Bundesministerium
für Verkehr und
digitale Infrastruktur

Bundesnetzagentur

Eisenbahn-Bundesamt

Sicherheitsregelung Fahrzeug

Überarbeitete Fassung 2019

Methode zum Festlegen und Nachweisen sicherheitsbezogener Anforderungen und Bewertung der Risiken im Rahmen der Umsetzung der CSM-RA und der EN 50126

Ausgabestand 16.11.2021

Editor: Dr. Stefan Pöting

Ersteller: Arbeitskreis APT/SIRF unter dem Lenkungskreis Fahrzeuge

Änderungsindex:

Rev.	Datum (TT.MM.JJJJ)	Beschreibung der Änderung	Verfasst	Freigabe
01	17.12.2019	Freigabe der Version	Arbeitskreis APT	Lenkungskreis
02	16.11.2021	Einarbeitung der redaktionellen Überarbeitung des Klima-Leitfadens	Arbeitskreis APT	Lenkungskreis

Inhaltsverzeichnis

1 Vorwort

Diese Regelung wurde von Fachleuten für Risiko-/Sicherheitsanalysen und für Fahrzeugabnahme bzw. -inbetriebnahme in dem Arbeitskreis **Si**cherheits**n**achweis **Fa**hrzeug (AK SINFA) erstellt. Der Arbeitskreis wurde vom Lenkungskreis Fahrzeuge beaufsichtigt und gesteuert, dem u.a. Vertreter

- des Eisenbahn-Bundesamtes (EBA),
- der Deutschen Bahn AG,
- der im Verband der Bahnindustrie in Deutschland e.V. (VDB) zusammengeschlossenen Eisenbahnfahrzeughersteller und
- des Verbandes Deutscher Verkehrsunternehmen e.V. (VDV)

angehören.

Die Sicherheitsregelung Fahrzeug wird auf der Internetseite des EBA https://www.eba.bund.de veröffentlicht.

Die Sicherheitsregelung Fahrzeug wird vom Abnahmeprozessteam (APT) als Nachfolgeorganisation des AK SINFA als deren Herausgeber im Auftrage des Lenkungskreises Fahrzeuge verwaltet und aktualisiert.

2 Anwendungsbereich und Motivation

2.1 Historie

Die Veränderungen am konzeptionellen Aufbau, der Struktur und der Architektur von Eisenbahnfahrzeugen erfordern, insbesondere durch den vermehrten Einsatz „neuer“ Technologien, z. B. software- / hardwarebasierter Systeme, Methodiken, die den Nachweis der Sicherheit mittels eines ganzheitlichen, an Eisenbahnfahrzeugfunktionen orientierten Ansatzes unter adäquater Berücksichtigung aller betriebsspezifischen Rahmenbedingungen ermöglichen.

Der AK SINFA wurde gegründet, um eine praktikable Nachweismethodik für die funktionsorientierte Sicherheit von Eisenbahnfahrzeugen in Deutschland unter Berücksichtigung der gesetzlichen Rahmenbedingungen zu entwickeln. Hierzu wurden insbesondere die Normen EN 50126, 50128, 50129 und IEC 61508 berücksichtigt.

Das Ergebnis der Arbeit war die Erstausgabe der Regelung unter dem Titel Sicherheitsrichtlinie Fahrzeug (SIRF) im Jahr 2011.

2.2 Anwendungsbereich

Die vorliegende Regelung betrachtet das Teilsystem Fahrzeuge. Für Fahrzeuge gilt die Definition im Sinne des Artikels 2 Nummer 3 der Richtlinie (EU) 2016/797 bzw. weiterführend Anhang I, 2. Abschnitt Fahrzeuge.

Die Regelung kann auch für Schienenfahrzeuge anderer Bahnen (beispielsweise Straßenbahnen, Stadtbahnen und Untergrundbahnen) angewendet werden.

Darüber hinaus kann sie mit ihrem Verfahren und der beschreibenden Methode auch für die Umrüstung und zur Sicherheitsnachweisführung bei Innovationen von Eisenbahnfahrzeugen angewendet werden. In diesen Fällen sind die Verfahren dieser Regelung für den von der Umrüstung / Innovation betroffenen Eisenbahnfahrzeugteil anzuwenden. Dabei sind die Schnittstellen zum unveränderten Eisenbahnfahrzeugteil zu beschreiben.

Bei Innovationen, insbesondere solcher, für die für das Teilsystem Eisenbahnfahrzeug keine Regelungen existieren, wird ein Weg aufgezeigt, wie mit Regelungen aus anderen Industriezweigen ein Nachweis auf deren Regelwerken für das Teilsystem Fahrzeug zu führen ist.

Diese Regelung beschreibt ein Sicherheitsnachweisverfahren für Eisenbahnfahrzeuge, das im Rahmen der Umsetzung des Artikel 5 der CSM-RA [42, 43, 44, 45] verwendet werden kann. Mit der Anwendung der hier beschriebenen Verfahrensschritte und der Erfüllung aller daraus folgenden Maßnahmen werden die Anforderungen der CSM-RA an ein Risikomanagementverfahren nach Artikel 5 erfüllt. Die Anwendung eines anderen Risikobewertungsverfahrens ist möglich, wenn vergleichbare Schritte und Ergebnisse Bestandteil des Verfahrens sind.

2.3 **Zielstellung / Motivation**

Mit der Neuausgabe der EN 50126 [5, 6, 7, 8], EN 50128 [9, 10, 35, 36,], EN 50129 [11, 12, 13] und der Erst-Veröffentlichung der EN 50657 [18, 19] ist die SIRF auf Aktualität überprüft und an die aktuellen Festlegungen in den genannten Normen angepasst worden. Zusätzlich wurden die Verfahren der SIRF ausgehend von den Anforderungen der CSM-RA (VO (EU) 402/2013) [42, 43] und der VO (EU) 2015/1136 [44, 45] angepasst.

Die Anforderungen an ein Risikomanagementverfahren für Eisenbahnfahrzeuge sind in der CSM-RA beschrieben. Diese Verordnung beinhaltet u.a. organisatorische Anforderungen, Rollenbeschreibungen und Anforderungen zur Einbindung eines Assessment Body (AsBo). Als zentraler Punkt enthält die CSM-RA generelle Anforderungen an Aspekte der Sicherheit, z.B. Systemdefinition, Gefährdungsanalyse, Risikobewertung, Nachweisführung, u.a., die unter dem Sammelbegriff „Sicherheitsnachweis“ zusammengefasst werden können.

Ziel dieser Regelung ist es, für den Sicherheitsnachweis Regelungen zum Ablauf, Betrachtungsumfang und Nachweis unter Berücksichtigung aller für die Sicherheit eines Eisenbahnfahrzeugs relevanten Elemente der Sicherheitsarchitektur:

- technische (z.B. Software, Hardware, Mechanik, Pneumatik)
- menschliche (z.B. Kompetenzanforderungen, Bedienpersonal, Triebfahrzeugführer)
- betriebliche (z.B. Betriebsregeln, Anweisungen)

festzulegen und die erforderlichen Sicherheitsanforderungen zuzuweisen. Hierzu sind die bei der jeweiligen Funktion vorliegenden Umgebungsbedingungen derart zu berücksichtigen, dass der Sicherheitsbeitrag weiterer Sicherheitsarchitekturelemente eindeutig beschrieben und festgelegt ist.

Sie dient insbesondere dazu, den Nachweisprozess zu vereinheitlichen und somit diesen wirtschaftlicher und zeitlich planbarer zu machen.

Sie beschreibt Methodiken, sowie Art und Umfang der für einen Sicherheitsnachweis zu erstellenden Dokumentation.

Bei Änderungen oder Erneuerungen bestehender Fahrzeuge ist die Nachweisführung grundsätzlich zu beschränken auf den von der Umrüstung oder Erneuerung betroffenen Teil des Teilsystems Fahrzeug und seiner Auswirkungen auf Eisenbahnfahrzeugfunktionen. Hierbei gilt:

- Für die neue bzw. geänderte Funktion ist ein Nachweis gemäß der hierfür ermittelten Sicherheitsanforderungsstufe (SAS) zu führen.
- Für die Anpassung der bestehenden Architekturen, in die die erneuerte bzw. geänderte Funktion integriert wird, ergibt sich die (notwendige) Nachweisführung aus der Einstufung der geänderten Funktion bzw. ihrer vorherigen Einstufung (falls diese eine höhere SAS aufweist).

2.4 **Zusammenhang zwischen dieser Regelung und dem europäischen Eisenbahnrecht**

Der nach dieser Regelung durchgeführte Sicherheitsnachweis für Eisenbahnfahrzeuge und die Integration des fahrzeugseitigen Teils des Teilsystems ZZS stellt unter Berücksichtigung des Kapitels 6.1.4 eine geeignete Methode für die Risikobewertung im Rahmen des Risikomanagementverfahrens gemäß Anhang I der Durchführungsverordnung (EU) Nr. 402/2013 dar.

Hinsichtlich der Anwendung der Verordnung (EU) Nr. 1302/2014 gilt die Anwendung dieser Regelung als geeignete Methode zur Entwicklung und Bewertung von elektronischen Geräten und Software, die zur Erfüllung grundlegender sicherheitsrelevanter Funktionen verwendet werden (siehe TSI-Abschnitt 4.2.1.3, ff.). Dies ist ein annehmbarer nationaler Konformitätsnachweis (**acceptable national means of compliance**), unter Bezug zur, notifizierten nationalen, technischen Vorschrift (NNTV/NNTR).

Zudem unterstützt dieses Verfahren auch beim „Erfassen der Anforderungen“ (requirements capture) gemäß Art. 13[1] der Durchführungsverordnung (EU) 2018/545 sowie bei der Ermittlung der geltenden Vorschriften nach Art. 17[2] der Durchführungsverordnung (EU) 2018/545.

Dieser annehmbare nationale Konformitätsnachweis (**acceptable national means of compliance**) wird der europäischen Eisenbahnagentur (ERA) mit dem Ziel zur Verfügung gestellt, ihn in einen geeigneten Konformitätsnachweis (**acceptable means of compliance) für das** Risikomanagementverfahren gemäß Anhang I der Durchführungsverordnung (EU) Nr. 402/2013 zu übertragen.

[1] Dies betrifft in erster Linie das Ermitteln von Anforderungen und das Zuweisen zu Funktionen bzw. Teilsystemen.
[2] Dies betrifft in erster Linie das Ermitteln von Anforderungen aus den zu berücksichtigenden Rechtsvorschriften.

3 Zuständigkeiten und Verantwortlichkeiten

Um das in dieser Regelung beschriebene Sicherheitsnachweisverfahren richtig und vollständig durchzuführen, wird vorausgesetzt, dass die Zuständigkeiten und Verantwortlichkeiten der an Herstellung, Betrieb und Zulassung des Fahrzeuges beteiligten Stellen klar festgelegt bzw. definiert sind.

Der Sicherheitsnachweis Fahrzeug ist durch eine geeignete Sicherheitsorganisation zu erstellen, durchzuführen und zu dokumentieren. Dies ist erfüllt, wenn sie den Anforderungen der EN 50126 [5, 6] entspricht. Die Anwendung der Prozesse und Methoden hat die Sicherheitsorganisation sicherzustellen (z.B. durch Auditierung).

Diese Sicherheitsorganisation hat u.a. die

- Rollen,
- Verantwortlichkeiten,
- Kompetenzen,
- Unabhängigkeiten und
- Beziehungen der Organisationen

zuzuordnen.

Für jedes Fahrzeugprojekt ist die Person zu benennen, die die Rolle des Safety Manager (SM) im Projekt übernimmt. Dieser ist der Vertreter der Sicherheitsorganisation, der die Sicherheitsnachweisführung und alle erforderlichen Maßnahmen im Sinne dieser Regelung steuert, koordiniert und überwacht.

Hierbei gilt:

- Die Rollen SM und Projektleiter (PL) können auf Grund von Interessenskonflikten nicht von derselben Person in einem Projekt wahrgenommen werden.
- Der SM berichtet einer Entscheidungsebene oberhalb der Projektleitung oder einer von der Projektleitung unabhängigen Stelle.
- Der SM vertritt die Sicherheitsnachweisführung gegenüber Dritten z.B. Genehmigungsbehörden, unabhängigen Bewertungsstellen, Prüfstellen.
- Die Rolle des SM kann ggf. durch eine bevollmächtigte Person außerhalb des Unternehmens wahrgenommen werden.
- Der SM kann zur Bewertung der Themen der Sicherheitsnachweisführung andere Stellen und Fachexperten mit einbinden.

Der Safety Manager muss folgende Qualifikation mindestens erfüllen:

- mehrjährige praktische Erfahrungen im Sicherheitsmanagement;
- Kenntnisse der hier vorliegenden SIRF und der CSM-RA [42, 43, 44, 45];
- Kenntnisse der Sicherheitsmanagement-Normen [5, 6, 7, 8, 35, 36, 10, 9, 13, 18, 19].

4 Definitionen und Abkürzungen

4.1 Definitionen

Begriff	Definition
Architektur von Eisenbahnfahrzeugfunktionen:	Architektur ist der Aufbau und die logische Verknüpfung von Architekturelementen, um Eisenbahnfahrzeugfunktionen zu realisieren.
Architekturelemente:	Die Architektur besteht aus nachfolgenden funktionserfüllenden: • technischen (z.B. Software, Hardware, Mechanik, Pneumatik) • menschlichen (z.B. Kompetenzanforderungen, Bedienpersonal, Triebfahrzeugführer) • betrieblichen (z.B. Betriebsregeln, Anweisungen) Architekturelementen.
Ausfall aufgrund gemeinsamer Ursache (Common Cause Failure) [5, 6]:	Ausfälle mehrerer Einheiten, die ansonsten als voneinander unabhängig angesehen werden würden, aufgrund einer einzigen Ursache [QUELLE: IEC 60050-192:2015, 192-03-18]
Eisenbahnfahrzeugfunktionen:	Eisenbahnfahrzeugfunktionen im Sinne dieses Dokuments sind die Funktionen eines Eisenbahnfahrzeugs, die die wesentlichen, übergeordneten Funktionen für den Betrieb des Fahrzeugs erbringen. Diese sind die Funktionen in der ersten Gliederungsebene des TeSiPs.
Evaluierung	Im Allgemeinen lässt sich als Evaluation auch die grundsätzliche Untersuchung begreifen, ob und inwieweit etwas geeignet erscheint, einen angestrebten Zweck zu erfüllen.
Funktionen:	Funktionen im Sinne dieses Dokuments ist ein abstrakter Begriff, dessen Bedeutung sich aus dem jeweiligen Kontext ergibt. Zu den Funktionen gehören auch deren Überwachung und Diagnose.
Gefährdungsprotokoll	Gefährdungsprotokoll ist die Unterlage, in der erkannte Gefährdungen, die damit zusammenhängenden Maßnahmen und die Ursache der Gefährdungen dokumentiert und Angaben zu der für das Gefährdungsmanagement verantwortlichen Organisation gemacht werden. (gemäß CSM-RA Art. 3 (16) [42, 43])
Kohärenz	Kohärenz beschreibt, dass sowohl die Elemente eines Systems als auch das Gesamtsystem ein auf einander abgestimmtes und zusammenhängendes Verhalten zeigen. Die Kohärenz bezieht sich immer auf einen Betrachtungsgegenstand (System, Gerät, Komponente),

Begriff	Definition
	der in die vorhandene Umgebung eingebracht werden soll, beispielsweise die EMV des Teilsystems Fahrzeug gegenüber dem Bahnsystem oder Fahrzeugeigenschaften zur Gewährleistung der sicheren und hochverfügbaren Funktion der Gleisfreimeldung und der Gleisschaltmittel.
Maßgebliche Gefährdung:	Die maßgebliche Gefährdung einer Eisenbahnfahrzeugfunktion ist die Gefährdung, die zur höchsten Sicherheitsanforderungsstufe bei der Bewertung ihrer identifizierten Gefährdung führt.
Safety Manager:	Der Safety Manager im Rahmen der SIRF ist eine Rolle in der Sicherheitsorganisation des Unternehmens, die die hier festgelegten Anforderungen an die Rolle übernimmt. Die Rolle im Unternehmen kann auch eine andere Bezeichnung tragen.
Sicherheitsanforderungsstufe (SAS):	SAS ist eine von fünf diskreten Stufen, die in diesem Dokument zur Klassifizierung von Sicherheitsanforderungen verwendet werden. Die niedrigsten sind der Stufe Null, die höchsten Anforderungen der Stufe vier zugeordnet.
Sicherheitsarchitektur	Alle für die Sicherheit relevanten Architekturen stellen die Sicherheitsarchitektur dar.
Teilfunktionen:	Teilfunktionen sind die Funktionen, aus denen sich die Eisenbahnfahrzeugfunktionen im System Eisenbahnfahrzeug zusammensetzen. Diese sind die Funktionen in der zweiten Gliederungsebene des TeSiPs.
Wirkweg	Der Wirkweg beschreibt den funktionserfüllenden Pfad in der Architektur.

4.2 **Abkürzungen**

In Tabelle 1 sind die verwendeten Abkürzungen dargestellt. Die Abkürzungen folgen der Definition in dieser Regelung.

Tabelle 1: Verwendete Abkürzungen

Abkürzung	Bezeichnung
AE	Architekturelemente
AK	Arbeitskreis
APT	Abnahmeprozessteam
BAR	Broadly Acceptable Risk
BI	Basic Integrity
CSM-RA	Common Safety Methods on Risk Evaluation and Assessment Gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken
E/E/PE	elektrisch/elektronisch/programmierbar elektronisch
EBA	Eisenbahn-Bundesamt
EFF	Eisenbahnfahrzeugfunktionen
EU	Europäische Union
FMEA	Fehlermöglichkeitseinflussanalyse Failure modes and effects analysis (Ausfallart- und Effektanalyse)
HAZOP	Operationelle Gefährdungsanalyse, Hazard and operability studies
HR	Stark Empfohlen (Highly Recommended)
HW	Hardware
M	Erforderlich (Mandatory)
MA	Mitarbeiter
PL	Projektleiter
R	Empfohlen (Recommended)
SAS	Sicherheitsanforderungsstufe
SIL	Safety Integrity Level
SINFA	Sicherheitsnachweis Fahrzeug
SIRF	Sicherheitsregelung Fahrzeug
SM	Safety Manager
SSAS	Software Sicherheitsanforderungsstufe
SW	Software
TeSiP	Technischer Sicherheitsplan
Tf	Triebfahrzeugführer
VDB	Verband der Bahnindustrie in Deutschland e.V.
VDV	Verband Deutscher Verkehrsunternehmen e.V.
VO	Verordnung
TSI	Technischer Spezifikation Interoperabilität
NNTV	Notifizierte Nationale Technische Vorschriften
NNTR	Notifizierte Nationale Technische Regelwerke

5 Sicherheitsnachweis Fahrzeug

Diese Regelung beschreibt ein Verfahren und seine Methode für einen Sicherheitsnachweis Fahrzeug, das bei der Anwendung im Rahmen des Risikomanagementverfahren gemäß CSM-RA angewendet werden kann.

Der Sicherheitsnachweis im Sinne der vorliegenden Regelung unterteilt sich in vier, nachfolgend dargestellte Verfahrensschritte:

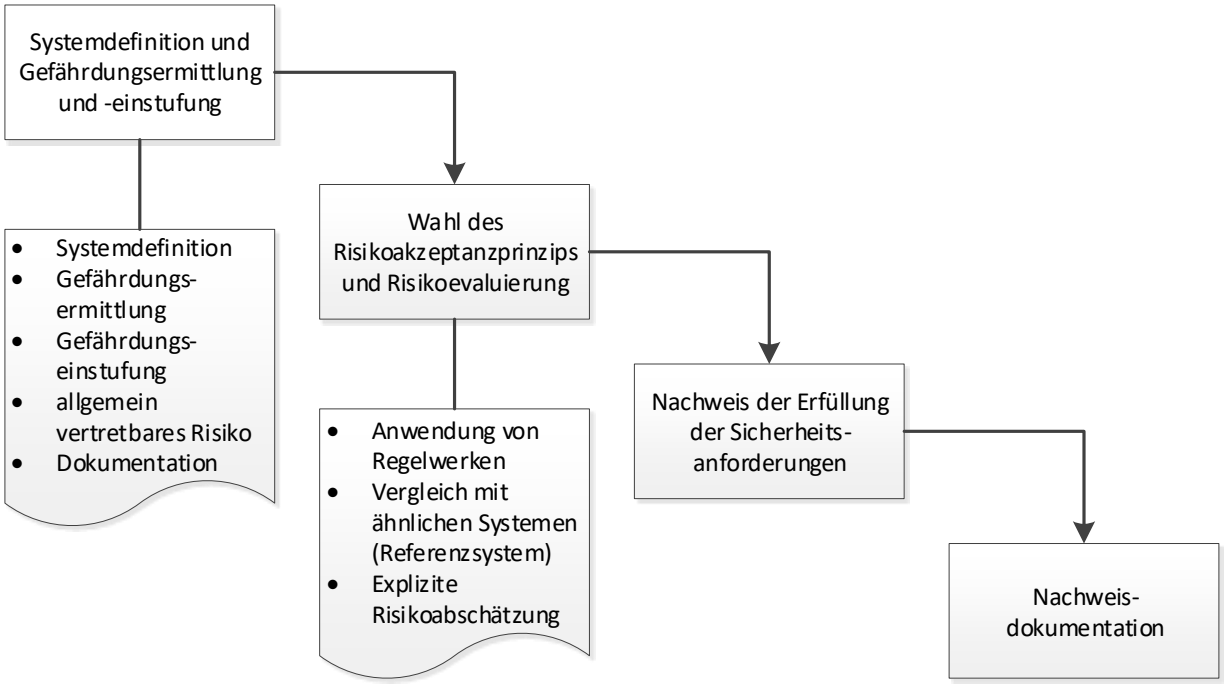


Abbildung 1: Verfahrensschritte des Sicherheitsnachweises

5.1 Systemdefinition und Gefährdungsermittlung und -einstufung

Der erste Verfahrensschritt des Risikomanagements umfasst:

- Systemdefinition, Abgrenzung und Funktionsidentifikation der Eisenbahnfahrzeug-funktionen und Teilfunktionen;
  [Systemdefinition];
- Identifikation der zugehörenden Gefährdungen für betroffene Personen
  [Gefährdungsermittlung];
- Zuweisung der Sicherheitsanforderungen und Sicherheitsanforderungsstufen
  [Gefährdungseinstufung];
- Bewertung allgemeinvertretbares Risiko
  [allgemein vertretbares Risiko]
- Dokumentation
  [Nachweisdokumentation]

5.2 **Wahl des Risikoakzeptanzprinzips / Risikoevaluierung**

Für die sicherheitsrelevanten Eisenbahnfahrzeugfunktionen bzw. deren Architekturelemente oder Teilfunktionen erfolgt die Auswahl des anzuwendenden Risikoakzeptanzprinzips:

- Anwendung von Regelwerken
- Vergleich mit ähnlichen Systemen (Referenzsystemen);
- Explizite Risikoabschätzung.

Im Anschluss erfolgt die Evaluierung, ob das gewählte Risikoakzeptanzprinzip geeignet ist, alle ermittelten Gefährdungen und damit verbundenen Risiken auf einem vertretbaren Niveau zu halten.

5.3 **Nachweis der Erfüllung der Sicherheitsanforderungen**

Auf Basis des ausgewählten Risikoakzeptanzprinzips werden die Sicherheitsanforderungen abgeleitet. Die Erfüllung der Sicherheitsanforderungen für die Eisenbahnfahrzeugfunktionen bzw. deren Architekturelemente ist im Nachweis zu zeigen. Dabei ist zu beachten, dass

- die Annahmen für die Teilnachweise zueinander widerspruchsfrei, eindeutig und schlüssig sind,
- die Elemente des Teilsystems Fahrzeug mitsamt ihren inneren Schnittstellen abgestimmt sind und
- das Teilsystem Fahrzeug mit anderen Systemen und dem System, in das es integriert (betrieblich, technisch) wird, korrekt zusammenwirkt.

Damit ist die sichere Integration bzw. Kohärenz gewährleistet.

Falls zusätzliche Maßnahmen zur Beherrschung der Risiken erforderlich sind, sind diese im Nachweis darzustellen.

5.4 **Nachweisdokumentation**

Eine zusammenfassende Dokumentation mit dem Ziel einer abschließenden Aussage zur Eignung sowohl der Anwendung des Risikomanagementverfahrens als auch seiner Ergebnisse ist zu erstellen.

5.4.1 Technischer Sicherheitsplan / TeSiP

Der „Technischer Sicherheitsplan“ (TeSiP) ist der zentrale Bestandteil für die Dokumentation der Sicherheitsnachweisführung im Rahmen des Risikomanagementverfahrens. Er ist eine Kombination aus Werkzeug und Ergebnisdokumentation. Hierin sind zusammengefasst:

- alle projektspezifischen Eisenbahnfahrzeugfunktionen;
- die Gefährdungsermittlungen unter Berücksichtigung der Systemannahmen;
- die Gefährdungseinstufungen (Zuweisung der Sicherheitsanforderungsstufen);
- Bewertung „allgemein vertretbares Risiko“ („Broadly Acceptable Risk“).

Damit deckt der TeSiP die ersten 2 Verfahrensschritte des Sicherheitsnachweises gemäß Abbildung 1 ab.

Der TeSiP kann verfahrensschrittweise begleitend in folgender Reihenfolge bearbeitet werden:

1. Funktionsliste
2. Gefährdungszuordnung
3. Sicherheitsanforderungszuweisung
4. Wahl des Risikoakzeptanzprinzips.

Ein generischer TeSiP liegt als Anhang A bei.

Der projektspezifische TeSiP ist Bestandteil des Gefährdungsprotokolls gemäß der CSM-RA [42, 43, 44, 45].

5.4.2 Nachweis der Sicherheitsanforderungen und Nachweisdokumentation

Zur Darstellung von Sicherheitsarchitekturen können die im Anhang C beispielhaft abgebildeten Gefährdungsbäume verwendet werden.

Weitere Dokumentationen im Rahmen der Sicherheitsnachweisführung sind gemäß normativer Vorgaben der Sicherheitsnormen [5, 6, 7, 8] zu erstellen.

6 Inhaltliche Anforderungen an den Sicherheitsnachweis Eisenbahnfahrzeug

Dieses Kapitel enthält konkrete Beschreibungen zu den inhaltlichen Anforderungen für die in Abbildung 1 dargestellten Verfahrensschritte. Ferner werden in diesem Kapitel die Anforderungen an die Dokumentation der einzelnen Schritte beschrieben.

6.1 Systemdefinition und Gefährdungsermittlung und -einstufung

6.1.1 Systemdefinition

Der generische TeSiP enthält eine Auflistung von Eisenbahnfahrzeugfunktionen als ein Teil der Systemdefinition.

Diese Auflistung wurde im Eisenbahnsektor von den Fachexperten des Arbeitskreises Sicherheitsnachweis Fahrzeug unter Berücksichtigung der im Eisenbahnsektor allgemein anerkannten Regelwerken für den funktionalen Aufbau von Eisenbahnfahrzeugen erarbeitet. Die im generischen TeSiP vorgenommenen Einstufungen beruhen auf Erkenntnissen aus dem Regelbetrieb von Eisenbahnen. Diese Struktur hat sich durch langjährige Praxis etabliert und bewährt. Insofern ist sichergestellt, dass die Eisenbahnfahrzeugfunktionen im Allgemeinen vollständig erfasst sind.

Dieser generische TeSiP ist projektspezifisch zu prüfen und ggf. anzupassen. Sofern Eisenbahnfahrzeugfunktionen zu ergänzen sind, ist deren Abstraktionsebene entsprechend dem generischen TeSiP vorzunehmen. Erweiterungen und Anpassungen sind systematisch im Expertenkreis in Verantwortung des Herstellers mit Einbindung der zuständigen Sicherheitsorganisation durchzuführen.

Die für den Eisenbahnfahrzeugbetrieb wesentlichen Betriebsbedingungen und Umgebungseinflüsse sind im projektspezifischen TeSiP für die beurteilten Eisenbahnfahrzeugfunktionen zu dokumentieren bzw. referenzieren. Beispiele hierfür sind: vollautomatischer Betrieb, Funkfernsteuerungsbetrieb, Steilstreckenbetrieb, usw. Diese Informationen zu den Betriebs- und Umgebungsbedingungen, Zweckbestimmung, Systemgrenzen, Schnittstellen sind ein weiterer Bestandteil der Systemdefinition und sind im TeSiP zu dokumentieren. Bereits bestehende Sicherheitsmaßnahmen und Annahmen, die die Grenzen der Risikobewertung / Sicherheitsnachweise bestimmen, sind zu benennen.

6.1.2 Gefährdungsermittlung

Die im Eisenbahnsektor erkannten, typischen Gefährdungen für Eisenbahnfahrzeuge sind in der Liste „Gefährdungen auf Systemebene Eisenbahnfahrzeug“ zusammengefasst und als Anhang B beigefügt. Ferner ist diese Auflistung als ein Bestandteil im generischen TeSiP enthalten, Anhang A. Diese generische Liste ist projektspezifisch zu prüfen und ggf. anzupassen (siehe auch Abschnitt 6.1.1).

Im Rahmen der projektspezifischen Gefährdungsermittlung werden ausgehend von den Eisenbahnfahrzeugfunktionen bzw. deren Funktionsverlust die Gefährdungen zugeordnet.

Das Ergebnis ist im projektspezifischen TeSiP in den Spalten für die ermittelten / betrachteten Gefährdungen zu dokumentieren. Hierbei ist die maßgebliche Teilgefährdung anzugeben. Wenn mehrere Gefährdungen für eine Funktion ermittelt wurden, ist die maßgebliche Gefährdung mit der Methode gemäß Kapitel 6.1.3 zu bestimmen und festzulegen.

6.1.3 Gefährdungseinstufungen

Die identifizierten Gefährdungen sind auf Basis des Einstufungsverfahrens in Sicherheitsanforderungsstufen (SAS) zu bewerten. Es ist zu beachten, dass die Einstufung der Eisenbahnfahrzeugfunktionen im Betriebsumfeld erfolgt.

In der Regel ist dies eine Kombination von:

- Mensch,
- Technik und
- Betriebsumfeld / externen Einflüssen.

Das Verfahren zur Einstufung von Eisenbahnfahrzeugfunktionen wurde in Anlehnung an die IEC 61508-5 (Anhang D) [29, 30] entwickelt und dient dazu, die identifizierten Gefährdungen für die Eisenbahnfahrzeugfunktionen, hinsichtlich ihrer Sicherheitskritikalität in Sicherheitsanforderungsstufen (SAS) qualitativ einzustufen.

Anmerkung:
Im Gegensatz zu üblichen Verfahren anderer Industrien berücksichtigt dieses Verfahren auch die Exposition von Fahrgästen, da diese nicht besonders geschult und eingewiesen sind.

Hierzu werden die folgenden Parameter verwendet:

- Schaden (S)
- Eintrittswahrscheinlichkeit (W)
- Expositionsdauer (E)
- Vermeidung (V)

Um die Einstufung konsistent und reproduzierbar zu gestalten sind die o. a. Parameter nachfolgend definiert.

6.1.3.1 Schaden (S)

Der Schaden kennzeichnet die mögliche Auswirkung der Gefährdung. Eingestuft wird der größtmögliche, realistische Schaden (Schadensausmaß). Er setzt sich aus dem Produkt der Anzahl der betroffenen Personen (S_A) und dem möglichen Verletzungsgrad dieser Personen (S_V) zusammen. Hierbei werden die Zuordnungen gemäß den Vorgaben der
Tabelle 2 verwendet.

Tabelle 2: Definition Schaden (S)

Schaden (S) = S_A x S_V	
Anzahl S_A	
Einer	1 Person
Mehrere	1 < x ≤ 10 Personen
Viele	> 10 Personen

Verletzungsgrad S_V	
Leichtverletzte (LV)	Gefährdung führt zu einem Unfall mit leichten Verletzungen (Prellungen, Frakturen) unterhalb von 2 Tagen Krankenhausaufenthalt und ohne irreversible Folgeschäden.
Schwerverletzte (SV)	Gefährdung führt zu einem Unfall mit mindestens 2 Tagen Krankenhausaufenthalt und/oder irreversible Folgeschäden.
Tote	Gefährdung führt zu Unfall mit tödlichen Verletzungen (Tod erfolgt innerhalb von 30 Tagen nach dem Unfall) oder zur sofortigen Todesfolge.

6.1.3.2 Eintrittswahrscheinlichkeit (W)

Bewertung der Wahrscheinlichkeit, dass nach dem Versagen der Funktion das angenommene Schadensausmaß eintritt, z. B: die Wahrscheinlichkeit, ob ein Bremsversagen mit Kollision auf Grund der Randbedingungen viele Tote zur Folge hat.

Tabelle 3: Definition Eintrittswahrscheinlichkeit (W)

Eintrittswahrscheinlichkeit (W)	
Niedrig	Die Eintrittswahrscheinlichkeit ist niedrig, wenn das Schadensausmaß nach Versagen der Funktion nahezu ausgeschlossen ist.
Mittel	Die Eintrittswahrscheinlichkeit ist mittel, wenn das Schadensausmaß nach Versagen der Funktion weder nahezu ausgeschlossen ist, noch nahezu zwangsläufig eintritt.
Hoch	Die Eintrittswahrscheinlichkeit ist hoch, wenn das Schadensausmaß nach Versagen der Funktion nahezu zwangsläufig eintritt.

6.1.3.3 Expositionsdauer (E)

Bewertung der mittleren Expositionsdauer (t_{exp}), in der die betroffenen Personen der möglichen Gefährdung ausgesetzt sind, z.B.

- Gefährdungen, die während des Ein-/Aussteigens eintreten können – kurz,
- Gefährdungen, die durch einen Schaden am Drehgestell, Brand, etc. eintreten können – lang.

Die Expositionsdauer ist in Relation zur Aufenthaltsdauer (t_{auf}) der betroffenen Person im betrachteten Gefahrenraum zu sehen.

Tabelle 4: Definition Expositionsdauer (E)

Expositionsdauer (E)	
Kurz	Die Expositionsdauer ist kurz, wenn diese klein im Vergleich zur gesamten Aufenthaltszeitdauer im Gefahrenbereich ist. $t_{exp} << t_{auf}$
Lang	Die Expositionsdauer ist lang, wenn die betroffene Person während der überwiegenden Aufenthaltsdauer im Gefahrenbereich der möglichen Gefährdung ausgesetzt ist. $t_{exp} \approx t_{auf}$

6.1.3.4 Vermeidung (V)

Bewertung der Vermeidungsmöglichkeit des Schadensausmaßes durch die betroffene(n) Person(en) durch eigenes Handeln nach dem Versagen der Eisenbahnfunktion (z. B. mögliche Flucht aus einem brennenden Abteil / Zugabschnitt).

Tabelle 5: Definition Vermeidung (V)

Vermeidung (V)	
Nicht möglich	Die betroffene Person hat durch eigenes Handeln keine Möglichkeit, den Schaden zu vermeiden
Möglich	Die betroffene Person hat durch eigenes Handeln Möglichkeiten, den Schaden zu vermindern oder zu vermeiden.

6.1.3.5 Ermittlung der Sicherheitsanforderungsstufe (SAS)

Die Sicherheitsanforderungsstufe (SAS) wird mit nachfolgender Berechnungsmethode ermittelt.

Aus den o. a. Parametern berechnet sich der Einstufungsindikator I anhand folgender Formel:

$$I = \frac{(S * W * E)}{V}$$

Abbildung 2: Einstufungsindikator I

Tabelle 6: Zulässige Parameter

Parameter für den Schaden (S) = S_A x S_V			
Anzahl S_A		**Verletzungsgrad S_V**	
einer	3	LV	2
mehrere	5	SV	4
viele	8	Tote	9
Parameter für die Eintrittswahrscheinlichkeit (W)			
niedrig		1	
mittel		1,7	
hoch		3	
Parameter für die Expositionsdauer (E)			
kurz		1	
lang		1,3	
Parameter für die Vermeidung (V)			
nicht möglich		1	
möglich		1,7	

6.1.3.6 Einstufungsindikator (Klassengrenzen)

Die Funktion ist anhand des berechneten Einstufungsindikators I in eine Sicherheitsanforderungsstufe gemäß der untenstehenden Tabelle einzustufen.

Tabelle 7: Einteilung der Sicherheitsanforderungsstufe (SAS)

Einstufungsindikator I	**Sicherheitsanforderungsstufe SAS**
I < 21	0
21 ≤ I < 36	1
36 ≤ I < 72	2
72 ≤ I < 122	3
122 ≤ I < 281	4

Das Ergebnis der Gefährdungseinstufung ist die Sicherheitsanforderungsstufe (SAS). Diese ist für jede Eisenbahnfahrzeugfunktion im projektspezifischen TeSiP zu dokumentieren.

6.1.4 Identifikation weiterer Sicherheitsanforderungen

Für alle identifizierten Eisenbahnfahrzeugfunktionen ist zu prüfen, ob weitere Sicherheitsanforderungen (z.B. aus Regelwerken) existieren. Hieraus ist die maßgebliche Sicherheitsanforderung zu bestimmen und in der entsprechenden Spalte im TeSiP zu dokumentieren.

6.1.5 Bewertung allgemein vertretbares Risiko

Eisenbahnfahrzeugfunktionen mit einer Einstufung SAS = 0 gelten als „allgemein vertretbares Risiko“ („Broadly Acceptable Risk“). Hierfür sind im Rahmen dieser Regelung keine weiteren Maßnahmen erforderlich.

Einstufungen mit SAS > 0 erfordern einen Sicherheitsnachweis nach den Vorgaben dieser Regelung.

6.2 Wahl des Risikoakzeptanzprinzips / Risikoevaluierung

Der nächste Verfahrensschritt ist die Wahl des geeigneten Risikoakzeptanzprinzips (vgl. Abbildung 3). Hiermit wird festgelegt, ob der Sicherheitsnachweis für die zu betrachtende Eisenbahnfahrzeugfunktion mit dem Nachweis auf Basis von

- der Anwendung von Regelwerken oder
- dem Vergleich mit ähnlichen Systemen (Referenzsystemen) oder
- einer expliziten Risikoabschätzung

geführt wird.

Zur Festlegung des anzuwendenden Grundsatzes der Risikoakzeptanz ist für jede zu betrachtende Eisenbahnfahrzeugfunktion eine Identifikation der funktionserfüllenden Teilsysteme (Teilsysteme und Komponenten des Wirkweges der Eisenbahnfahrzeugfunktion) durchzuführen.

Das nachfolgende Flussdiagramm veranschaulicht den in der Praxis bewährten Ablauf bei der Auswahl des Risikoakzeptanzprinzips.

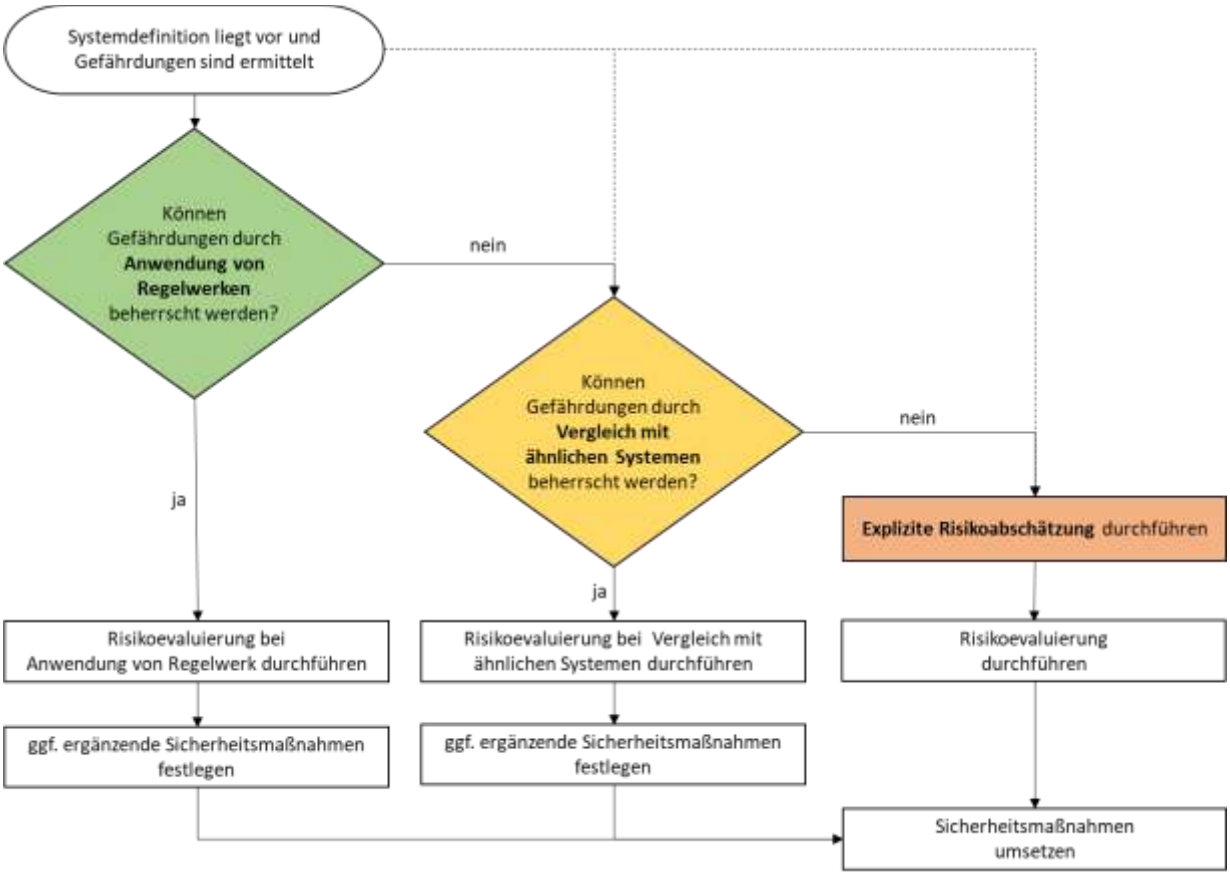


Abbildung 3: Möglicher Ablauf bei Auswahl des Risikoakzeptanzprinzips und Risikoevaluierung

Das auf der obersten Ebene gewählte Akzeptanzprinzip ist möglichst durchgängig für den Nachweis zu verwenden und im TeSiP zu dokumentieren. Ist diese Durchgängigkeit nicht möglich, ist eine Kombination bzw. ein Wechsel des Risikoakzeptanzprinzips zulässig.

Anmerkung / Empfehlung:
Grundsätzlich sind alle drei Nachweisverfahren möglich, wenn die entsprechenden Anwendungskriterien gegeben sind. Im Eisenbahnsektor (insbesondere für Eisenbahnfahrzeuge) hat es sich bewährt, das Nachweisverfahren auf Basis von Regelwerken (anerkannte Regeln der Technik) bevorzugt anzuwenden. In diesem Fall gilt die nachzuweisende SAS als erfüllt (Konformitätsvermutung), wenn die Relevanz der Regelwerke gegeben ist und von diesen nicht abgewichen wird.

Für die Auswahl des Risikoakzeptanzprinzips sind die nachfolgenden Kriterien zu beachten.

6.2.1 Nachweisverfahren auf Basis von Regelwerken (anerkannte Regeln der Technik)

Für die Wahl dieses Risikoakzeptanzprinzips sind nachfolgende Anforderungen zu erfüllen:

- Sie müssen im Eisenbahnsektor allgemein anerkannt sein. Ist dies nicht der Fall, müssen sie begründet werden.
  Dies gilt insbesondere für Innovationen, für die noch keine anerkannten Regeln der

Technik im Eisenbahnsektor existieren, Regelwerke anderer Industriezweige jedoch herangezogen werden können.

- Sie müssen für die Beherrschung der betreffenden Gefährdungen in dem System, das der Bewertung unterzogen wird, relevant sein. Die erfolgreiche Anwendung eines Regelwerks in ähnlichen Fällen des Umgangs mit Änderungen und der wirksamen Beherrschung der ermittelten Gefährdungen eines Systems reicht aus, damit dieses Regelwerk als relevant angesehen wird. Der im Regelwerk genannte Anwendungsbereich muss konform mit den spezifizierten Betriebsbedingungen und Umwelteinflüssen sein.
- Sie müssen auf Nachfrage zugänglich sein.
- Aktuelle Sicherheitsempfehlungen (z. B. aus Unfalluntersuchungen) oder Erkenntnisse und Maßnahmen von Sicherheitsbehörden hinsichtlich Architektur und Funktionalität von vergleichbaren Fahrzeugen sind zu beachten.

6.2.2 Nachweisverfahren durch Vergleich mit ähnlichen Systemen (auf Basis eines Referenzsystems)

Identifikation eines geeigneten Referenzsystems. Das Referenzsystem ist geeignet, wenn es in seinem Einsatz gezeigt hat, dass es die vorgesehenen Funktionen dauerhaft sicher erbringt (proven in use). Hierzu muss es folgende Kriterien erfüllen:

- Es muss in einer ausreichenden Kombination von Anzahl und Betriebsdauer unter vergleichbaren Betriebsbedingungen und Umgebungseinflüssen gezeigt haben, dass es die vorgesehenen Funktionen dauerhaft sicher erbringt.
- Es sollte funktional unverändert übernommen werden. Für Systeme mit ähnlicher Funktion und ähnlichen Betriebsbedingungen sind die Abweichungen zu ermitteln und die Anwendbarkeit zu begründen.
- Die Schnittstellenkompatibilität muss nachgewiesen werden.
- Das gewählte Referenzsystem darf nicht im Widerspruch zu bestehenden und gültigen Vorgaben stehen und hat keine sicherheitsrelevanten Auffälligkeiten gezeigt.

6.2.3 Nachweisverfahren der expliziten Risikoabschätzung

Für die Wahl dieses Risikoakzeptanzprinzips sind nachfolgende Anforderungen zu erfüllen:

- Kann für die zu betrachtenden Funktionen der Sicherheitsnachweis nicht vollständig oder gar nicht mit Nachweisverfahren auf Basis von Regelwerken (anerkannte Regeln der Technik) oder dem Nachweis auf Basis eines Referenzsystems geführt werden, ist das Nachweisverfahren der expliziten Risikoabschätzung für den Teil, der nicht von Regelwerken oder Referenzsystemen abgedeckt wird, anzuwenden. Die Anforderungen zur funktionalen Sicherheit aus Kapitel 6.3.3.6 sind in diesem Fall für die Teile der Eisenbahnfahrzeugfunktion nachzuweisen, die durch andere Risikoakzeptanzprinzipen abgedeckt werden.
- Im Rahmen dieses Verfahrens ist es auch möglich, einzelnen an der Eisenbahnfahrzeugfunktion beteiligten Architekturelementen eines der zuvor genannten Nachweisverfahren zuzuordnen.
- Dieses Verfahren kann qualitativ oder quantitativ geführt werden.

6.2.4 Festlegung des Risikoakzeptanzprinzips

Das Ergebnis der Auswahl der Risikoakzeptanz ist für die identifizierten sicherheitsrelevanten Eisenbahnfahrzeugfunktionen, bzw. die Architekturelemente in der Spalte (27) im projektspezifischen TeSiP zu dokumentieren. Hierbei ist die nachfolgende Kennzeichnung oder Adäquates zu verwenden:

• COP Code of Practice	Anwendung von Regelwerken
• SRS Similar Reference System	Vergleich mit ähnlichen Systemen (Referenzsystemen)
• ERE Explicit Risk Estimation	explizite Risikoabschätzung

Folgende Punkte sind zu dokumentieren:

- die Kriterien zur Auswahl des Risikoakzeptanzprinzips
- den Nachweis, dass durch die Anwendung des gewählten Risikoakzeptanzprinzips die mit den identifizierten Gefährdungen verbundenen Risiken vertretbar sind und angemessen abgedeckt werden.

6.3 Nachweis der Erfüllung der Sicherheitsanforderungen

Das ausgewählte Nachweisverfahren ist auf die zu betrachtenden Eisenbahnfahrzeugfunktionen bzw. die Architekturelemente anzuwenden.

Für alle Nachweismethoden muss gezeigt werden, dass die ermittelten Sicherheitsanforderungen über den kompletten Lebenszyklus und für alle betriebsspezifischen Rahmenbedingungen (Einsatz- und Umweltbedingungen) erfüllt werden.

6.3.1 Nachweisverfahren auf Basis von Regelwerken (anerkannte Regeln der Technik)

Es gilt als ausreichend, wenn gezeigt wird, dass für die mit den Eisenbahnfahrzeugfunktionen bzw. den Architekturelementen verbundenen Gefährdungen durch die Anwendung relevanter Anteile eines Regelwerkes, diese angemessen abgedeckt werden (Grenzwerte, Schutzziel, Gestaltungsvorgaben, etc.).

6.3.2 Nachweisverfahren durch Vergleich mit ähnlichen Systemen (auf Basis eines Referenzsystems)

Der Nachweis umfasst das Referenzsystem und das zu bewertende System.

- Für das Referenzsystem ist über eine ausreichende Anzahl von Betrachtungseinheiten und deren Betriebsdauer bei vergleichbaren Betriebsbedingungen und Umgebungseinflüssen eine dauerhafte, sichere Funktionserfüllung nachzuweisen.

- Für das zu bewertende System ist in einem Nachweis zu zeigen, dass die

    - vollständige Kompatibilität der Funktion einschließlich der Schnittstellen, sowie

    - die Konformität der funktionserfüllenden Systeme (Systeme und Komponenten des Wirkweges der Funktion) bzw. der funktionserfüllenden Architekturelemente zwischen den Systemen mittels Vergleiches, inkl. der zu Grunde liegenden Betriebsbedingungen und Umgebungseinflüssen

  gegeben ist.

Anmerkung / Hinweis:
Ein Beispiel für ein mögliches Referenzsystem für die Funktion Datenübertragung ist die Frequenzmultiplexe Zugsteuerung (FMZ), die zur Übertragung von Binärinformationen zwischen Lok, Mittelwagen und Steuerwagen z.B. im Wendezugbetrieb genutzt wird. Diese wird seit 1990-er Jahren in großer Stückzahl bei lokbespannten Reisezügen eingesetzt. Als Übertragungsmedium dient das durch alle Fahrzeuge eines Zuges laufende UIC-Kabel. Die bisherigen Systeme sind seit Jahren fehlerfrei im Einsatz und soweit „sicher und bewährt".

6.3.3 Nachweisverfahren auf Basis der expliziten Risikoabschätzung

Dieses Nachweisverfahren ist anhand der nachfolgend genannten Verfahrensschritte durchzuführen:

Für die zu betrachtenden Eisenbahnfahrzeugfunktionen sind:

- eine Architekturaufteilung zur Identifikation der funktionserfüllenden (beteiligten) Architekturelemente durchzuführen.
- Auf diese funktionserfüllenden Architekturelemente ist die Sicherheitsverantwortung ausgehend von der Sicherheitsanforderungsstufe (SAS) der Eisenbahnfahrzeugfunktion aufzuteilen.
- Für die Architekturelemente ist die Erfüllung der nach der jeweiligen Sicherheitsanforderung erforderlichen Maßnahmen nachzuweisen.
- Die Funktionserfüllung, sowie die sicherheitsgerichtete Ausfallreaktion unter allen zu erwartenden Betriebs- und Umgebungseinflüssen ist für die zu betrachtende Eisenbahnfahrzeugfahrzeugfunktion nachzuweisen.

Die Architekturaufteilung ist anhand folgender Regeln durchzuführen:

- Es sind alle Architekturelemente der betrachteten Eisenbahnfahrzeugfunktion mit Angaben des Funktionsumfanges und der Zuständigkeit bzw. Verantwortlichkeit bei den Akteuren (z.B. Hersteller, Betreiber, Halter, etc.) zu identifizieren.
- Die Identifikation der Architekturelemente soll bis zu einer Ebene erfolgen, auf der sinnvoll zwischen sicherheitsrelevanten und nicht sicherheitsrelevanten Architekturelementen unterschieden werden kann.
- Das Zusammenwirken der identifizierten Architekturelemente mit ihren Gefährdungsbeiträgen ist in einem Gefährdungsbaum mit logischen Verknüpfungen (z.B. „UND", „ODER") darzustellen, dessen Top-Ereignis die maßgebliche im TeSiP festgelegte Gefährdung der Eisenbahnfahrzeugfunktion ist.
- Die logische Verknüpfung „ODER" bedeutet, dass ein Versagen eines der zur Verknüpfung gehörenden Architekturelemente zum Versagen der übergeordneten Funktion führt.
- Die logische Verknüpfung „UND" bedeutet, dass das Versagen der übergeordneten Funktion erst gegeben ist, wenn alle zugeordneten Architekturelemente versagen.

Den identifizierten Architekturelementen können unterschiedliche sicherheitstechnische Verantwortungen (Aufteilung der Sicherheitsverantwortung) zugeordnet werden, demnach wird die Sicherheitsarchitektur identifiziert. Dabei sind die Aufteilungsregeln Anhang D dieser Regelung zu beachten.

Für jedes identifizierte Architekturelement ist die Erfüllung der nach der jeweiligen Sicherheitsanforderungsstufe erforderlichen Maßnahmen nachzuweisen.

6.3.3.1 Nachweis für die Architekturelemente “Software”

Beinhalten die Architekturelemente Software, ist der Nachweis in Abhängigkeit der jeweiligen Sicherheitsanforderungsstufe (SAS) für die Software zu führen:

- für SAS = 0 sind die Nachweise
  - nach DIN EN 50657:2017 für BI (Basic Integrity)
  - nach DIN EN 50128:2011 für SSAS 0
- für SAS > 0 sind die Nachweise
  - nach DIN EN 50657:2017 für jeweilige SIL
  - nach DIN EN 50128:2011 für die jeweilige SSAS

zu führen.

Tabelle 8: Übertragung der SAS in Kategorie Software Normen für Fahrzeuge

SIRF		DIN EN 50657	DIN EN 50128
SAS 0	➔	BI	SSAS 0
SAS 1	➔	SIL 1	SSAS 1
SAS 2	➔	SIL 2	SSAS 2
SAS 3	➔	SIL 3	SSAS 3
SAS 4	➔	SIL 4	SSAS 4

Für Software von Steuergeräten (z. B. ASG, BSG, etc.), die mehrere Architekturelemente bzw. Funktionen beinhalten, ist die maximale SAS-Einstufung maßgebend für die Maßnahmen gegen systematische Fehler der Gesamtsoftwarefunktionalität.

Zusätzlich ist die gegenseitige Wechselwirkung (Rückwirkungsfreiheit) von Software Architekturelementen zu prüfen. Hierzu ist mittels einer Matrix nach Anhang E zu bewerten, ob eine Verbindung von Software mit einer niedrigeren Einstufung zu Software mit einer höheren Einstufung besteht (z.B. durch Nutzung gemeinsamer Rechner, Kommunikationswege, etc.). Hierzu ist einem Nachweis der Rückwirkungsfreiheit gemäß den Anforderungen in Anhang E zu darzustellen.

6.3.3.2 Nachweis für die Architekturelemente “Hardware”

Beinhalten die Architekturelemente Hardware (E/E/PE), so ist für diese Anteile die Erfüllung des Kriterienkatalogs zur Hardware Steuerungsfunktionen in Abhängigkeit der, dem Architekturelement zugeordneten SAS, zu zeigen, vgl. Anhang F.

6.3.3.3 Nachweis für die Architekturelemente “externe Einflüsse / Infrastruktur“

Beinhaltet ein Architekturelement externe Einflüsse / Infrastruktur sind diese Einflüsse im Hinblick auf die übertragene Sicherheitsverantwortung darzulegen. Die diesbezüglichen sicherheitsrelevanten Annahmen sind in einem Bedienerhandbuch und / oder sonstigen sicherheitsrelevanten Unterlagen im Zusammenhang mit dem bestimmungsgemäßen Betrieb des Fahrzeugs auszuhändigen.

6.3.3.4 Nachweis für die Architekturelemente “Akteure (z.B. Bedienpersonal, Betreiber)“

Beinhaltet ein Architekturelement Tätigkeiten durch Bedienpersonal oder weitere am Betrieb beteiligte Akteure, ist ein Nachweis über den Informationsaustausch mit diesen darzulegen. Dieser muss zeigen, dass ein Prozess vorhanden ist, der gewährleistet, dass diese Tätigkeiten inklusive deren Sicherheitsverantwortung dem Akteur dergestalt bewusstgemacht werden, dass er diese in sein Sicherheits- und Qualitätsmanagement übernimmt. Zusätzlich bzw. ergänzend hierzu müssen sicherheitsrelevante Anwendungsbedingungen in einem Bedienerhandbuch und/oder sonstigen sicherheitsrelevanten Unterlagen im Zusammenhang mit dem bestimmungsgemäßen Betrieb des Fahrzeugs ausgehändigt werden.

6.3.3.5 Nachweis für weitere Architekturelemente (z.B. „nicht-E/E/PE“-Elemente)

Für diese Architekturelemente ist ein geeignetes Risikoakzeptanzprinzip gemäß Kapitel 6.2 zu wählen. Die Eignung des Risikoakzeptanzprinzips ist zu begründen, siehe Kapitel 6.2.4. In der Regel wird dies das Risikoakzeptanzprinzip Anwendung von produktspezifischen Regelwerken (Grenzwerte, Schutzziel, Gestaltungsvorgaben, etc.) sein. Es gilt als ausreichend, wenn die in Kapitel 6.3.1 genannten Anforderungen erfüllt sind.

Anmerkung:
Eine Zuweisung von Ausfallraten auf Basis der Sicherheitsanforderungsstufen (SAS) erfolgt nicht.

6.3.3.6 Nachweisverfahren der funktionalen Sicherheit

Im Rahmen des Nachweises der funktionalen Sicherheit wird die Sicherheitsarchitektur der Eisenbahnfahrzeugfunktionen hinsichtlich folgender Aspekte bewertet:

- spezifikationsgerechtes funktionales Verhalten;
- Ausfallauswirkungen;
- Betrieb mit externen Einflüssen.

6.3.3.6.1 Bewertung des spezifikationsgerechten funktionalen Verhaltens

Hierin wird bewertet, dass

- die Anforderungsspezifikationen der Eisenbahnfahrzeugfunktionen die Sicherheitsanforderungen beinhaltet und
- die Eisenbahnfahrzeugfunktionen im ausfallfreien, normalen Zustand den Anforderungsspezifikationen entsprechen.

6.3.3.6.2 Bewertung von Ausfallauswirkungen

Hier wird bewertet, dass auch bei Ausfällen von einzelnen Architekturelementen ein definierter, sicherer Zustand des Fahrzeugs erhalten bzw. eingenommen wird. Dies erfolgt durch eine Analyse und Bewertung von:

- möglichen Ausfällen der Architekturelemente der Sicherheitsarchitektur sowie von Teilfunktionen, die einen Einfluss auf Sicherheitsarchitekturen haben;
- der Sicherheitsreaktion bei Auftreten der oben betrachteten Ausfälle (definierter Ausfallzustand);
- Erkennungsmechanismen der Ausfalloffenbarung in Art und Zeitverhalten;
- Verbleiben im definierten Ausfallzustand auch bei weiteren Ausfällen sowie die Kriterien für das Verlassen dieses Zustandes;

- der Testanforderungsspezifikation (strukturiertes Verfahren, Stichprobengröße, etc.), hierbei sind
  besondere Anforderungen (TSI, NNTR/NNTV, Betriebsvorgaben, Netzzugang, etc.) zu berücksichtigen.

6.3.3.6.3 Bewertung von Betrieb mit externen Einflüssen

Hier wird bewertet, dass

- die Anforderungsspezifikationen der Eisenbahnfahrzeugfunktionen den Betrieb unter festgelegten externen Einflüssen beinhalten und diese dem Regelbetrieb von Eisenbahnen entsprechen und
- die Eisenbahnfahrzeugfunktionen auch bei externen Einflüssen den Anforderungsspezifikationen entsprechen.

6.4 **Nachweisdokumentation**

Die Ergebnisse der Sicherheitsnachweisführung sind gemäß nachfolgender Tabelle zu dokumentieren.

Tabelle 9: Übersicht und Zuordnung der Nachweisdokumentationsmöglichkeiten

Kapitel	Inhaltliche Anforderung	Dokumentation	Spalte
6.1.1	Eisenbahnfahrzeugfunktionen	TeSiP	(1) - (6)
6.1.2	Gefährdungsermittlung	TeSiP	(7) - (11)
6.1.3	Gefährdungseinstufungen	TeSiP	(12) - (24)
6.1.3.1	Schaden (S)	TeSiP	(12) - (15)
6.1.3.2	Eintrittswahrscheinlichkeit (W)	TeSiP	(16) - (17)
6.1.3.3	Expositionszeitdauer (E)	TeSiP	(18) - (19)
6.1.3.4	Vermeidung (V)	TeSiP	(20) - (21)
6.1.3.5	Ermittlung der Sicherheitsanforderungsstufe (SAS)	TeSiP	(23)
6.1.3.6	Einstufungsindikator (Klassengrenzen)	TeSiP	(22)
6.1.4	Bewertung allgemein vertretbares Risiko	TeSiP	(27)
6.2.1	Nachweisverfahren auf Basis von Regelwerken (anerkannte Regeln der Technik)	TeSiP (Ergebnis) Herleitung, Darstellung der Eignung erfolgt im separaten Dokument	(27)
6.2.2	Nachweisverfahren auf Basis eines Referenzsystems	TeSiP (Ergebnis) Herleitung, Darstellung der Eignung erfolgt im separaten Dokument	(27)
6.2.3	Nachweisverfahren der expliziten Risikoabschätzung	TeSiP (Ergebnis) Herleitung, Darstellung der Eignung erfolgt im separaten Dokument	(27)

Kapitel	Inhaltliche Anforderung	Dokumentation	Spalte
6.3.1	Nachweisverfahren auf Basis von Regelwerken (anerkannte Regeln der Technik)	Separates Dokument mit Angaben zu: Eisenbahnfahrzeugfunktionen, herangezogene Regelwerke, Auflistung der Nachweisdokumentation	(28)
6.3.2	Nachweisverfahren auf Basis eines Referenzsystems	Separates Dokument mit Angaben zu: Eisenbahnfahrzeugfunktionen, Dokumentation des Referenzsystems, Nachweis der Kriterien aus Kapitel 6.2.2	(28)
6.3.3	Nachweisverfahren auf Basis der expliziten Risikoabschätzung	Sicherheitsarchitektur über Gefährdungsbäume dokumentieren begleitende Beschreibung der Eisenbahnfahrzeugfunktionen, Schnittstellen, Annahmen, Szenarien Nachweisführung zu allen Architekturelementen	(28)
6.3.3.1	Nachweis für die Architekturelemene “Software”	Nachweis für Erfüllung der in 6.3.3.1 genannten Regelwerke	(28)
6.3.3.2	Nachweis für die Architekturelemente “Hardware”	Nachweis für Erfüllung des HW-Kriterienkatalogs gemäß Anhang	(28)
6.3.3.3	Nachweis für die Architekturelement “externe Einflüsse / Infrastruktur“	Separates Nachweisdokument zur Erfüllung der Anforderungen aus Kapitel 6.3.3.3	(28)
6.3.3.4	Nachweis für die Architekturelemente “Akteure (z.B. Bedienpersonal, Betreiber)“	Separates Nachweisdokument zur Erfüllung der Anforderungen aus Kapitel 6.3.3.4	(28)
6.3.3.5	Nachweis für weitere Architekturelemente (z.B. „nicht-E/E/PE“-Elemente)	Separates Nachweisdokument	(28)
6.3.3.6	Nachweisverfahren der funktionalen Sicherheit	Separates Nachweisdokument zur Erfüllung der Anforderungen aus Kapitel 6.3.3.6	(28)

7 Abschluss des Risikomanagementverfahrens im Sinne der SIRF

7.1 Gesamthafte Sicherheitsnachweisdokumentation

Zusammenfassende Dokumentation auf Basis der einzelnen Teildokumentationen mit dem Ziel einer abschließenden Aussage, zur Vollständigkeit der Umsetzung des Risikomanagementverfahrens einschließlich dessen Ergebnisse. Diese muss mindestens enthalten:

- Auflistung bzw. nachvollziehbare Referenzierung der Dokumentation zu den einzelnen Schritten und Nachweisen des Risikomanagementverfahrens (Kapitel 5).
- Abschließende Aussage zur Erfüllung der Vollständigkeit der Umsetzung des Risikomanagementverfahrens einschließlich aller gegebenenfalls ermittelten Einschränkungen, Auflagen oder Empfehlungen.
- Auflistung und Beschreibung aller an weitere Akteure (z.B. Betreiber, Infrastruktur, Instandhaltung) weiterzugebender Informationen.

Die Dokumentation muss in sich konsistent sein und die Aspekte der sicheren Integration bzw. Kohärenz abdecken.

7.2 Nachweisdokumentation zum Informationsaustausch

Als Nachweis der Erfüllung des Informationsaustausches mit den beteiligten Akteuren (z.B. Information des Betreibers / Halters) muss der Nachweisführende die erforderlichen Informationen übergeben. Für das vorliegende Sicherheitsnachweisverfahren nach SIRF ist dies erfüllt, wenn alle sicherheitsrelevanten Unterlagen, die im Zusammenhang mit dem bestimmungsgemäßen Betrieb des Fahrzeugs stehen (z.B. sicherheitsrelevante Anwendungsbedingungen, Angaben aus dem Gefährdungsprotokoll die nicht von einem Akteur alleine beherrscht werden können) ausgehändigt und die Akteure darauf hingewiesen wurden.

8 Referenzen

[1]	DIN EN 50124-1:2017; VDE 0115-107-1; Bahnanwendungen - Isolationskoordination - Teil 1: Grundlegende Anforderungen - Luft- und Kriechstrecken für alle elektrischen und elektronischen Betriebsmittel; Deutsche Fassung EN 50124-1:2017 (; Ausgabe: 01.12.2017
[2]	EN 50124-1:2017; Railway applications - Insulation coordination - Part 1: Basic requirements - Clearances and creepage distances for all electrical and electronic equipment; Englisches Original; Ausgabe: 01.12.2017
[3]	DIN EN 50124-2:2017; VDE 0115-107-2; Bahnanwendungen - Isolationskoordination - Teil 2: Überspannungen und zugeordnete Schutzmaßnahmen; Deutsche Fassung EN 50124-2:2017; Ausgabe: 01.12.2017
[4]	EN 50124-2:2017; Railway applications - Insulation coordination - Part 2: Overvoltages and related protection; Englisches Original; Ausgabe: 01.12.2017
[5]	DIN EN 50126-1: 2018; VDE 0115-103-1:2018: Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 1: Generischer RAMS-Prozess; Deutsche Fassung EN 50126-1:2017; Ausgabe: 01.10.2018
[6]	EN 50126-1: 2017: Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process; Englisches Original; Ausgabe: 01.10.2017
[7]	DIN EN 50126-2: 2018; VDE 0115-103-2:2018: Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 2: Systembezogene Sicherheitsmethodik; Deutsche Fassung EN 50126-1:2017; Ausgabe: 01.10.2018
[8]	EN 50126-2: 2017: Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety; Englisches Original; Ausgabe: 01.10.2017
[9]	DIN EN 50128: 2012; VDE 0831-128:2012: Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software für Eisenbahnsteuerungs- und Überwachungssysteme; Deutsche Fassung EN 50128:2011; Ausgabe: 01.03.2012
[10]	EN 50128: 2011: Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems; Englisches Original; Ausgabe: 01.06.2011
[11]	DIN EN 50129: 2003; VDE 0831-129:2003-12: Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik; Deutsche Fassung EN 50129:2003; Ausgabe: 01.12.2012
[12]	EN 50129: 2003: Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signaling; Englisches Original; Ausgabe: 01.02.2003

[13]	DIN EN 50129: 2017; VDE 0831-129:2017 – Entwurf: Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik; Deutsche Fassung prEN 50129: 2016; Ausgabe 09.06.2017
[14]	DIN 50159-1: 2015; Metallische Werkstoffe - Härteprüfung nach dem UCI-Verfahren - Teil 1: Prüfverfahren; Deutsche Fassung EN 50159-1: 2015; Ausgabe 01.01.2015
[15]	DIN 50159-1: 2015; Metallic materials - Hardness testing with the UCI method - Part 1: Test method; Englisches Original EN 50159-1: 2015; Ausgabe 01.01.2015
[16]	DIN 50159-1: 2015; Metallische Werkstoffe - Härteprüfung nach dem UCI-Verfahren - Teil 1: Prüfverfahren; Deutsche Fassung EN 50159-1: 2015; Ausgabe 01.01.2015
[17]	DIN 50159-2: 2015; Metallic materials - Hardness testing with the UCI method - Part 2: Verification and calibration of the testing devices; Englisches Original EN 50159-2: 2015; Ausgabe 01.01.2015
[18]	DIN EN 50567: 2017; VDE 0831-657: Bahnanwendungen – Anwendungen für Schienenfahrzeuge – Software auf Schienenfahrzeugen; Deutsche Fassung EN 50657:2017; Ausgabe: 06.11.2017
[19]	EN 50567: 2017: Railways Applications – Rolling stock applications – Software on Board Rolling Stock; Englisches Original; Ausgabe: 08.05.2017
[20]	DIN EN 15380: Bahnanwendungen – Kennzeichnungssystematik für Schienenfahrzeuge – Teil 4: Funktionsgruppen; Deutsche Fassung EN 15380-4:2013; Ausgabe 05/2013
[21]	IEC 61508-1: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010; Ausgabe 01.02.2011
[22]	IEC 61508-1: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements (IEC 61508-1:2010); Englische Ausgabe EN 61508-1:2010; Ausgabe: 05.2010
[23]	IEC 61508-2: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010); Deutsche Fassung EN 61508-2:2010; Ausgabe: 01.02.2011
[24]	IEC 61508-2: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems; Englische Ausgabe EN 61508-2:2010; Ausgabe: 05.2010
[25]	IEC 61508-3: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 3: Anforderungen an Software (IEC 61508-3:2010); Deutsche Fassung EN 61508-3:2010; Ausgabe 01.02.2011
[26]	IEC 61508-3: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements; Englische Ausgabe EN 61508-1:2010; Ausgabe: 05.2010

[27]	IEC 61508-4: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010); Deutsche Fassung EN 61508-4:2010; Ausgabe 01.02.2011
[28]	IEC 61508-4: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations; Englische Ausgabe EN 61508-1:2010; Ausgabe: 05.2010
[29]	IEC 61508-5: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:2010); Deutsche Fassung EN 61508-5:2010; Ausgabe 01.02.2011
[30]	IEC 61508-5: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels; Englische Ausgabe EN 61508-1:2010; Ausgabe: 05.2010
[31]	IEC 61508-6: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2010); Deutsche Fassung EN 61508-6:2010; Ausgabe 01.02.2011
[32]	IEC 61508-6: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 Englische Ausgabe EN 61508-1:2010; Ausgabe: 04.2010
[33]	IEC 61508-7: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 7: Überblick über Verfahren und Maßnahmen (IEC 61508-7:2010); Deutsche Fassung EN 61508-7:2010; Ausgabe 01.02.2011
[34]	IEC 61508-7: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures; Englische Ausgabe EN 61508-1:2010; Ausgabe: 07.2010
[35]	IEC 60812 – Failure modes and effects analysis (FMEA and FMECA), Edition 3.0, Ausgabe: 2018-08DIN EN 50128: 2001: Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software für Eisenbahnsteuerungs- und Überwachungssysteme; Deutsche Fassung EN 50128:2001; Ausgabe: 01.11.2001
[36]	IEC 61882 – Hazard and operability studies (HAZOP studies) – Application guide, Edition 2.0, Ausgabe: 2016-03; Englische Ausgabe EN 61508-1:2010; Ausgabe: 15.05.2001
[37]	IEC 62278; CEI 62278: 2002: Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS); Ausgabe: 01.09.2002

[38]	DIRECTIVE 2004/49/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive); Ausgabe: 30.04.2004
[39]	RICHTLINIE 2004/49/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 29. April 2004 über Eisenbahnsicherheit in der Gemeinschaft und zur Änderung der Richtlinie 95/18/EG des Rates über die Erteilung von Genehmigungen an Eisenbahnunternehmen und der Richtlinie 2001/14/EG über die Zuweisung von Fahrwegkapazität der Eisenbahn, die Erhebung von Entgelten für die Nutzung von Eisenbahninfrastruktur und die Sicherheitsbescheinigung ("Richtlinie über die Eisenbahnsicherheit"); Ausgabe: 30.04.2004
[40]	RICHTLINIE (EU) 2016/798 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 11. Mai 2016 über Eisenbahnsicherheit (Neufassung); Amtsblatt der Europäischen Union; 11.5.2016
[41]	DIRECTIVE (EU) 2016/798 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016 on railway safety (recast); Official Journal of the European Union; 11.5.2016
[42]	Durchführungsverordnung (EU) Nr. 402/2013 der Kommission vom 30. April 2013 über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken und zur Aufhebung der Verordnung (EG) Nr. 352/2009; Ausgabe 30.4.2013
[43]	COMMISSION IMPLEMENTING REGULATION (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009; Ausgabe 30.4.2013
[44]	Durchführungsverordnung (EU) 2015/1136 der Kommission vom 13. Juli 2015 zur Änderung der Durchführungsverordnung (EU) Nr. 402/2013 über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken; Ausgabe 13.7.2015
[45]	COMMISSION IMPLEMENTING REGULATION (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment; Ausgabe 13.7.2015
[46]	Fachmitteilung 09 / 2017: Übergangsregelung zur Abkündigung der DIN EN 50128, Thema: Fahrzeuge; Quelle: Internet Seite des Eisenbahnbundesamtes - Service ; Ausgabe 11.05.2017
[47]	Leitfaden - zum Nachweis der Klimafunktionen des TESIP nach SIRF; Unterarbeitskreises (UAK) Klimafunktionen SIRF; Quelle: Internet Seite des Eisenbahnbundesamtes - Service; 16.11.2021
[48]	Handbuch Eisenbahnfahrzeuge; Bundesministerium für Verkehr, Bau und Stadtentwicklung; Version A; 5.5.2011
[49]	SYNOPSE Risikomanagement Verfahren nach CSM Verordnung, Inbetriebnahme Genehmigungsverfahren nach TEIV/VV IBG/EBA-Checkliste; Deutschen Bahn AG, Verband der Bahnindustrie in Deutschland e.V. (VDB), Verbandes Deutscher Verkehrsunternehmen e.V. (VDV) und Verband der Güterwagenhalter in Deutschland e. V. (VPI); 18.2.2011

9 Tabellen

10 Abbildungen

Anhang A. Muster technischer Sicherheitsplan TeSiP

Bebilderte Beschreibung zum TeSiP

Abbildung 4: Eisenbahnfahrzeugfunktionen – Gefährdungsermittlung

Abbildung 5: Gefährdungseinstufung

Abbildung 6: Risikoakzeptanzprinzip

Tabelle 10: Beschreibung der TeSiP Spalten

Spalte Nr.	Bedeutung der TeSiP Spalte
(1)	Definition der Eisenbahnfahrzeugfunktion - Hauptfunktion
(2)	Definition der Eisenbahnfahrzeugfunktion - Teilfunktion
(3)	Definition der Eisenbahnfahrzeugfunktion - Laufende Nummer gleicher Haupt- und Teilfunktionalität
(4)	Definition der Eisenbahnfahrzeugfunktion - Funktion
(5)	Definition der Eisenbahnfahrzeugfunktion - Erläuterung der Funktion
(6)	Sicherheitsanforderung – sichere Gewährleistung von ….
(7)	Sicherheitsanforderung – Gefährdung ist gegeben, wenn … - Bedingung für das Eintreten der möglichen Gefährdung
(8)	Beispiele zur Funktionsdefinition und der Gefährdung
(9)	Kenner für die Identifikation der Gefährdungen auf Systemebene Eisenbahnfahrzeug für die maßgebliche Gefährdung
(10)	Verbale Beschreibung der mit Nr. identifizierten Teilgefährdung durch die für die maßgebliche Gefährdungen auf Systemebene Eisenbahnfahrzeug
(11)	S_a: Schadensparameter für die Anzahl der Geschädigten
(12)	Verbale Beschreibung des Schadens für die Anzahl
(13)	S_v: Schadensparameter für den Verletzungsgrad der Geschädigten
(14)	Verbale Beschreibung des Schadens für den Verletzungsgrad
(15)	W: Parameter für die Wahrscheinlichkeit für den Eintritt der maßgeblichen Gefährdung
(16)	Verbale Beschreibung der Wahrscheinlichkeit für den Eintritt der maßgeblichen Gefährdung
(17)	E: Parameter für die Expositionsdauer, der die geschädigten Personen der möglichen Gefahr ausgesetzt sind
(18)	Verbale Beschreibung der Expositionsdauer, der die geschädigten Personen der möglichen Gefahr ausgesetzt sind
(19)	V: Parameter für die mögliche Vermeidung des Schadens für den möglicherweise Geschädigten

Spalte Nr.	Bedeutung der TeSiP Spalte
(20)	Verbale Beschreibung für die mögliche Vermeidung des Schadens für den möglicherweise Geschädigten
(21)	I: Einstufungsindikators auf Basis der Parameter der Gefährdungseinstufung
(22)	SAS – ermittelte Sicherheitsanforderungsstufe gemäß des Einstufungsindikators (Klassengrenzen) auf Basis der Parameter der Gefährdungseinstufung
(23)	für Gefährdungseinstufung relevante Bemerkung
(24)	Bemerkungen
(25)	Festlegung des gewählten Risikoakzeptanzprinzips
(26)	Randbedingungen für die Einstufung der Eisenbahnfahrzeugfunktion – Szenario für die Maßgebliche Gefährdung
(27)	Randbedingungen für die Einstufung der Eisenbahnfahrzeugfunktion – Annahmen für die Maßgebliche Gefährdung
(28)	Randbedingungen für die Einstufung der Eisenbahnfahrzeugfunktion – Randbedingungen für die Maßgebliche Gefährdung unter der Sie eintreten kenn
(29)	Informativ: Spalte für zusätzliche Informationen und Hinweise

Anhang B. Gefährdungen auf Systemebene Eisenbahnfahrzeug

Tabelle 11: Gefährdungen auf Systemebene Eisenbahnfahrzeug

Gefährdungen auf Systemebene Eisenbahnfahrzeug			Fahrzeugsystem-Relevanz			
Nr. Gefährdung	Nr. Teil-Gefährdung	Beschreibung	Lok	Triebzug	Reisezug-wagen	Güterwagen
1	Kontrolle über Zugbewegung vermindert oder nicht gegeben					
	1a	Fahrzeug setzt sich ungewollt durch Aufschalten von Traktion in Bewegung	x	x		
	1b	Fahrzeug fährt in falsche Richtung	x	x		
	1c	Unbemerkt zu hohe Geschwindigkeit	x	x		
	1d	Ausfall Tf wird nicht erkannt	x	x		
	1e	Ergonomie des Führerstands unzureichend / Unzureichende Sicht Tf	x	x	x	
2	Bremsung des Fahrzeugs unzeitig, vermindert oder nicht gegeben					
	2a	Bremskraft vermindert oder nicht gegeben	x	x	x	x
	2b	Unzeitige Bremskraft (ungewollt unerkannt anliegende Bremse)	x	x	x	x
	2c	Fahrgast-Notbremsanforderung versagt	x	x	x	
3	Spurführung nicht ausreichend					
	3a	Spurführung versagt, Entgleisung	x	x	x	x
4	Gefährdung bei Ein- und Ausstieg					
	4a	Gefährdung von Personen im Ein- bzw. Ausstiegbereich im Stillstand	x	x	x	
	4b	Gefährdung von Personen im Ein- bzw. Ausstiegsbereich während der Fahrt	x	x	x	
	4c	Gefährdung beim Ein- u. Ausstieg von Personal	x	(x)	(x)	
	4d	Gefährdung durch Einklemmen		x	x	
5	Entzündung / Brand / Rauchentwicklung					
	5a	Brandgefährdung, Rauchentwicklung	x	x	x	x
6	Explosionsgefährdung					
	6a	Explosion, Bersten von Geräten/ Komponenten (Druck, umherfliegende Teile, Splitterwirkung, austretende Gase oder Flüssigkeiten.)	x	x	x	x
7	Verletzung des Fahrzeugumgrenzungsprofils					
	7a	Verletzung des Fahrzeugumgrenzungsprofils durch den Wagenkasten	x	x	x	x
	7b	Verletzung des Fahrzeugumgrenzungsprofils durch bewegliche Anbauteile (Spiegel, Klappen, Einschübe, Stromabnehmer)	x	x	x	x
	7c	Verletzung des Fahrzeugumgrenzungsprofils durch Fahrwerkschaden (Federn, Dämpfer)	x	x	x	x
	7d	Verletzung des Fahrzeugumgrenzungsprofils durch Steuerungen (Neigetechnik)		x	x	
8	Störungen durch elektrische Wechselwirkungen mit anderen Anlagen und Fahrzeugen					

Gefährdungen auf Systemebene Eisenbahnfahrzeug			Fahrzeugsystem-Relevanz			
Nr. Gefährdung	Nr. Teil-Gefährdung	Beschreibung	Lok	Triebzug	Reisezug-wagen	Güterwagen
	8a	Fahrzeug verursacht Störungen von externen Anlagen (z.B. Signalanlagen, Sicherheitseinrichtungen, andere Fahrzeuge)	x	x	x	
	8b	Störung von sicherheitsrelevanten Funktionen innerhalb des Fahrzeuges durch Störstrahlung	x	x	x	
9	Ungewollte Zugtrennung					
	9a	Ungewollte Zugtrennung durch undefiniertes Traktionsverhalten, zu hohe, ruckartige Zugkräfte	x	x		
	9b	Ungewollte Zugtrennung bzw. Überpufferung durch undefiniertes Bremsverhalten (betriebliches Überbremsen)	x	x	x	x
	9c	Ungewollte Zugtrennung durch sonstige Ursachen (z.B. mechanischer Schaden)	x	x	x	x
	9d	Ungewollte Zugtrennung durch automatisches Entkuppeln		x		
10	Aufenthaltsbedingungen im Fahrzeug nicht gewährleistet (Führerraum, Maschinenraum, Fahrgastraum)					
	10a	Gefährdungen durch unzureichende Belüftung/ Klimatisierung	x	x	x	
	10b	Gefährdungen durch Luftdruckschwankungen (Druckstöße) im Fahrzeug	x	x	x	
	10c	Gefährdungen durch Innenraumgestaltung (z.B. Sturzgefahr, Verletzungsgefahr an scharfen Ecken und Kanten, Einklemmen, Scheibenbruch, heiße Teile)	x	x	x	
	10d	Gefährdungen durch zu hohen Schallpegel	x	x	x	x
	10e	Gefährdungen durch Beeinflussung von Implantaten		x	x	
	10f	Unzureichende Festigkeit des Wagenkastens und befestigter Strukturen	x	x	x	x
	10g	Gefährdungen durch Lebensmittelvergiftung (z.B. Galley Speisewagen, Wasseraufbereitung)		x	x	
	10h	Sonstige Gefährdungen (z.B. toxische Stoffe, Ausdampfungen)	x	x	x	
	10j	Elektrische Berührungsspannung im Fahrbetrieb zu hoch	x	x	x	
	10k	Elektrische Berührungsspannung bei Wartung und Instandhaltung zu hoch	x	x	x	
	10l	Gefährdung von Insassen durch zu hohe Beschleunigungen während der Fahrt, (z.B. Rucke, im Innenraum herumfliegende Teile)	x	x	x	
11	Gefährdungen von Personen außerhalb des Zuges / an der Strecke					
	11a	Gefährdung durch Nichterkennen des Fahrzeugs (z.B. Spitzensignal, Typhon)	x	x	x	x
	11b	Gefährdung durch ungünstiges aerodynamisches Verhalten bei Vorbeifahrt (Bugwelle)	x	x	x	x
	11c	Gefährdung durch abgerissene Fahrzeugteile, Betriebsmittel	x	x	x	x
	11d	Unzureichend gesicherte Ladung				x

Gefährdungen auf Systemebene Eisenbahnfahrzeug			Fahrzeugsystem-Relevanz			
Nr. Gefährdung	Nr. Teil-Gefährdung	Beschreibung	Lok	Triebzug	Reisezug-wagen	Güterwagen
Hat ein externes Ereignis oder eine der genannten Gefährdungen zu einem Unfall geführt, sind folgende weitergehende Gefährdungspotentiale zu berücksichtigen:						
12	Nichtbeherrschen von Notsituationen					
	12a	Evakuierung von Personen im Notfall nicht möglich, Fluchtwege unzureichend (z.B. Tf-Fluchttür, Notausstiege)	x	x	x	
	12b	Unzureichende Crashfestigkeit	x	x	x	x
	12c	Unzureichende Zugänglichkeit im Notfall (z.B. Türöffnung von außen)	x	x	x	
	12d	Unzureichende Verfügbarkeit von im Notfall erforderlichen Eisenbahnfahrzeug (z. B. keine Traktion im Tunnel, Ausfall Notruffunktion, ungewollte Bremsung in kritischer Umgebung, Notbeleuchtung)	x	x	x	
	12e	Unzureichende Rettungsmittel	x	x	x	

Anmerkung:

Die in der Tabelle aufgeführten Gefährdungen sind auf Vollständigkeit für das betroffene Eisenbahnfahrzeug zu prüfen und ggf. zu ergänzen. Die Angaben zur Relevanz für das Fahrzeugsystem sind gemäß der Anwendung zu prüfen.

Anhang C. Gefährdungsbäume

Zur Darstellung der Architekturaufteilung und der Aufteilung der sicherheitstechnischen Verantwortung wurde die Methode des Gefährdungsbaums vereinbart.

Das Prinzip des Gefährdungsbaums:

- Oberstes Element ist die maßgebliche Gefährdung für die betrachtete Eisenbahnfahrzeugfunktion.
- Darunter schließen sich Architekturelemente an, deren Fehlfunktionen einen Beitrag zum möglichen Eintreten der maßgeblichen Gefährdung hat.
- Diesen Architekturelementen werden Sicherheitsanforderungsstufen gemäß der Aufteilungsregeln dieser Regelung (Anhang D) zugeordnet.
- Die Sicherheitsanforderungsstufen der identifizierten Architekturelemente haben die Aufgabe, die möglichen Fehlfunktionen in ausreichendem Maße zu beherrschen.

Der grundlegende Aufbau ist in diesem Anhang „Gefährdungsbaum“ dargestellt. Die Aufteilungsregeln sind in zusätzlich im Anhang D festgelegt und bei der Erstellung der Gefährdungsbäume zu beachten.

Der Gefährdungsbaum enthält folgende Bestandteile:

- Die zugeordnete Gefährdung / der Eisenbahnfahrzugfunktion gemäß TeSiP als Top-Ereignis;
- Beschreibungen für die zu Grunde liegenden Szenarien;
- Kennzeichnung der Verantwortungsbereiche;
- Nachweisbare Architekturelemente (AE);
- Logische Beziehungen (UND, ODER) zwischen den AE;
- Eindeutige Zuordnung der SAS unter Berücksichtigung der Aufteilungsregeln.

Für nachfolgende Eisenbahnfahrzeugfunktionen wurden Gefährdungsbäume unter Berücksichtigung allgemein bekannter Betriebsbedingungen und Umgebungseinflüssen im Expertenkreis erarbeitet. Diese speziellen Funktionen sind im Eisenbahnsektor abgestimmt, vgl. Tabelle 12

Tabelle 12: Liste speziell im Eisenbahnsektor abgestimmter Gefährdungsbäume

Funktion	Bezeichnung
DC3	Automatischen Kuppelvorgang gewährleisten
FD2 (a)	Vortriebskraft erzeugen – Triebzüge/Triebwagen
FD2 (b)	Vortriebskraft erzeugen – Lok bespannte Züge
GD1 (a)	Bremskraft erzeugen (ED-Bremse) – Triebzüge/Triebwagen
GD1 (b)	Bremskraft erzeugen (ED-Bremse) – Lok bespannte Züge
GD3	Bremskraft erzeugen (Parkbremse anlegen)
GD3	Bremskraft erzeugen (Parkbremse lösen)
K4	Fahrzeug übergeordnet steuern (Fahrgast-Notbremse)

Funktion	Bezeichnung
K5	Fahrzeug übergeordnet steuern (Fahrgastnotbremsüberbrückung, NBÜ)
K9	Fahrzeug übergeordnet steuern (Automatische Fahrbremssteuerung)
K10	Fahrzeug übergeordnet steuern (Automatische Bremsprobe)
LH 2	Gewährleisten der Funktion der Gleisfreimeldung
TSI 4.2.5.5.8	Beherrschung von Türöffnungsgefährdungen

Bei Anwendung ist zu prüfen, dass die angenommenen Betriebsbedingungen und Umgebungseinflüsse im jeweiligen Projekt zutreffend sind oder sie entsprechend anzupassen sind.

Für die Gefährdungsbäume gilt allgemein, dass sie:

- vorrangig eine Art Anleitung für die Gestaltung der Sicherheitsarchitektur sind,
- nicht den Anspruch auf Vollständigkeit erheben können,
- nicht eine technische Realisierung vollständig vorwegnehmen können.

Zusätzlich wurden ergänzend in dieser Überarbeitung der Sicherheitsregelung Gefährdungsbäume zur Klimatisierung mit aufgenommen, die das Ergebnis einer Abstimmung zum Umgang mit den Risiken bei der Klimatisierung zusammenfassen.

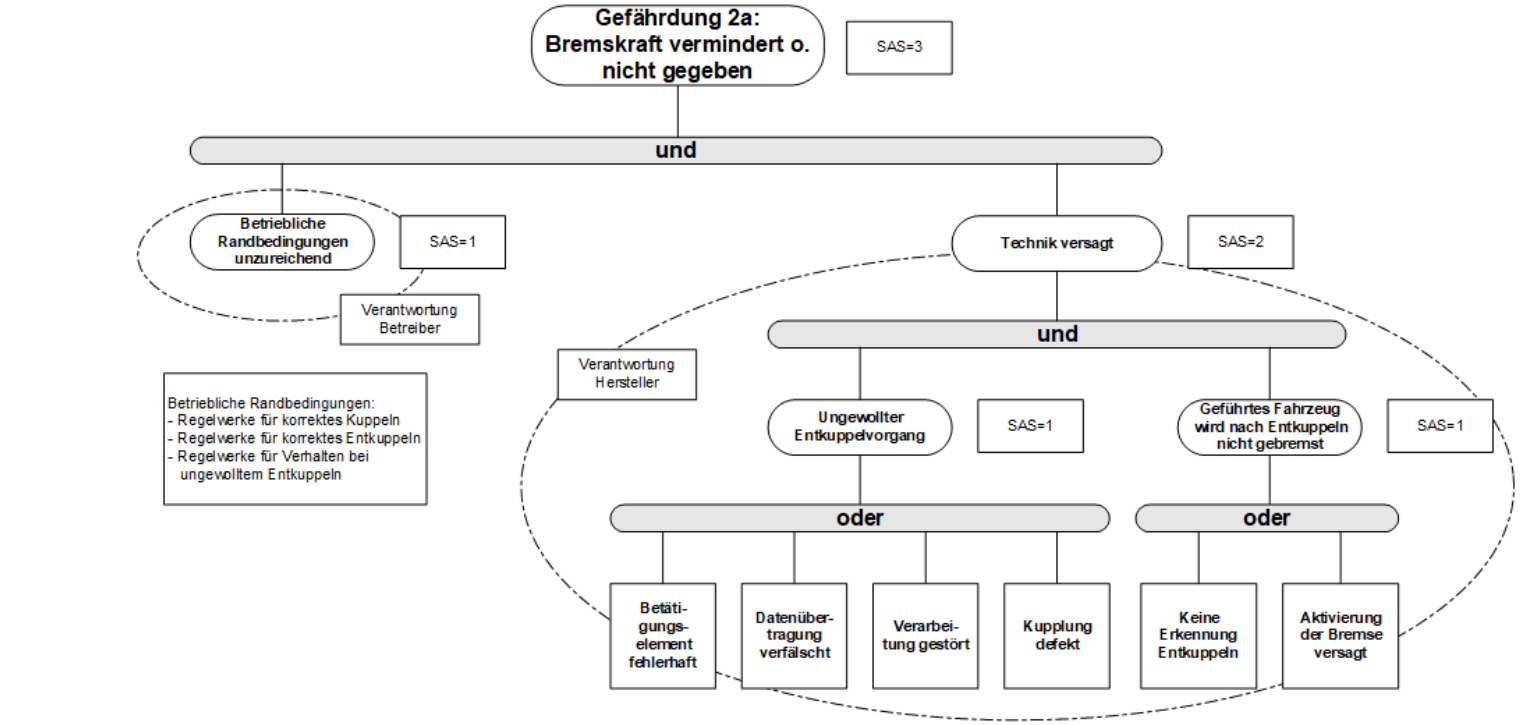
Tabelle 13: Liste speziell im Eisenbahnsektor abgestimmter Gefährdungsbäume für Klimafunktionen

Funktion	Bezeichnung
HH2	Verteilen von Brandgasen durch Nicht-Abschalten (des betroffenen HKL Gerätes)
HH3	unzureichende Belüftung / Klimatisierung (Alternativpfad A)
HH3	unzureichende Belüftung / Klimatisierung (Alternativpfad A – Teil 1)
HH3	unzureichende Belüftung / Klimatisierung (Alternativpfad A – Teil 2)
HH3	unzureichende Belüftung / Klimatisierung (Alternativpfad B – Teil 1)
HH3	unzureichende Belüftung / Klimatisierung (Alternativpfad B – Teil 2)

Weitere technische Hintergrundinformation zu den Klimatisierungsfunktionen sind im Leitfaden - Präzisierung bzw. Klärung offener Punkte zu den Anforderungen der SIRF [47] zu finden.

TeSiP-Funktion
D C 3

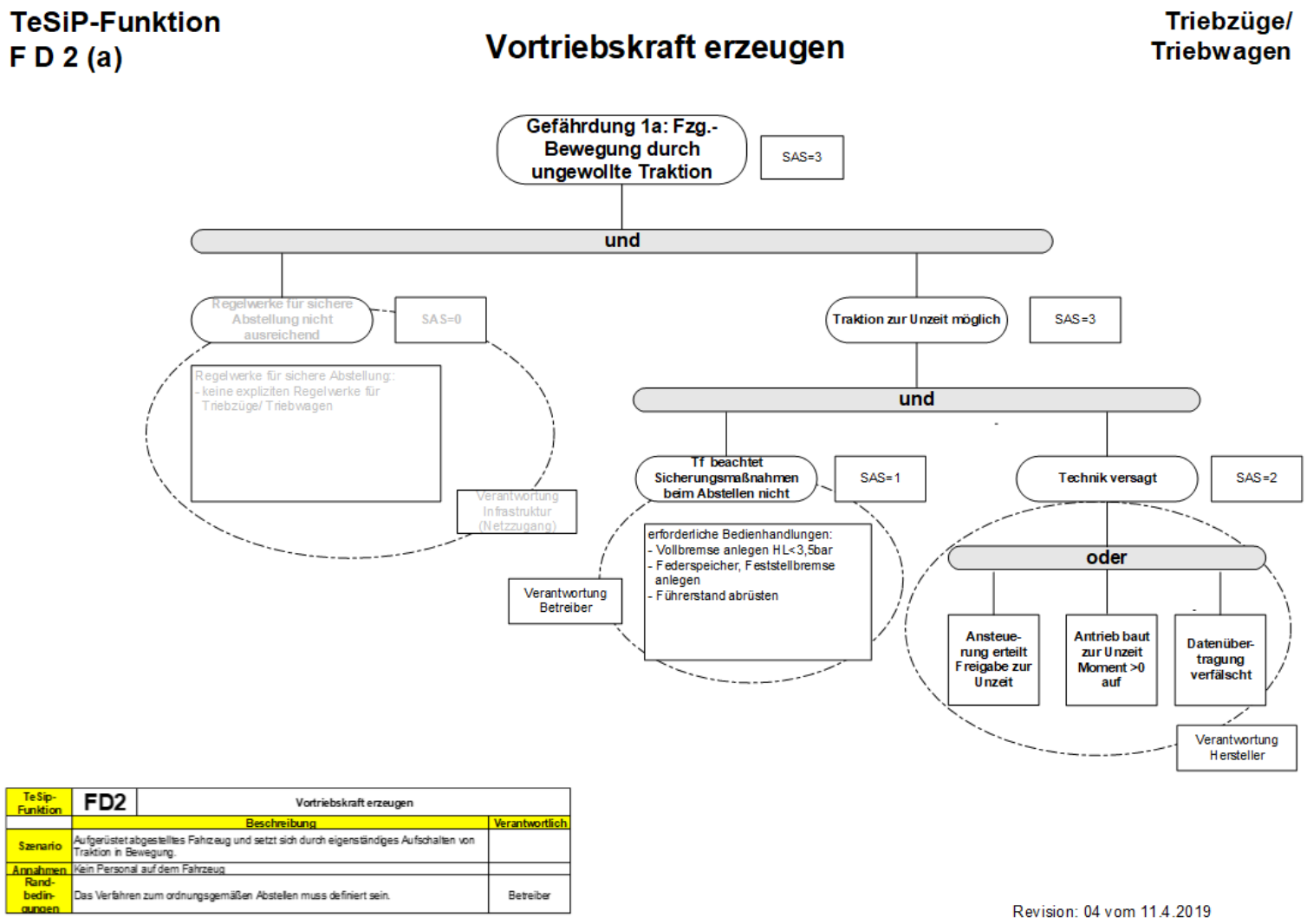
Automatischen Kuppelvorgang gewährleisten



TeSip-Funktion	DC3	Automatischen Kuppelvorgang gewährleisten	
	Beschreibung		Verantwortlich
Szenario	Ein in Mehrfachtraktion gekuppeltes Fahrzeug wird unbeabsichtigt entkuppelt. Gefährdung gegeben, wenn das geführte Fahrzeug nicht gebremst wird.		
Annahmen	Es wird nur die Auslösung der Bremsung, aber nicht der eigentliche Bremsvorgang betrachtet.		
Rand-bedin-gungen	Es wird nur das Nichtbremsen des geführten Fahrzeugs betrachtet. Die betrieblichen Folgen des ungewollten Entkuppelns und deren betriebliche Behandlung ist nicht Gegenstand des Sicherheitsnachweises Fahrzeug.		Betreiber

Revision: 04 vom 11.4.2019

Abbildung 7: DC3 - Automatischen Kuppelvorgang gewährleisten



TeSip-Funktion	FD2	Vortriebskraft erzeugen	
	Beschreibung		Verantwortlich
Szenario	Aufgerüstet abgestelltes Fahrzeug und setzt sich durch eigenständiges Aufschalten von Traktion in Bewegung.		
Annahmen	Kein Personal auf dem Fahrzeug		
Rand-bedin-gungen	Das Verfahren zum ordnungsgemäßen Abstellen muss definiert sein.		Betreiber

Abbildung 8: FD2(a) - Vortriebskraft erzeugen

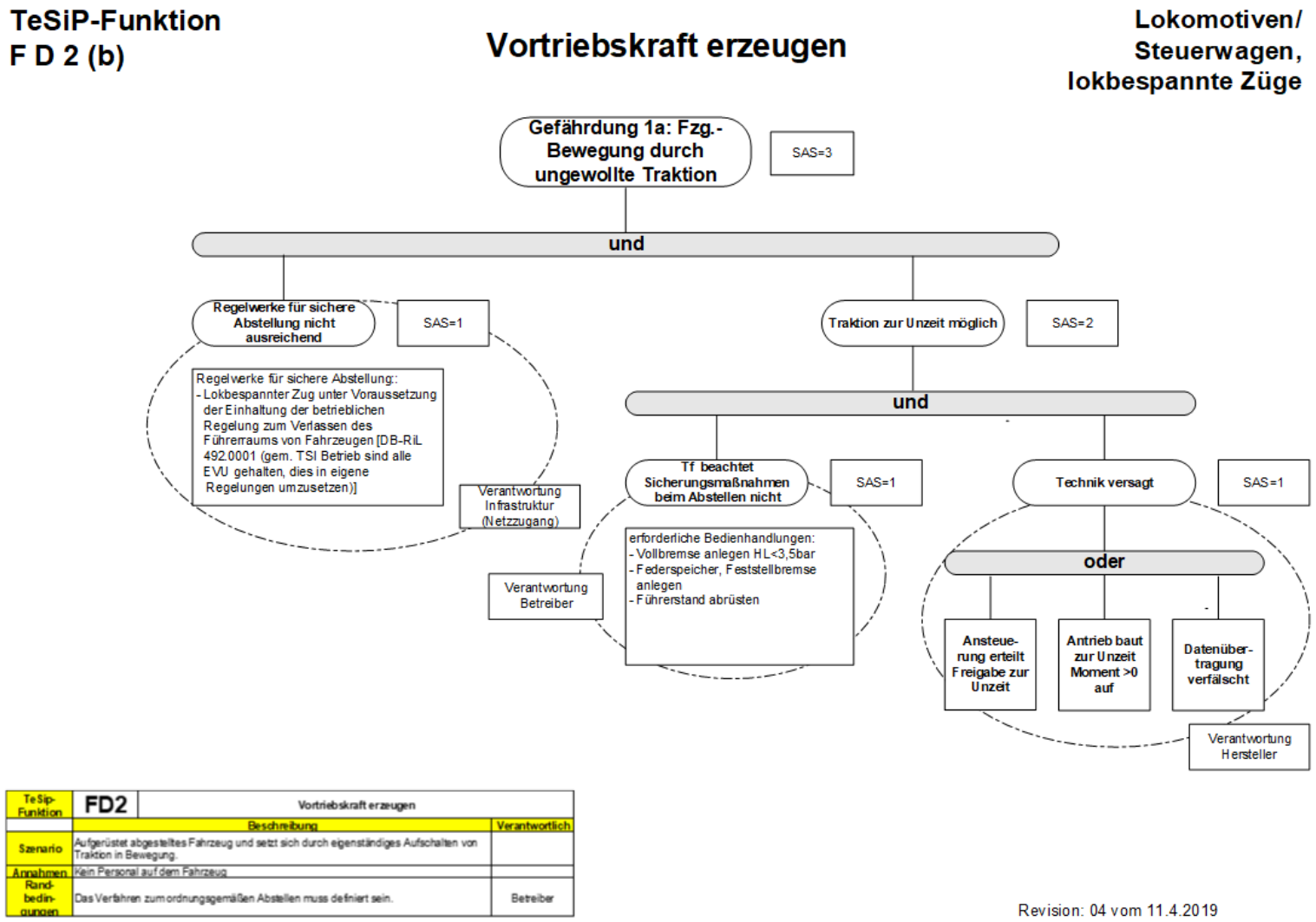


Abbildung 9: FD2(b) - Vortriebskraft erzeugen

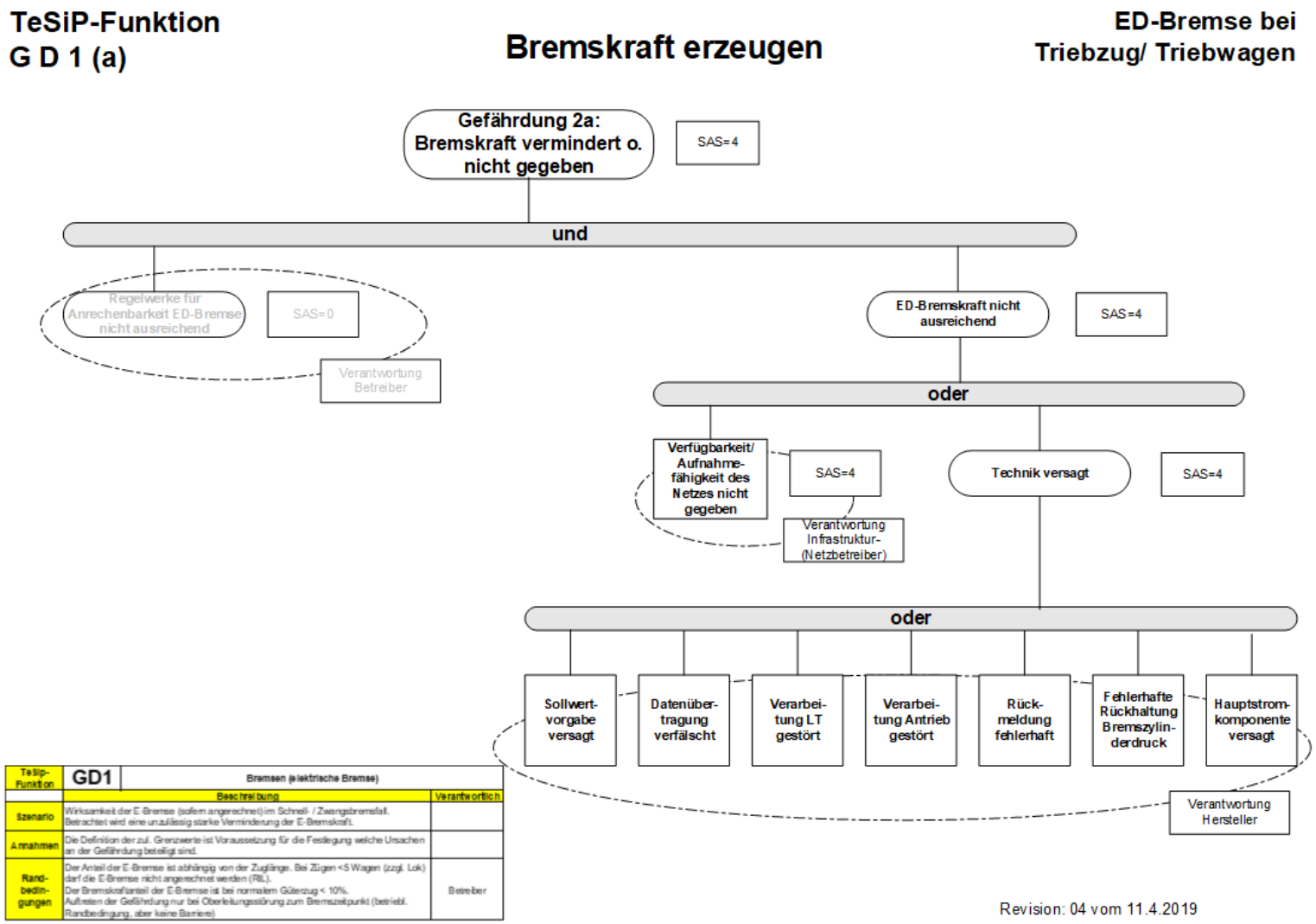


Abbildung 10: GD1(a) - Bremskraft erzeugen (ED-Bremse)

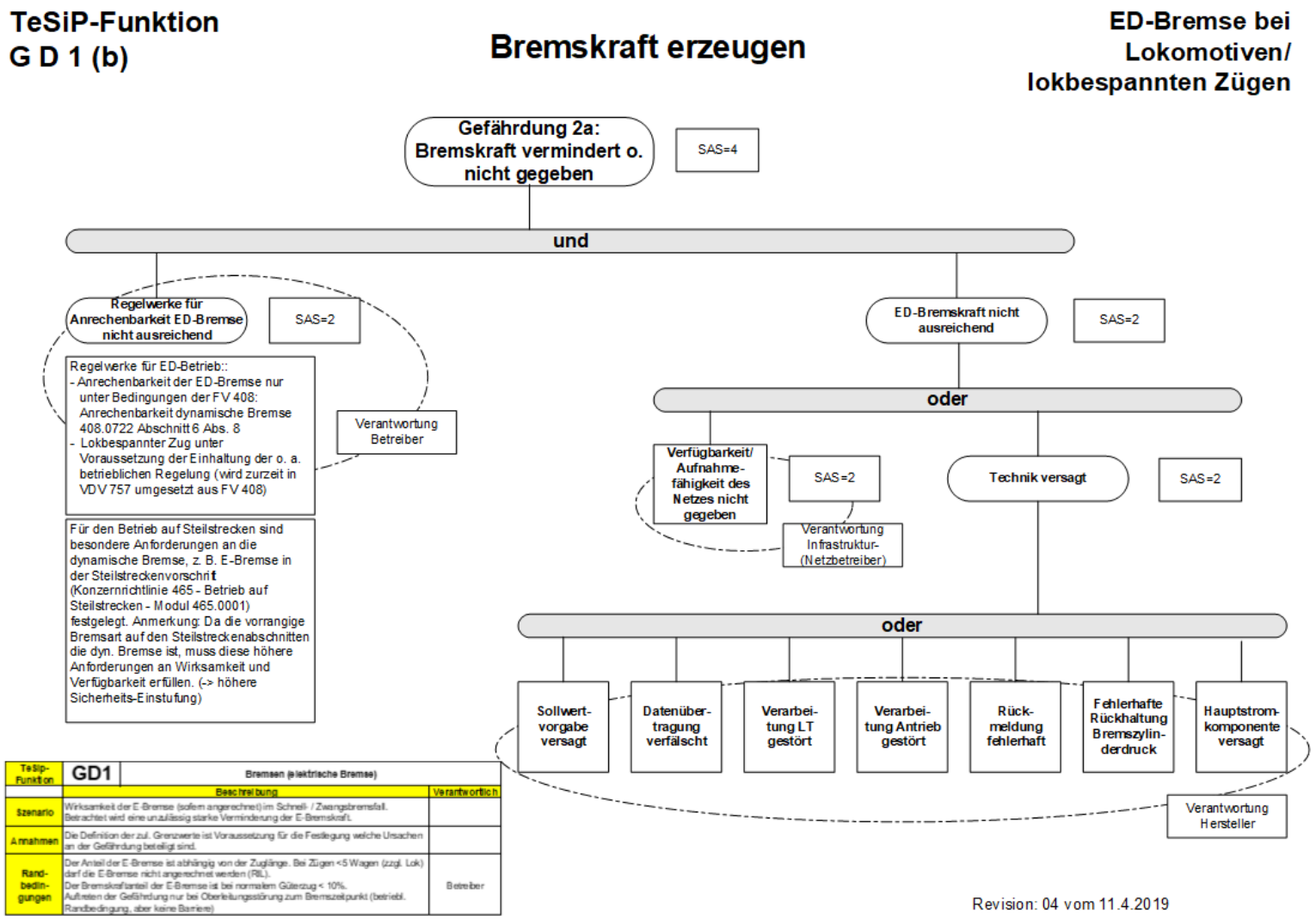


Abbildung 11: GD1(b) - Bremskraft erzeugen (ED-Bremse)

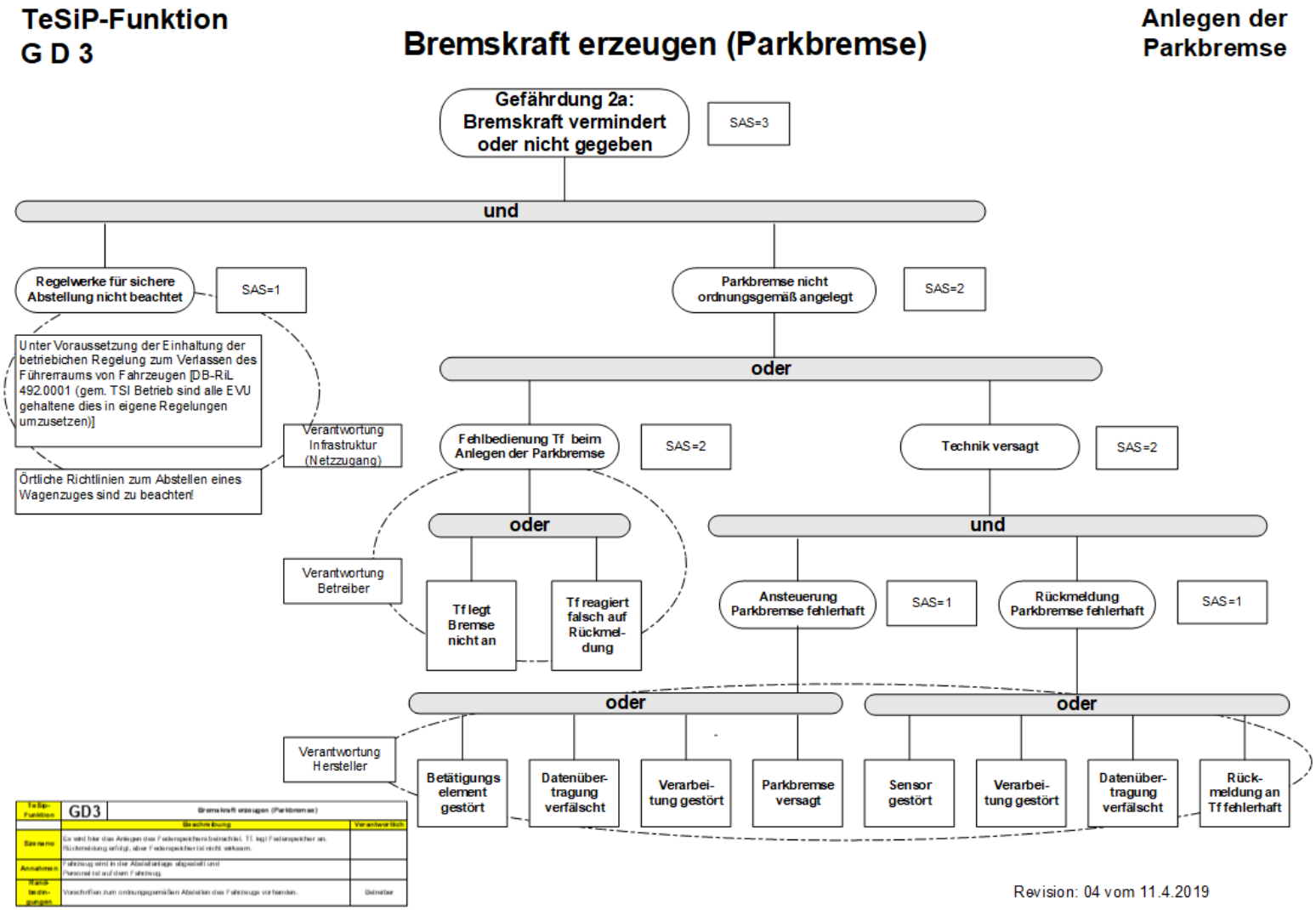
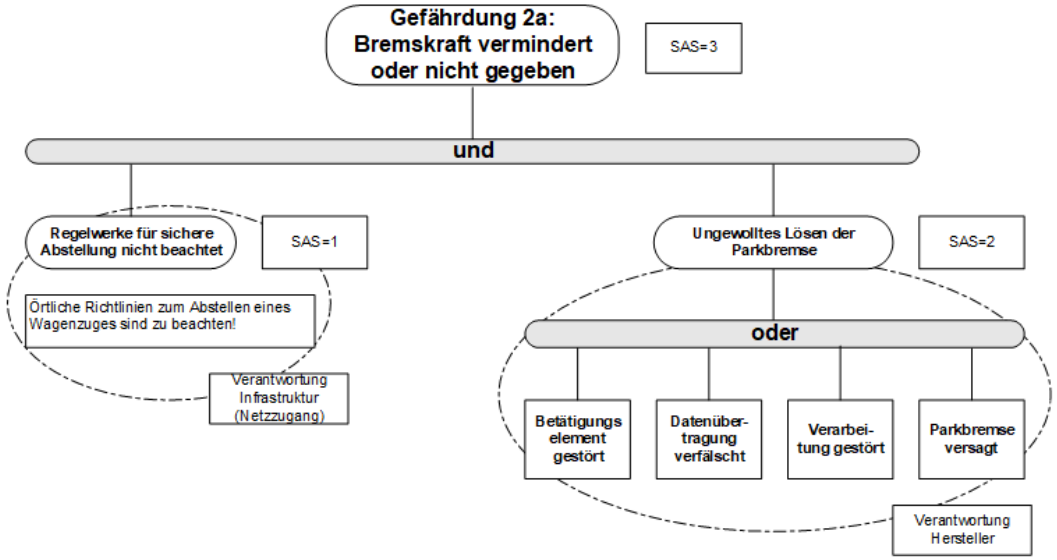


Abbildung 12: GD3 - Bremskraft erzeugen (Parkbremse anlegen)

TeSiP-Funktion
G D 3

Bremskraft erzeugen (Parkbremse)

Lösen der Parkbremse



TeSip-Funktion	GD3	Bremskraft erzeugen (Parkbremse)	
	Beschreibung		Verantwortlich
Szenario	Das Fahrzeug ist mit angelegtem Federspeicher abgestellt. Es wird das ungewollte Lösen des Federspeichers betrachtet.		
Annahmen	Personal ist nicht auf dem Fahrzeug. (Führerstandswechsel bei Wendezugbetrieb oder Funktionalität "Aufgerüstet abgestellt").		
Rand-bedin-gungen			

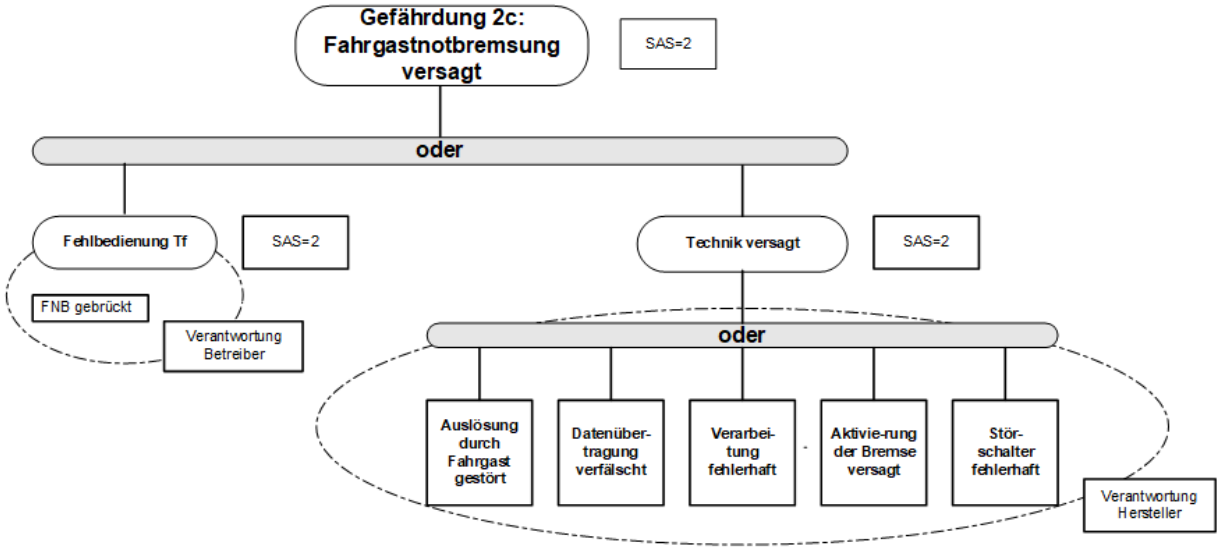
Revision: 04 vom 11.4.2019

Abbildung 13: GD3 - Bremskraft erzeugen (Parkbremse lösen)

TeSiP-Funktion K 4

Fahrzeug übergeordnet steuern, diagnostizieren, überwachen

Fahrgastnot-bremsung



TeSip-Funktion	K4	Fahrzeug übergeordnet steuern, diagnostizieren, überwachen	
	Beschreibung		Verantwortlich
Szenario	Fahrgast kann in Notfallsituation keine Fahrgastnotbremse auslösen.		
Annahmen	Es wird nur der Wirkweg von der Auslösung durch den Fahrgast bis zur Einleitung des eigentlichen Bremsvorganges (z. B. Schutzkontakt in der Schnellbremsschleife) betrachtet.		
Rand-bedin-gungen			

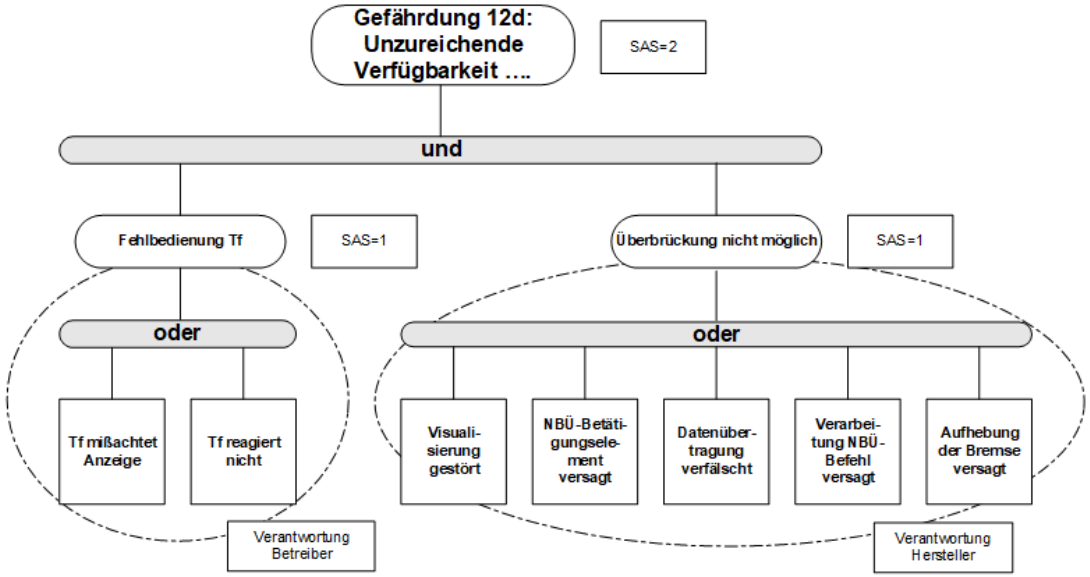
Revision: 04 vom 11.4.2019

Abbildung 14: K4 - Fahrzeug übergeordnet steuern (Fahrgast-Notbremse)

TeSiP-Funktion K 5

Fahrzeug übergeordnet steuern, diagnostizieren, überwachen

Fahrgastnotbrems-überbrückung (NBÜ)



TeSip-Funktion	K5	Fahrzeug übergeordnet steuern, diagnostizieren, überwachen
	Beschreibung	Verantwortlich
Szenario	Eine Fahrgastnotbremsung wird eingeleitet und Fahrzeug befindet sich an einem betrieblich ungeeigneten Ort (z. B. im Tunnel, auf einer Brücke) und kann durch Tf. nicht aufgehoben werden.	
Annahmen	Es wird nur der Wirkweg der Eingriffsmöglichkeit des Tf zur Aufhebung der durch den Fahrgast eingeleiteten Notbremsung betrachtet	
Rand-bedin-gungen	Das Rettungskonzept mindert nur den Schaden und greift erst nach Stillstand. Wenn eine Fahrgastnotbremsung bei geringen Geschwindigkeiten eingeleitet wird, kommt der Zug zum Stillstand, bevor NBÜ lösen kann!	

Revision: 04 vom 11.4.2019

Abbildung 15: K5 - Fahrzeug übergeordnet steuern (Fahrgastnotbremsüberbrückung, NBÜ)

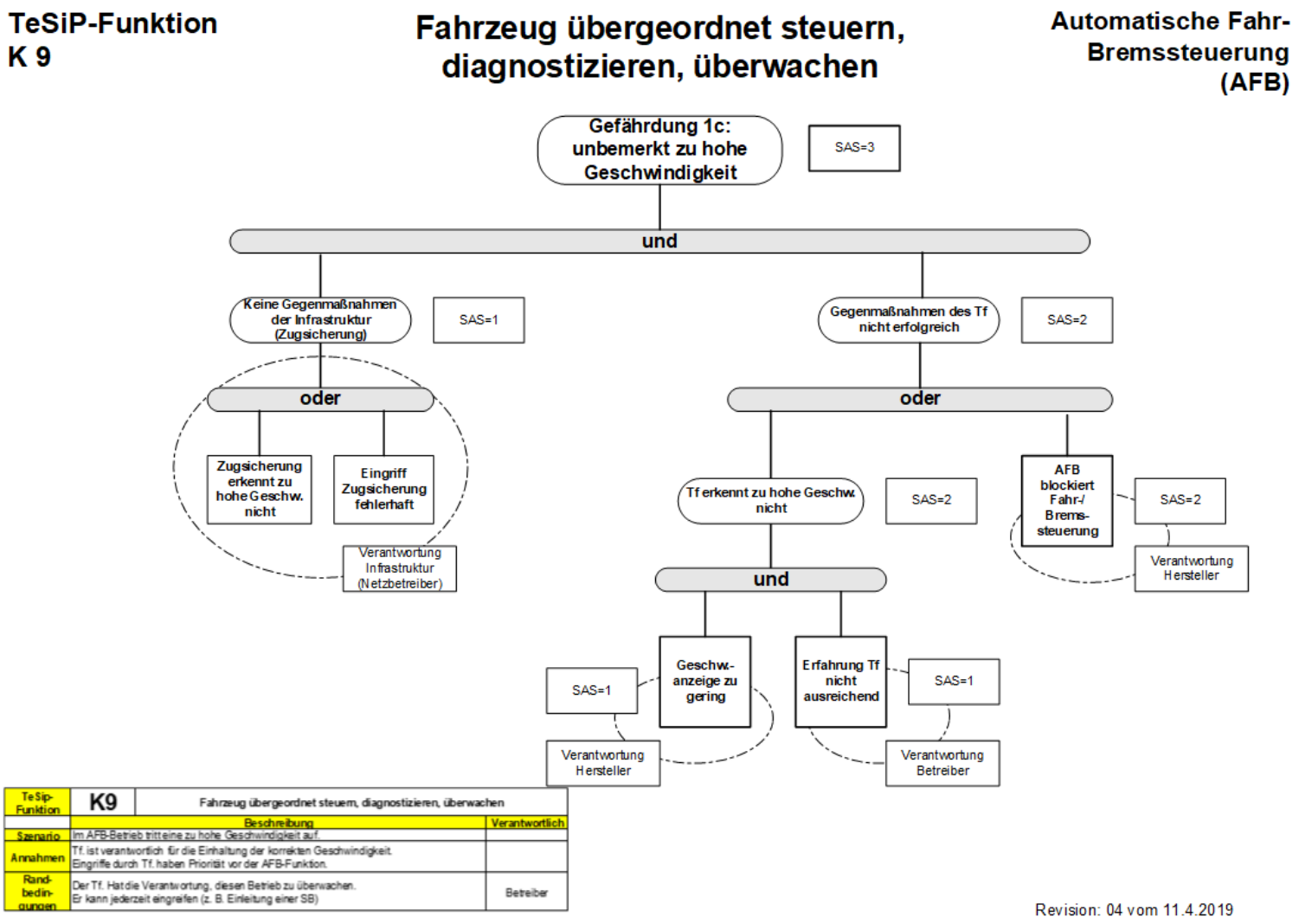


Abbildung 16: K9 - Fahrzeug übergeordnet steuern (Automatische Fahrbremssteuerung)

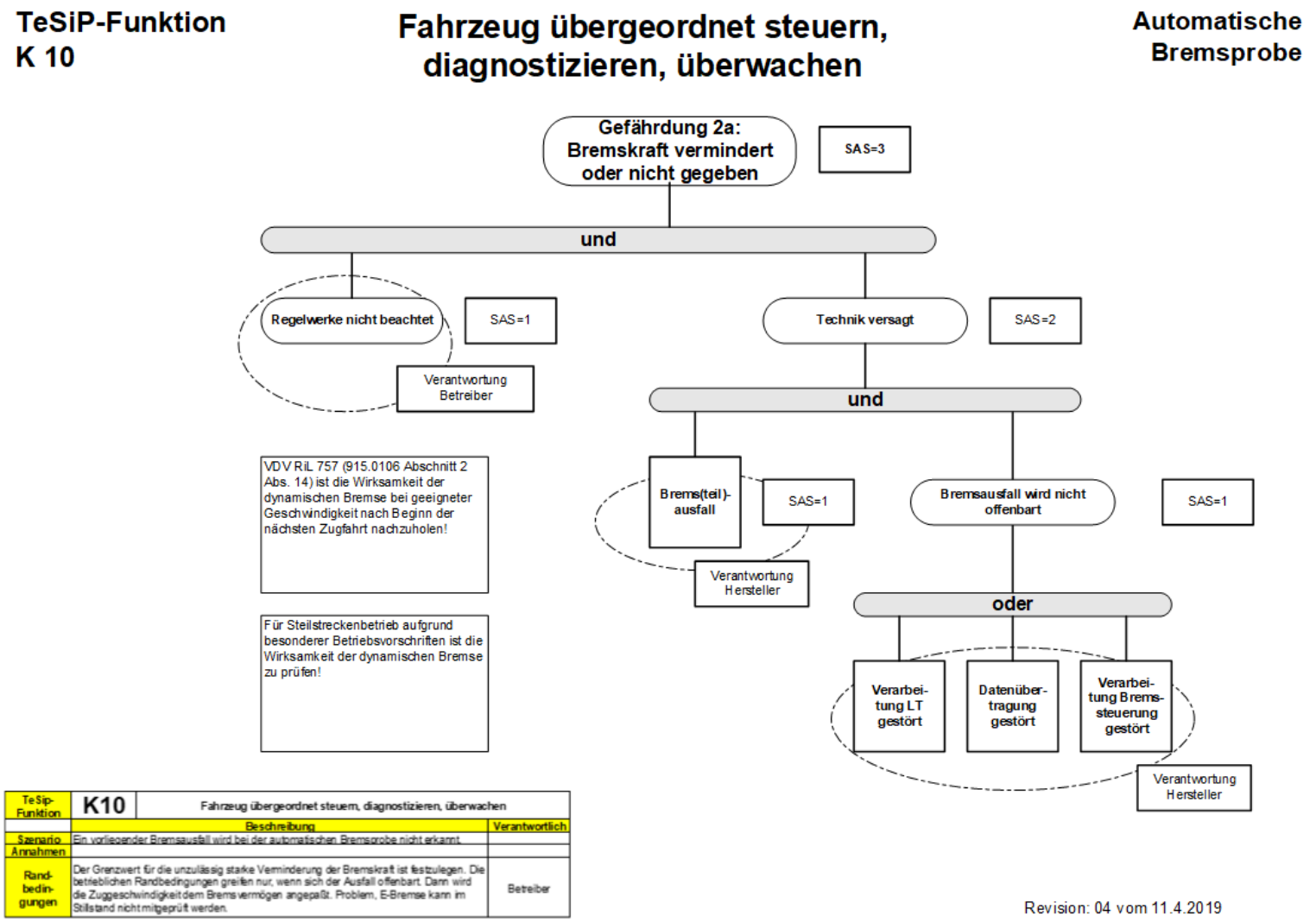


Abbildung 17: K10 - Fahrzeug übergeordnet steuern (Automatische Bremsprobe)

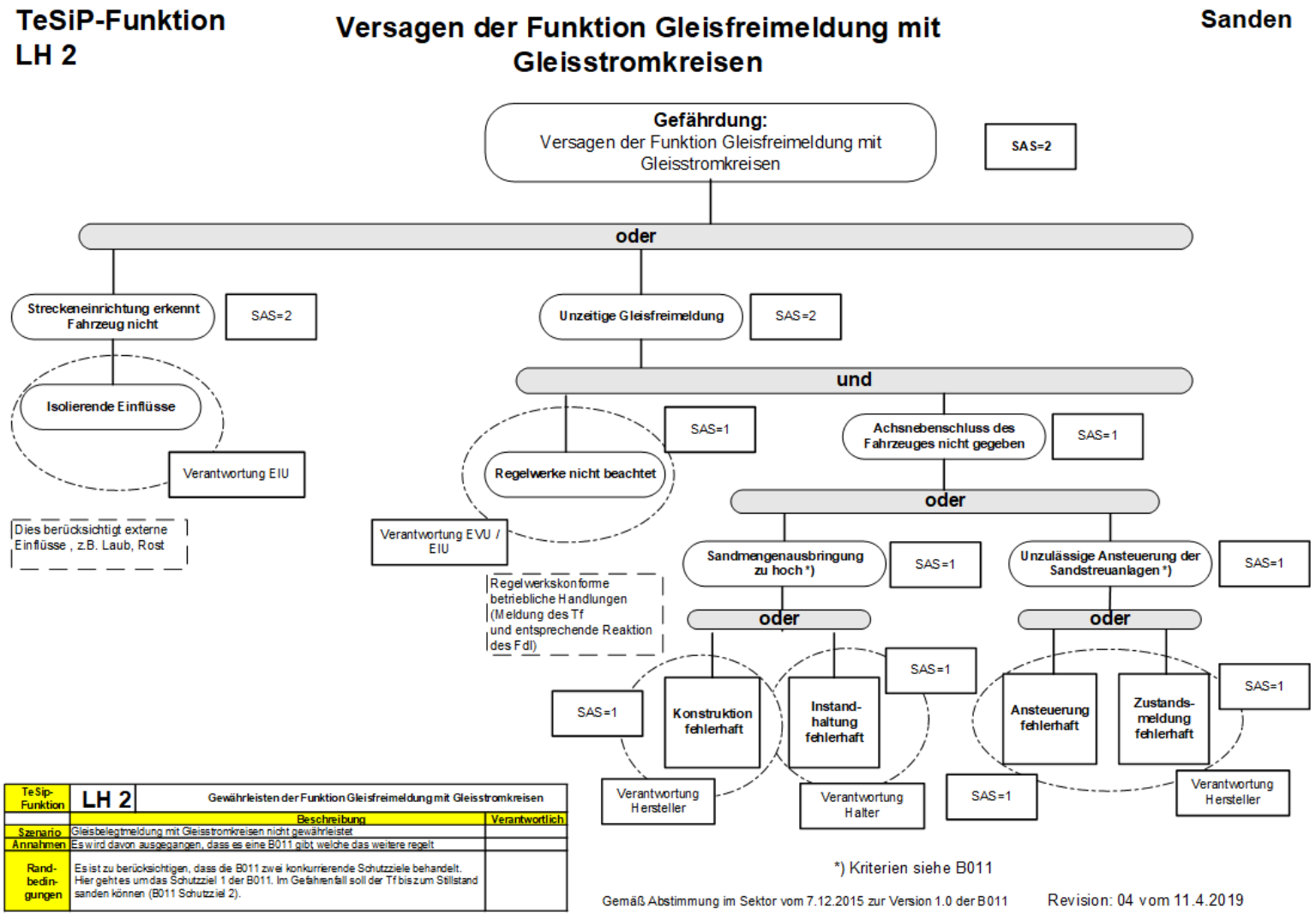


Abbildung 18: LH2 - Gewährleisten der Funktion der Gleisfreimeldung

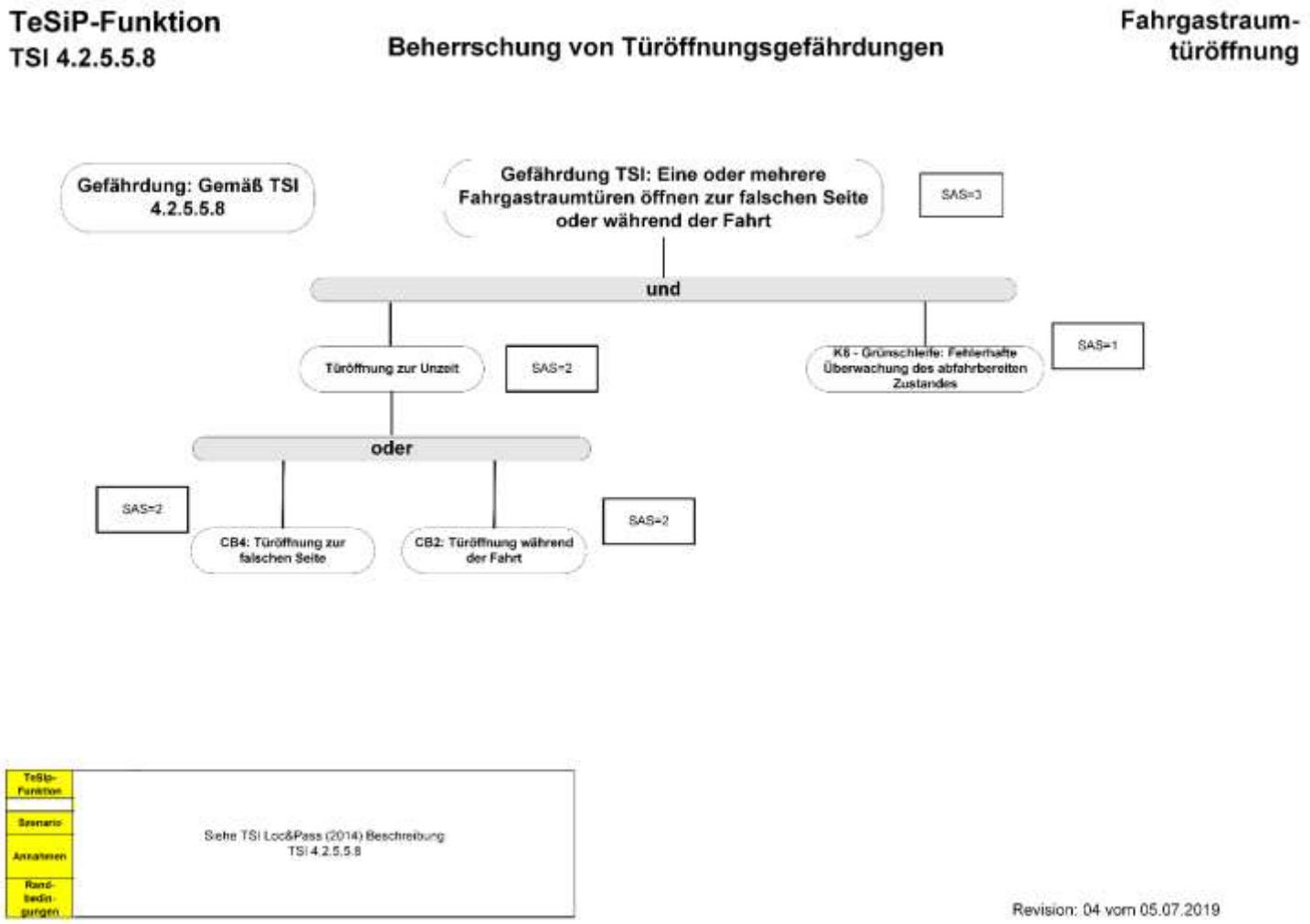


Abbildung 19: TSI 4.2.5.5.8 - Beherrschung von Türöffnungsgefährdungen

HH 2: TeSiP-Funktion Gefährdungsbaum

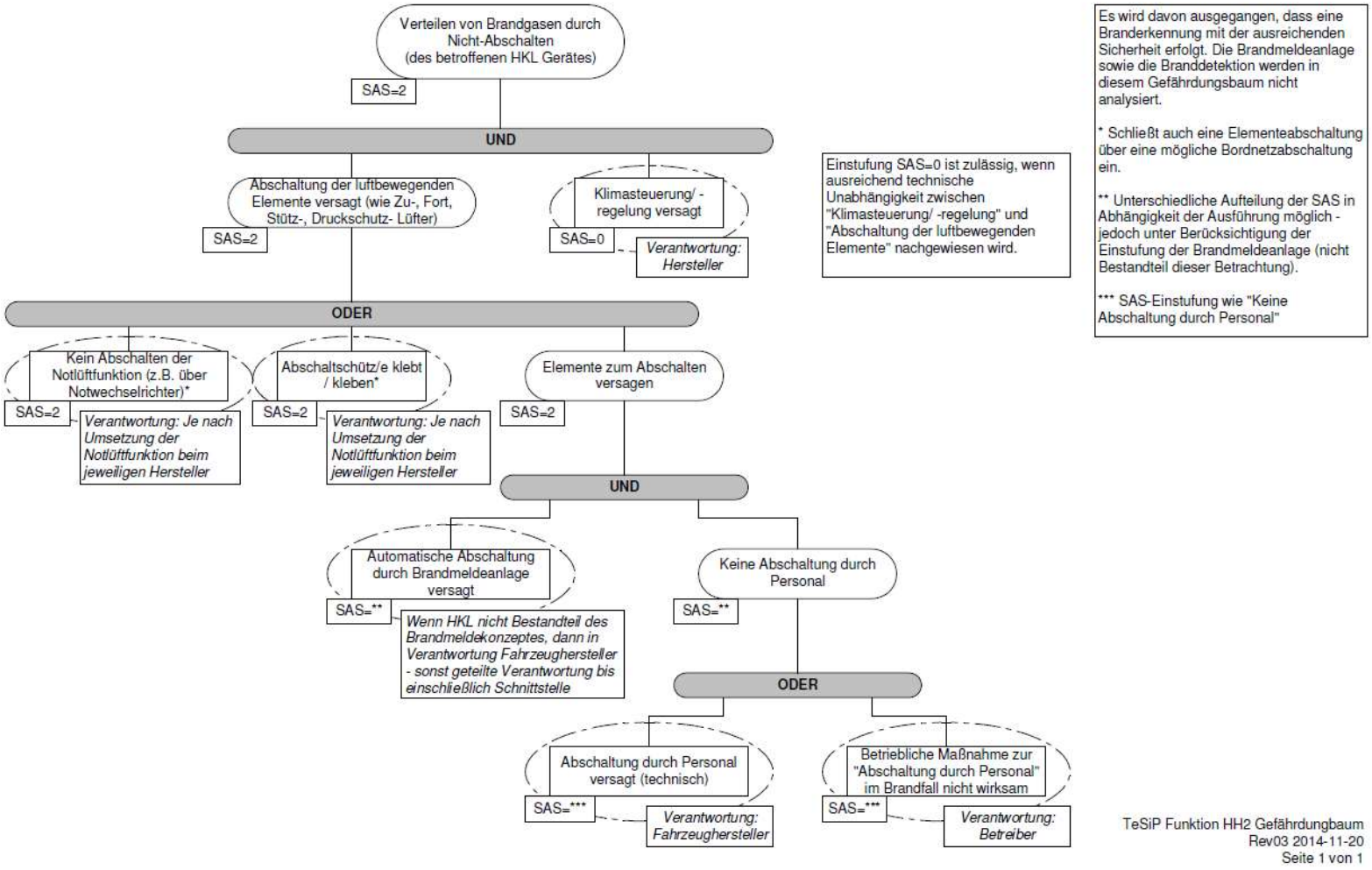


Abbildung 20: HH2 – Verteilen von Brandgasen durch Nicht-Abschalten (des betroffenen HKL Gerätes)

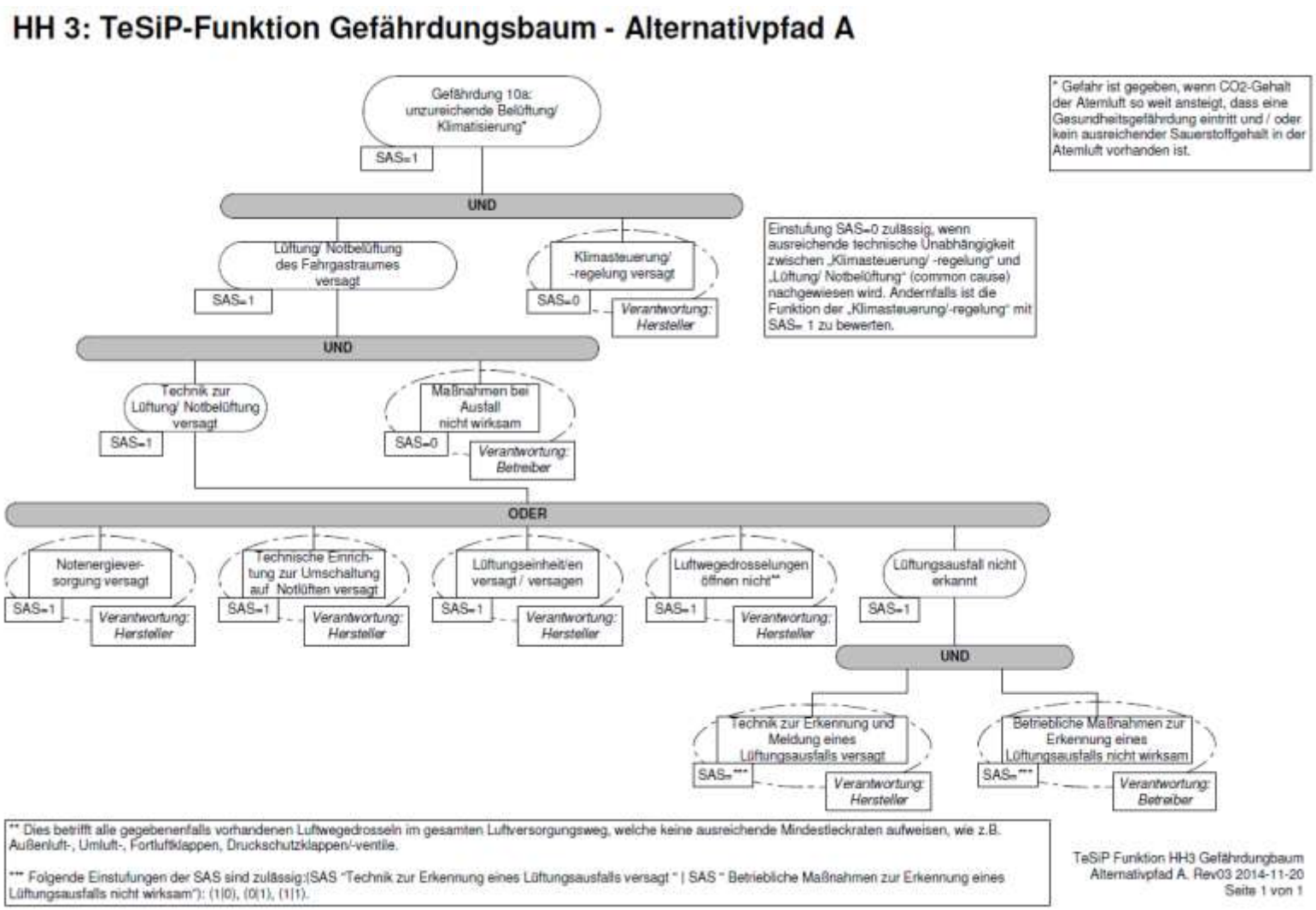


Abbildung 21: HH3 – unzureichende Belüftung / Klimatisierung (Alternativpfad A)

HH 3: Gefährdungsbaum zur Musteranlage Alternativpfad A - Teil1

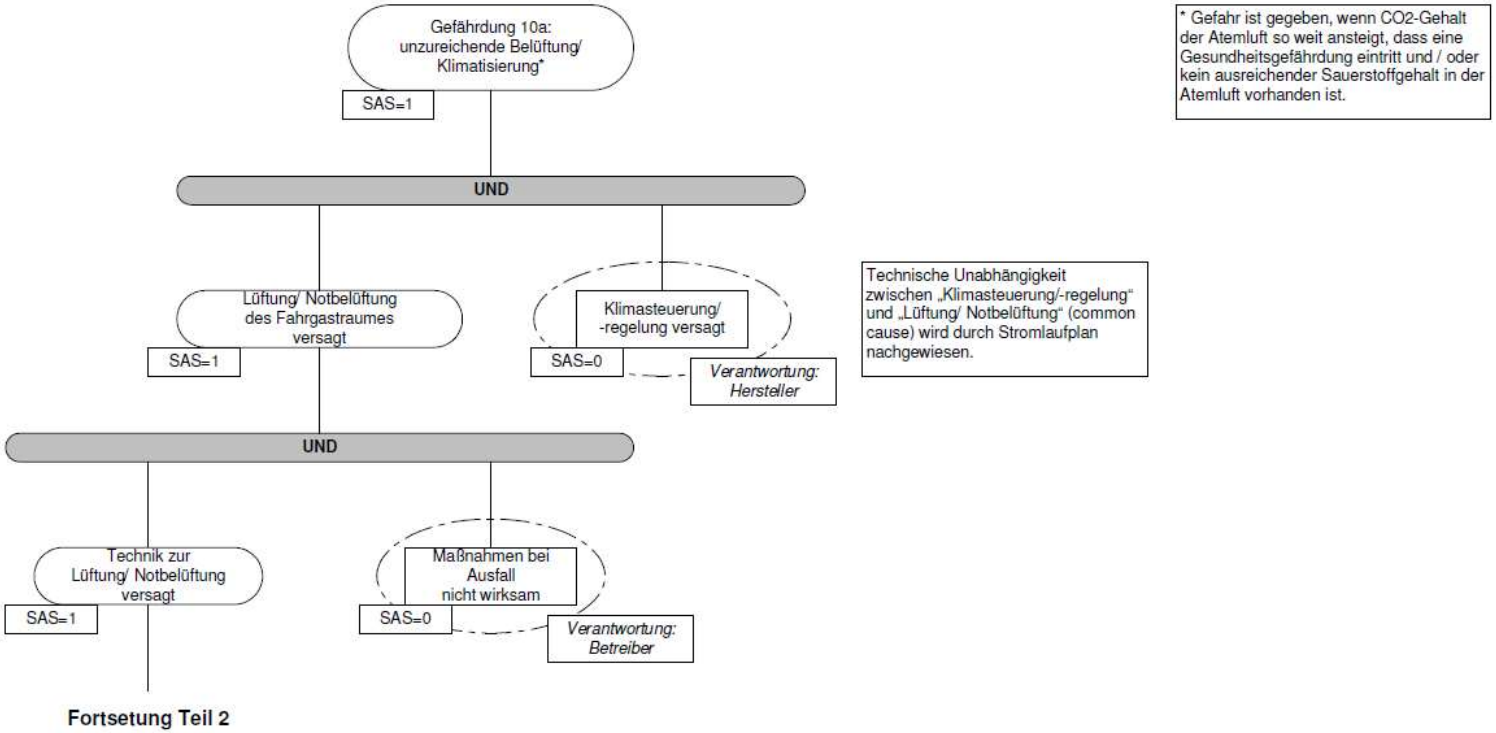


Abbildung 22: HH3 – unzureichende Belüftung / Klimatisierung (Alternativpfad A – Teil 1)

HH 3: Gefährdungsbaum zur Musteranlage Alternativpfad A - Teil2

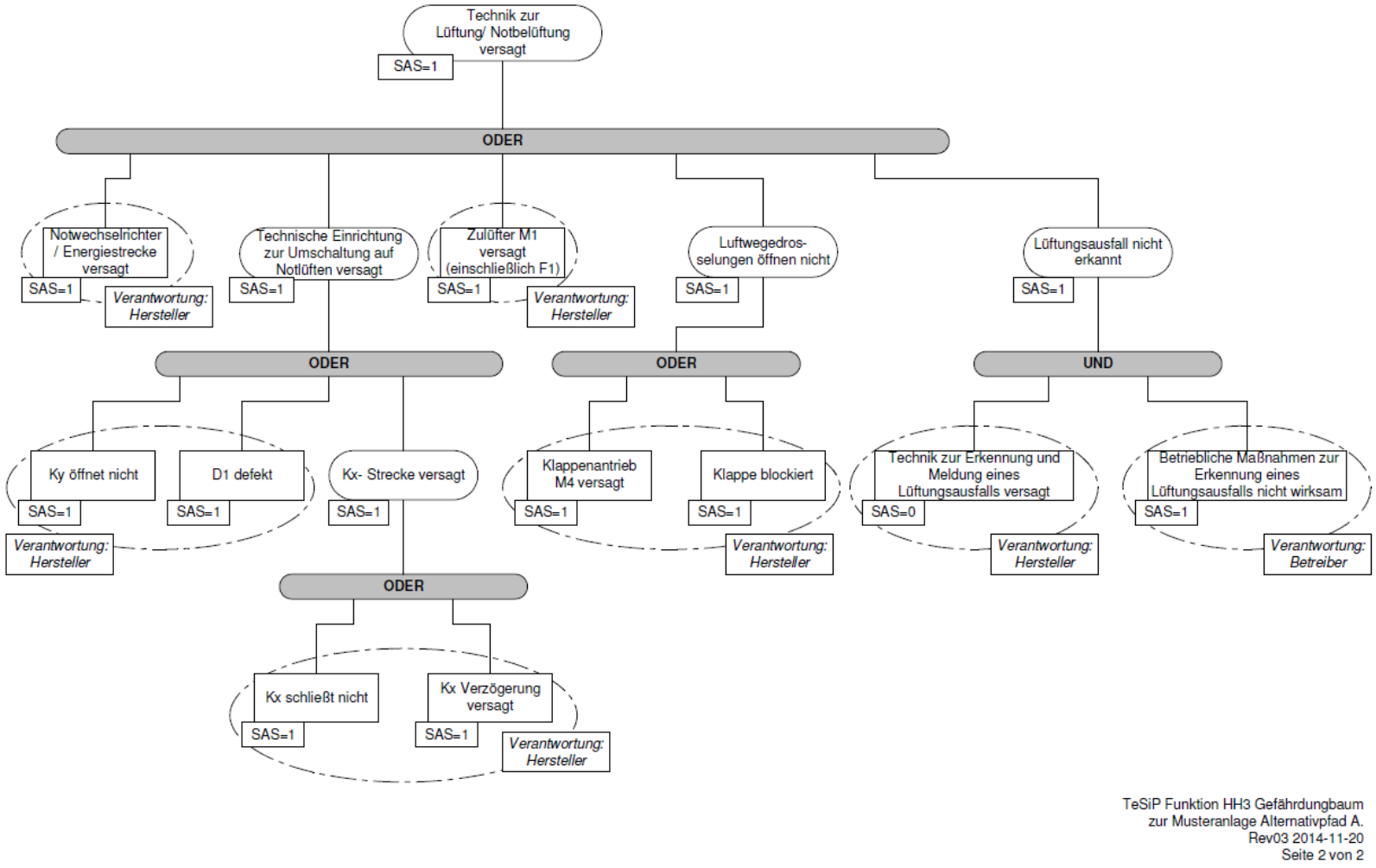
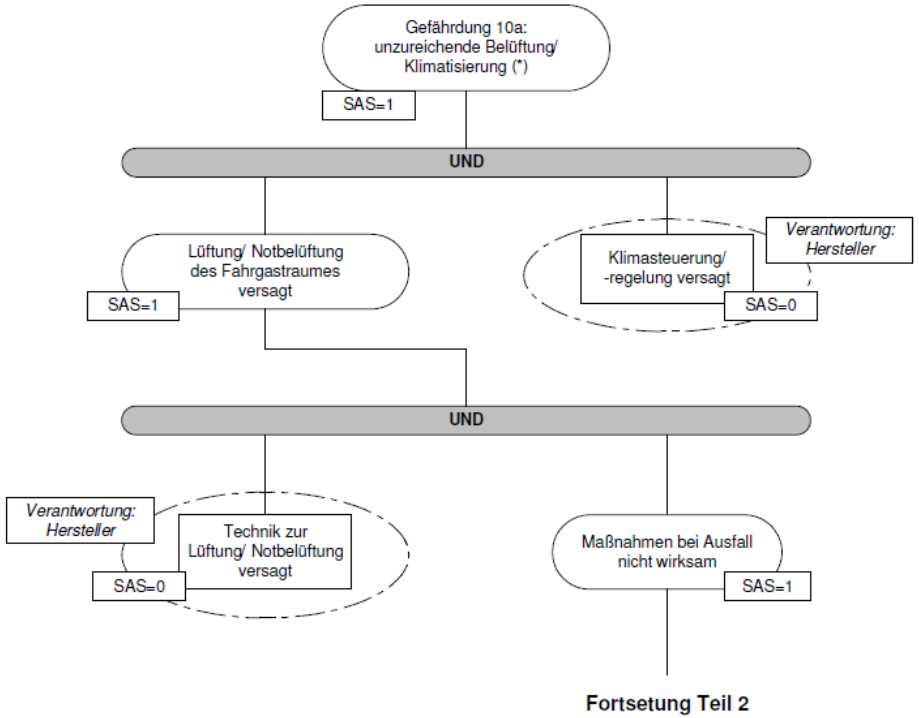


Abbildung 23: HH3 – unzureichende Belüftung / Klimatisierung (Alternativpfad A – Teil 2)

HH 3: TeSiP-Funktion Gefährdungsbaum - Alternativpfad B - Teil 1



TeSiP Funktion HH3 Gefährdungbaum
Alternativpfad B. Rev03 2014-11-20
Seite 1 von 2

Abbildung 24: HH3 – unzureichende Belüftung / Klimatisierung (Alternativpfad B – Teil 1)

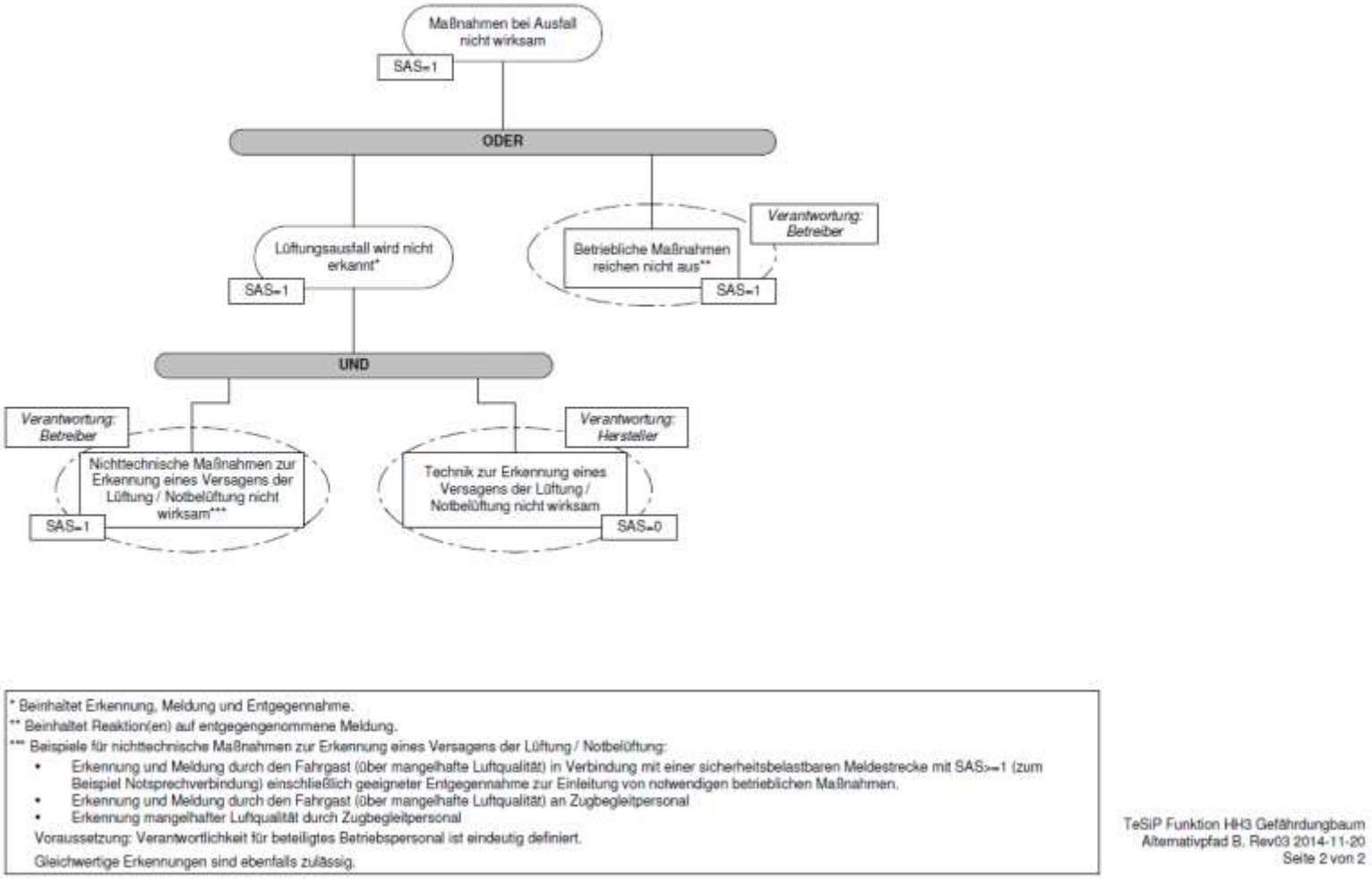


Abbildung 25: HH3 – unzureichende Belüftung / Klimatisierung (Alternativpfad B – Teil 2)

Anhang D. Aufteilungsregeln

Zur Aufteilung der sicherheitstechnischen Verantwortung gelten die nachfolgenden Regeln.

Wird eine Aufteilung der sicherheitstechnischen Verantwortung nicht angestrebt, gilt für jedes identifizierte Architekturelement die SAS der betrachteten Eisenbahnfahrzeugfunktion.

Wird eine Aufteilung der sicherheitstechnischen Verantwortung angestrebt, gilt:

- Jede sicherheitstechnische Einstufung leitet sich von der SAS der betrachteten Eisenbahnfahrzeugfunktion ab. Kein Architekturelement des Gefährdungsbaumes kann eine höhere Einstufung als diese Funktion haben.
- Bei „ODER“- Verknüpfungen erhalten die Architekturelemente die gleiche sicherheitstechnische Einstufung wie die übergeordnete Funktion. Eine Aufteilung der Verantwortung ist in diesem Fall nicht möglich.
- Voraussetzung für eine Aufteilung der sicherheitstechnischen Verantwortung ist eine „UND“-Verknüpfung im Gefährdungsbaum.
- Eine Aufteilung der sicherheitstechnischen Verantwortung bei "UND"-Verknüpfungen ist nur möglich, wenn die jeweiligen Architekturelemente voneinander unabhängig sind, d.h. keine gemeinsamen Ausfallursachen (Common-Cause) vorliegen, die zu einem Versagen mehrerer Architekturelemente führen können.

  Anmerkung: Sind bei einer „UND“-Verknüpfung die jeweiligen Architekturelemente voneinander abhängig (Common-Cause), empfiehlt sich eine Darstellung der Common-Cause-Elemente als separates Element mittels "ODER"-Verknüpfung im Gefährdungsbaum.

- Die Aufteilung der sicherheitstechnischen Verantwortung an einer „UND“-Verknüpfung ist so vorzunehmen, dass sich in der Summe mindestens die Einstufung der übergeordneten realisierten Eisenbahnfahrzeugfunktion ergibt **(a)**.
  Realisierte Funktionen mit der Einstufung SAS > 0 können sich nie ausschließlich aus Architekturelementen mit der Einstufung SAS = 0 zusammensetzen **(b)**.
  Hierbei ist zu beachten, dass in jeder (Abstufungs-)Ebene des qualitativen Gefährdungsbaums jeweils ein Architekturelement um maximal eine Sicherheitsanforderungsstufe (SAS) zurückgenommen wird **(c)**,
  es sei denn, dass die vollständige Sicherheitsverantwortung von einem Zweig des Gefährdungsbaums übernommen wird **(d)**.
- Wird von dieser Regel abgewichen (z. B. SAS = 4 in 2 x SAS = 2), ist dies mittels einer tiefgreifenden Common-Cause-Analyse zu zeigen **(e)**.
  Hierbei ist mittels geeigneter, systematischer Methoden (FMEA, HAZOP, etc.) bis auf untere Ebenen des Gefährdungsbaums zu analysieren, ob die Möglichkeit einer gemeinsamen Fehler-/Ausfallursache besteht. Nur bei einem Ausschluss solcher gemeinsamer Fehler-/ Ausfallursachen ist die Aufteilung zulässig.

  Anmerkung: Bei komplexen Funktionen sollte aus Gründen der Übersichtlichkeit und Nachvollziehbarkeit der qualitative Gefährdungsbaum in sinnvolle Teil-Gefährdungsbäume aufgeteilt werden.

- Der Gefährdungsbaum kann um quantifizierte Ausfallraten ergänzt werden, um eine Nachweisführung der Eignung von Hardware-Bauelementen zu ermöglichen. Hierbei leiten sich die zu erreichenden Sicherheitsziele aus der SAS ab.
- Ist ein Architekturelement in mehreren Funktionen oder Teilfunktionen einer Eisenbahnfahrzeugfunktion vorhanden, ist es in die jeweils höchste SAS einzustufen.

Die im Anschluss dargestellten Grafiken sollen die Anwendung dieser Regel verdeutlichen. Die Darstellungen beziehen sich auf ein Top-Ereignis, das sich aus zwei bzw. 3 Architekturelementen zusammensetzt. Für Top-Ereignisse mit mehr Eingangselementen gelten die Angaben entsprechend.

Tabelle 14: Legende zu den nachfolgenden Tabellen zulässiger Kombinationen von Elementen

	Kombination nicht zulässig, da (a) oder (b) nicht erfüllt ist.
	Kombination zulässig, da (a), (b), (c) und (d) erfüllt sind.
	Kombination zulässig, sofern (e) beachtet wird.
Erläuterung eines Zahlenbeispiels	
2 2	2 2 steht für die SAS-Einstufung der jeweiligen kombinierten Elemente. Hier 2 Elemente mit der jeweiligen SAS-Einstufung 2

Tabelle 15: Kombinationsmöglichkeiten bei UND-Verknüpfung von 2 Elementen

SAS= 1

0 0	0 1
1 0	1 1

SAS= 2

0 0	0 1	0 2
1 0	1 1	1 2
2 0	2 1	2 2

SAS= 3

0 0	0 1	0 2	0 3
1 0	1 1	1 2	1 3
2 0	2 1	2 2	2 3
3 0	3 1	3 2	3 3

SAS= 4

0 0	0 1	0 2	0 3	0 4
1 0	1 1	1 2	1 3	1 4
2 0	2 1	2 2	2 3	2 4
3 0	3 1	3 2	3 3	3 4
4 0	4 1	4 2	4 3	4 4

Tabelle 16: Kombinationsmöglichkeiten bei UND-Verknüpfung von 3 Elementen

SAS= 1	
000	001
010	011
100	101
110	111

SAS= 2		
000	001	002
010	011	012
020	021	022
100	101	102
110	111	112
120	121	122
200	201	202
210	211	212
220	221	222

SAS= 3			
000	001	002	003
010	011	012	013
020	021	022	023
030	031	032	033
100	101	102	103
110	111	112	113
120	121	122	123
130	131	132	133
200	201	202	203
210	211	212	213
220	221	222	223
230	231	232	233
300	301	302	303
310	311	312	313
320	321	322	323
330	331	332	333

SAS= 4				
000	001	002	003	004
010	011	012	013	014
020	021	022	023	024
030	031	032	033	034
040	041	042	043	044
100	101	102	103	104
110	111	112	113	114
120	121	122	123	124
130	131	132	133	134
140	141	142	143	144
200	201	202	203	204
210	211	212	213	214
220	221	222	223	224
230	231	232	233	234
240	241	242	243	244
300	301	302	303	304
310	311	312	313	314
320	321	322	323	324
330	331	332	333	334
340	341	342	343	344
400	401	402	403	404
410	411	412	413	414
420	421	422	423	424
430	431	432	433	434
440	441	442	443	444

Anhang E. Nachweis der Rückwirkungsfreiheit

Dieser Nachweis ist grundsätzlich erforderlich für alle Eisenbahnfahrzeugfunktionen (EFF) / Architekturelemente (AE) der Einstufung SAS = 0 mit Bezug zu EFF / AE mit Einstufung SAS > 0.

Die Betrachtung der Rückwirkungsfreiheit erfordert eine systematische Vorgehensweise. Hierzu ist in jedem Fall mit geeigneten Methoden (Ereignisablaufbäume, etc.) zu prüfen ob eine Verbindung zwischen den EFF / AE mit Einstufung SAS = 0 zu EFF / AE SAS > 0 besteht (z.B. im Fall von SW-Elementen mit Bezug von Software mit SAS = 0 bzw. Steuergeräten zu Software mit einer höheren SAS, wie etwa Nutzung gemeinsamer Rechner, Kommunikationswege, etc.). Hierzu sind mindestens folgende Kriterien zu prüfen:

- funktionale Verbindungen
  Es existiert eine funktionale Auswirkung vom
  "SAS = 0"-Gerät (EFF / AE) zum "SAS > 0"-Gerät (EFF / AE)
  (z.B. Diagnose: "SAS = 0"- Gerät (EFF / AE) löst Diagnoseeintrag im "SAS > 0"-Gerät (EFF / AE) aus),
- softwaretechnische Verbindungen
  Es existiert eine softwarebasierte Verbindung zwischen
  "SAS = 0"- Gerät (EFF / AE) zum "SAS > 0"- Gerät (EFF / AE)
  (z.B. Busverbindung: "SAS = 0"-Gerät (EFF / AE) benutzt gleichen Bus wie SAS > 0"-Gerät (EFF / AE)),
- hardwaretechnische Verbindungen
  Es existiert eine hardwarebasierte Verbindung zwischen
  "SAS = 0"- Gerät (EFF / AE) zum "SAS > 0"- Gerät (EFF / AE)
  (z.B. KLIP-Station: "SAS = 0"- Gerät (EFF / AE) nutzt gleichen KLIP (Klemme für intelligente Peripherieanbindung) wie SAS > 0"-Gerät (EFF / AE)),
- Datenverfälschung bzw. -beeinflussung
  Es existieren offene Schnittstellen mit externen Medien
  (z. B. Funk-/Datenverbindungen, USB, etc.).

EFF / AE die diese Kriterien nicht erfüllen, sind als rückwirkungsfrei zu betrachten. Der Sachverhalt ist zu dokumentieren.

Für alle anderen EFF / AE sind die nachfolgend aufgeführten Maßnahmen in einem Nachweis der Rückwirkungsfreiheit darzulegen, der folgendes beinhalten muss:

- Kapselung der nicht sicherheitsrelevanten Steuergeräte bzw. Steuerungen mit SAS = 0,
- Abkopplung/Entfernung von Schnittstellen,
- Schutz gegen Datenverfälschung,
- Schutz gegen Überlastung/Priorisierungsregeln bei gemeinsam genutzten Kommunikations- bzw. Übertragungswegen,
- Darstellung sicherheitsgerichteter Ausfallreaktionen,
- Definition von Betriebsbedingungen und Umgebungseinflüssen zur Festlegung des Einsatzbereiches (z. B. Funktionsausschlüsse).

Anhang F. Kriterienkatalog Hardware Steuerungsfunktionen

1 Einleitung / Anwendungsbereich

Hier werden die Anforderungen an die Hardware für Steuerungsfunktionen (konventionelle Elektrotechnik, Rechner, elektronische sowie mechatronische Geräte, Bauteile, etc.), die für Sicherheitsaufgaben in Bahnanwendungen auf Schienenfahrzeugen eingesetzt werden, definiert. Die Anforderungen sind aus den Normen DIN EN 50129 und DIN EN / IEC 61508 abgeleitet.

2 Aufteilung der HW Steuerungsfunktionen

Die HW für Steuerungsfunktionen teilt sich auf in

- konventionelle E-Technik und
- HW datenverarbeitender Systeme.

3 Anforderung an konventionelle E-Technik

Tabelle 17: Anforderungen an konventionelle E-Technik

Komponente	Sicherheitsanforderungsstufe		
	0	1/2	3/4
Mechanische Elemente	Keine Nachweis pflicht	Ist der Sicherheitsnachweis mit dem etablierten Nachweisverfahren nicht vollständig möglich, ist das normierte Sicherheitsziel für die zu betrachtende Funktion durch ergänzende Maßnahmen (z.B. Instandhaltung, Betrieblichen Anweisungen) zu erfüllen.	
Verdrahtung + Steckverbindung	Keine Nachweis -pflicht	einfache Isolation, einfache Anforderungen an die Leitungsverlegung	erhöhte Isolation, erhöhte Anforderungen an die Leitungsverlegung, vorkonfektionierte Leitungen, besondere Steckerbelegung
Kontakte	Keine Nachweis -pflicht	Zwangsgeführt	Zwangsöffnend Schalt-, Bedienelemente
Elektro-pneumatische Elemente	Keine Nachweis -pflicht	stellungsabhängige Überwachung	Fail-Safe Verhalten
Konventionelle E-Technik (nicht rechnerbasiert) allgemein (zufällige interne Fehler)	Keine Nachweis -pflicht	Fehlervermeidung: geeignete Überdimensionierung, Vermeidung von Stressfaktoren usw. Fehlerbeherrschung: Einkanalig mit Prüfung	Fehlervermeidung: Auswahl von Geräten mit nachgewiesener Zuverlässigkeit (z.B. durch Betriebsbewährung) Sicherheitsbauform (die geforderten Funktionseigenschaften des Bauteils/der Komponente bleiben über die spezifizierte Lebensdauer erhalten) Fehlerbeherrschung: sicherheitsgerichtetes Ausfallverhalten, mehrkanalig unabhängige Pfade mit Prüfung, einkanalig mit Selbstüberwachung
Konventionelle E-Technik (nicht rechnerbasiert) allgemein (zufällige Fehler durch Einflüsse von aussen)	Keine Nachweis -pflicht	Fehlervermeidung: Maßnahmen gegen Einflüsse, die für den Anwendungsfall wahrscheinlich sind Fehlerbeherrschung: einkanalig mit Prüfung (Funktionsprüfung in regelmäßigen Abständen (z. B. Durchsicht, Nachschau)	Fehlervermeidung: Maßnahmen gegen für den Anwendungsfall weniger wahrscheinliche Einflüsse Fehlerbeherrschung: sicherheitsgerichtetes Ausfallverhalten, mehrkanalig unabhängige Pfade mit Prüfung, einkanalig mit Selbstüberwachung, regelmäßige Prüfung (z. B. Bremsprobe alle 24h, Sichtkontrollen, Wartungsarbeiten, Systemtests))

4 Anforderung an HW datenverarbeitender Systeme

4.1 Konstruktive Maßnahmen zur Fehlerbeherrschung

Die Anforderungen gliedern sich in:

- Maßnahmen in der Hardware-Architektur
- Maßnahmen im Hardware-Entwurf
- Maßnahmen zur Selbstüberwachung

Die Anforderungen an konkrete Architektur- und Entwurfsmerkmale zur Beherrschung von Fehlern auf Systemebene sind aus Tabelle E.4 und E.5 der DIN EN 50129 [11, 12] entnommen. Speziell für die Datenübertragung werden in der DIN EN 50159 [14, 15, 16, 17] geeignete Mechanismen genannt.

In den Tabellen ist durch die Bezeichnungen „R“, „HR“ und „M“ die Empfehlungsstärke für die Maßnahmen angegeben. Hierbei bedeuten diese Empfehlungsstärken:

Tabelle 18: Empfehlungsstärken für die Maßnahmen

Empfehlungs-stärke	Bedeutung	Nachweis
-	keine Empfehlung für oder gegen die Maßnahme	kein Nachweis erforderlich
„R“	recommended (Technik/Maßnahme wird empfohlen)	Technik/Maßnahme ist bei der Entwicklung zu berücksichtigen.
„HR“	highly recommended (Technik Maßnahme wird dringend empfohlen)	Begründung erforderlich, wenn Anwendung nicht erfolgt.
„M“	Mandatory	Anwendung der Technik/Maßnahme ist zwingend erforderlich

4.2 Anforderungen an die Qualität der Hardware

Tabelle 19: Empfehlungsstärken für die Qualität der Hardware

Es ist nachzuweisen, dass die Bauelemente geeignet sind, die Sicherheitsziele zu erreichen.	**SAS 1-2**	**SAS 3 - 4**
Hinweis: Nachweis kann geführt werden z. B. - durch den Nachweis der Betriebsbewährung - durch die Beachtung von Errata Sheets - durch die Anwendung in anderen sicherheitsrelevanten Systemen - auf der Grundlage der vom Hersteller genannten Ausfallraten.	HR	M
Die komplexen Bauelemente wie Prozessoren, RAM, ROM, Speicherelemente, FPGA, CPLD etc. müssen eine Möglichkeit der Testbarkeit und Fehleroffenbarung aufweisen.	HR	M

4.3 Maßnahmen in der Hardware-Architektur

Bei der Hardware-Architektur ist je nach Anforderungsstufe die physikalische oder logische/funktionale Trennung der sicherheitsrelevanten von den nicht sicherheitsrelevanten Teilen des Systems zu berücksichtigen, sowie der grundsätzliche strukturelle Aufbau (einkanalig mit Selbsttests und Überwachung, zweikanalig etc.). Aus dem Aufbau des Systems ergeben sich dann auch die entsprechenden Aufgaben der Software in den Systemkomponenten (z. B. könnte es eine spezielle Software nur für die Überwachungseinrichtung geben).

Anforderungen in Anlehnung an die Tabelle E.4 der DIN EN 50129 [11, 12].

Tabelle 20: Maßnahmen für die Hardware Architektur (allg.) in Abhängigkeit von der Sicherheitsanforderungsstufe

Technik/Maßnahme **Maßnahmen für die Hardware Architektur (allg.)**	**SAS 1-2**	**SAS 3 - 4**
Trennung von sicherheitsrelevanten Systemen von nicht sicherheitsrelevanten Systemen. Nicht sicherheitsrelevante (Teil-)Funktionen können auf sicherheitsrelevanten Systemen ausgeführt werden, wobei ein Nachweis geeigneter Abgrenzungsmaßnahmen (Rückwirkungsfreiheit / Nicht-Vorhandensein einer ungewollten Wechselwirkung) zu führen ist.	R	HR

Tabelle 21: Maßnahmen für die Hardware Architektur (sich ausschließende Alternativen) in Abhängigkeit von der Sicherheitsanforderungsstufe

Technik/Maßnahme **Maßnahmen für die Hardware Architektur (sich ausschließende Alternativen) in Abhängigkeit von der Sicherheitsanforderungsstufe**	**SAS 1 - 2**	**SAS 3 - 4**
Einkanalige elektronische Struktur mit Selbsttests und Überwachung.	R	–
Zweikanalige elektronische Struktur.	R	–
Zweikanalige elektronische Struktur basierend auf der Fail-Safe-Struktur durch Redundanz (composite fail-safe) mit Fail-Safe-Vergleich.	R	HR
Einkanalige elektronische Struktur basierend auf der Fail-Safe-Struktur durch unverlierbare Eigenschaften (inherent fail safe.	R	HR
Einkanalige elektronische Struktur basierend auf der Fail-Safe-Struktur durch sicherheitsgerichtete Ausfallreaktion (reactive fail safe).	R	HR
Diversitäre elektronische Struktur mit Fail-safe-Vergleich.	R	HR

4.4 Maßnahmen im Hardware-Entwurf

Im Entwurf des Systems müssen Maßnahmen gegen Ausfälle und Fehler vorgesehen werden, wie z. B. Programmsequenzüberwachung zur Erkennung grober Fehler im Programmablauf, einschließlich "hängender" Programme.

Anforderungen in Anlehnung an Tabelle E.5 der EN 50129 [11, 12].

Tabelle 22: Maßnahmen für die Hardware Architektur zum Schutz gegen Einzelausfälle von diskreten Bauteilen in Abhängigkeit von der Sicherheitsanforderungsstufe

Technik / Maßnahme zum Schutz gegen Einzelausfälle von diskreten Bauteilen	**SAS 1-2**	**SAS 3 - 4**
Alle gefährlichen Ausfallarten müssen zur sicherheitsgerichteten Ausfallreaktion führen, oder man muss die unverlierbare Sicherheit (vgl. DIN EN 50129) zeigen aufgrund von unverlierbaren physikalischen Eigenschaften.	R	HR

Tabelle 23: Maßnahmen für die Hardware Architektur zum Schutz gegen Einzelausfälle von integrierten digitalen elektronischen Schaltkreisen in Abhängigkeit von der Sicherheitsanforderungsstufe

Technik / Maßnahme zum Schutz gegen Einzelausfälle von integrierten digitalen elektronischen Schaltkreisen	**SAS 1**	**SAS 2**	**SAS 3 - 4**
Stuck-at-Fehlermodell Erklärung IEC 61508: Stuck-at“ ist eine Fehlerkategorie, die mit einem dauerhaften Zustand „0“ oder „1“ oder „Ein“ an den Anschlüssen eines Bauteils beschrieben werden kann.	R		
DC-Fehlermodell Erklärung IEC 61508: Das „DC-Fehlermodell“ (DC = Gleichstrom) umfasst die folgenden Ausfallarten: Stuck-at Fehler, Stuck-open, offene oder Ausgänge mit hoher Impedanz sowie Kurzschlüsse zwischen Signalleitungen.		R	
Fehlermodell für permanente und transiente Fehlfunktionen auf Betrachtungseinheitsebene (Beispiele für Fehlfunktionen von integrierten Schaltkreisen sind in der DIN EN 50129 definiert).			HR

Tabelle 24: Maßnahmen für die Hardware Architektur für Physikalische Unabhängigkeit innerhalb der sicherheitsrelevanten Architektur in Abhängigkeit von der Sicherheitsanforderungsstufe

Technik / Maßnahme für Physikalische Unabhängigkeit innerhalb der sicherheitsrelevanten Architektur	**SAS 1**	**SAS 2**	**SAS 3 - 4**
Isolationsabstände sollten mindestens entsprechend EN 50124-1 [1, 2] (Basisisolation) dimensioniert sein.	R		
Isolationsabstände sollten mindestens entsprechend EN 50124-1 [1, 2] (verstärkte Isolation) dimensioniert sein.			HR

Tabelle 25: Maßnahmen für die Hardware Architektur zur Beibehaltung des sicheren Zustandes in Abhängigkeit von der Sicherheitsanforderungsstufe

Technik / Maßnahme zur Beibehaltung des sicheren Zustandes	**SAS 1**	**SAS 2**	**SAS 3 - 4**
Anzeige an den Bediener, dass er sich auf die sicherheitsrelevanten Funktionen der defekten Betrachtungseinheit nicht mehr verlassen kann.	R		
Automatisches Abschalten der/des defekten Betrachtungseinheit / Teil- / Systems vom Prozess oder entsprechendes Blockieren aller sicherheitsrelevanten Funktionen der/des defekten Betrachtungseinheit / Teil- / Systems.			HR

Tabelle 26: Maßnahmen für die Hardware Architektur zur zyklischen Ausfalloffenbarung in Abhängigkeit von der Sicherheitsanforderungsstufe

Technik / Maßnahme zur zyklischen Ausfalloffenbarung	**SAS 1**	**SAS 2**	**SAS 3 - 4**
Zyklisches Testen (z. B. bei Auf- / Abrüsten und / oder Betrieb des Systems, Zyklen sind festzulegen) um das korrekte Arbeiten des sicherheitsrelevanten Systems zu prüfen und um eine Anzeige an den Bediener zu liefern.	R	HR	
Zyklisches Testen (z. B. bei Auf- / Abrüsten und / oder Betrieb des Systems Zyklen sind festzulegen), um das korrekte Arbeiten des sicherheitsrelevanten Systems zu prüfen und einen automatischen Übergang in einen sicheren Zustand.			HR

Tabelle 27: Maßnahmen für die Hardware Architektur zur Programmsequenzüberwachung in Abhängigkeit von der Sicherheitsanforderungsstufe

Technik / Maßnahme zur Programmsequenzüberwachung	**SAS 1**	**SAS 2**	**SAS 3 - 4**
Zeitliche oder logische Überwachung der Programmfolge plus Anzeige an den Bediener.	R	HR	
Zeitliche und logische Überwachung der Programmfolge an vielen Kontrollpunkten im Programm und automatischer Übergang in einen sicheren Zustand.			HR

Tabelle 28: Maßnahmen für die Hardware Architektur (sich ausschließende Alternativen) in Abhängigkeit von der Sicherheitsanforderungsstufe

Technik / Maßnahme bei Spannungszusammen-bruch, Spannungsänderungen, Überspannung, Unterspannung	**SAS 1**	**SAS 2**	**SAS 3 - 4**
Maßnahmen bei Spannungszusammenbruch, Spannungsänderungen, Überspannung, Unterspannung.	HR		
Erweiterte Maßnahmen bei Spannungszusammenbruch, Spannungsänderungen, Überspannung, Unterspannung.			HR

Tabelle 29: Maßnahmen für die Hardware Architektur bei Temperaturanstieg in Abhängigkeit von der Sicherheitsanforderungsstufe

Technik / Maßnahme bei Temperaturanstieg	**SAS 1**	**SAS 2**	**SAS 3 - 4**
Offenbaren von Übertemperatur und eine Sicherheitsreaktion realisieren.	HR		HR

Tabelle 30: Maßnahmen für die Hardware Architektur bei Temperaturanstieg in Abhängigkeit von der Sicherheitsanforderungsstufe

Technik / Maßnahme zum Schutz gegen systematische Fehler	SAS 1	SAS 2	SAS 3	SAS 4
unabhängiger zweiter Schutz (für einfache Systeme).			R	R
unabhängiger zweiter Schutz (für komplexe Systeme).			R	HR

4.5 Maßnahmen zur Selbstüberwachung

Die implementierten Mechanismen zur Fehlererkennung und -beherrschung sind in den Normen DIN EN 50126, DIN EN 50128, DIN EN 50657 und DIN EN 50129 nur recht allgemein, d.h. unter zusammenfassenden Oberbegriffen und nicht durch Angabe konkreter spezifischer Lösungen benannt. In Zusammenhang mit den in der DIN EN 50128 [35, 36] bzw. DIN EN 50657 genannten Maßnahmen:

- „Defensive Programmierung“,
- „Fehlererkennung und Diagnose“,
- „Fehlererkennende Codes“,
- „Failure-Assertion“-Programmierung und
- „externe Überwachungseinrichtung“

sowie den in DIN EN 50129 [11, 12] genannten

- „Struktur mit Selbsttests und Überwachung“,
- „sicherheitsgerichtete Ausfallreaktion“,
- „Plausibilitätsprüfungen“,
- „automatisches Abschalten“,
- „dynamischen Online-Testen“,
- „Überwachung der Programmfolge“

stehen die in der folgenden Tabelle aufgeführten „typischen“ Selbstüberwachungsfunktionen, die sowohl den Programmablauf und den Datenfluss, wie auch den Zustand der Hardware überwachen.

Zu vielen der Maßnahmen sind Implementierungsbeispiele im Anhang A der IEC 61508-7 [33, 34] angegeben und die erwartete Wirksamkeit in Anhang A der IEC 61508-2 [23, 24].

Bei der Angabe der „Empfehlungsstärke“ („R“ bzw. „HR“) handelt es sich um einen Vorschlag, der die in den Normen angegeben Empfehlungsstärke der o.g. Mechanismen zur Fehlererkennung und -beherrschung berücksichtigt. Die Einzelmaßnahmen können je nach konkreter Ausprägung eine unterschiedliche Wirksamkeit bezüglich der Erkennung von Fehlern haben (z. B. „mittlere“ Wirksamkeit bei einem 8-Bit-CRC und „hohe“ Wirksamkeit bei einem 16-bit-CRC für einen Speicherblock definierter Größe).

Entsprechend den Vorgaben der IEC 61508-2 [23, 24], Anhang A ist für:

- SAS 1 und 2 eine niedrig wirksame Variante der Maßnahme ausreichend
- SAS 3 eine mittlere und für SAS 4 eine hohe Wirksamkeit erforderlich.

Anmerkung zum Verfahren:
Diese Verfahrensweise ist gegenüber dem Vorgehen nach IEC 61508 vereinfacht, da die Mechanismenstärken (und somit die Fehleraufdeckungsrate) hier pauschal ohne Berücksichtigung der im spezifischen System zu erwartenden Ausfallraten vorgegeben werden. Sie hat aber den Vorteil, dass „Grundschutz"- Maßnahmen ohne detaillierte Analysen für ein System vorgegeben werden können.

Folgende Maßnahmen zur Hardwareüberwachung sind gemäß SAS entsprechend der folgenden Tabellen vorzusehen:

Tabelle 31: Maßnahmen für die Hardwareüberwachung in Abhängigkeit von der Sicherheitsanforderungsstufe

Technik / Maßnahme für Hardwareüberwachung	**Beispiele** s. IEC 61508-7	**SAS 1 - 2**	**SAS 3 - 4**
Selbsttest des Prozessors (Register, Operationen ...). Aufgrund der Komplexität moderner Prozessoren nur teilweise möglich.	A.3	R	HR
Selbsttest unterstützt durch Hardware.		R	HR
Gegenseitiger Vergleich durch Software mit Testergebnissen eines redundanten Prozessors (meist bei 2-kanaligen Anlagen). Hinweis: Es ist eine der Techniken zu wählen.		R	HR
Test des Arbeitsspeichers (RAM) auf Funktion: Test beim Start oder in einer Ruhephase zur Erkennung realer Fehler der verwendeten Speichertypen. Hinweis 1: z. B. erweiterte MARCH-Tests (Adressfehler, statische und dynamische Fehler, Koppelfehler). Hinweis 2: Um die Startzeit zu in vernünftigen Grenzen zu halten, kann beim Start auch ein einfacher Test durchgeführt werden, der durch einen besseren Test in einer Ruhephase oder beim Abschalten ergänzt wird. Transiente Fehler können von permanenten Fehlern unterschieden werden. Dazu müssen gefundene Fehler gespeichert werden. Transiente Fehler dürfen wieder gelöscht werden. Hinweis 3: Speichersektionen, in die invariante SW geladen wird, müssen nicht durch einen RAM-Test geprüft werden, wenn die invarianten Sektionen vor dem RAM-Test der variablen Sektionen geladen werden und danach die invarianten Sektionen	A.5	HR	HR

Technik / Maßnahme für Hardwareüberwachung	Beispiele s. IEC 61508-7	SAS 1 - 2	SAS 3 - 4
geprüft werden. **Online RAM Tests sind nicht empfohlen!** Hinweis 4: Variable Speicher müssen ganzheitlich getestet werden (wg. Koppelfehlern). Online Tests, die Variable wiederherstellen müssen, sind komplex, schwierig zu implementieren und, wie die Praxis zeigt, schwer testbar und fehleranfällig.		–	–
Online Fehlerentdeckung durch HW-Unterstützung, durch Parity-Bit, Single Error Correction / Double-Error Detection RAM (mit Abfragemöglichkeit).		R	–
Online Fehlerentdeckung durch Plausibilitätsprüfungen der Software auf Redundanz in Variablen, z. B. digitale Variablen/Signale: 2-Bit invers, analoge Variablen: Bereichseinschränkung, Offset.		–	HR
Online Fehlerentdeckung durch redundante Variablen in unabhängigen RAMs, z. B. doppelte Ausführung auf redundanten RAM-Sektionen und Vergleich der Ergebnisse, ggf. 2-kanalig. Genereller Hinweis: Um diese Anforderungen zu erfüllen, kann eine ausreichend wirksame Technik gewählt werden oder eine Kombination von Techniken gewählt werden, die zusammen einen ausreichenden Deckungsgrad ergeben.		–	HR
Test des Programms auf ungewollte Veränderungen (CRC oder Vergleich redundanter Code-Sektionen). Hinweis 1: Der Fehlerdeckungsgrad eines CRC ist abhängig von der Länge und der Güte des Generatorpolynom und der zu sichernden Blocklänge. Geeignete 32-Bit Generatorpolynome für größere Code-Sektionen siehe: SCSI und 802.3/FDDI/AAL5. Hinweis 2: Um die Startzeit in vernünftigen Grenzen zu halten, dürfen Programmsektionen statt beim Start im Betrieb, in freier oder eingeplanter Prozessorzeit, geprüft werden; eine regelmäßige	A.4	HR	HR

Technik / Maßnahme für Hardwareüberwachung	**Beispiele** s. IEC 61508-7	**SAS 1 - 2**	**SAS 3 - 4**
Prüfung muss jedoch gewährleistet werden. Transiente Fehler können von permanenten Fehlern unterschieden werden. Dazu müssen gefundene Fehler gespeichert werden. Transiente Fehler dürfen wieder gelöscht werden.			
Test gesicherter Datenbereiche (z. B. Parameter) auf ungewollte Veränderungen (CRC oder Vergleich redundanter Daten-Sektionen). Hinweis: Der Fehlerdeckungsgrad eines CRC ist abhängig von der Länge und der Güte des Generatorpolynoms und der zu sichernden Blocklänge. Es empfiehlt sich, auch wenn kleinere Polynome ausreichen würden, die Sicherungs-Software der Programmsektionen zu verwenden.		HR	HR
Überwachung des Programmlaufs mittels (Hardware-) Watchdog mit separater Zeitbasis **- und Zeitablauf (time out)** **- und Zeitfenster (time window).** Hinweis 1: WD mit Zeitablauf ist für SAS1 ausreichend, vgl. Tabelle E.5: Technik/Maßnahme zur Programmsequenzüberwachung. Die Qualität der Maßnahme hängt von der Wahl der Zeitgrenzen ab (auch im Hinblick auf unnötige Reaktionen). Hinweis 2: Bei mehrkanaliger Ausführung mit zeitüberwachtem Vergleich durch Software kann durch die gegenseitige Überwachung der Systeme auf einen WD verzichtet werden.	A.9	HR	HR
Test des Watchdogs (durch ablaufen lassen beim Neustart, in einer Ruhephase oder beim Abschalten), um einen unerkannten Ausfall der Programmlaufüberwachung zu vermeiden. Hinweis: Transiente Fehler können von permanenten Fehlern unterschieden werden. Dazu müssen gefundene Fehler gespeichert werden. Transiente Fehler dürfen wieder gelöscht werden.		R	HR
Tests übertragener Daten auf richtige Reihenfolge (Nachrichtenzähler) und Aktualität (Nachrichten- Timeout).		HR	HR

Technik / Maßnahme für Hardwareüberwachung	**Beispiele** s. IEC 61508-7	**SAS 1 - 2**	**SAS 3 - 4**
Hinweis: Da Sender und Empfänger in ihren Zyklen meist nicht synchron arbeiten, ist es nicht ausgeschlossen, dass Eingabedaten vorgefunden werden, die noch nicht erneuert wurden bzw. dass nachfolgende Daten bereits durch neue ersetzt wurden. Der Test muss dies berücksichtigen.			
Tests übertragener Daten auf ungewollte Veränderungen.	A.7	HR	HR
Vergleich redundanter Eingaben oder Plausibilisierung von Eingaben (Einhaltung des Wertebereichs und nicht im Widerspruch zu anderen logisch zusammenhängenden Signalen oder bekannten Systemzuständen, Zulässigkeit von Bedienkommandos etc.).	A.6.5 A.2.7	HR	HR
Überwachen von Ausgaben durch direktes Rücklesen oder durch Rücklesen angeschlossener Aktuatoren. Falls Test der Eingangssignale beim Empfänger als nicht ausreichend erachtet wird.	A.6.4	R	HR
Kontrolle der Datenübertragung durch Auswertung von Rückmeldungen. Falls keine anderen Verfahren angewendet werden. Siehe „Tests übertragener Daten".	A.6.4	R	HR
Entdeckung und Behandlung von nicht vorgesehenen Interrupts und automatisch durch den Prozessor erkannten Ausnahmen, die nicht explizit durch die Anwendungs-Software behandelt werden (wie z. B. Division durch Null, Werteüberlauf, Genauigkeitsverlust, Zugriffsverletzung, Überlauf des Stacks, ungültige Anweisung, allgemeine Schutzausnahme etc). Es ist eine geeignete Kombination von Maßnahmen zu wählen und deren Wirksamkeit darzulegen.		HR	HR
Steuerung der Abarbeitung, so dass sicherheitsgerichtete Funktionen rechtzeitig abgearbeitet werden (vorzugsweise sind Echtzeitsysteme zu verwenden, oder Multitasking mit geeigneten Scheduling-Verfahren).		R	HR

5 Sicherheitsbezogene Anwendungsbedingungen

Sicherheitsbezogene Anwendungsbedingungen der rechnerbasierten Hardware sind zu definieren und zu dokumentieren. Ihre Einhaltung ist im Rahmen des Sicherheitsnachweises nachzuweisen.