitsmanagements

2.2.2.2.1 Sicherheitslebenszyklus

- 7.1.3.1 Verwendeter Sicherheitslebenszyklus
- 7.1.3.2 Parallele Ausführung der Verfahren zum Management der funktionalen Sicherheit
- 7.1.3.3 Aufteilung der Phasen in Aktivitäten

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

- 7.1.3.4 Dokumentation der Ausgaben von Phasen
- 7.1.3.5 Anforderungen für Ausgaben von Phasen

2.2.2.2.2 Sicherheitsorganisation

2.2.2.2.3 Sicherheitsplan

2.2.2.2.4 Gefährdungslogbuch

2.2.2.2.5 Sicherheitsanforderungsspezifikation

- 7.2.2.1 Ableitung von E/E/PES Sicherheitsanforderungen
- 7.2.2.2 Qualitative Anforderungen an Ausdruck und Struktur von E/E/PES Sicherheitsanforderungen
- 7.2.2.3 Anforderungen für E/E/PES Sicherheitsfunktionen und für die E/E/PES Sicherheitsintegrität sind E/E/PES Sicherheitsanforderungen
- 7.2.3.1.a Beschreibung aller notwendigen Sicherheitsfunktionen
- 7.2.3.1.b Mengendurchsatz und Antwortverhalten
- 7.2.3.1.c System- und Betreiberschnittstellen
- 7.2.3.1.d Relevante Informationen zur funktionalen Sicherheit mit Auswirkungen auf das Systemdesign
- 7.2.3.1.e Alle Schnittstellen zwischen E/E/PES sicherheitsgerichteten Systemen und Umsystemen
- 7.2.3.1.f Alle Relevanten Betriebsmodi der kontrollierten Geräte
- 7.2.3.1.g Alle notwendigen Verhaltensmodi von E/E/PES sicherheitsgerichteten Systemen
- 7.2.3.1.h Bedeutung aller Hardware/Software Interaktionen
- 7.2.3.1.i Grenzen und Bedingungen für E/E/PES sicherheitsgerichtete Systeme
- 7.2.3.1.j Spezifische Anforderungen zu Start- und Wiederanlaufverfahren
- 7.2.3.2.a Sicherheitsanforderungsstufe (SIL) für Sicherheitsfunktionen
- 7.2.3.2.b Betriebsmodus für Sicherheitsfunktionen
- 7.2.3.2.c Prüfvoraussetzungen
- 7.2.3.3 Maßnahmen zur Vermeidung von Fehlern bei der Spezifikation der Sicherheitsanforderungen
- 7.4.3.2 Anforderungen zum Abschätzen der Wahrscheinlichkeit eines Versagens von Sicherheitsfunktionen aufgrund von Hardwarefehlern

2.2.2.2.6 System-/Teilsystem-/Einrichtungs-Entwurf

- 7.4.2.1 Übereinstimmung von Entwurf und Sicherheitsanforderungsspezifikation
- 7.4.2.2.a Übereinstimmung von Entwurf und den Anforderungen der Hardware-Sicherheitsintegrität
- 7.4.2.2.b Übereinstimmung von Entwurf und den Anforderungen der systematischen Sicherheitsintegrität
- 7.4.2.2.c Übereinstimmung von Entwurf und den Anforderungen für das Systemverhalten bei Fehleroffenbarung
- 7.4.2.3 Gemeinsame Implementierung von Sicherheits- und Nicht-Sicherheits-Funktionen

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

- 7.4.2.4 Sicherheitsintegrationsstufe bei unterschiedlichen Sicherheitsfunktionen
- 7.4.2.5 Nachweis der Unabhängigkeit von Sicherheitsfunktionen
- 7.4.2.6 Verfügbarkeit der Anforderungen an sicherheitsgerichtete Software
- 7.4.2.7 Review der Anforderungen an sicherheitsgerichtete Software und Hardware
- 7.4.2.8 Notwendige Techniken und Maßnahmen im Lebenszyklus zur Erreichung der Sicherheitsintegrationsstufe
- 7.4.2.9 Begründung der Auswahl von Techniken und Maßnahmen zur Erreichung der Sicherheitsintegrationsstufe
- 7.4.2.10 Bedeutung der Hardware und Software-Interaktionen
- 7.4.2.11 Zerlegung des Entwurfs in Subsysteme
- 7.4.2.12 Sicherheitsfunktionen zur Vermeidung gefährlicher Ausgangskombination von Subsystemen
- 7.4.2.13 Einsatz von Derating-Techniken
- 7.4.3.1 Architektonische Bedingungen für die Hardware-Sicherheitsintegrität
- 7.4.7.1 Implementation des E/E/PES nach dem Entwurf
- 7.4.7.2 Identifikation sicherheitsrelevanter Subsysteme
- 7.4.7.3.a Funktionale Spezifikation von Funktionen und Schnittstellen, die von Sicherheitsfunktionen verwendet werden können
- 7.4.7.3.b Geschätzte Ausfallraten für gefährliche Fehler, die durch diagnostische Prüfungen offenbart werden
- 7.4.7.3.c Geschätzte Ausfallraten für gefährliche Fehler, die durch diagnostische Prüfungen nicht offenbart werden
- 7.4.7.3.d Umweltbedingungen, die beobachtet werden müssen, um die Gültigkeit der geschätzten Ausfallraten zu bestätigen
- 7.4.7.3.e Lebensdauer, die nicht überschritten werden darf, um die Gültigkeit der geschätzten Ausfallraten zu bestätigen
- 7.4.7.3.f Periodische Wiederholungsprüfungen und Wartungsanforderungen
- 7.4.7.3.g Diagnoseniveau
- 7.4.7.3.h Diagnose-Testintervall
- 7.4.7.3.i Zusatzinformationen zur Ableitung der mittleren Reparaturzeit
- 7.4.7.3.j Informationen zur Ableitung des Gesamtanteils sicherer Ausfälle
- 7.4.7.3.k Hardware Fehlertoleranz
- 7.4.7.3.l Anwendungsgrenzen zur Vermeidung systematischer Fehler
- 7.4.7.3.m Höchste Sicherheitsintegritätsstufe für Sicherheitsfunktion
- 7.4.7.3.n Konfigurationsinformationen
- 7.4.7.3.o Validierungsnachweise
- 7.4.7.4 Geschätzte Ausfallrate wegen zufälliger Hardwarefehler
- 7.4.7.5 Kontrolle von systematischen Fehlern bei Betriebsbewährtheit nicht notwendig
- 7.4.7.6 Kriterien für Betriebsbewährtheit zuvor entwickelter Subsysteme

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

- 7.4.7.7 Nachweis ähnlicher Anwendungsbedingungen bei Vergleich von Subsystemen
- 7.4.7.8 Identifikation unterschiedlicher Anwendungsbedingungen bei Vergleich von Subsystemen
- 7.4.7.9 Mindestdauer der Betriebsbewährtheit
- 7.4.7.10 Betriebsbewährtheit nur bei Fehleroffenbarung
- 7.4.7.11 Faktoren zur Beurteilung Anforderungen für Betriebsbewährtheit
- 7.4.7.12 Funktionseinschränkung von betriebsbewährten Subsystemen
- 7.4.8.1 Abschätzung der Wahrscheinlichkeit unentdeckter Fehler bei der Datenkommunikation
- 7.4.8.2 Parameter für die Abschätzung der Wahrscheinlichkeit von Fehlern bei der Datenkommunikation

2.2.2.2.7 Sicherheitsreviews

2.2.2.2.8 Sicherheitsverifikation und -validation

- 7.3.2.1 Planung des Nachweises der Erfüllung der Sicherheitsanforderungen
- 7.3.2.2.a Berücksichtigung aller Anforderungen der Sicherheitsanforderungsspezifikation
- 7.3.2.2.b Verfahren zur Validierung der Sicherheitsfunktionen
- 7.3.2.2.c Verfahren zur Validierung der Sicherheitsintegrität
- 7.3.2.2.d Berücksichtigung der Testumgebung
- 7.3.2.2.e Verfahren zur Testauswertung (mit Begründung)
- 7.3.2.2.f Testverfahren und Leistungsmerkmale zum Nachweis der elektromagnetischen Störfestigkeit
- 7.3.2.2.g Richtlinien zur Auflösung bei fehlgeschlagener Validierung
- 7.5.2.1 Integration nach Entwurf und Test nach spezifizierten Integrationstests
- 7.5.2.2 Ziel der Systemtests
- 7.5.2.3 Integration von Hardware und Software
- 7.5.2.4 Dokumentation von Testergebnissen
- 7.5.2.5 Änderungen während der Integration und Prüfung
- 7.5.2.6 Umfang der Testdokumentation
- 7.5.2.7 Maßnahmen und Techniken zur Vermeidung von Fehlern bei der E/E/PES Integration
- 7.7.2.1 Übereinstimmung der Validierung mit einem Validierungsplan
- 7.7.2.2 Kalibrierung der Testumgebung
- 7.7.2.3 Prüfung aller Sicherheitsfunktionen und aller Verfahren für Betrieb und Wartung
- 7.7.2.4 Umfang der Sicherheitsvalidierungsdokumentation
- 7.7.2.5 Dokumentation von Abweichungen
- 7.7.2.6 Verfügbarkeit der Validierungsergebnisse für Entwickler der kontrollierten Geräte und des Kontrollsystems für kontrollierte Geräte
- 7.7.2.7 Maßnahmen und Techniken zur Vermeidung von Fehlern bei der E/E/PES Sicherheitsvalidierung
- 7.9.2.1 Planung und Dokumentation der Verifikation

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

- 7.9.2.2 Die Verifikationsplanung soll sich auf alle genutzten Argumente, Techniken und Werkzeuge beziehen
- 7.9.2.3 Spezifikation aller Aktivitäten zur Sicherstellung der Konsistenz zu Produkten und Normen der Phaseneingabe
- 7.9.2.4 Umfang der Verifikationsplanung
- 7.9.2.5 Nachweis der Anforderungen der Funktions- und Sicherheitsintegrität
- 7.9.2.6 Dokumentation der Verifikationsergebnisse
- 7.9.2.7 Eignung und Widerspruchsfreiheit von Sicherheitsanforderungen
- 7.9.2.8 Qualitätsmerkmale für Entwurf, Entwicklung und Tests
- 7.9.2.9 Verifikation der Integration von sicherheitsgerichteten Systemen
- 7.9.2.10 Dokumentation von Testfällen

2.2.2.2.9 Sicherheitsbegründung

2.2.2.2.10 System-/Teilsystem-/Einrichtungsübergabe

2.2.2.2.11 Betrieb und Instandhaltung

- 7.6.2.1 Vorbereitung von Verfahren für Betrieb und Wartung
- 7.6.2.2 Kontinuierliche Aktualisierung der Verfahren für Betrieb und Wartung
- 7.6.2.3 Systematisch Bestimmung von Routine-Wartungsarbeiten
- 7.6.2.4 Bewertung von Verfahren für Betrieb und Wartung auf die kontrollierten Geräte
- 7.6.2.5 Maßnahmen und Techniken zur Vermeidung von Fehlern bei Verfahren für Betrieb und Wartung

2.2.2.2.12 Stilllegung und Entsorgung

2.2.2.3 Nachweis der funktionalen und technischen Sicherheit

2.2.2.3.1 Einleitung

2.2.2.3.2 Nachweis des korrekten funktionalen Verhaltens

2.2.2.3.3 Ausfallauswirkungen

- 7.4.6.1 Reaktion bei Fehleroffenbarung in Subsystemen mit Fehlertoleranz
- 7.4.6.2 Reaktion bei Fehleroffenbarung in Subsystemen ohne Fehlertoleranz bei niedriger Anforderungsrate
- 7.4.6.3 Reaktion bei Fehleroffenbarung in Subsystemen ohne Fehlertoleranz bei hoher Anforderungsrate oder kontinuierlicher Anforderung

2.2.2.3.4 Betrieb mit externen Einflüssen

- 7.2.3.2.d Extreme Umweltbedingungen
- 7.2.3.2.e Elektromagnetische Störfestigkeit

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

2.2.2.3.5 Sicherheitsbezogene Anwendungsbedingungen

2.2.2.3.6 Sicherheitserprobung

2.2.2.4 Sicherheitsanerkennung und -zulassung

2.2.2.4.1 Sicherheitszulassungsverfahren

2.2.2.4.2 Nach der Sicherheitszulassung

- 7.8.2.1 Umfang der Dokumentation bei Änderungsaktivitäten
- 7.8.2.2 Unterhaltung eines Systems zur Auslösung von Änderungen
- 7.8.2.3 Beibehaltung des Kompetenz-, Automatisierungs-, Planungs- und Managementgrades bei Änderungen
- 7.8.2.4 Wiederholungs-Verifizierung und -Validierung

2.2.2.4.3 Abhängigkeiten zwischen Sicherheitszulassungen

2.2.3 Software

Hier werden im Wesentlichen die Bedingungen der Industrienorm IEC 61508-3 mit den Bedingungen der Bahnnorm EN 50128 verglichen. An den Stellen, an denen die Bereiche von IEC 61508-3 bzw. EN 50128 verlassen werden, wird dies ausdrücklich angegeben.

2.2.3.1 Dokumentation und Management

Da die Anforderungen zu dem Thema auf die Teile 1 und 3 der Industrienorm aufgeteilt sind, findet hier eine gemeinsame Diskussion dieser Teile statt. Die Bezüge werden daher um T1 (Teil 1) bzw. T3 (Teil 3) ergänzt.

Industrienorm	**Bahnnorm**
T1.5.2.1 Informationen für Lebenszyklusphasen T1.6.2.1.c Angewendete Lebenszyklusphasen T3.7.1.2.1 Lebenszyklusmodell für Softwareentwicklung T3.7.1.2.2 Integration von Qualitäts- und Sicherheitsmanagement in das Lebenszyklusmodell T3.7.1.2.4 Anpassung von Phasen T3.7.1.2.5 Organisation des Softwareprojekts T3.7.1.2.7 Ergebnisdokumentation T3.7.1.2.8 Wiederholung von Phasen	7.2.1 Lebenszyklusmodell für Software-Entwicklung
T3.7.1.2.3 Aufteilung der Phasen in Aktivitäten T3.7.1.2.6 Techniken und Maßnahmen der Phasen	7.2.3 Definition von Aktivitäten einer Phase
T1.5.2.4 Begründung von Abweichungen in den Bestimmungen der Industrienorm	
T1.5.2.5 Ausreichende Verfügbarkeit	7.2.7 Geeignete Form für Handhabung, Bearbeitung und Aufbewahrung
T1.5.2.6 Qualitative Anforderungen an Form und Inhalt T1.5.2.7 Titel, Bezeichner, Index-Organisation T1.5.2.9 Versionierung T1.5.2.10 Recherche, Identifikation aktueller Versionen T3.6.2.3 Aufgaben des Softwarekonfigurationsmanagements	7.2.5 Struktur für fortlaufende Erweiterung 7.2.6 Verfolgbarkeit und Konsistenz
T1.5.2.8 Sektor- und firmenspezifische Arbeitsweisen	5.2.1 Dokumentationsumfang
T1.5.2.11 Änderungswesen und Qualitätssicherung	7.2.2 Parallele Durchführung von Qualitätssicherungsverfahren
T1.6.2.1.a Grundsätze und Strategien zur Erreichung funktionaler Sicherheit	

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

Industrienorm	Bahnnorm
T1.6.2.1.b Identifikation verantwortlicher Personen, Abteilungen und Organisationen	6.2.6 Ernennung eines unabhängigen Gutachters
	6.2.7 Autorität des Gutachters
	6.2.8 Unabhängigkeit beteiligter Gruppen
	6.2.9 Verantwortliche Parteien
	6.2.10 Organisation des Gutachters
T1.5.2.2 Informationen zum Management der funktionalen Sicherheit T1.5.2.3 Informationen zur Durchführung der Bewertung der funktionalen Sicherheit T1.6.2.1.d Umfang und Struktur der Dokumentation	7.2.4 Beschreibung der Verifikationsschritte und Verifikationsberichte 7.2.8 Umfang der Dokumentation nach DCRT 7.2.9 Kombination von Dokumenten 7.2.10 Dokumenten-Cross-Referenz-Tabelle
T1.6.2.1.e Ausgewählte Maßnahmen und Techniken zur Erreichung der Anforderungen von Bestimmungen	
T1.6.2.1.f Aktivitäten zu Bewertung der funktionalen Sicherheit	
T1.6.2.1.g Verfahren zur Verfolgung von Empfehlungen aus Analyse- und Managementaktivitäten	
T1.6.2.1.h Verfahren zur Ermittlung des Schulungsbedarfs	6.2.3 Ausbildung, Erfahrung und Qualifikation
	6.2.4 Begründung der Ausbildung, Erfahrung und Qualifikation
	6.2.5 Umfang der Begründung für Ausbildung, Erfahrung und Qualifikation
T1.6.2.1.i Verfahren zur Analyse von Gefahrensituationen	
T1.6.2.1.j Verfahren zur Analyse der Betriebs- und Wartungsleistung	
T1.6.2.1.k Anforderungen für regelmäßige Überprüfungen der funktionalen Sicherheit	
T1.6.2.1.l Verfahren zur Einleitung von Änderung an dem sicherheitsgerichteten System	
T1.6.2.1.m Notwendige Verfahren und Behörden für die Genehmigung von Änderungen	
T1.6.2.1.n Verfahren zum Erhalt korrekter Informationen zu möglichen Gefahren und sicherheitsgerichteten Systemen	
T1.6.2.1.o Verfahren zum Konfigurationsmanagement	
T1.6.2.1.p Versorgung, Training und Information von Notfalldiensten	
T1.6.2.2 Implementation und Überwachung der Aktivitäten aus T1.6.2.1	
T1.6.2.3 Formale Prüfung durch und Zustimmung von allen betroffenen Organisationen	
T1.6.2.4 Information von Management und Funktionsträgern	
T1.6.2.5 Übertragung auf Zulieferer	
	6.2.1 Umsetzung ISO 9001
	6.2.2 Sicherheitsorganisation
T3.6.2.1 Es gelten die Anforderungen aus T1.6.2	
T3.6.2.2 Planung der funktionalen Sicherheit definiert Strategien für Software-Belange	

Tabelle 17: Vergleich von Software

2.2.3.2 Softwareanforderungsspezifikation

Industrienorm	Bahnnorm
7.2.2.1 Keine Wiederholung der Softwareanforderungsspezifikation	

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

Industrienorm	Bahnnorm
7.2.2.2 Ableitung der Softwareanforderungsspezifikation	8.4.1 Softwareanforderungsspezifikation für Eigenschaften der Software
7.2.2.3 Detailgrad der Softwareanforderungsspezifikation	8.4.4 Schnittstellenspezifikation
7.2.2.4 Review der Softwareanforderungsspezifikation	
7.2.2.5 Verfahren zur Lösung von Unstimmigkeiten bei der Zuweisung von Sicherheitsintegrationsstufen	
7.2.2.6 Qualitätsmerkmale der Softwareanforderungsspezifikation	8.4.2 Qualitätsmerkmale der Softwareanforderungsspezifikation
	8.4.3 Verständlichkeit der Softwareanforderungsspezifikation
	8.4.15 Verfolgbarkeit von Anforderungen
	8.4.16 Umgang mit nicht-verfolgtem Material
7.2.2.7 Spezifikation der Betriebsmodi der kontrollierten Geräte	8.4.5 Darstellung relevanter Betriebsarten
7.2.2.8 Spezifikation von Sicherheitsbedingungen zwischen Hardware und Software	8.4.7 Identifikation und Beschreibung von Zwangsbedingungen zwischen Hardware und Software
7.2.2.9 Berücksichtigung von Überwachungs- und Testfunktionen	8.4.8 Hinweis auf Umfang von Software-Selbsttests und Hardware-Prüfungen
	8.4.9 Periodisches Testen von Funktionen
	8.4.10 Tests von Sicherheitsfunktionen im Betrieb
7.2.2.10 Identifikation von Nicht-Sicherheitsfunktionen	8.4.12 Kennzeichnung von Funktionen ohne Sicherheitsanforderung
7.2.2.11 Spezifikation der Sicherheitseigenschaften des Produkts	8.4.6 Beschreibung von relevanten Verhaltensweisen, insbesondere Ausfallverhalten
	8.4.11 Kennzeichnung von Funktionen zur Erreichung der System-Sicherheitsanforderungsstufe
	8.4.13 Ableitung einer Software-Anforderungstestspezifikation
	8.4.14 Testfälle für Software-Anforderungstestspezifikation

Tabelle 18: Vergleich der Software

2.2.3.3 Softwaredesign und -entwicklung

Industrienorm	Bahnnorm
7.4.2.1 Aufteilung der Verantwortung für Designkonformität	
7.4.2.2 Eigenschaften der Designmethode	9.4.2 Möglichst einfache Umsetzung der Software-Anforderungsspezifikation
	9.4.10 Festlegung der Strategie für die Softwareentwicklung
	9.4.15 Merkmale des gewählten Entwurfsverfahren
	9.4.12 Bildung eines integrierten Satzes von Techniken und Maßnahmen für Software-Anforderungsspezifikation
7.4.2.3 Berücksichtigung von Test- und Wartungsfreundlichkeit	
7.4.2.4 Designmethode soll Änderungen erleichtern	10.4.16 Eigenschaften zur Erleiterung der Softwarewartung
7.4.2.5 Eindeutigkeit der Darstellungsnotation	9.4.1 Detaillierte Beschreibung in der Software-Architekturspezifikation
	9.4.3 Bedeutung der Wechselwirkungen zwischen Hardware und Software
7.4.2.6 Minimierung des sicherheitsrelevanten Anteils	9.4.8 Minimierung des sicherheitsrelevanten Anteils
	10.4.2 Minimierung von Umfang und Komplexität

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

Industrienorm	**Bahnnorm**
7.4.2.7 Gemeinsame Implementierung von Sicherheits- und Nicht-Sicherheits-Funktionen	9.4.9 Software aus Teilen unterschiedlicher Software-Anforderungsstufe
7.4.2.8 Sicherheitsintegrationsstufe bei unterschiedlichen Sicherheitsfunktionen	
7.4.2.9 Diagnostische Prüfungen	9.4.11 Begründung der Abwägung zwischen fehlervermeidenden und fehlerbeherrschenden Strategien
7.4.2.10 Selbsttests	
7.4.2.11 Standard- oder vorher entwickelte Software	9.4.5 Einschränkungen für die Verwendung von COTS-Software
	9.4.6 Einsatz von vorher entwickelter Software
	9.4.7 Bevorzugung von nach Norm entwickelter Software
7.4.2.12 Gültigkeit für Daten	
7.4.3.1 Aufteilung der Verantwortung für Designkonformität	
7.4.3.2 Umfang der Entwurfsdokumentation	10.4.4 Umfang der Software-Designspezifikation
	10.4.5 Umfang der Software-Modulspezifikation
7.4.3.3 Berücksichtigung von Änderungen der Sicherheitsanforderungen	
7.4.4.1 Aufteilung der Verantwortung für Werkzeugkonformität	
7.4.4.2 Auswahl von Werkzeugen und Programmiersprachen	10.4.7 Angemessene Auswahl von Werkzeugen
	10.4.8 Automatische Testwerkzeuge und Integrierte Entwicklungswerkzeuge
7.4.4.3 Eigenschaften der ausgewählten Programmiersprache	10.4.9 Merkmale für Compiler oder Übersetzer der ausgewählten Programmiersprache
	10.4.10 Anforderungen an die ausgewählte Programmiersprache
7.4.4.4 Begründung für alternative Programmiersprache	10.4.11 Begründung für alternative Programmiersprache
7.4.4.5 Verwendung von Codierstandards	10.4.12 Entwicklung und Verwendung von Codierstandards
7.4.4.6 Eigenschaften der Codierstandards und Quellcodedokumentation	10.4.13 Eigenschaften der Codierstandards und Quellcodedokumentation
7.4.5.1 Aufteilung der Verantwortung für Detailentwurf-Konformität	
7.4.5.2 Voraussetzungen für Detailentwurf	10.4.1 Voraussetzungen für den Entwurfsprozess
7.4.5.3 Modulare, testbare und wartungsfreundliche Software	
7.4.5.4 Zerlegung der Softwarearchitektur	9.4.4 Identifikation aller Softwarekomponenten
	10.4.3 Software-Entwurf basiert auf Zerlegung in Module
	10.4.14 Spezifikation von Software-Modultests
7.4.5.5 Spezifikation geeigneter Software-Systemintegrationstests	11.4.5 Inhalt des Software-Integrationsplans
7.4.6.1 Qualitative Anforderungen an den Quellcode	10.4.6 Jedes Software-Modul muss lesbar, verständlich und testbar sein.
7.4.6.2 Review von Softwaremodulen	
7.4.7.1 Test von Softwaremodulen	11.4.13 Verifikation der Software-Modulentwurfsspezifikation
7.4.7.2 Ziele von Softwaremodultests	
7.4.7.3 Dokumentation von Softwaremodultestergebnissen	
7.4.7.4 Verfahren zur Korrektur bei fehlgeschlagenen Tests	
7.4.8.1 Planung von Software-Integrationstests	
7.4.8.2 Inhalt von Software-Integrationstests	10.4.17 Integration von Software-Modulen
7.4.8.3 Durchführung von Software-Integrationstests	

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

Industrienorm	Bahnnorm
7.4.8.4 Dokumentation der Software-Integrations-testergebisse	11.4.15 Erstellung eines Software-Integrations-testberichts
7.4.8.5 Durchführung einer Auswirkungsanalyse	
	10.4.18 Verfolgbarkeit von Anforderungen und Ent-wurfsobjekten

Tabelle 19: Vergleich von Software

2.2.3.4 Software/Hardwareintegration

Industrienorm	Bahnnorm
7.5.2.1 Spezifikation von Integrationstests	11.4.16 Software/Hardwareintegration
	12.4.1 Erstellung eines Software/Hardware-Integrationstestplans
7.5.2.2 Inhalt von Integrationstests für programmier-bare Elektronik	12.4.2 Inhalt des Integrationstestplans
7.5.2.3 Unterscheidung von Aktivitäten, die im Werk oder beim Kunden durchgeführt werden	12.4.3 Unterscheidung von Aktivitäten, die beim Her-steller oder beim Betreiber durchgeführt werden
7.5.2.4 Einsatzszenarien für Integrationstests	12.4.4 Unterscheidung zwischen Portierung und Sys-temintegration
	12.4.5 Fertigstellungstermin für Werkzeuge und Hilfsmittel
7.5.2.5 Verwendung der Integrationstest für die Software	
7.5.2.6 Durchführung einer Auswirkungsanalyse	12.4.6 Durchführung einer Auswirkungsanalyse
7.5.2.7 Dokumentation von Testfällen und Ergebnis-sen	12.4.7 Aufzeichnung von Testfällen
7.5.2.8 Dokumentation der Integrationstests; Not-wendige Wiederholungsprüfungen bei Änderungen	12.4.8 Erstellung eines Software/Hardware-Integrationstestberichts

Tabelle 20: Vergleich von Software

2.2.3.5 Planung und Durchführung der Software-Validierung

Industrienorm	Bahnnorm
7.3.2.1 Ziele der Software-Validierungsplanung	13.4.3 Erstellung eines Software-Validierungsplans
	13.4.14 Test gegen Software-Anforderungstest-spezifikation
7.3.2.2 Inhalt der Software-Validierungsplanung	13.4.7 Inhalt des Software-Validierungsplans
	13.4.9 Nachbildung von Eingangssignalen bei unter-schiedlichen Bedingungen
7.3.2.3 Technische Strategie der Software-Validierungsplanung	13.4.6 Zusammenfassung der Validierungsstrategie
7.3.2.4 Review der Software-Validierungsplanung	13.4.4 Bewertung des Software-Validierungsplans
	13.4.5 Abstimmung des Software-Validierungsplans
7.3.2.5 Umfang der Erfüllungs- und Ausfallkriterien	
7.7.2.1 Keine Wiederholung der Software-Validierung	
7.7.2.2 Ausführung der Validierung nach Planung	
7.7.2.3 Dokumentation der Ergebnisse der Validie-rung	13.4.10 Dokumentation der Validierungsergebnisse
7.7.2.4 Umfang der Dokumentation für Sicherheits-funktionen	13.4.11 Umfang der Validierungsergebnisse
	13.4.12 Identität und Konfiguration von Gegenständen der Validierung
7.7.2.5 Dokumentation der Maßnahmen bei Abwei-chungen	13.4.13 Dokumentation gefundener Mängel
7.7.2.6 Anforderungen an die Validierung von si-cherheitsgerichteter Software	13.4.1 Hauptaktivitäten der Validierung
	13.4.2 Ergänzende Aktivitäten der Validierung
7.7.2.7 Fähigkeiten von Softwarewerkzeugen	13.4.8 Eignung von Softwarewerkzeugen
7.7.2.8 Anforderungen an Validierungsergebnisse	

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

Tabelle 21: Vergleich von Software

2.2.3.6 Software-Wartung

Industrienorm	Bahnnorm
	16.4.1 Ausführung nach ISO 9000-3
	16.4.2 Berücksichtigung von Wartbarkeit beim Entwurf
7.8.2.1 Verfügen von Verfahren zur Softwaremodifikation 7.8.2.2 Auslösung durch formalen Änderungsantrag	16.4.3 Aufstellen von Verfahren zur Software-Wartung
	16.4.4 Auditierung von Wartungsaktivitäten
	16.4.5 Verwendung der Projektumgebung aus der Entwicklung
	16.4.6 Anwendung auf Altsysteme
	16.4.7 Handhabung der Software-Qualitätssicherung
7.8.2.6 Inhalt der Sicherheitsplanung	
7.8.2.7 Durchführung der Änderung	
7.8.2.3 Durchführung einer Auswirkungsanalyse 7.8.2.4 Dokumentation der Auswirkungsanalyse 7.8.2.5 Wiederholung geeigneter Lebenszyklusphasen 7.8.2.8 Dokumentation der Änderung 7.8.2.9 Dokumentation der Änderungsdetails 7.8.2.10 Bewertung der Modifikation	16.4.8 Software-Wartungsaufzeichnungen 16.4.9 Software-Änderungsbericht

Tabelle 22: Vergleich von Software

2.2.3.7 Software-Verifikation

Industrienorm	Bahnnorm
7.9.2.1 Planung der Software-Verifikation	11.4.1 Erstellung eines Software-Verifikationsplans
7.9.2.2 Umfang der Planung der Software-Verifikation	11.4.2 Beschreibung von Kriterien, Techniken und Werkzeugen für den Verifikationsprozess
	11.4.4 Inhalt des Software-Verifikationsplans
7.9.2.3 Durchführung der Software-Verifikation nach Plan	
7.9.2.4 Dokumentation/Nachweis von Phasenabschlüssen	11.4.3 Beschreibung von Aktivitäten zur Gewährleistung von Korrektheit und Konsistenz
7.9.2.5 Dokumentation der Software-Verifikation	11.4.9 Dokumentation der Ergebnisse der Verifikation 11.4.10 Erstellung von Verifikationsberichten
7.9.2.6 Verifikation wesentlicher Informationen der Phasenübergänge	
7.9.2.7 Verifikationsaktivitäten	
	11.4.6 Nachweis der Anforderungen an Funktion, Zuverlässigkeit, Leistung und Sicherheit
7.9.2.8 Verifikation der Software-Sicherheitsanforderungen	11.4.11 Verifikation der Software-Anforderungsspezifikation
7.9.2.9 Verifikation der Software-Architektur	11.4.12 Verifikation der Software-Architektur- und Entwurfsspezifikation
7.9.2.10 Verifikation des Software-Systemdesigns	
7.9.2.11 Verifikation der Software-Moduldesignverifikation	
7.9.2.12 Quellcodeverifikation	11.4.14 Verifikation des Software-Quellcode
7.9.2.13 Datenverifikation	17 Anwendungsspezifisch konfigurierbare Systeme
	11.4.7 Durchführung von unabhängiger Stelle
	11.4.8 Nicht vollständig dokumentierte Tests

Tabelle 23: Vergleich von Software

2.2.3.8 Software-Begutachtung

Bzgl. der Anforderungen der Industrienorm wird auf Teil 1 verwiesen. Die Bezüge der Industrienorm beziehen sich hier also ohne die Verwendung eines bestimmten Präfixes auf EN 61508-1.

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

Industrienorm	Bahnnorm
	14.4.1 Spezialfall für Software der Sicherheitsanforderungsstufe 0
	14.4.2 Berücksichtigung vorhandener Gutachten
8.2.1 Berufung zur Bewertung der funktionalen Sicherheit	14.4.4 Unabhängige Begutachtung der Software
8.2.12 Unabhängigkeit der Sicherheitsbewertung	
8.2.13 Hinweise zur Unabhängigkeit der Sicherheitsbewertung	
8.2.14 Hinweise zur Unabhängigkeit der Sicherheitsbewertung	
8.2.2 Zugriff auf Personen, Informationen und Ausrüstung	14.4.3 Zugang zum Entwurfs- und Entwicklungsprozess und zu allen Projektunterlagen
8.2.3 Sicherheitsbewertung aller Phasen des Lebenszyklus	14.4.6 Entscheidung über Verfahren des Software-Lebenszyklus
8.2.4 Ausführung der Sicherheitsbewertung	
8.2.5 Sicherheitsbewertung von Werkzeugen	
8.2.6 Berücksichtigung vorheriger Sicherheitsbewertungen, Pläne und Empfehlungen	
8.2.7 Planung einer konsistenten Sicherheitsbewertung	
8.2.8 Inhalt der Planung der Sicherheitsbewertung	
8.2.9 Genehmigung der Planung der Sicherheitsbewertung	
8.2.10 Abschluss der Sicherheitsbewertung	14.4.5 Feststellung des Gutachters
8.2.11 Sachkundige Sicherheitsbewertung	
	14.4.7 Zustimmung zu Geltungsbereich und Inhalt des Software-Validierungsplans
	14.4.8 Zusätzliche Verifikations- und Validierungsschritte
	14.4.9 Ergebnisbericht jeder Begutachtung
	14.4.10 Abschließendes Software-Gutachten
	14.4.11 Keine Angabe technischer Lösungen bei Mängeln

Tabelle 24: Vergleich von Software

2.2.4 Sicherheitsnachweis

Einer der grundlegenden Unterschiede beider Normen ist das Dokument des Sicherheitsnachweises. Dieser wird nach CENELEC als das Dokument gefordert, dass zusammenfassend den gesamten Prozess dokumentiert. In der IEC ist dieses Dokument nicht in dieser Form explizit gefordert.

In diesem Abschnitt werden speziell die Anforderungen an den Sicherheitsnachweis verglichen.

2.2.4.1 Erstellung

Die Bahnnorm sieht die Erstellung eines Anwendungs-Sicherheitsnachweises in der Phase 9 „System-Validierung“ vor (vgl. EN 50126, 6.9.3.3). In der Industrienorm wird entsprechend in der Phase 13 „Validierung der gesamten Sicherheit“ die Dokumentation der Sicherheitsvalidierung vorgesehen (vgl. IEC 61508-1, 7.14.2.3). Zusätzlich ist in der Phase 9.2 des Software-Sicherheitslebenszyklus die Planung der Software-Validierung vorgesehen (vgl. IEC 61508-3, 7.3.2.2).

2.2.4.2 Inhalt

Industrienorm	Bahnnorm
	Systemüberblick
Plan: Zeitpunkt der Validierung	
Plan: Durchführende der Validierung	
Plan: Identifikation relevanter Betriebsmodi der kontrollierten Geräte	

Vergleich der Zulassungsbedingungen IEC 61508 – CENELEC

Industrienorm	**Bahnnorm**
Plan: Identifikation sicherheitsgerichteter Software	Zusammenfassung der Sicherheitsbewertung und der Sicherheitsaudits
Plan: Technische Strategie der Validierung	Übersicht über die Sicherheits-Engineering-Techniken
Plan: Maßnahmen und Verfahren der Validierung	Zusammenfassung der Kontrollen des Qualitäts- und Sicherheitsmanagements
Plan: Verweise auf spezifische Software-Sicherheits-anforderungen	Zusammenfassung oder Bezug auf die Sicherheitsan-forderungen
	Zusammenfassung der Aufgaben zur Sicherheitsana-lyse
Plan: Erforderliche Testumgebung	
Plan: Erfolgs- und Ausfallkriterien	
Plan: Richtlinien und Verfahren zur Bewertung der Validierungsergebnisse, speziell von Ausfällen	
Bericht: Chronologische Dokumentation der Validie-rungsaktivitäten	
Bericht: Version der Gesamt-Sicherheitsanforderungsspezifikation	
Bericht: Validierte Sicherheitsfunktion und Art der Untersuchung (Analyse oder Test)	
Bericht: Verwendete Werkzeuge und Ausrüstung inkl. Kalibrierungsdaten	
Bericht: Ergebnis der Validierungsaktivitäten	Nachweis der Erfüllung der Sicherheitsanforderungen
	Zusammenfassung aller Beschränkungen und Zwänge
Bericht: Konfigurationsidentifikation des untersuch-ten Gegenstandes, der angewendeten Validierungs-verfahren und der Testumgebung	
Bericht: Abweichungen zwischen erwarteten und tatsächlichen Ergebnissen	

Tabelle 25: Vergleich des Inhalts des Sicherheitsnachweises

Der Vergleich zeigt, dass der Inhalt des Sicherheitsnachweises nach der Bahnnorm einen deutlich abstrakteren Charakter hat. Auf eine konkrete Dokumentenstruktur geht die Industrienorm gar nicht ein. Es ist aber anzunehmen, dass zumindest ein Plan und ein Bericht zu erstellen sind.

3 Ausblick und Zusammenfassung

3.1 Ziele und Schwerpunkte des Berichts

Dieser Bericht ist in erster Linie als Hilfestellung für mögliche gemeinsame oder ergänzende Zulassungsprozesse gedacht. Der Schwerpunkt lag auf den formulierten Anforderungen der Normenwerke und einer tabellarischen Darstellung. Die Vergleichstabellen können als Index und Orientierungshilfe bei weiteren Ergänzungs- oder Forschungsvorhaben dienen.

3.2 Allgemeine Anforderungen

3.2.1 Lebenszyklen

Beide Normenwerke erlauben eine Anpassung der Lebenszyklusphasen (IEC 61508-1, 7.1.1.1; EN 50126, 5.3.4.a), erwarten aber eine grundsätzliche Übereinstimmung mit den übrigen Zielen der Norm. Wird ein, zu beiden Normenwerken kompatibler, Lebenszyklus gesucht, dürfte dies am leichtesten nachzuweisen sein, wenn eine Verfeinerung der Zyklusphasen angestrebt wird. Mit Hilfe von Tabelle 5 kann man sehen, dass es ausreicht, lediglich die jeweils feinere Aufteilung der entsprechenden Lebenszyklen für bestimmte Phasen auszuwählen.

3.2.2 Dokumentation, Management und RAMS

Die Industrienorm benennt nur wenige Dokumente und spricht eher allgemein von z.B. „Planung“ oder „Dokumentation“. Daher ist es für eine kompatible Verwendung hier vermutlich sinnvoll, die Bezeichnungen aus der Bahnnorm zu übernehmen. Ebenso finden sich nur hier ausdrückliche Bezüge zu RAMS, so dass auch hier die Bahnnormen ausschlaggebend sind.

3.3 System und Hardware

Hier kann man anhand der fehlenden Zuordnung aus der Industrienorm sehen, an welchen Stellen die Nachweisführung im Sinne der Bahnnorm ergänzt werden muss. Die Darstellung in 2.2.2 ist tatsächlich nur für eine Abbildung in Richtung der Bahnnorm geeignet. Für eine Zuordnung in Richtung der Industrienorm müsste eine Kapitelnummerierung entsprechend der Industrienorm aufgebaut werden.

3.4 Software

Bei der Betrachtung der Vergleichstabellen sieht man hier streckenweise große Übereinstimmungen, und nur wenige, isolierte Schwerpunkte. Im Sinne einer gemeinsamen Nachweisstruktur, wäre es sinnvoll, hier die Anforderungen beider Normen zu erfüllen und strukturell Themen aus beiden Normwerken einzugliedern.

4 Anhang

4.1 Anhang 1: Referenzen

IN	Functional safety of electrical/electronic/programmable electronic safety-related systems; Französisch/Englische Fassung CEI/IEC 61508-1:1998, 61508-2:2000, 61508-3:1998, 61508-4:1998, 61508-5:1998, 61508-6:2000, 61508-7:2000
BN6	Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS); Deutsche Fassung EN 50126:1999
BN8	Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme; Deutsche Fassung EN 50128:2001
BN9	Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik; Deutsche Fassung EN 50129:2003
SSE	TÜV-Präsentation – SPS für den sicherheitsgerichteten Einsatz in der Bahntechnik 5_SPS_für_den_sicherheitsgerichteten_Einsatz.pdf, Version von 2009-11-03
ESS	Josef Börcsök; Elektronische Sicherheitssysteme – Hardwarekonzepte, Modelle und Berechnung; Hüthig, 2004

4.2 Anhang 2: Abkürzungen

Abk.	**Langform / Erläuterung**
EBA	Eisenbahn Bundesamt
EN	Europäische Norm
ESTW	Elektronisches Stellwerk
FRACAS	Failure reporting, analysis and corrective action system
GA	Generische Applikation
HR	Hazard Rate
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LST	Leit- und Sicherungstechnik
PFH	Probability of a dangerous Failure per Hour
RAMS	Reliability Availability, Maintainability, Safety
SA	Spezifische Applikation
SIL	Sicherheitsintegritätslevel
SPS	Speicherprogrammierbare Steuerung
THR	Tolerierbare Hazard-Rate
TÜV	Technischer Überwachungsverein